CROWDSTRIKE

Professional Services Catalog

Dated 2/15/2024
Contains proprietary and confidential information subject to non-disclosure requirements.

Table of Contents

CROWDSTRIKE

Retainer Terms

Retainer Terms

CrowdStrike may provide Services listed in this Professional Services Catalog to Customer under a prepaid-balance account (the "Retainer") purchased from CrowdStrike pursuant to a Statement of Work and/or Order. The Professional Services Catalog is subject to and governed by the terms and conditions located **here**[1] unless CrowdStrike and Customer have otherwise executed an agreement (as applicable, the "Agreement"), in which case, the executed agreement governs this Catalog. The order of precedence is as follows: (1) the Agreement, (2) the Order and/or SOW, and (3) this Professional Services Catalog.

Authorizing Work Under the Retainer

In the event Customer wants to draw down the Retainer for the Services listed in this Professional Services Catalog, either (i) an authorization will be issued in the form attached hereto as Exhibit A ("Authorization"), or (ii) a separate signed writing for Services provided under privilege will be executed, in each case describing the Services to be performed and the number of hours for such Services. Please reach out to your CrowdStrike representative to initiate an Authorization for such Services.

An Authorization for all Services (excluding Incident Response) must be approved by Customer and/or signed by Customer during the first ten (10) months of the Retainer Term. Such Services authorized by Customer may be scheduled to be delivered during the Retainer Term.

An authorized Customer representative may contact CrowdStrike by email or phone to request Incident Response Services and draw down the Retainer. In the event a Customer wants to draw down the Retainer for Incident Response Services under privilege, a Privileged Engagement Letter ("PEL") attached hereto as Exhibit B or other separate agreement must be mutually executed by CrowdStrike, the Customer and their legal counsel.

CrowdStrike will notify the Customer via email if the estimate for authorized Services will be exceeded. Customer is responsible for hours in excess of the estimate without the need for any additional approvals.

Delivery Schedule

Work will begin on a mutually agreed upon date. Customer-initiated changes or delays to the mutually agreed timeline for the Services may result in CrowdStrike rescheduling the Services in their entirety. If CrowdStrike is not able to reschedule the Services prior to the expiration of the Retainer Term, then the Retainer hours will expire.

Retainer Term

Unused Retainer hours will be forfeited after one (1) year following the SOW Effective Date and/or Order Effective Date ("Retainer Term"). Customer must use the Retainer hours within the Retainer Term.

Retainer Draw-down

As Services are performed, the Retainer hours will be drawn down by the Retainer amount at the corresponding rate indicated in the table in the Fees Section below. Each request for Services from Customer will draw down the Retainer by a minimum of 40 hours unless otherwise set forth on the applicable Authorization (defined above). Remaining Retainer hours (if any) may be used for Incident Response Services

[1]https://www.crowdstrike.com/terms-conditions/

or Other Services as described herein. Time spent creating reports is charged against the Retainer. Customer must use the Retainer hours within the Retainer Term. Unused hours will be forfeited upon termination or at the expiration of the Retainer Term.

Exceeding the Retainer Hours

If the pre-purchased Retainer hours are drawn to zero, CrowdStrike will notify Customer's Technical Contact or other authorized representative(s). At Customer's request, CrowdStrike will continue to provide Services for engagements that are then in progress at CrowdStrike's then-current hourly rate. If Services exceed remaining Retainer hours, CrowdStrike will draw down additional hours as set forth in the Authorization or as otherwise agreed upon by the parties.

Change Management

Any change to the scope of Services will be agreed upon in writing by the parties in advance of the change and any additional fees associated therewith.

CROWDSTRIKE

Retainer Tiers and Response Times

Retainer Tiers and Response Times

CrowdStrike will respond to Customer's request for Incident Response Services under the Retainer within the committed response times shown below. Committed response times are only honored after an initial onset period of 7 days from the purchase of the Retainer hours. Committed response times require Customer to contact CrowdStrike by phone at the international toll-free and regional numbers found below or by email at **services@crowdstrike.com****.

Response times outside the continental US, UK, EU, Australia, New Zealand, Singapore and Japan are subject to travel carrier and visa availability. CrowdStrike will make commercially reasonable efforts to respond to Customer's travel requests.

**If you are unsure if your email infrastructure may be compromised, consider sending us an email from a 3rd party email address (e.g., Gmail)*

International Toll-Free Lines:**

North America:	+1-855-276-9347
Australia:	+61 1800 290 853
Japan:	+81 800 170 5401
India:	000 800 040 3447
UK/Ireland:	+44 800 0487187
France:	+33 801840073
Germany:	+49 (0) 800 3252669
Saudi Arabia:	+966 8008803012
UAE	+971 8000320534
Qatar	+974 800101302

***Please note that toll-free numbers only operate within each country/region.*

Regional Lines*:**

Americas:	+1 (408) 663-5300 (US)
Europe:	+44 (118) 3701800 (UK)
APAC:	+61 (2) 99254300 (AU)

**** Please note that regional telephone numbers can be dialed internationally.*

Service Component	Tier 1	Tier 2	Tier 3	Tier 4
Minimum Hours included in Retainer	110	160	248	480
Response time (24/7 phone and email IR Hotline) – remote*	8 hours	6 hours	4 hours	2 hours
Response time – En route on-site*	2 Days	2 Days	1 Day	1 Day

*Subject to resource availability, travel advisories/restrictions, and/or visa/work permits, and/or privileged engagement letter, if required.

CROWDSTRIKE

Invoicing, Fees & Expenses

Invoicing, Fees & Expenses

Travel & Expenses

CrowdStrike will charge actual expense amounts as incurred and will provide access to copies of receipts for those expense amounts upon request. CrowdStrike will not travel unless coordinated with the Customer. Travel expenses shall be reimbursed as follows: coach class airfare for flight times of 4 hours or less, economy plus for flight times between 4 and 8 hours, and business class airfare for flight times of more than 8 hours or for urgent international travel in support of Incident Response Services; moderate class lodging; full size rental car; ground transportation including taxi or similar transportation services, parking, and/or mileage at the local government approved rate (e.g. IRS rates for U.S.); visa, work permit or similar fees; meal allowance of USD 125 per person per day. Time spent traveling will be charged at USD 225 per person per hour. Travel time estimates are not included in any Services time estimates.

Legal Request Fees

In the event CrowdStrike is legally required to respond to a request for information, and/or provide documents or testimony in connection with the Services as part of: (a) a legal proceeding to which the Customer is a party and CrowdStrike is not; or (b) a government or regulatory investigation of the Customer, the Customer shall: (i) pay all of CrowdStrike's reasonable and actual out of pocket legal fees and expenses (as evidenced by reasonably detailed invoices) in connection therewith, and (ii) pay the hourly rate set forth in the Order/SOW (if no hourly rate is stated, then CrowdStrike's then-current hourly rate) for CrowdStrike's consultants' actual hours worked in responding to such requirement, including, time spent preparing for, and participating in, depositions and other testimony.

Taxes

Customer agrees to be responsible for the collection, remittance and reporting of all Value Added Taxes or similar taxes related to the Services if work is performed outside the United States. Customer is not responsible for any income tax liability incurred by CrowdStrike.

If Payor is claiming a governmental exemption from sales tax, Payor agrees to provide an official purchase order, or other documentation demonstrating direct payment from Payor's agency, and CrowdStrike will confirm whether or not such an exemption is applicable in Payor's particular jurisdiction. Purchases by individuals and reimbursed to them by a federal, state, or local government do not qualify for a sales tax exemption.

Invoicing and Payment

In the event time and materials Services are provided, CrowdStrike will invoice Customer at the end of each month for all Services fees. CrowdStrike will invoice for: (i) CrowdStrike Tools fees and/or Post-Engagement Data Retention fees, if any, (ii) travel time, if any, and (iii) actual expense amounts, all incurred in arrears. The Retainer Fee is charged to the Customer for the set-up and management of the Retainer during the initial Term.

If Customer requires a purchase order to be referenced for incurred billable expenses, the Customer shall issue a purchase order(s) to CrowdStrike. Customer shall pay in US dollars all invoices within 30 days of receipt, unless otherwise set forth in the Agreement.

CROWDSTRIKE

CrowdStrike Tools

CrowdStrike Tools

Use of CrowdStrike Tools

Definition

CrowdStrike may use tools while performing the Services (the "CrowdStrike Tools"). CrowdStrike Falcon is not subject to the tools fees as defined in this Professional Services Catalog. Data collected by CrowdStrike Tools is encrypted and stored in the United States or European Union and viewed by personnel in locations that include, but are not limited to, the United States, Canada, United Kingdom, the European Union, New Zealand and Australia.

Falcon Forensics

CrowdStrike personnel may use the Falcon Forensics tool to collect specific data points relevant to the investigation based upon their expertise and knowledge of specific actors/threats. The following are some of the functions performed by Falcon Forensics: directory parsing, handles dump, file hashing, network data dump, detailed process listing, strings extraction, services enumeration, drivers enumeration, environment variables dump, jobs and task enumeration, users and group enumeration.

Falcon Horizon & CrowdStrike Cloud Collectors

CrowdStrike personnel may use Falcon Horizon, a cloud security posture management and detection application, and the CrowdStrike Cloud Collectors, a cloud data collection toolset, to collect and analyze cloud service plane-related information in order to help identify adversary tradecraft and activity.

Falcon Network

CrowdStrike may utilize a threat-specific network monitoring tool referred to as Falcon Network to identify potential outbound malicious communications. CrowdStrike's threat signatures focus on targeted attackers, advanced persistent threats, organized crime and hacktivist groups. Falcon Network is connected to a network egress location and passively captures suspicious traffic in a packet capture library (PCAP). CrowdStrike will not capture any data or signatures other than those necessary to perform the Services. Falcon Network utilizes Corelight and proprietary configurations and tools to maintain a stealth packet capture capability.

CrowdStrike Falcon

CrowdStrike personnel may use CrowdStrike Falcon, a cloud-managed end point detection and response application. CrowdStrike Falcon is comprised of two core components, the cloud-based application and the on-premise device sensor application (Falcon Sensor). CrowdStrike Falcon leverages the lightweight Falcon Sensor that shadows, captures, and correlates low-level operating system events, including, but not limited to: machine event data, executed scripts, code, systems files, log files, DLL files; login data, usernames, binary files, file names, tasks, resource information, commands, protocol identifiers, Internet protocol addresses, URLs, network data, and/or other executable code and metadata. To the extent data collected by the CrowdStrike Tools is aggregated and/or anonymous it is referred to as Execution Profile/Metric Data. Execution Profile/Metric Data, similar to Threat Actor Data, is used for collective security purposes and is not considered Customer Confidential Information. The analysis of the collected data helps identify the adversary tradecraft and activity as opposed to focusing on malware signatures, indicators of compromise, exploits, and vulnerabilities, used in older information security technology. CrowdStrike uses Execution Profile/Metric Data to analyze, characterize, attribute, warn of, and/or respond to threats against you and others, and to analyze trends and to optimize the functionality of CrowdStrike's products and services. CrowdStrike Falcon is equipped with response functionality, including but not limited to advanced information gathering (e.g.,

suspicious or unknown file collection) and actions such as executing scripts and executables, deleting a file, terminating processes, and deleting or modifying Windows registry key or value. CrowdStrike provides automatic updates to CrowdStrike Falcon.

CrowdStrike Tools Fee and Post-Engagement Data Retention Fees

If CrowdStrike Tools (defined in section entitled CrowdStrike Tools) are used in performing Services, the CrowdStrike Tools fee shall be incurred on a per month basis as set forth in Tools Fee(s) Table below and set forth in a signed writing. If Falcon Network Sensors (Corelight) are used, a refund will not be provided for partial use. If CrowdStrike is directed, in writing, to retain evidence/data beyond standard retention periods, then the Customer shall pay the post-engagement data retention fees set forth in the Post-Engagement Data Retention Fee(s) Table.

Tools Fee(s) Table

CrowdStrike Tool	Type & Size	Fee per month (or any portion thereof)
Falcon Network Sensor (Legacy)	Hardware/1G	USD 5,500
Falcon Network Sensor (Legacy)	Hardware/10G	USD 16,500
Falcon Network Sensor (Legacy)	Virtual/One Instance	USD 1,100
Falcon Network Sensor (Corelight)	Varies	USD 2, 500 per Gbs per month
Falcon Forensics Collector	One endpoint	USD 1.00/end point
CrowdStrike Cloud Collector	One platform	USD 2,500/platform

Post-Engagement Data Retention Fee(s) Table

Evidence/Data	If retention period is longer than…	Fees per month (or any portion thereof)
Physical Evidence (e.g., removable media, hard drives)	90 days from the completion of the engagement*	USD 500.00 per physical evidence device
Virtual Evidence (e.g., system images, memory capture) and Falcon Forensics Collector data	90 days from the completion of the engagement*	USD 25.00 per GB (or any portion thereof)

*The completion of the engagement date will be specified in an email from CrowdStrike at the conclusion of the Services.

CROWDSTRIKE

Incident Response Services

Incident Response Services

Non-Privileged Incident Response

CrowdStrike will assist Customer with responding to a suspected computer security incident.

Concept of Operations

During the response to the suspected computer security incident, CrowdStrike may, as needed:

- Determine compromised or accessed systems, develop a timeline of attacker activity, investigate the likely attack vector, and what data and user accounts may have been compromised or accessed;
- Provide recommendations for containment actions and as directed, use CrowdStrike Tools to perform tactical containment actions, including but not limited to advanced information gathering (e.g., suspicious or unknown file collection) and actions such as removing malware, terminating processes, and removing or modifying a malicious Windows registry key or value;

During the investigation CrowdStrike may, as needed, analyze data provided by Customer, including but not limited to:

- Forensic images of disk and/or memory from systems of interest;
- Data collected by CrowdStrike Tools;
- Live response data from suspected systems of interest;
- Logs from computer systems, including network traffic, firewalls, DNS and DHCP servers, authentication servers, VPN or remote access servers, and system logs;
- Documentation of system and network architecture, tools and capabilities;
- How the incident was detected, and business concerns related to the incident;
- Malware, attack tools, malicious software or documents, adversary tactics or other Threat Actor Data;

- Provide, assist with the deployment of, and use CrowdStrike Tools as well as use existing Customer tools to gather data for analysis;
- Discuss the incident with Customer staff in remote or in-person meetings;
- Perform this analysis on or off Customer's site;

The performance of Incident Response may require the use of CrowdStrike Tools. The CrowdStrike Tools fee is set forth in the section entitled CrowdStrike Tools.

Network Analysis

CrowdStrike shall, as needed:

- Provide network analysis services;

- Provide to Customer for use during the engagement Falcon Network (defined in the section entitled *CrowdStrike Tools***)** that monitor network traffic near Internet egress designated by Customer;
- Help Customer's staff position and connect Falcon Network hardware (if any) to Customer's network;
- Collect and analyze network traffic;

Potential Engagement Artifacts

CrowdStrike may produce recommendations for long-term continuous security posture improvement.

- CrowdStrike may, as requested, construct and present draft and final reports containing findings and observations. A report is initially delivered in a draft format and then discussed with Customer. The draft report is then revised and delivered as a final report if Customer has not requested revisions or provided questions regarding the report in 10 business days. CrowdStrike will conduct discussion and status meetings as defined above. The written engagement artifacts (report) may contain information summarizing the Services for an executive reader, as well as detailed technical information for a technical reader.

Privileged Incident Response

Customer's legal counsel may engage CrowdStrike to provide incident response services at the direction of counsel subject to the attorney-client privilege by executing the PEL attached hereto as Exhibit B or other signed writing.

CROWDSTRIKE

Response Readiness Services

Response Readiness Services

Response Readiness Exercise Level 1

CrowdStrike will conduct a collaborative Response Readiness Exercise Level 1 held remotely over two half-day periods to assist Customer with responding to incidents faster and avoiding common incident response pitfalls.

Document Review

Customer will provide, and CrowdStrike will review, certain Customer documentation requested by CrowdStrike, such as Customer's Incident Response Plan, in order to understand Customer's security incident response processes and security posture.

Workshops

CrowdStrike will conduct a series of up to six incident response preparedness workshops in areas including forensic data acquisition, Customer security posture, legal privilege, and CrowdStrike technologies. Additionally, CrowdStrike will guide Customer through deploying CrowdStrike Falcon and/or Falcon Forensics Collector on a small sample of systems to ensure quick deployment during an incident.

Customer workshop attendees may include:

- Information Security Leadership
- Information Security Team Members
- Software Deployment Team
- Legal Counsel
- Communications

Deliverables

At Customer's request, CrowdStrike will provide:

- A Retainer Summary document containing consolidated key data on Customer's environment to facilitate CrowdStrike's responders to rapidly engage during an incident response
- A copy of the slides used in each of the workshops

Response Readiness Exercise Level 2

CrowdStrike will conduct a collaborative Response Readiness Exercise Level 2 held remotely over two half-day periods to assist Customer with preparing for and responding to select trending attacks.

Note: Customers are required to first complete the Response Readiness Exercise Level 1 before this engagement.

Documentation Review

Customer will provide, and CrowdStrike will review, certain Customer documentation requested by CrowdStrike, such as Customer's Incident Response Plan and Network Diagrams, in order to understand Customer's security incident response processes and security posture.

Workshops

CrowdStrike will conduct a series of up to six incident response preparedness workshops in areas including ransomware, cloud (Amazon Web Services or Azure), and supply chain attacks as well as incident response plan best practices.

Customer workshop attendees may include:

- Information Security Leadership
- Information Security Team Members
- Falcon Analysts
- Cloud Infrastructure Architects

Deliverables

At Customer's request, CrowdStrike will construct and provide:

- An addendum to the Retainer Summary document initially constructed during the previous Response Readiness Exercise Level 1 containing red / yellow / green scoring against best practices for incident response preparedness such as ransomware, cloud, and supply chain attacks as well as incident response plan best practices discussed during the workshops
- A copy of the slides used in each of the workshops

CROWDSTRIKE

Strategic Advisory Services

Strategic Advisory Services

SOC Assessment

In order to understand and improve the current maturity of Customer's SOC CIRT function, CrowdStrike will assess current SOC capabilities in relation to people, process, and technology. This will comprise of the following activities:

Documentation Review

Customer will provide, and CrowdStrike will review, Customer's documentation relevant to supporting the onsite workshops and development of deliverables. CrowdStrike may request documentation including, but not limited to:

- Information Security policies, procedures, playbooks
- Incident Response policies, procedures, playbooks
- Information Security and SOC organizational chart
- SIEM or monitoring and alerting process documentation
- List of forensic and IR tools
- List of security prevention/detection tools
- Multi-factor authentication platform and coverage information
- Threat intelligence platform and feed information
- Information Security roadmap, projects and/or initiatives
- Logical network diagrams

Workshops

CrowdStrike will conduct interactive workshops and information gathering with Customer's key stakeholders to understand the SOC CIRT people, processes, and technologies. The purpose of these workshops is not only to collect information to inform CrowdStrike's assessment, but also to provide a forum for sharing knowledge of best practices and common techniques across each capability area. In most situations, the workshops can be conducted over the course of one week, schedules permitting. CrowdStrike recognizes that not everyone it wants to speak with will be available in all cases, so it can support additional time onsite or alternatively, conduct any remaining discussions remotely.

The workshops will require participation from relevant Customer employees and will comprise of the following core topics:

- Governance
- Staffing
- Detection
- Response

- Threat Intelligence

CrowdStrike Falcon Enrichment

CrowdStrike will leverage the CrowdStrike Falcon agent to enrich the assessment by gathering additional information about Customer's security hygiene leveraging the following modules:

- Falcon Spotlight: A vulnerability management module that identifies unpatched vulnerabilities in the operating system and third-party applications.
- Falcon Discover: A network management and IT hygiene module that identifies unmanaged devices, credential use, and application use across an environment.
- Other modules: CrowdStrike may use other modules within the CrowdStrike Falcon platform to collect and report upon additional information relevant to Customer's security posture. CrowdStrike will leverage these additional modules upon mutual agreement with Customer.

If they are not already turned on, CrowdStrike will enable these modules during the information gathering and analysis phases of this assessment. Customer will have access to these modules during this time.

If Customer does not already have the Falcon agent deployed, CrowdStrike will provide Falcon for the duration of the assessment and can assist with deployment support. Alternatively, Customer can request that the SOC Assessment be conducted without the enhanced additional technical information from Falcon.

Location

These Services can be delivered either remotely or onsite at a Customer's location, as agreed between CrowdStrike and Customer.

Status Meetings

CrowdStrike will provide Customer regular updates on the progress of the Services. Brief updates will be provided on a schedule as agreed between Customer and CrowdStrike.

Deliverables

CrowdStrike will construct and deliver draft and final deliverables as follows:

- Engagement Report. This will be in the form of a Powerpoint document. CrowdStrike will provide current state strengths and detailed recommendations for achieving target state maturity. The report will include current state, future state maturity ratings, and recommendations prioritized by criticality and difficulty. Customer will have ten days to review and provide feedback on the draft report. If Customer has not provided feedback or comments within ten days after delivery, CrowdStrike will finalize the report.

Cybersecurity Maturity Assessment

CrowdStrike evaluates an organization's cybersecurity maturity level in relation to its ability to prevent, detect, and respond to advanced adversaries. Within this context, CrowdStrike will assess the Customer's environment for opportunities to close gaps in their cybersecurity people, processes, and technologies. Customer will select from among three available Cybersecurity Maturity Assessment ("CSMA") offerings designed to scale with the complexity and size of their organizations.

Concept of Operations

CrowdStrike's Cybersecurity Maturity Assessment ("CSMA") offering takes a multi-faceted approach to gaining an understanding of the Customer's existing cybersecurity program. CrowdStrike will review relevant internal cybersecurity documentation and then conduct workshops with individuals within the organization who understand how the Customer's existing cybersecurity program works in reality – regardless of what the documentation may say. We also use our Falcon agent to collect information from the Customer's endpoints in order to gain a better understanding of the technical hygiene in the environment. Optionally, the CSMA can be performed without the use of the Falcon agent. By combining these information sources, CrowdStrike will help to paint the picture of where the organization's capabilities are strong, where it can improve, and what steps are recommended for the organization to mature.

Scope of Assessment

CrowdStrike's three CSMA offerings utilize similar methodologies but vary in scope and scale. The assessment scope and scale will depend on the specific offering that Customer selects:

CSMA (Core)

CrowdStrike will focus its assessment across six core cybersecurity areas:

- Security Foundations
- Detection
- Prevention
- Response
- Governance
- Threat Intelligence

CSMA (Expanded)

CrowdStrike will assess the six core cybersecurity areas, as well as three additional focus areas agreed by CrowdStrike and Customer based on Customer's risk profile or operational challenges.

Core cybersecurity areas:

- Security Foundations
- Detection
- Prevention
- Response
- Governance
- Threat Intelligence

Additional focus areas may include:

- Identity and Access Management
- Asset and Vulnerability Management
- Disaster Recovery and Business Continuity
- Server and Endpoint Security

- Network Security
- Cloud Security
- Application and Database Security
- Cybersecurity Incident Detection and Response
- Operational Technology Security

CSMA (Enterprise)

CrowdStrike will focus its assessment across areas to include:

- Strategy and Governance
- Culture, Awareness, and Training
- Risk and Compliance
- Identity and Access Management
- Asset and Vulnerability Management
- Disaster Recovery and Business Continuity
- Server and Endpoint Security
- Network Security
- Cloud Security
- Application and Database Security
- Cybersecurity Incident Detection and Response
- Threat Intelligence

Depending on the Customer's risk profile or operational challenges, an additional area of focus could include:

- Operational Technology Security

Potential Engagement Artifacts

CrowdStrike may provide the following artifact for this engagement:

- An executive summary that succinctly summarizes the scope of the assessment and surveys, at a high level, the primary observations noted during the assessment. Observations include key strengths, areas for improvement, and associated recommendations. This report will also, at Customer's discretion, include the graphical representation of the organization's cybersecurity maturity, as determined through the assessment.
- A full assessment report with descriptions of the CSMA methodology, maturity scores and proposed target maturity levels for each capability area, recommendations for achieving the target maturity levels, prioritization of which recommendations to pursue first, and any technical hygiene findings from Falcon enrichment analysis. Customer will have ten days to review and provide feedback on the draft report. If Customer has not provided feedback or comments within ten days after delivery, CrowdStrike will finalize the report.
- Mapping to NIST Cybersecurity Framework (CSF) (Optional)

Cybersecurity Program Semi-Annual Review

After completing an assessment in connection with which Customer has ordered a Cybersecurity Program Semi-Annual Review, CrowdStrike will help a Customer stay abreast of the attack landscape as it relates to that organization, meeting with the Customer on a semi-annual basis to assess its cybersecurity program and roadmap for improvement.

Concept of Operations

CrowdStrike will meet with Customer's security and executive staff to review and discuss progress against CrowdStrike's previously completed Cybersecurity Maturity Assessment. These review sessions will assist Customer with enhancing, modifying, or accelerating aspects of its cybersecurity program in relation to shifts in the industry, technologies, or Customer's business model.

- **Customer Inputs**
  - Customer will provide CrowdStrike with:
    - Appropriate attendees for the advisory meetings, and provide a location for them
- **Semi-Annual Review Activities**
  - CrowdStrike will:
    - Travel to Customer's site, or coordinate remote interviews, two times per year;
    - Provide two consultants for up to two days of meetings, as mutually agreed with Customer;
    - Meet with Customer's technical and executive personnel, discussing Customer's progress against the previously completed Cybersecurity Maturity Assessment. More specifically, over the course of the two semi-annual sessions, CrowdStrike will discuss changes in Customer's security posture, the status of security projects and initiatives, trends in targeted attacks, and trends in defensive strategies. Customer must complete both sessions within 18 months of the previously completed Cybersecurity Maturity Assessment;
    - Review documentation related to Customer's cybersecurity program status and projects (no more than 3-5 documents, up to 50 pages in total);

Potential Engagement Artifacts

CrowdStrike will construct and deliver two Semi-Annual Review reports. Time spent constructing these reports is chargeable time. Customer will have ten days to review and provide feedback on the draft report. If Customer has not provided feedback or comments within ten days after delivery, CrowdStrike will finalize the report. CrowdStrike will conduct discussion and status meetings as defined above.

Security Program In-Depth Assessment

CrowdStrike's Security Program In-Depth Assessment is a holistic review of your security program's strengths and areas for improvement.

The Security Program In-Depth Assessment is currently only offered to Customers based in EMEA region.

Concept of Operations

CrowdStrike will review existing documentation and facilitate a series of interactive workshops with key stakeholders across twelve security program domains. These workshops are intended to be educational for your organization and are used by CrowdStrike to collect information for the resulting gap analysis. In addition to documentation review and workshops, CrowdStrike can optionally leverage the CrowdStrike Falcon agent to enrich the assessment by gathering additional information about Customer's security hygiene. CrowdStrike will use this information to determine how mature the Customer's organization is today and provides guidance on achieving its desired future state.

General Timeline

Weeks 0 - 1 – Kick-off, Falcon Deployment (Optional), and Documentation Review

CrowdStrike will conduct a kick-off meeting, where it confirms its understanding of the Customer's objectives and explain its approach to meeting the Customer's goals for the engagement. CrowdStrike will then begin reviewing existing documentation to orient our team to the organization's environment, prepare for the workshops, and develop the report deliverables.

Week 2 – Workshops and Analysis

CrowdStrike will conduct interactive workshops and information gathering with the organization's key stakeholders across the following core domains:

- Strategy and Governance
- Culture, Awareness, and Training
- Risk and Compliance
- Identity and Access Management
- Asset and Vulnerability Management
- Disaster Recovery and Business Continuity
- Server and Endpoint Security
- Network Security
- Cloud Security
- Application and Database Security
- Cybersecurity Incident Response
- Threat Intelligence

Weeks 3 - 6 – Follow-up Requests and Reporting

At the conclusion of our workshops, CrowdStrike will determine if there are any additional data points that it requires to complete its understanding of the Customer's environment. Where necessary, it will request additional documentation or schedule a corresponding follow-up meeting. While CrowdStrike closes out these items, it will begin formalizing its observations and recommendations.

Potential Engagement Artifacts

CrowdStrike may provide the following artifacts for this engagement:

- Security Program In-Depth Assessment Report: Executive Summary, Methodology and Maturity Scoring, Detailed Recommendations, and an execution roadmap graphic. Customer will have ten days to review and provide feedback on the draft report. If Customer has not provided feedback or comments within ten days after delivery, CrowdStrike will finalize the report.
- Technical Findings from CrowdStrike Falcon Enrichment: Using Spotlight and Discover Falcon modules, this area of the report highlights technical hygiene issues associated with software and operating system vulnerabilities, account usage, and unmanaged or outdated assets.
- Mapping to Industry Standard Framework (Optional)

Ransomware Defense Assessment

The CrowdStrike Ransomware Defense Assessment will evaluate Customer's ability to prevent, detect, respond to, and recover from a ransomware attack as well as recommend improvements to strengthen a Customer's defensive posture. This will comprise the following activities:

Documentation Review

Customer will provide, and CrowdStrike will review, Customer's documentation relevant to supporting workshops and development of deliverables. CrowdStrike may request documentation including, but not limited to:

- Information Security roadmap, projects and/or initiatives
- Incident Response policies, procedures, playbooks
- Information Security and SOC organizational chart
- Active Directory architecture documentation
- Crisis management plans
- List of forensic and IR tools
- List of security prevention/detection tools
- Disaster recovery and business continuity plans and test results
- SIEM or monitoring and alerting process documentation
- Threat intelligence platform and feed information
- Logical network diagrams

Technical Review

CrowdStrike will conduct the following activities:

- Execute Active Directory collection tools, including common system administration and typical attacker software, to determine hidden relationships between Customer user accounts and groups, and attack paths likely to be utilized during a ransomware attack;
- Identify domain accounts with weak or exposed passwords, risky configurations, stealthy privileges, and anomalous activity; and
- Review vulnerability information to identify ransomware-related Application and Windows vulnerabilities that exist in the environment.

Customer will work with CrowdStrike to ensure the proper deployment, configuration, and activation of CrowdStrike Tools and other required software tooling necessary to perform the Services set forth herein.

Workshops

CrowdStrike will conduct interactive workshops and information gathering with Customer's key stakeholders to understand the Information Security program people, processes, and technologies as it

relates to ransomware. The purpose of these workshops is not only to collect information to inform CrowdStrike's assessment, but also to provide a forum for sharing knowledge of best practices and common techniques across each capability area. In most situations, the five workshops can be conducted over the course of one week, schedules permitting. The workshops will require participation from relevant Customer employees and will comprise the following core topics:

- Ransomware Threat Landscape;
- Prevention & Detection: Identity;
- Prevention & Detection: Endpoint;
- Prevention & Detection: Network;
- Response & Recovery.

Location

CrowdStrike will perform work under this task remotely.

Status Meetings

CrowdStrike will provide Customer regular written updates on the progress of the Services. Summary status reports will be provided weekly, prior to the weekly status meetings.

Deliverables

CrowdStrike will:

- Document and deliver a report consisting of the following sections:
    - Executive Summary - a high-level overview of Customer's ransomware readiness posture;
    - Recommendations Overview;
    - Recommendations – specific actions or considerations to address documented issues
- Customer will have ten days to review and provide feedback on the draft report. If Customer has not provided feedback or comments within ten days after delivery, CrowdStrike will finalize the report.

Cybersecurity Technical Tabletop Exercise

CrowdStrike will exercise Customer's ability to respond to a targeted attack. CrowdStrike will provide one simulated exercise for Customer's technical response team focused on identification, triage, containment, analysis, and remediation. For Customers in the United States, this Service is only delivered in conjunction with a Management Tabletop Exercise and/or Executive Tabletop Exercise.

Information Gathering Phase

Documentation Review

- Customer will provide, and CrowdStrike will review, Customer's documentation to understand Customer's security processes. CrowdStrike may request documentation including, but not limited to:
  - Information Security policies, procedures, playbooks
  - Incident Response policies, procedures, playbooks
  - Information Security organizational chart
  - SIEM or monitoring and alerting process documentation
  - List of forensic and IR tools
  - List of security prevention/detection tools
  - Two factor authentication usage information

Interviews

- CrowdStrike will conduct interviews with one or more of Customer's key stakeholders to understand how security processes are conducted.
- CrowdStrike will require multiple conversations with individuals who are:
  - Knowledgeable of the organization's security infrastructure and processes, who can attest to the plausibility of different attack methods
  - Knowledgeable of the security team's detection and response processes who can help CrowdStrike anticipate likely responses to different scenario inputs
- Additional documents and meetings may be requested or scheduled to facilitate follow up questions and additional areas of interest.

CrowdStrike Falcon Enrichment

CrowdStrike will leverage the CrowdStrike Falcon agent to inform the exercise scenario by gathering additional information about Customer's security hygiene leveraging the following modules:

- **Falcon Spotlight:** A vulnerability management module that identifies unpatched vulnerabilities in the operating system and third-party applications.
- **Falcon Discover:** A network management and IT hygiene module that identifies unmanaged devices, credential use, and application use across an environment.

- **Other modules:** CrowdStrike may use other modules within the CrowdStrike Falcon platform to collect and report upon additional information relevant to Customer's security posture. CrowdStrike will leverage these additional modules upon mutual agreement with Customer.

If they are not already turned on, CrowdStrike will enable these modules during the information gathering and analysis phases of this assessment. Customer will have access to these modules during this time.

If Customer does not already have the Falcon agent deployed, or upon Customer request, the exercise can be conducted without the additional technical information from Falcon.

Exercise Development and Delivery Phase

CrowdStrike will prepare and conduct one tabletop simulation.

- **Scenario Development**
  - CrowdStrike will work with Customer to develop a mutually agreeable scenario resulting from Customer's areas of interest, CrowdStrike's research into likely threats against the Customer from a cyber intelligence perspective, and CrowdStrike's experience conducting incident response investigations.

- **Delivery**
  - CrowdStrike will conduct the simulated incident in the following manner.
    - **Location.** These Services can be delivered either remotely or onsite at a Customer's location, as agreed between CrowdStrike and Customer.
    - **Duration.** The exercise will be up to four hours in length, including introductions, breaks, and wrap-up.
    - **Audio Visuals.** Customer will ensure that an appropriate office space is provided as well as basic audio-visual cables including USB-C, VDI, or HDMI.

- **Status Meetings**
  - CrowdStrike will provide Customer regular updates on the progress of the Services. Brief updates will be provided on a schedule as agreed between Customer and CrowdStrike. Summary written status reports will be provided weekly.

- **Project Schedule**
  - CrowdStrike and Customer will agree upon a delivery date for the Service. Any request by Customer to reschedule the delivery date may result in a delay in the provision of the Service. If the parties are not able to reschedule prior to the expiration of the Retainer Term, then the Retainer hours may expire.

Deliverables

CrowdStrike will produce two written deliverables:

- CrowdStrike will construct and deliver the slides utilized during the tabletop exercise.
- CrowdStrike will construct and deliver a summary report deck in PowerPoint format that contains an overview of the scenario, a list of participants, and the lessons learned, or key takeaways identified during the tabletop exercise. Customer will have ten days to review and provide feedback on the draft report. If Customer has not provided feedback or comments within ten days after delivery, CrowdStrike will finalize the report.

Cybersecurity Management Tabletop Exercise

CrowdStrike will exercise Customer's ability to respond to a targeted attack. CrowdStrike will provide one simulated exercise for Customer's management team focused on incident response decision making and crisis management.

CrowdStrike may use subcontractors in its provision of the Service. To the extent that such use of a subcontractor conflicts with the terms of the Agreement, Customer may be required to consent in writing to receive this Service.

Information Gathering Phase

Documentation Review

Customer will provide, and CrowdStrike will review, Customer's documentation to understand Customer's security processes. CrowdStrike may request documentation including, but not limited to:

- Information Security policies, procedures, playbooks
- Incident Response policies, procedures, playbooks
- Information Security organizational chart
- SIEM or monitoring and alerting process documentation
- List of forensic and IR tools
- List of security prevention/detection tools
- Two factor authentication usage information

Interviews

CrowdStrike will conduct interviews with one or more of Customer's key stakeholders to understand how security processes are conducted. CrowdStrike will require multiple conversations with individuals who are:

- Familiar with the organization's security infrastructure and processes, who can discuss to the plausibility of different attack methods
- Familiar with the organization's crisis management processes at the operational and management level

Additional documents and meetings may be requested or scheduled to facilitate follow up questions and additional areas of interest.

CrowdStrike Falcon Enrichment

CrowdStrike will leverage the CrowdStrike Falcon agent to inform the exercise scenario by gathering additional information about Customer's security hygiene leveraging the following modules:

- **Falcon Spotlight:** A vulnerability management module that identifies unpatched vulnerabilities in the operating system and third-party applications.
- **Falcon Discover:** A network management and IT hygiene module that identifies unmanaged devices, credential use, and application use across an environment.

- **Other modules:** CrowdStrike may use other modules within the CrowdStrike Falcon platform to collect and report upon additional information relevant to Customer's security posture. CrowdStrike will leverage these additional modules upon mutual agreement with Customer.

If they are not already turned on, CrowdStrike will enable these modules during the information gathering and analysis phases of this assessment. Customer will have access to these modules during this time.

If Customer does not already have the Falcon agent deployed, or upon Customer request, the exercise can be conducted without the additional technical information from Falcon.

Exercise Development and Delivery Phase

CrowdStrike will prepare and conduct one tabletop simulation.

Scenario Development

CrowdStrike will work with Customer to develop a mutually agreeable scenario resulting from Customer's areas of interest, CrowdStrike's research into likely threats against the Customer from a cyber intelligence perspective, and CrowdStrike's experience conducting incident response investigations.

Delivery

CrowdStrike will conduct the simulated incident in the following manner.

- **Location.** These Services can be delivered either remotely or onsite at a Customer's location, as agreed between CrowdStrike and Customer.
- **Duration**. The exercise will be up to four hours in length, including introductions, breaks, and wrap-up.
- **Audio Visuals.** Customer will ensure that an appropriate office space is provided as well as basic audio-visual cables including USB-C, VDI, or HDMI.

Status Meetings

CrowdStrike will provide Customer regular updates on the progress of the Services. Brief updates will be provided on a schedule as agreed between Customer and CrowdStrike. Summary written status reports will be provided weekly.

Project Schedule

CrowdStrike and Customer will agree upon a delivery date for the Service. Any request by Customer to reschedule the delivery date may result in a delay in the provision of the Service. If the parties are not able to reschedule prior to the expiration of the Retainer Term, then the Retainer hours may expire

Deliverables

CrowdStrike will produce two written deliverables:

- CrowdStrike will construct and deliver the slides utilized during the tabletop exercise.

- CrowdStrike will construct and deliver a summary report deck in PowerPoint format that contains an overview of the scenario, a list of participants, and the lessons learned, or key takeaways identified during the tabletop exercise. Customer will have ten days to review and provide feedback on the draft report. If Customer has not provided feedback or comments within ten days after delivery, CrowdStrike will finalize the report.

Cybersecurity Executive Tabletop Exercise

CrowdStrike will exercise Customer's ability to respond to a targeted attack. CrowdStrike will provide one simulated exercise for Customer's executive team focused on executive-level incident response decision making and crisis management.

CrowdStrike may use subcontractors in its provision of the Service. To the extent that such use of a subcontractor conflicts with the terms of the Agreement, Customer may be required to consent in writing to receive this Service.

Information Gathering Phase

Documentation Review

Customer will provide, and CrowdStrike will review, Customer's documentation to understand Customer's security processes. CrowdStrike may request documentation including, but not limited to:

- Information Security policies, procedures, playbooks
- Incident Response policies, procedures, playbooks
- Information Security organizational chart
- SIEM or monitoring and alerting process documentation
- List of forensic and IR tools
- List of security prevention/detection tools
- Two factor authentication usage information

Interviews

CrowdStrike will conduct interviews with one or more of Customer's key stakeholders to understand how security processes are conducted. CrowdStrike will require multiple conversations with individuals who are:

- Familiar with the organization's security infrastructure and processes, who can discuss to the plausibility of different attack methods
- Familiar with the executive team's operating dynamic—particularly with respect to crisis-response—who can help CrowdStrike anticipate likely responses to different scenario inputs

Additional documents and meetings may be requested or scheduled to facilitate follow up questions and additional areas of interest.

CrowdStrike Falcon Enrichment

CrowdStrike will leverage the CrowdStrike Falcon agent to inform the exercise scenario by gathering additional information about Customer's security hygiene leveraging the following modules:

- Falcon Spotlight: A vulnerability management module that identifies unpatched vulnerabilities in the operating system and third-party applications.

- Falcon Discover: A network management and IT hygiene module that identifies unmanaged devices, credential use, and application use across an environment.
- Other modules: CrowdStrike may use other modules within the CrowdStrike Falcon platform to collect and report upon additional information relevant to Customer's security posture. CrowdStrike will leverage these additional modules upon mutual agreement with Customer.

If they are not already turned on, CrowdStrike will enable these modules during the information gathering and analysis phases of this assessment. Customer will have access to these modules during this time.

If Customer does not already have the Falcon agent deployed, or upon Customer request, the exercise can be conducted without the additional technical information from Falcon.

Exercise Development and Delivery Phase

CrowdStrike will prepare and conduct one tabletop simulation.

Scenario Development

CrowdStrike will work with Customer to develop a mutually agreeable scenario resulting from Customer's areas of interest, CrowdStrike's research into likely threats against the Customer from a cyber intelligence perspective, and CrowdStrike's experience conducting incident response investigations.

Delivery

CrowdStrike will conduct the simulated incident in the following manner.

- Location. These Services can be delivered either remotely or onsite at a Customer's location, as agreed between CrowdStrike and Customer.
- Duration. The exercise will be up to four hours in length, including introductions, breaks, and wrap-up.
- Audio Visuals. Customer will ensure that an appropriate office space is provided as well as basic audio-visual cables including USB-C, VDI, or HDMI.

Status Meetings

CrowdStrike will provide Customer regular updates on the progress of the Services. Brief updates will be provided on a schedule as agreed between Customer and CrowdStrike. Summary written status reports will be provided weekly.

Project Schedule

CrowdStrike and Customer will agree upon a delivery date for the Service. Any request by Customer to reschedule the delivery date may result in a delay in the provision of the Service. If the parties are not able to reschedule prior to the expiration of the Retainer Term, then the Retainer hours may expire.

Deliverables

CrowdStrike will produce two written deliverables:

- CrowdStrike will construct and deliver the slides utilized during the tabletop exercise.
- CrowdStrike will construct and deliver a summary report deck in PowerPoint format that contains an overview of the scenario, a list of participants, and the lessons learned, or key takeaways identified during the tabletop exercise. Customer will have ten days to review and provide feedback on the draft report. If Customer has not provided feedback or comments within ten days after delivery, CrowdStrike will finalize the report.

Cybersecurity Management and Technical Tabletop Exercises

CrowdStrike will exercise Customer's ability to respond to a targeted attack. CrowdStrike will provide one simulated exercise for Customer's technical and management teams. The exercise will focus initially on the technical aspects of responding to a cybersecurity incident while the second half of the exercise will test the organization's incident response decision making and crisis management capabilities.

CrowdStrike may use subcontractors in its provision of the Service. To the extent that such use of a subcontractor conflicts with the terms of the Agreement, Customer may be required to consent in writing to receive this Service.

Information Gathering Phase

Documentation Review

Customer will provide, and CrowdStrike will review, Customer's documentation to understand Customer's security processes. CrowdStrike may request documentation including, but not limited to:

- Information Security policies, procedures, playbooks
- Incident Response policies, procedures, playbooks
- Information Security organizational chart
- SIEM or monitoring and alerting process documentation
- List of forensic and IR tools
- List of security prevention/detection tools
- Two factor authentication usage information

Interviews

CrowdStrike will conduct interviews with one or more of Customer's key stakeholders to understand how security processes are conducted.

CrowdStrike will require multiple conversations with individuals who are:

- Knowledgeable of the organization's security infrastructure and processes, who can attest to the plausibility of different attack methods
- Knowledgeable of the security team's detection and response processes who can help CrowdStrike anticipate likely responses to different scenario inputs
- Knowledgeable of the organization's crisis management processes at the operational and management level

Additional meetings may be scheduled to facilitate follow up questions and additional areas of interest.

CrowdStrike Falcon Enrichment

CrowdStrike will leverage the CrowdStrike Falcon agent to inform the exercise scenario by gathering additional information about Customer's security hygiene leveraging the following modules:

- **Falcon Spotlight:** A vulnerability management module that identifies unpatched vulnerabilities in the operating system and third-party applications.
- **Falcon Discover:** A network management and IT hygiene module that identifies unmanaged devices, credential use, and application use across an environment.
- **Other modules:** CrowdStrike may use other modules within the CrowdStrike Falcon platform to collect and report upon additional information relevant to Customer's security posture. CrowdStrike will leverage these additional modules upon mutual agreement with Customer.

If they are not already turned on, CrowdStrike will enable these modules during the information gathering and analysis phases of this assessment. Customer will have access to these modules during this time.

If Customer does not already have the Falcon agent deployed, or upon Customer request, the exercise can be conducted without the additional technical information from Falcon.

Exercise Development and Delivery Phase

CrowdStrike will prepare and conduct one tabletop simulation, leveraged for a technical response session and then for a management response session.

Scenario Development

CrowdStrike will work with Customer to develop a mutually agreeable scenario resulting from Customer's areas of interest, CrowdStrike's research into likely threats against the Customer from a cyber intelligence perspective, and CrowdStrike's experience conducting incident response investigations.

Delivery

CrowdStrike will conduct the simulated incident in the following manner**;**

- **Location.** These Services can be delivered either remotely or onsite at a Customer's location, as agreed between CrowdStrike and Customer.
- **Duration.** The exercise will be conducted in two sessions, which leverage the same scenario. The technical response session will be conducted first, over a period lasting up to four hours. The management response session will be conducted within the following month, over a separate period of up to four hours.
- **Audio Visuals.** Customer will ensure that an appropriate office space is provided as well as basic audio-visual cables including USB-C, VDI, or HDMI.

Status Meetings

CrowdStrike will provide Customer regular updates on the progress of the Services. Brief updates will be provided on a schedule as agreed between Customer and CrowdStrike. Summary written status reports will be provided weekly.

Project Schedule

CrowdStrike and Customer will agree upon a delivery date for the Service. Any request by Customer to reschedule the delivery date may result in a delay in the provision of the Service. If the parties are not able to reschedule prior to the expiration of the Retainer Term, then the Retainer hours may expire.

Deliverables

The primary deliverable from this engagement will be the exercises themselves. In addition, CrowdStrike will produce two written deliverables:

- CrowdStrike will construct and deliver the slides utilized during the tabletop exercises.
- CrowdStrike will construct and deliver a summary report deck in PowerPoint format that contains an overview of the scenario, a list of participants from each session, and the lessons learned, or key takeaways identified during the tabletop exercises. Customer will have ten days to review and provide feedback on the draft report. If Customer has not provided feedback or comments within ten days after delivery, CrowdStrike will finalize the report.

Cybersecurity Executive, Management, and Technical Tabletop Exercises

CrowdStrike will provide simulated exercises for Customer's Technical, Management, and Executive teams. The different exercise sessions will focus, respectively, on the technical aspects, the business operations and crisis management aspects, and the executive aspects of responding to a cybersecurity incident.

CrowdStrike may use subcontractors in its provision of the Service. To the extent that such use of a subcontractor conflicts with the terms of the Agreement, Customer may be required to consent in writing to receive this Service.

Information Gathering Phase

Documentation Review

Customer will provide, and CrowdStrike will review, Customer's documentation to understand Customer's security processes. CrowdStrike may request documentation including, but not limited to:

- Information Security policies, procedures, playbooks
- Incident Response policies, procedures, playbooks
- Information Security organizational chart
- SIEM or monitoring and alerting process documentation
- List of forensic and IR tools
- List of security prevention/detection tools
- Two factor authentication usage information

Interviews

CrowdStrike will conduct interviews with one or more of Customer's key stakeholders to understand how security processes are conducted.

CrowdStrike will require multiple conversations with individuals who are:

- Knowledgeable of the organization's security infrastructure and processes, who can attest to the plausibility of different attack methods
- Knowledgeable of the security team's detection and response processes who can help CrowdStrike anticipate likely responses to different scenario inputs
- Knowledgeable of the organization's crisis management processes at the operational and management level
- Knowledgeable of the executive team's operating dynamic—particularly with respect to crisis response—who can help CrowdStrike anticipate likely responses to different scenario inputs

Additional documents and meetings may be requested or scheduled to facilitate follow up questions and additional areas of interest.

CrowdStrike Falcon Enrichment

CrowdStrike will leverage the CrowdStrike Falcon agent to inform the exercise scenario by gathering additional information about Customer's security hygiene leveraging the following modules:

- Falcon Spotlight: A vulnerability management module that identifies unpatched vulnerabilities in the operating system and third-party applications.
- Falcon Discover: A network management and IT hygiene module that identifies unmanaged devices, credential use, and application use across an environment.
- Other modules: CrowdStrike may use other modules within the CrowdStrike Falcon platform to collect and report upon additional information relevant to Customer's security posture. CrowdStrike will leverage these additional modules upon mutual agreement with Customer.

If they are not already turned on, CrowdStrike will enable these modules during the information gathering and analysis phases of this assessment. Customer will have access to these modules during this time.

If Customer does not already have the Falcon agent deployed, or upon Customer request, the exercise can be conducted without the additional technical information from Falcon.

Exercise Development and Delivery Phase

CrowdStrike will prepare a single scenario, which will form the basis for each of the three exercise sessions. The content for each session will be tailored to the roles of the participants, but the underlying scenario will remain consistent across all sessions.

Scenario Development

CrowdStrike will work with Customer to develop a mutually agreeable scenario resulting from Customer's areas of interest, CrowdStrike's research into likely threats against the Customer from a cyber intelligence perspective, and CrowdStrike's experience conducting incident response investigations.

Delivery

CrowdStrike will conduct the simulated incident in the following manner.

- **Location.** These Services can be delivered either remotely or onsite at a Customer's location, as agreed between CrowdStrike and Customer.
- **Duration.** The exercise will be conducted in three sessions, which leverage the same scenario. The technical response session will be conducted first, over a maximum of a four-hour period. The management response session will be conducted within the following month, also over a maximum of a four-hour period. The executive exercise will be conducted within a month of the management exercise and will last no more than three hours.
- **Audio Visuals.** If necessary, Customer will ensure that an appropriate office space is provided as well as basic audio-visual cables including USB-C, VDI, or HDMI.
- **Facilitators.** CrowdStrike anticipates the core delivery team will consist of 2-3 consultants who develop and facilitate the exercise. CrowdStrike may involve additional personnel to assist in other phases of development, delivery, and reporting, as appropriate.

Status Meetings

CrowdStrike will provide Customer regular updates on the progress of the Services. Brief updates will be provided on a schedule as agreed between Customer and CrowdStrike. Summary written status reports will be provided weekly.

Project Schedule

CrowdStrike and Customer will agree upon a delivery date for the Service. Any request by Customer to reschedule the delivery date may result in a delay in the provision of the Service. If the parties are not able to reschedule prior to the expiration of the Retainer Term, then the Retainer hours may expire.

Deliverables

CrowdStrike will produce two written deliverables:

- CrowdStrike will construct and deliver the slides utilized during the tabletop exercise sessions.
- CrowdStrike will construct and deliver a summary report deck in PowerPoint format that contains an overview of the scenario, a list of participants, and the lessons learned, or key takeaways identified during the tabletop exercise sessions. Customer will have ten days to review and provide feedback on the draft report. If Customer has not provided feedback or comments within ten days after delivery, CrowdStrike will finalize the report.

Cybersecurity Management and Executive Tabletop Exercises

CrowdStrike will exercise Customer's ability to respond to a targeted attack. CrowdStrike will provide one simulated exercise for Customer's management and executive teams. The exercise will take place across two sessions, the first will test the organization's incident response decision making and crisis management capabilities at a management level, the second will focus on executive-level decisions informed by those management actions.

CrowdStrike may use subcontractors in its provision of the Service. To the extent that such use of a subcontractor conflicts with the terms of the Agreement, Customer may be required to consent in writing to receive this Service.

Information Gathering Phase

Documentation Review

Customer will provide, and CrowdStrike will review, Customer's documentation to understand Customer's security processes. CrowdStrike may request documentation including, but not limited to:

- Information Security policies, procedures, playbooks
- Incident Response policies, procedures, playbooks
- Information Security organizational chart
- SIEM or monitoring and alerting process documentation
- List of forensic and IR tools
- List of security prevention/detection tools
- Two factor authentication usage information

Interviews

CrowdStrike will conduct interviews with one or more of Customer's key stakeholders to understand how security processes are conducted.

CrowdStrike will require multiple conversations with individuals who are:

- Knowledgeable of the organization's security infrastructure and processes, who can attest to the plausibility of different attack methods
- Knowledgeable of the organization's crisis management processes at the operational and management level
- Knowledgeable of the executive team's operating dynamic—particularly with respect to crisis response—who can help CrowdStrike anticipate likely responses to different scenario inputs.

Additional meetings may be scheduled to facilitate follow up questions and additional areas of interest.

CrowdStrike Falcon Enrichment

CrowdStrike will leverage the CrowdStrike Falcon agent to inform the exercise scenario by gathering additional information about Customer's security hygiene leveraging the following modules:

- **Falcon Spotlight:** A vulnerability management module that identifies unpatched vulnerabilities in the operating system and third-party applications.
- **Falcon Discover:** A network management and IT hygiene module that identifies unmanaged devices, credential use, and application use across an environment.
- **Other modules:** CrowdStrike may use other modules within the CrowdStrike Falcon platform to collect and report upon additional information relevant to Customer's security posture. CrowdStrike will leverage these additional modules upon mutual agreement with Customer.

If they are not already turned on, CrowdStrike will enable these modules during the information gathering and analysis phases of this assessment. Customer will have access to these modules during this time.

If Customer does not already have the Falcon agent deployed, or upon Customer request, the exercise can be conducted without the additional technical information from Falcon.

Exercise Development and Delivery Phase

CrowdStrike will prepare and conduct one tabletop simulation, leveraged for a management response session and then for an executive response session.

Scenario Development

CrowdStrike will work with Customer to develop a mutually agreeable scenario resulting from Customer's areas of interest, CrowdStrike's research into likely threats against the Customer from a cyber intelligence perspective, and CrowdStrike's experience conducting incident response investigations.

Delivery

CrowdStrike will conduct the simulated incident in the following manner**;**

- **Location.** These Services can be delivered either remotely or onsite at a Customer's location, as agreed between CrowdStrike and Customer.
- **Duration.** The exercise will be conducted in two sessions, which leverage the same scenario. The management response session will be conducted first, over a period lasting up to four hours. The executive response session will be conducted some time in the following 30 days, over a separate period of up to four hours.
- **Audio Visuals.** Customer will ensure that an appropriate office space is provided as well as basic audio-visual cables including USB-C, VDI, or HDMI.

Status Meetings

CrowdStrike will provide Customer regular updates on the progress of the Services. Brief updates will be provided on a schedule as agreed between Customer and CrowdStrike. Summary written status reports will be provided weekly.

Project Schedule

CrowdStrike and Customer will agree upon a delivery date for the Service. Any request by Customer to reschedule the delivery date may result in a delay in the provision of the Service. If the parties are not able to reschedule prior to the expiration of the Retainer Term, then the Retainer hours may expire.

Deliverables

The primary deliverable from this engagement will be the exercises themselves. In addition, CrowdStrike will produce two written deliverables:

- CrowdStrike will construct and deliver the slides utilized during the tabletop exercises.
- CrowdStrike will construct and deliver a summary report deck in PowerPoint format that contains an overview of the scenario, a list of participants from each session, and the lessons learned, or key takeaways identified during the tabletop exercises. Customer will have ten days to review and provide feedback on the draft report. If Customer has not provided feedback or comments within ten days after delivery, CrowdStrike will finalize the report.

Executive Briefings

Executive Cybersecurity Briefing for Assessments

After completing an assessment in connection with which Customer has ordered an Executive Cybersecurity Briefing, CrowdStrike will, in consultation with Customer, prepare and deliver a briefing directed to members of Customer's executive team. CrowdStrike will propose an outline for what information will be covered in the briefing. CrowdStrike and Customer will review this outline and identify any revisions required to align with Customer's objectives. As needed, CrowdStrike can walk through the briefing in advance and make iterative revisions based on customer feedback, though multiple rounds of revisions may increase the level of effort.

The briefing will address the security posture of the organization based on the results of the assessment, and may, upon mutual agreement between CrowdStrike and Customer, also include additional items of interest such as cybersecurity news, trends, or general information. Customer will decide whether the briefing will be entirely verbal or if it will include any presentation materials (i.e., PowerPoint slides). Any presentation materials developed in support of the briefing will be provided to Customer, upon request. CrowdStrike and Customer will mutually agree upon whether CrowdStrike will present the briefing in person or remotely.

Executive Cybersecurity Briefing for Tabletops

After completing a tabletop exercise in connection with which Customer has ordered an Executive Cybersecurity Briefing, CrowdStrike will, in consultation with Customer, prepare and deliver a briefing directed to members of Customer's executive team. CrowdStrike will propose an outline for what information will be covered in the briefing. CrowdStrike and Customer will review this outline and identify any revisions required to align with Customer's objectives. As needed, CrowdStrike can walk through the briefing in advance and make iterative revisions based on customer feedback, though multiple rounds of revisions may increase the level of effort.

The briefing will address key organizational challenges, as well as strengths and areas for improvement, based on the results of the tabletop exercise, and may, upon mutual agreement between CrowdStrike and Customer, also include additional items of interest such as cybersecurity news, trends, or general information. Customer will decide whether the briefing will be entirely verbal or if it will include any presentation materials (i.e., PowerPoint slides). Any presentation materials developed in support of the briefing will be provided to Customer, upon request. CrowdStrike and Customer will mutually agree upon whether CrowdStrike will present the briefing in person or remotely.

Board Education Services

CrowdStrike will, in the form and manner specified below, prepare and deliver a briefing to members of Customer's Board of Directors. The focus of this briefing will be educating Board Members on selected topics related to cyber risk management and the evolving threat landscape.

Briefing Proposal

CrowdStrike will propose an outline with suggested topics for the briefing based on Customer's risk profile and relevant threat landscape. Typical briefing topics include risk management, emerging threat, cyber crisis management, and the respective roles of the Board and the management team. CrowdStrike and Customer will review this outline and identify any additional topics or revisions required to align with Customer's objectives. CrowdStrike and Customer will mutually agree to the inclusion of any additional topics.

Briefing Design and Delivery

CrowdStrike will then work with Customer to develop the outline into a presentation as follows:

- Format: Customer will advise CrowdStrike whether the briefing will be entirely verbal or if it will include any presentation materials (i.e., PowerPoint slides). Any presentation materials developed in support of the briefing will be provided to Customer, upon request.
- Location: CrowdStrike and Customer will mutually agree upon whether CrowdStrike will present the briefing in person or remotely.
- Review: Customer may request CrowdStrike to walk through the briefing in advance and make any iterative revisions based on Customer's feedback, though Customer acknowledges rounds of revisions may increase the level of effort.
- Delivery: CrowdStrike will conduct a briefing lasting up to 90 minutes, including Q&A.

Customer must provide information about the format, location, and duration of the briefing at least 15 business days prior to the briefing in order to allow for adequate preparation and review.

Status Updates

CrowdStrike will provide Customer regular updates on the progress of the Services. Brief updates will be provided on a schedule as agreed between Customer and CrowdStrike. Summary written reports will be provided weekly unless otherwise agreed.

Engagement Artifacts

If Customer requests that the briefing include presentation materials, the PowerPoint slides or other materials will be provided to Customer upon request. If Customer requests a verbal briefing only, there will be no written deliverables for this engagement.

Risk Management Review

CrowdStrike will help Customer review its technical risk exposure and cybersecurity risk management processes. This engagement will consist of a technical review and a programmatic review. The technical review will identify potential risk areas or enforcement gaps in security policy as applied. The programmatic review will evaluate the elements of the security program that support cyber risk management.

Phase 1: Technical Review

CrowdStrike will assist the Customer with identifying system inventory, missing patches, application usage, and account usage within the Customer's environment. This engagement supports Windows Active Directory environments only.

CrowdStrike Tools

CrowdStrike will help Customer deploy certain CrowdStrike software and hardware tools in Customer's environment as described below (the "CrowdStrike Tools" as defined below);

- CrowdStrike will:
  - Provide to Customer for use during the engagement the CrowdStrike Falcon tool, unless Customer is already permitted to use CrowdStrike Falcon under a different agreement;
  - Provide limited deployment support, including up to two 30-minute troubleshooting discussions via telephone and additional support via email;
- Customer will:
  - Deploy CrowdStrike Tools in Customer's environment;
  - Work with CrowdStrike to configure the tools to the necessary specifications;
  - Approve CrowdStrike usage of real time response (RTR) functionality within the Falcon platform.
- The CrowdStrike Tools are licensed to Customer as-is for internal evaluation use only and not sold, and no title or ownership to the CrowdStrike Tools or the intellectual property embodied therein passes as a result of this Agreement or any act pursuant to this Agreement. The Tools are not Deliverables.
- Service time estimates do not include the time for deployment defined in this section, because deployment is the Customer's responsibility.

Assessment

CrowdStrike will:

- Discover unmanaged systems, related to Falcon supported systems, and disk encryption status across the environment;
- Provide a real-time application inventory and provide context around what applications and versions are within the Customer's environment;
- Detect whether unpatched or vulnerable applications are being used, so you can patch them before an attacker can take advantage.

- Analyze user account data to determine administrator account usage;
- Analyze user password reset history;
- Execute Active Directory collection tools to determine hidden relationships user accounts and groups;

Location

CrowdStrike will perform work under this Phase 1 remotely.

Phase 2: Programmatic Review

CrowdStrike will evaluate the elements of Customer's cybersecurity program that support cyber risk management. Specifically, CrowdStrike will evaluate Customer's cybersecurity strategy, governance, risk, and compliance functions, identifying strengths and identifying opportunities for improvement across people, processes, and technologies.

CrowdStrike will review relevant internal cybersecurity documentation and then conduct workshops with individuals within the organization who understand how the Customer's existing cybersecurity program works in reality – regardless of what the documentation may say.

Scope of Assessment

CrowdStrike will focus its evaluation across two primary focus areas:

- Strategy and Governance
- Risk and Compliance

Location

CrowdStrike may perform Phase 2 remotely or, upon mutual agreement, on location at Customer's offices.

Status Meetings

CrowdStrike will provide Customer regular updates on the progress of the Services. Brief updates will be provided on a schedule as agreed between Customer and CrowdStrike.

Executive Briefing

Upon completion of both phases of this review, CrowdStrike will, if requested, prepare and present a briefing to Customer's leadership team. The briefing will focus on the findings of the Risk Management Review, and may include additional topics, as mutually agreed between CrowdStrike and Customer.

Engagement Artifacts

CrowdStrike will provide the following artifacts for this engagement:

- An executive summary that succinctly summarizes the primary observations, key strengths, and areas for improvement.
- A detailed report containing the full set of technical and programmatic findings and analysis.

Disclaimer

CrowdStrike is not providing legal or regulatory advice or services to Customer with respect to the Services contemplated herein, and nothing in this description of the Services, the Agreement, or otherwise creates an attorney-client relationship with respect to the same. So long as CrowdStrike performs the Services in compliance with the express warranties set forth in the applicable Section of the Agreement, CrowdStrike disclaims responsibility for costs in connection with disruptions of and/or damage to Customer's or a third party's information systems and the information and data contained therein, including, but not limited to, denial of access to a legitimate system user, automatic shut-down of information systems caused by intrusion detection software or hardware, or failure of the information system resulting from the provision of the Services.

CROWDSTRIKE

Technical Services

Technical Services

Compromise Assessment

The CrowdStrike Compromise Assessment is designed to identify current and past attacker activity in an organization's environment. CrowdStrike's team of threat hunters leverages the Falcon Platform, Network sensors, historical operating system artifacts, and cyber threat intelligence to monitor the environment and gather forensically important datapoints for compromise analysis.

Concept of Operations

Using CrowdStrike Tools and other technology, CrowdStrike will attempt to find evidence of the tactics, techniques and procedures commonly used by targeted attackers, and if such evidence is found, CrowdStrike looks for information that will help determine who the attackers are.

CrowdStrike will perform an assessment using data from the organization's hosts. CrowdStrike will provide the organization with a software package that gathers information from its endpoints (laptops, desktops and servers) running the Windows, MacOS, and Linux operating systems. CrowdStrike will help the organization's staff deploy the software package and collect information about its environment that may lead to evidence of additional attacker activity. CrowdStrike uses its CrowdStrike Tools including, without limitation, Falcon Platform, Falcon Forensics Collector, and/or Falcon Network Sensor technology for this analysis. The CrowdStrike Tools fee is set forth in the section entitled *CrowdStrike Tools.*

In addition to the automated artifact detection, CrowdStrike will perform data collection, investigation and hunting. This data investigation will be performed off site, using CrowdStrike's big data collection and analysis capabilities.

Potential Engagement Artifacts

CrowdStrike may provide the following artifacts for this engagement:

- A final report with executive summary, technical details of significant findings, and summary recommendations;
- A technical datasheet including all findings related to our assessment;
- If CrowdStrike identifies targeted attack groups, selected information from CrowdStrike's intelligence library about the attack groups' goals, motivations, capabilities and historical actions; and
- If CrowdStrike identifies attacker activity, CrowdStrike's estimate of the level of effort it would take to eject the attacker and regain control of an organization's environment.

Technical Risk Assessment

The CrowdStrike Technical Risk Assessment is designed to help gain real-time visibility into who and what is in the organization's network. The CrowdStrike Technical Risk Assessment team leverages the Falcon Platform to understand how systems and accounts are being used. This engagement supports Windows Active Directory environments only.

Concept of Operations

CrowdStrike will perform an assessment using data from the organization's hosts. CrowdStrike will provide the Customer with a software package (CrowdStrike Falcon sensor) that gathers information from the end systems (laptops, desktops and servers) running the Windows, Linux and Mac OS operating systems. CrowdStrike will help Customer's staff deploy the software package and collect information about the Customer's environment that may lead to evidence of additional attacker activity. CrowdStrike uses its CrowdStrike Falcon Platform software (in detect only mode) for this analysis.

Account Activity - Account monitoring provides visibility into the use of administrator credentials and password resets across the enterprise.

Vulnerability Summary - Review vulnerability information to identify critical Application and Windows vulnerabilities that exist in the environment.

Device Summary - The system inventory allows the Customer to find and remediate unmanaged systems and also address systems that could be a risk on the organization's network, such as unprotected BYOD or third-party systems.

Application Activity - Detect whether unpatched or vulnerable applications are being used, so the Customer can patch them before an attacker can take advantage.

Active Directory – Discover hidden attack paths for getting access to Users, Computers and Domain Administrator/Controllers in an Active Directory.

Disclaimer

So long as CrowdStrike performs the Services in compliance with the warranties set forth in the Agreement, CrowdStrike disclaims responsibility for costs in connection with disruptions of and/or damage to Customer's or a third party's information systems and the information and data contained therein, including, but not limited to, denial of access to a legitimate system user, automatic shut-down of information systems caused by intrusion detection software or hardware, or failure of the information system resulting from the provision of the Services.

Cyber Threat Risk Evaluation

CrowdStrike will assist Customer with evaluating security controls related to cyber insurability based on common cyber insurance underwriting evaluation criteria. This engagement supports Microsoft Active Directory environments only and requires the CrowdStrike Falcon Platform to be enabled throughout Customer's environment.

CrowdStrike will:

- Provide to Customer for use during the engagement the CrowdStrike Falcon Platform, unless Customer is already permitted to use the CrowdStrike Falcon Platform under a different agreement;
- Provide limited deployment support, including up to two 30-minute troubleshooting discussions via telephone and additional support via email;

Customer will:

- Deploy CrowdStrike Falcon Platform in Customer's environment;
- Work with CrowdStrike to configure the Falcon Platform to the necessary specifications;
- Provide CrowdStrike network and location information related to:
  - Backup Solutions
  - Server and Workstation Logs
- Provide CrowdStrike the following related documentation:
  - List of Email Security Products
  - List of Web Security Technologies
  - Cybersecurity Incident Response Plan
  - Cybersecurity Employee Awareness Training Plan
  - Digital Supply Chain Risk Mitigation Plan

The CrowdStrike Tools are licensed to Customer as-is for internal evaluation use only and not sold, and no title or ownership to the CrowdStrike Tools or the intellectual property embodied therein passes as a result of this Agreement or any act pursuant to this Agreement. The Tools are not Deliverables.

Service time estimates do not include the time for deployment defined in this section, because deployment is the Customer's responsibility.

Assessment

For the following assessment areas, CrowdStrike will:

- Multi-Factor and Remote Access – Review methods used to regulate who or what can authenticate or use resources within an environment.
- Endpoint Detection and Response – Review presence of advanced endpoint security solutions and alert information related to malicious activity within the environment.

- Backup – Review backup strategy documentation and testing process.
- Privileged Access Management – Review possible attack paths related to privileged users, groups, systems, and domain trusts.
- Review provided documentation related to Email Filtering and Web Security
- Vulnerability Management – Discover vulnerabilities within the environment based on data with Falcon Spotlight.
- Cybersecurity Incident Response Plan – Review incident response plan documentation and testing process.
- Cybersecurity Employee Awareness Training – Review employee security awareness training documentation and testing process.
- System Hardening Review – Review Windows, Mac, and Linux security settings as it relates to endpoint hardening.
- Logging and Monitoring – Review logging implementation within the environment.
- End-of-Life Software – Discover end-of-life software usage within the environment.
- Review provided documentation related to Supply Chain Risk Management

Reporting

CrowdStrike will construct and deliver draft and final reports containing findings and observations.

- Executive Summary - a high-level overview of the security posture;
- Key Findings Overview;
- Assessment Findings Summary and Detail; and
- Recommendations – specific actions or considerations to address documented issues.

Disclaimer

So long as CrowdStrike performs the Services in compliance with the warranties set forth in the Section entitled Warranties and Remedies in the Agreement, CrowdStrike disclaims responsibility for costs in connection with disruptions of and/or damage to Customer's or a third party's information systems and the information and data contained therein, including, but not limited to, denial of access to a legitimate system user, automatic shut-down of information systems caused by intrusion detection software or hardware, or failure of the information system resulting from the provision of the Services.

Cloud Security Assessment

CrowdStrike's Cloud Security Assessment combines cloud service plane configuration review, documentation review and interviews to help customers prepare to prevent, detect, and rapidly recover from targeted attacks in their cloud environments.

This assessment supports AWS, Azure infrastructure, Office 365, and/or Google Cloud (GCP) environments.

Concept of Operations

During a Cloud Security Assessment, CrowdStrike assesses the organization's cloud infrastructure for security capabilities and weaknesses in preventing, detecting, and recovering from targeted attacks. CrowdStrike will meet with key stakeholders, review cloud security documentation and perform an in-depth review of the configuration settings of accounts (AWS), subscriptions and tenants (Azure), or projects (GCP) to determine if the design, implementation and operation of the organization's cloud infrastructure are capable of defending against targeted attack.

Potential Engagement Artifacts

CrowdStrike may provide the following artifact for this engagement:

- Final report documenting findings related cloud security weaknesses, along with associated recommendations organized by criticality and impact.

Disclaimer

So long as CrowdStrike performs the Services in compliance with the warranties set forth in the Agreement, CrowdStrike disclaims responsibility for costs in connection with disruptions of and/or damage to Customer's or a third party's information systems and the information and data contained therein, including, but not limited to, denial of access to a legitimate system user, automatic shut-down of information systems caused by intrusion detection software or hardware, or failure of the information system resulting from the provision of the Services.

Cloud Compromise Assessment

CrowdStrike will assist Customer with identifying evidence of targeted compromise activity at the control plane of Customer's cloud environment. This engagement type is supported for the customer's choice of (i) Amazon Web Services (AWS); (ii) Microsoft Azure AD & Office 365; (iii) Microsoft Azure platform, or (iv) Google Cloud Platform (GCP) cloud infrastructure.

Concept of Operations

During a Cloud Compromise Assessment, CrowdStrike collects configuration and log information from the cloud service plane using CrowdStrike Tools, Falcon Horizon and a proprietary toolset called the CrowdStrike Cloud Collectors. This information is analyzed by CrowdStrike analysts to identify and explore any evidence of access or configuration changes consistent with targeted unauthorized activity. Additionally, CrowdStrike reviews the active configuration for any critical cloud security configuration findings in need of urgent remediation, and promptly shares any urgent findings with the customer to permit rapid resolution.

CrowdStrike uses its CrowdStrike Tools including, without limitation, the CrowdStrike Falcon platform, Falcon Horizon, and/or CrowdStrike Cloud Collectors for this analysis. The CrowdStrike Tools fee is set forth in the section entitled CrowdStrike Tools.

Customer access to Falcon Horizon during the course of the engagement is included, to permit detection of any known Indicators of Attack (IOAs) during the analysis.

Potential Engagement Artifacts

CrowdStrike may provide the following artifacts for this engagement:

- Debrief deck identifying key findings related to evidence of targeted compromise activity and any critical cloud security configuration findings
- Report containing findings and observations, information summarizing the Services for an executive reader, and technical information for a technical reader.

Disclaimer

So long as CrowdStrike performs the Services in compliance with the warranties set forth in the Agreement, CrowdStrike disclaims responsibility for costs in connection with disruptions of and/or damage to Customer's or a third party's information systems and the information and data contained therein, including, but not limited to, denial of access to a legitimate system user, automatic shut-down of information systems caused by intrusion detection software or hardware, or failure of the information system resulting from the provision of the Services.

Identity Security Assessment

The CrowdStrike Identity Security Assessment is designed to provide insight into your organization's Active Directory attack surface. CrowdStrike leverages the Falcon Identity Threat Detection module and custom tools to understand excessive or stealthy permissions, common misconfigurations, weak passwords, attack paths, and settings which present the most risk. This engagement supports Microsoft Windows Active Directory environments only.

CrowdStrike Tools

CrowdStrike will help Customer deploy certain CrowdStrike software and hardware tools in Customer's environment as described below (the "CrowdStrike Tools").

- CrowdStrike will:
  - Provide to Customer for use during the engagement the CrowdStrike Tools, unless Customer is already permitted to use CrowdStrike Tools under an existing license agreement.; and
  - Provide limited CrowdStrike Tools deployment support, including up to two 30-minute troubleshooting discussions via telephone and additional support via email.
- Customer will:
  - Deploy CrowdStrike Tools in Customer's environment;
  - Work with CrowdStrike to configure the CrowdStrike Tools to the necessary specifications; and
  - Approve CrowdStrike use of real time response ("RTR") functionality within the Falcon platform.
- The CrowdStrike Tools are licensed to Customer as-is for internal evaluation use only and not sold, and no title or ownership to the CrowdStrike Tools or the intellectual property embodied therein passes as a result of this SOW or any act pursuant to this SOW. The CrowdStrike Tools are not Deliverables.
- Deployment of CrowdStrike Tools is a Customer responsibility and is not included in the Service time.

Services Description - Assessment

CrowdStrike will:

- Run Falcon Identity Threat Detection which is intended to discover unmanaged systems, related to Falcon supported systems;
- Analyze Customer user account data to determine administrator account usage;
- Analyze Customer domain user password reset history;
- Execute Active Directory collection tools to determine hidden relationships between Customer user accounts and groups, and attack paths likely to be utilized during an attack;
- Identify domain accounts with weak or exposed passwords, risky configurations, stealthy privileges, and anomalous activity; and

- Identify domain groups which grant or are granted excessive privileges.

Reporting

CrowdStrike will construct and deliver draft and final reports containing findings and observations as follows:

- Executive Summary;
- Key Findings Overview;
- Assessment Findings Summary and Detail; and
- Recommendations.

Location

All CrowdStrike services will be performed remotely.

Status Reporting

During the engagement CrowdStrike will:

- Provide written weekly summary updates which includes task status issues and progress, and overall status of work and budget.

Engagement Artifacts

CrowdStrike may, as requested, construct and present draft and final reports containing findings and observations. A report is initially delivered in a draft format and reviewed with Customer. The draft report is then revised and delivered as a final report within ten business days unless Customer has requested further revisions or questions. CrowdStrike will conduct discussion and status meetings as defined above. The written engagement artifacts (report) may contain information summarizing the Services for an executive reader, as well as detailed technical information for a technical reader.

CROWDSTRIKE

CrowdStrike Falcon® Platform Services

CrowdStrike Falcon® Platform Services

CrowdStrike Falcon® Platform Operational Support Services

Operational Support from CrowdStrike and Certified Partners helps organizations implement the CrowdStrike Falcon® platform.

Concept of Operations

A CrowdStrike Falcon ® Platform Operational Support services engagement provides for expert advice on the installation and configuration of the organization's CrowdStrike Falcon platform as follows:

- Aligns your deployment and configuration of the Falcon platform with your environment for faster and broader coverage of your endpoints
- Provides custom playbooks for each of the deployment technologies allowing Falcon customer a more rapid deployment of Falcon
- Implements the Falcon platform according to CrowdStrike best practices
- Transfers knowledge of CrowdStrike Falcon configuration best practices
- Tunes your Falcon alerts to assist with lower false-positive rates by configuring whitelisting

Disclaimer

So long as CrowdStrike performs the Services in compliance with the warranties set forth in the Agreement, CrowdStrike disclaims responsibility for costs in connection with disruptions of and/or damage to Customer's or a third party's information systems and the information and data contained therein, including, but not limited to, denial of access to a legitimate system user, automatic shut-down of information systems caused by intrusion detection software or hardware, or failure of the information system resulting from the provision of the Services.

CrowdStrike Falcon® Platform Health Check

The CrowdStrike Health Check is designed to help maximize the value out of the Falcon platform. The intent is to provide the status of the current configuration of the Falcon platform and provide recommendations based on CrowdStrike Falcon best practices.

Concept of Operations

CrowdStrike will perform an assessment reviewing the configurations of the Customer's implementation of the Falcon Platform. Additionally, CrowdStrike will provide recommendations on configuration changes and sensor upgrades are made to improve their overall security posture.

Deployment - Summarize the systems Falcon is deployed to and other areas around initial and continuous deployment of Falcon.

Detections - Summarize the detections of malicious activity throughout the environment where the Falcon Platform has visibility.

Policy/Configurations – Summarize how policies and groups are configured in the Falcon Platform UI.

Whitelisting - Identify whitelist issues and requests.

Falcon UI Users - Summarize user roles within the Falcon Platform UI.

Potential Engagement Artifacts

CrowdStrike may provide the following artifact for this engagement:

- A report of findings that summarize current Falcon configurations and recommendations.

Disclaimer

So long as CrowdStrike performs the Services in compliance with the warranties set forth in the Agreement, CrowdStrike disclaims responsibility for costs in connection with disruptions of and/or damage to Customer's or a third party's information systems and the information and data contained therein, including, but not limited to, denial of access to a legitimate system user, automatic shut-down of information systems caused by intrusion detection software or hardware, or failure of the information system resulting from the provision of the Services.

CrowdStrike Falcon® Identity Protection Support

Falcon Identity Protection Support from CrowdStrike and Certified Partners helps organizations implement and configure the CrowdStrike Falcon® Identity Protection module.

Concept of Operations

CrowdStrike Falcon® Identity Protection Support services engagement provides expert advice on the configuration of CrowdStrike Identity Protection solution as follows:

- Operationalize the CrowdStrike Falcon Identity Protection (IDP) solutions: Falcon Identity Threat Detection (non-Prevent) and Falcon Zero Trust (Prevention).
- Integrate the Falcon Identity Protection platform with on-premise and cloud-based identity and access management solutions.
- Conduct post implementation threat hunting activities and policy enhancements
- Transfers knowledge of CrowdStrike best practices related to the Falcon Identity Protection module;

Disclaimer

So long as CrowdStrike performs the Services in compliance with the warranties set forth in the Agreement, CrowdStrike disclaims responsibility for costs in connection with disruptions of and/or damage to Customer's or a third party's information systems and the information and data contained therein, including, but not limited to, denial of access to a legitimate system user, automatic shut-down of information systems caused by intrusion detection software or hardware, or failure of the information system resulting from the provision of the Services.

CrowdStrike Falcon® LogScale Operational Support Service

The CrowdStrike Falcon LogScale Operational Support Service engagement provides customized advice on Customer's configuration of the CrowdStrike Falcon LogScale platform. Key benefits of this engagement may include one or more of the following, based on Customer's individual business needs:

- Defines Customer's desired business outcomes and prioritized use-cases for Falcon LogScale
- Provides assistance architecting the Falcon LogScale platform according to best practices
- Aligns Customer's configuration of the Falcon LogScale platform to prioritized use-cases

Key Service Activities

- Conduct a remote kick-off call to review Customer's project timeline and identify key stakeholders
- Assess Customer's readiness for Falcon LogScale Operational Support services
- Assist with Falcon LogScale planning and install, data onboarding, content customization and knowledge transfer

Planning & Installation

CrowdStrike will review Customer's infrastructure and critical use cases. CrowdStrike may then provide guidance on architectural best practices and use case configuration sequence planning. CrowdStrike may review the project scope and determine resource scheduling. To assist with installation of Falcon LogScale, CrowdStrike may advise on configurations like:

- Authentication
- Environment variables2
- IP filter2
- JVM configuration2
- Kafka configuration2
- TLS2

Additionally, CrowdStrike may assist with optional platform integrations during the installation process such as:

- Email configuration

---

[2] Applicable to self-hosted Falcon LogScale environments only

- HTTP Proxy Setup[2]

Customer responsibilities include providing a single owner of technical decisions, providing a single owner of business decisions, providing a single owner of project management and change management, reviewing the Falcon LogScale installation documentation, completing the preparation for installing Falcon LogScale tasks, reviewing configuration settings documentation, and completing Falcon LogScale training available via CrowdStrike University.

Data Onboarding

During the course of the engagement, CrowdStrike may assist with onboarding log data into the Falcon LogScale platform, creating and/or modifying parsers to match ingested data sources, and providing advisory support on logging best practices. Customer responsibilities include ingesting data documentation, preparing Data Sources for transport to Falcon LogScale environment, and reviewing Parser documentation.

Content Customization

CrowdStrike may assist with customization of dashboards, dashboard properties, dashboard parameters and widgets. CrowdStrike may also create and configure alerts, actions, and scheduled searches to support dashboards and use case configurations. Customer responsibilities include reviewing Dashboard documentation and reviewing Automation and Alerts documentation.

Knowledge Transfer & Project Closeout

CrowdStrike may conduct a review of work performed during the course of the engagement to include sharing relevant documentation and conducting knowledge transfer discussions on topics such as:

- Falcon LogScale UI
- Account management
- Data ingestion
- Repositories
- Parsers
- Dashboards
- Automation and alerts
- Packages
- Administration
- Security and authentication
- Cluster management1

Customer responsibilities include designating a recipient of knowledge transfer and stakeholders to attend project review session.

Assumptions

- Customer will provide a single point of contact who will serve as the primary interface with the CrowdStrike Falcon LogScale Services Team.
- CrowdStrike will only service the CrowdStrike Falcon LogScale platform. CrowdStrike will not directly interact with or configure any other client or other source information systems.
- CrowdStrike may require browser-based virtual remote access solutions such as Virtual Desktop (VDI), remote support meeting software, VPN or other access in order to assist with configuring Falcon LogScale. CrowdStrike will not utilize physical devices from Customer such as Customer-issued laptops and/or multi-factor tokens (MFA) for remote access.
- All communication between the Customer and CrowdStrike, verbal and written, will be in English.
- CrowdStrike resources will not be responsible for updating Customer project tracking tools and systems.
- If transitioning content from other log management, SIEM or other security tools, CrowdStrike will configure platform integrations and content (e.g., parsers, dashboards, and alerts) within the existing, supported functionality of Falcon LogScale platform. CrowdStrike will not develop new features or functionality for the core Falcon LogScale platform as part of this engagement.
- Custom scripting and building integrations are NOT covered under this service, but may be included within a separate detailed Statement of Work.
- Instructor led training courses via CrowdStrike University are not included in this engagement, but may be purchased separately.
- Services not specifically described in this document will require customized scoping and the use of a separate Statement of Work.
- For onsite support, travel will be conducted on Monday and Friday of the work week. Night and weekend support are not included.
- Non-project activities requested by the Customer including, but not limited to, onboarding training to obtain network access must be approved by CrowdStrike management and time spent on these activities will be debited from your engagements.
- Any customization of configurations, content, and platform integrations, including third party log shipper configurations, parsers, dashboards, alerts and automation, does not extend the standard support agreement.

Location

CrowdStrike will perform work under this task remotely or at the Customer’s site, as mutually agreed between CrowdStrike and Customer.

Status Reporting

CrowdStrike may:

- As requested, provide daily status updates verbally or by email, including information about activities performed, findings and their criticality, and plans for upcoming work;
- Provide written weekly summary updates, reviewing tasks, issues and progress, and advising of the status of work and the budget;

CROWDSTRIKE

Red Team Services

Red Team Services

General Penetration Testing Notice

The following General Penetration Testing Notice shall apply to all Red Team Services, including, but not limited to, the Adversary Emulation Exercise, Persistent Adversary Emulation Exercise, Red Team/Blue Team Exercise, Internal Red Team Exercise, External Network Penetration Testing, Social Engineering Assessment, Web Application Penetration Testing, Wireless Penetration Testing, Cloud Red Team/Blue Team Exercise, System Hardening Penetration Testing, Mobile Web Application Penetration Testing, Network Segmentation Testing, and Penetration Testing Retest.

Reconnaissance and Access

Customer authorizes CrowdStrike to use offensive software and tactics to attempt access to Customer's network. CrowdStrike access may include access to information stored on permanent or removable media; information obtained from computer memory; data that is in transit, including but not limited to audio/video teleconferencing communications; and, information obtained through social interaction with employees (for example, by email, phone, or in-person). Information access may include access to digital data, audio files, documents, photographs, or other forms of information.

Privilege Enumeration and Lateral Movement

CrowdStrike may use common system administration and attacker software to research and enumerate the privileges available. CrowdStrike may attempt to secure access to other networked computing systems located within the Customer's network.

Privilege Escalation and Passwords

If CrowdStrike determines that network access privileges in excess of those available are necessary to achieve engagement objectives, CrowdStrike may attempt to escalate those privileges beyond those that were initially provided. CrowdStrike may attempt to extract passwords and credentials in various forms to include, but not limited to; memory extraction, password cracking, network monitoring, and keystroke logging. During the delivery of the Services, CrowdStrike may use credentials identified by CrowdStrike Falcon Intelligence Recon (or successor product) in the open, deep, and dark web for the purpose of authenticating to the Customer network.

Data Access and Copying

If necessary, CrowdStrike may attempt to access and copy the target data and information from one or more of Customer's systems. If CrowdStrike has to access data in order to accomplish engagement objectives, CrowdStrike will not share the data outside of CrowdStrike engagement infrastructure, unless mutually agreed upon by Customer and CrowdStrike.

Shortcuts

If CrowdStrike determines that it is likely the effort estimates will be inaccurate due to Customer's technical environment, or other factors outside CrowdStrike's control, CrowdStrike will advise Principal Customer Technical Contact and will request he or she decide whether CrowdStrike shall continue in excess of the effort estimate, or whether Customer shall provide the information CrowdStrike seeks. CrowdStrike will recommend, and Customer will decide on the course of action. Shortcuts taken will be documented in engagement Deliverables.

Additional Authorizations

The Principal Customer Technical Contact, or other customer designee(s), will be available as needed during the engagement to authorize CrowdStrike in writing or email to proceed, or not to proceed, regarding any aspect of the engagement.

Out of Scope

The following activities will not be performed by CrowdStrike unless specific documentation is presented.

- Intentional Denial of Service
- Hardware Reverse Engineering

Remaining Artifacts

CrowdStrike will attempt to remove applications or services it installed during the Services. However, situations may occur where CrowdStrike is unable to fully remove all applications installed during testing. CrowdStrike will provide the Customer specific details regarding filenames and systems of the remaining applications.

Deliverables

CrowdStrike will construct and deliver draft and final reports containing findings and observations. Reports are initially delivered in a draft format and then discussed with Customer. The draft reports are then revised and delivered as final reports if Customer requests. The written deliverables will contain information summarizing the Services for an executive reader, as well as detailed technical information for a technology reader.

Identification of Compromise

Identification of compromise is not part of normal penetration testing activities. However, if CrowdStrike discovers indicators of compromise during penetration testing activities CrowdStrike will halt all penetration testing activities in the Customer's in-scope environment.

Disclaimer

So long as CrowdStrike performs the Services in compliance with the express warranties set forth in the applicable Section of the Agreement, CrowdStrike disclaims responsibility for costs in connection with disruptions of and/or damage to Customer's or a third party's information systems and the information and data contained therein, including, but not limited to, denial of access to a legitimate system user, automatic shut-down of information systems caused by intrusion detection software or hardware, or failure of the information system resulting from the provision of the Services.

Adversary Emulation Exercise

CrowdStrike will demonstrate how an attacker targeting the Customer might compromise Customer's computing environment. CrowdStrike will emulate the tactics, techniques, and procedures of an attacker.

This engagement may involve social engineering activities to assess the Customer's security posture. Activities may include, but not limited to, registering similar domains and resources, as well as impersonating customer employees, brands, and services.

The General Penetration Testing Notice applies to this service.

Customer Activities

The Customer will conduct the following activities:

- Designate point(s) of contact to attend kickoff meetings and status updates
- If CrowdStrike is unable to obtain access to Customer's environment through social engineering or compromise of Internet-facing services, Customer will provision CrowdStrike access to their internal network to facilitate execution of a malicious link or software to simulate an assumed breach scenario. Network access can be provisioned through:
    - Virtual Private Network ("VPN") and remote desktop access**,** Virtual Desktop Infrastructure ("VDI") access**,** or an alternative access method that is mutually agreed upon
    - If remote access is not possible, Customer will provide CrowdStrike with a point of contact that will perform the execution of a malicious link or software
    - The provisioned user and system should be representative of a standard user within the Customer's organization, or an alternative non-standard user and system mutually agreed upon by Customer and CrowdStrike

CrowdStrike Testing Activities

CrowdStrike will conduct the following activities:

- Conduct remote operations aligned with engagement objectives
- Perform information gathering to discover external/publicly facing networks and resources (domain names, IP addresses, and, if possible, hostnames)
- Perform open source research in an attempt to discover exposed credentials or sensitive information related to the Customer's external resources and employees
- Perform at least one targeted social engineering campaign to attempt to obtain initial access
    - In the event that CrowdStrike is not successful with social engineering activities CrowdStrike and the Customer will mutually agree on an alternative method of access to include assisted link execution or assisted software execution

- Customer can forgo the social engineering exercise if they would prefer to start the exercise by an alternate method of access such as the execution of a malicious link or software

- Enumerate the local system and network for sensitive data
- Perform privilege escalation activities
- Access areas of the network that contain sensitive data
- As applicable, analyze, and document its findings and recommendations to be documented in Deliverables

Testing Location

CrowdStrike will perform work under this task remotely.

Status Meetings

CrowdStrike will provide Customer weekly summary status reports, or as otherwise mutually agreed.

Deliverables

CrowdStrike will:

- Document and deliver an Adversary Emulation Exercise Report consisting of the following sections:
    - Executive Summary
    - Key Findings Overview
    - Testing Activities and Associated Observations
    - Recommendations – specific actions or considerations to address findings identified
- CrowdStrike will deliver one copy of the Adversary Emulation Exercise Report to Customer Principal Technical Contact within ten business days following completion of the “Adversary Emulation Exercise” activity, or as otherwise mutually agreed. Customer will have ten days to review and provide feedback on the draft report. If Customer has not provided feedback or comments within ten days after delivery, CrowdStrike will finalize the report.

Optional Debrief

CrowdStrike will hold one remote debrief meeting with the Customer to review findings of the draft report, if requested by Customer.

Persistent Adversary Emulation Exercise

CrowdStrike will demonstrate how a targeted persistent cyber attacker might compromise Customer's computing environment over an extended period as defined below in the General Timeline section. CrowdStrike will emulate the tactics, techniques, and procedures of a persistent cyber attacker in order to accomplish exercise objectives agreed upon between Customer and CrowdStrike.

This engagement may involve social engineering activities to assess the Customer's security posture. Activities may include, but not limited to, registering similar domains and resources, as well as impersonating customer employees, brands, and services.

The General Penetration Testing Notice applies to this service.

Customer Activities

The Customer will conduct the following activities:

- Designate point(s) of contact to attend kickoff meetings and status updates
- If CrowdStrike is unable to obtain access to Customer's environment through social engineering or compromise of Internet-facing services, Customer will provision CrowdStrike access to their internal network to facilitate execution of a malicious link or software to simulate an assumed breach scenario. Network access can be provisioned through:
    - Virtual Private Network ("VPN") and remote desktop access**,** Virtual Desktop Infrastructure ("VDI") access**,** or an alternative access method that is mutually agreed upon
    - If remote access is not possible, Customer will provide CrowdStrike with a point of contact that will perform the execution of a malicious link or software
    - The provisioned user and system should be representative of a standard user within the Customer's organization, or an alternative non-standard user and system mutually agreed upon by Customer and CrowdStrike

CrowdStrike Exercise Activities

CrowdStrike shall, as needed:

- Research adversaries that are likely to attack Customer's network to determine appropriate simulation objectives
- Conduct remote operations aligned with engagement objectives
- Conduct information gathering activities to discover external/publicly facing networks and resources (domain names, IP addresses, and, if possible, hostnames)
- Perform open-source research in an attempt to discover exposed credentials or sensitive information related to the Customer's external resources and employees.
- Perform at least one targeted social engineering campaign in an attempt obtain initial access;
    - In the event that CrowdStrike is not successful with phishing activities or external reconnaissance, CrowdStrike and the Customer will mutually agree on an

alternative method of access to include provisioned account access, assisted link execution, or assisted software execution.

- Enumerate the local system and network for sensitive data;
- Perform privilege escalation activities;
- Attempt to access additional systems and services on the network in order to accomplish exercise objectives;
- And as applicable, analyze, and document findings and recommendations to be included in the project deliverables.

General Timeline

This engagement will occur over a mutually agreed upon duration over the course of Customer's current or subsequent Retainer Terms, typically 4-11 months.

- **Phase 0 (Kickoff Call & Setup)**

CrowdStrike will conduct a kick-off meeting to confirm understanding of the Customer's objectives and explain its approach to meet the Customer's goals for the engagement.

- **Phase 1 (Reconnaissance and Initial Access)**

CrowdStrike will conduct open-source research to collect information about Customer network to identify possible initial access vectors. CrowdStrike will conduct initial targeting activities such as but not limited to social engineering activities and external service exploitation. If access has not been obtained CrowdStrike and the Customer will mutually agree on an alternative method of access to facilitate an assumed breach scenario.

- **Phase 2 (Active Operations)**

CrowdStrike will conduct adversary emulation type activities in an effort to gain and maintain access into the Customer's network and achieve exercise objectives. CrowdStrike will hold monthly status update meetings to track the progress of the exercise.

- **Phase 3 (Reporting and Debrief)**

CrowdStrike will create a report that documents findings and recommendations of the exercise as defined further in Deliverables. CrowdStrike will hold one debrief meetings to review exercise activities and findings.

Testing Location

CrowdStrike will perform work under this task remotely.

Status Meetings

CrowdStrike will provide Customer monthly status reports, or as otherwise mutually agreed.

Deliverables

CrowdStrike will:

- Document and deliver a Persistent Adversary Emulation Exercise Report consisting of the following sections:
    - Executive Summary;
    - Key Findings Overview;
    - Testing Activities and Associated Observations;
    - Recommendation – specific actions or considerations to address findings identified
- CrowdStrike will deliver Persistent Adversary Emulation Report in draft form to Customer within ten business days following completion of the “Persistent Adversary Emulation Exercise” activity, or as otherwise mutually agreed. Customer will have ten days to review and provide feedback on the draft report. If Customer has not provided feedback or comments within ten days after delivery, CrowdStrike will finalize the report.

Optional Debrief

CrowdStrike will hold one remote debrief meeting with the Customer to review findings of the draft report, if requested by Customer.

Red Team / Blue Team Exercise

The purpose of this activity is to identify gaps in the Customer's security posture when detecting and responding to a target attack. CrowdStrike will operate in a step-by-step manner following common attacker techniques, pausing after each phase of the attack to conduct simulated incident triage and response with the Customer's security team.

The General Penetration Testing Notice applies to this service.

Customer Activities

The Customer will perform the following activities:

- Designate point(s) of contact to attend kickoff meetings and status updates
- Provision CrowdStrike access to their internal network to facilitate execution of a malicious or assisted to simulate an assumed breach scenario. Network access can be provisioned through:
    - Virtual Private Network ("VPN") and remote desktop access**,** Virtual Desktop Infrastructure ("VDI") access**,** or an alternative access method that is mutually agreed upon
    - If remote access is not possible, Customer will provide CrowdStrike with a point of contact that will perform the execution of a malicious link or software
    - The provisioned user and system should be representative of a standard user within the Customer's organization, or an alternative non-standard user and system mutually agreed upon by Customer and CrowdStrike. The user and system must be provisioned ahead of the agreed upon testing start date.
- Provide CrowdStrike with authorized access to Customer security tools to facilitate review of security data and processes

CrowdStrike Red Team Activities

CrowdStrike Red Team will conduct the following activities:

- Perform remote operations aligned with engagement objectives
- Enumerate the local system and network for sensitive data
- Perform privilege escalation activities
- Access areas of the network that contain sensitive data

CrowdStrike Blue Team Activities

CrowdStrike will conduct the following activities:

- Provide at least one consultant to support engagement activities at the Customer's location
- Coordinate communications with Customer security team
- Support CrowdStrike Red Team attack activities

- Assist Customer through the triage and discovery process to identify Red Team activities
- Discuss defensive processes and countermeasures
- Identify gaps in the Customer's detection process (including technology, people, and processes)

CrowdStrike General Activities

CrowdStrike will conduct the following activities:

- Conduct daily meetings to review Red Team and Blue Team activities
- As applicable, analyze and document findings and provide recommendations to be included in Deliverables

Testing Location

CrowdStrike will perform work under this task remotely.

CrowdStrike may travel to the Customer's site, if mutually agreed between CrowdStrike and Customer.

Status Meetings

CrowdStrike will provide Customer weekly summary status reports, or as otherwise mutually agreed.

Deliverables

CrowdStrike will:

- Document and deliver a Red Team/ Blue Team Report consisting of the following sections:
    - Executive Summary - a high-level overview of the security posture;
    - Key Findings Overview;
    - Assessment Findings Summary and Detail; and
    - Recommendations – specific actions or considerations to address documented issues.
- CrowdStrike will deliver one copy of the Red Team/ Blue Team Final Report to Principal Customer Technical Contact within ten business days following completion of the "Red Team/ Blue Team" activity, or as otherwise mutually agreed. Customer will have ten days to review and provide feedback on the draft report. If Customer has not provided feedback or comments within ten days after delivery, CrowdStrike will finalize the report.

Internal Red Team Exercise

CrowdStrike will demonstrate how an attacker might operate within the Customer's network once a successful initial attack vector is achieved. CrowdStrike will conduct an Internal Red Team Exercise using a threat actor methodology.

The General Penetration Testing Notice applies to this service.

Customer Activities

The Customer will conduct the following activities:

- Designate point(s) of contact to attend kickoff meetings and status updates
- Provision CrowdStrike access to their internal network to facilitate the execution of a malicious link or software to simulate an assumed breach scenario. Network access can be provisioned through:
    - Virtual Private Network ("VPN") and remote desktop access**,** Virtual Desktop Infrastructure ("VDI") access**,** or an alternative access method that is mutually agreed upon
    - If remote access is not possible, Customer will provide CrowdStrike with a point of contact that will perform the execution of a malicious link or software
    - The provisioned user and system should be representative of a standard user within the Customer's organization, or an alternative non-standard user and system mutually agreed upon by Customer and CrowdStrike. The user and system must be provisioned ahead of the agreed upon testing start date.

CrowdStrike Testing Activities

CrowdStrike will conduct the following activities:

- Conduct remote operations aligned with engagement objectives
- Use common system administration and attacker tools to enumerate the local system and network
- Perform privilege escalation activities
- Attempt to access additional systems on the network
- As applicable, analyze, and document its findings and recommendations to be documented in Deliverables

Testing Location

CrowdStrike will perform work under this task remotely.

Status Meetings

CrowdStrike will provide Customer weekly summary status reports, or as otherwise mutually agreed.

Deliverables

CrowdStrike will:

- Document and deliver an Internal Red Team Exercise Report consisting of the following sections:
    - Executive Summary - a high-level overview of the security posture;
    - Key Findings Overview;
    - Assessment Findings Summary and Detail; and
    - Recommendations – specific actions or considerations to address documented issues.
- CrowdStrike will deliver one copy of the Internal Red Team Exercise Final Report to Customer's Principal Customer Technical Contact within ten business days following completion of the "Internal Red Team Exercise" activity, or as otherwise mutually agreed. Customer will have ten days to review and provide feedback on the draft report. If Customer has not provided feedback or comments within ten days after delivery, CrowdStrike will finalize the report.

Optional Debrief

CrowdStrike will hold one remote debrief meeting with the Customer to review findings of the draft report, if requested by Customer.

External Network Penetration Testing

CrowdStrike will identify the Customer's publicly available resources, attempt to discover vulnerabilities and insecure resources, and attempt to gain unauthorized access to the Customer's publicly available resources.

The General Penetration Testing Notice applies to this service.

CrowdStrike may use subcontractors in its provision of the Service. To the extent that such use of a subcontractor conflicts with the terms of the Agreement, Customer may be required to consent in writing to receive this Service.

Customer Activities

Customer will conduct the following activities:

- Customer will designate point(s) of contact to attend kickoff meetings and status updates
- Provide in-scope IP addresses, domain names, and any other relevant target information
- If, during Information Gathering Activities, CrowdStrike provides Customer a list of additional IP addresses and domain names not initially included in-scope, Customer will review the list to identify out-of-scope IP addresses

CrowdStrike Testing Activities

CrowdStrike will conduct the following activities:

- Perform information gathering activities to discover all external/publicly facing networks and resources (domain names and IP addresses)
- Perform open source research in an attempt to discover exposed credentials or sensitive information related to the Customer's resources
- Discover publicly available services, applications, and other technologies
- Perform automated and manual vulnerability discovery activities related to publicly available resources
- Attempt to exploit design and infrastructure weaknesses related to publicly available resources to gain access to or obtain code execution on systems
- Web applications: CrowdStrike will conduct an unauthenticated triage assessment of Internet facing web applications vulnerabilities. This triage will focus on common and critical web server vulnerabilities accessible as an unauthenticated external user.
- IP Addresses: CrowdStrike will attempt to exploit vulnerabilities at the host and service level that are exposed to the Internet

Assumptions

- CrowdStrike will not attempt lateral movement. Activities under External Network Penetration Testing will stop at demonstrating code execution or remote command line access, if possible.

Out of Scope

- Authenticated web application penetration testing is out of scope for External Network Penetration Testing activities.
- Social engineering testing is out of scope for External Network Penetration Testing activities.
- Testing that may cause denial of service is out of scope for External Network Penetration Testing activities.

Testing Location

CrowdStrike will perform work under this task remotely.

Status Meetings

CrowdStrike will provide Customer weekly summary status reports, or as otherwise mutually agreed.

Deliverables

CrowdStrike will:

- Document and deliver an External Network Penetration Test Report consisting of the following sections:
  - Executive Summary - a high-level overview of the security posture
  - Key Findings Overview
  - Assessment Findings Summary and Detail
  - Recommendations – specific actions or considerations to address documented issues
- Deliver one copy of the draft External Network Penetration Test Report to Principal Customer Technical Contact within ten business days following completion of the “External Network Penetration Testing” activity, or as otherwise mutually agreed. Customer will have ten days to review and provide feedback on the draft report. If Customer has not provided feedback or comments within ten days after delivery, CrowdStrike will finalize the report.

Social Engineering Assessment

Social Engineering Assessment Exercise is only delivered by CrowdStrike to Customer in conjunction with one or more of the following Services: Red Team Blue Team Exercise, Adversary Emulation Exercise, Persistent Adversary Emulation Exercise, Internal Red Team Exercise, External Network Penetration Testing, or Web Application Penetration Testing.

CrowdStrike will test Customer's ability to protect against malicious social engineering activities. CrowdStrike will demonstrate how Customer personnel respond to social engineering attacks.

This engagement may involve social engineering activities to assess the Customer's security posture. Activities may include, but not limited to, registering similar domains and resources, as well as impersonating customer employees, brands, and services.

The General Penetration Testing Notice applies to this service.

CrowdStrike may use subcontractors in its provision of the Service. To the extent that such use of a subcontractor conflicts with the terms of the Agreement, Customer may be required to consent in writing to receive this Service.

Assessment Activities

CrowdStrike may include:

- VPhishing/Pre-Text Calling - Place phone calls attempting to persuade Customer personnel to disclose Confidential Information, execute a payload or enter network credentials;
- Phishing - Conduct a targeted phishing campaign to persuade Customer personnel to execute a payload or enter network credentials; and
- Analyze and document findings and provide recommendations in the Social Engineering Assessment report.

Testing Location

CrowdStrike will perform work under this task remotely.

Status Meetings

CrowdStrike will provide Customer weekly summary status reports, or as otherwise mutually agreed.

Deliverables

CrowdStrike will:

- Document and deliver a Social Engineering Assessment Report consisting of the following sections:
  - Executive Summary - a high-level overview of the security posture;
  - Key Findings Overview;
  - Assessment Findings Summary and Detail; and
  - Recommendations – specific actions or considerations to address documented issues.

- Deliver one copy of the Social Engineering Assessment Report, in draft copy, to Principal Customer Technical Contact within ten business days following completion of the “Social Engineering Assessment” activity, or as otherwise mutually agreed. Customer will have ten days to review and provide feedback on the draft report. If Customer has not provided feedback or comments within ten days after delivery, CrowdStrike will finalize the report.

Web Application Penetration Testing

CrowdStrike will perform web application testing to attempt to discover exploitable vulnerabilities and gain access to sensitive data.

The General Penetration Testing Notice applies to this service.

CrowdStrike may use subcontractors in its provision of the Service. To the extent that such use of a subcontractor conflicts with the terms of the Agreement, Customer may be required to consent in writing to receive this Service.

Customer Activities

- Designate point(s) of contact to attend kickoff meetings and status updates
- Provision CrowdStrike accounts

CrowdStrike Testing Activities

CrowdStrike will conduct the following activities:

- Perform web application vulnerability discovery and exploitation of mutually (CrowdStrike and Customer) agreed upon web applications
- Perform authenticated and unauthenticated web application testing focusing on OWASP Top 10 security issues and business logic errors
- As applicable, analyze, and document its findings and recommendations to be included in the Web Application Penetration Testing Report

Assumptions

- If the in-scope resources exceed scoped amount (defined in the Testing Activities), CrowdStrike may request additional hours
- CrowdStrike will not attempt lateral movement activities under Web Application Penetration Testing will stop at demonstrating code execution or remote command line access
- Code review, API fuzzing, and denial of service testing are not included in these testing activities

Testing Location

CrowdStrike will perform work under this task remotely.

Status Meetings

CrowdStrike will provide Customer weekly summary status reports, or as otherwise mutually agreed.

Deliverables

CrowdStrike will:

- Document and deliver a Web Application Penetration Testing Report consisting of the following sections:
    - Executive Summary - a high-level overview of the security posture
    - Key Findings Overview
    - Assessment Findings Summary and Detail
    - Recommendations – specific actions or considerations to address documented issues
- CrowdStrike will deliver one copy of the Web Application Penetration Testing Final Report to Principal Customer Technical Contact within ten business days following completion of the “Web Application Penetration Testing” activity, or as otherwise mutually agreed. Customer will have ten days to review and provide feedback on the draft report. If Customer has not provided feedback or comments within ten days after delivery, CrowdStrike will finalize the report.

Wireless Penetration Testing

Wireless Penetration Testing Exercise is only delivered by CrowdStrike to Customer in conjunction with one or more of the following Services: Red Team Blue Team Exercise, Adversary Emulation Exercise, Persistent Adversary Emulation Exercise, Internal Red Team Exercise, External Network Penetration Testing, or Web Application Penetration Testing.

CrowdStrike will conduct wireless penetration testing to gain unauthorized access to the Customer's wireless network.

The General Penetration Testing Notice applies to this service.

Testing Activities

CrowdStrike may conduct various attack scenarios, but limited to:

- Wireless Injection
- Man-in-the-middle
- ARP Poisoning
- Session Hijacking
- Impersonation

Testing Location

CrowdStrike will perform work under this task at the Customer's site, as agreed between CrowdStrike and Customer.

Status Meetings

CrowdStrike will provide Customer weekly summary status reports, or as otherwise mutually agreed.

Deliverables

CrowdStrike will:

- Document and deliver a Wireless Penetration Testing Report consisting of the following sections:
  - Executive Summary - a high-level overview of the security posture;
  - Key Findings Overview;
  - Assessment Findings Summary and Detail; and
  - Recommendations – specific actions or considerations to address documented issues.
- CrowdStrike will deliver one copy of the Wireless Penetration Testing Final Report to Principal Customer Technical Contact within ten business days following completion of the "Wireless Penetration Testing" activity, or as otherwise mutually agreed.

Cloud Red Team / Blue Team Exercise

The purpose of this activity is to identify gaps in the Customer's security posture when detecting and responding to a targeted attack. CrowdStrike will operate in a step-by-step manner following common attacker techniques, pausing after each phase of the attack to conduct simulated incident triage and response with the Customer's security team.

The General Penetration Testing Notice applies to this service.

Note: At this time, this exercise is supported in AWS, Azure infrastructure, and Azure AD / O365 environments.

Customer Activities

The Customer will perform the following activities:

- Provide CrowdStrike with privileged credential access to a production AWS environment.
- Provide CrowdStrike a project sponsor/owner, a dedicated project manager to facilitate access and coordinate inter-team activities, and a dedicated technical contact on the incident response team.
- Participate in the testing exercise by working with the CrowdStrike Blue Team consultant to review detective security controls, adapt and build detective logic, and avoid terminating or blocking testing operations where possible, except as agreed by Customer and CrowdStrike, to maximize the diagnostic and capacity-building value of the exercise.

CrowdStrike Activities

CrowdStrike will conduct the following activities:

- Red Team Activities. CrowdStrike will:
  - Conduct remote operations, aligned with engagement objectives;
  - Document attack activities and indicators of attack;

Blue Team Activities

CrowdStrike will:

- Provide at least one consultant to support engagement activities;
- Coordinate communications with Customer security team;
- Support CrowdStrike Red Team attack activities;
- Assist Customer through the triage and discovery process to identify Red Team activities;
- Discuss defensive processes and countermeasures;
- Identify gaps in the Customer's detection processes for the cloud environment (including technology, people, and processes);

General Activities

CrowdStrike will:

- Conduct daily meetings to review Red Team and Blue Team activities;
- As applicable, analyze and document findings and provide recommendations to be included in the Red Team / Blue Team Final Report.

Testing Location

CrowdStrike may perform work under this task at the Customer's site, as agreed between CrowdStrike and Customer, or may perform work under this task remotely.

Status Meetings

CrowdStrike will provide Customer weekly summary status reports, or as otherwise mutually agreed.

Deliverables

CrowdStrike may, as requested:

- Construct and present draft and final reports containing findings and observations. The report may contain information summarizing the Services for an executive reader, as well as technical information for a technical reader, and summary recommendations. The report is initially delivered in a draft format and then discussed with Customer, at Customer's option. CrowdStrike will then revise the draft in response to revisions and questions provided by Customer. If Customer has not requested such revisions or provided questions regarding the report within ten (10) business days, then CrowdStrike will deliver the draft as a final report.

If a draft report is requested, Customer will:

- Review the draft report and provide feedback to CrowdStrike within ten (10) business days.

System Hardening Penetration Testing

CrowdStrike will assess test systems provided by the customer for known vulnerabilities, local privilege escalation, installed application and operating system misconfigurations.

The General Penetration Testing Notice applies to this service.

This Service may be provided by a third-party subcontractor. To the extent that such use of a subcontractor conflicts with the terms of the Agreement, Customer may be required to consent in writing to receive this Service.

Customer Activities

The Customer will perform the following activities:

- Customer will provide CrowdStrike with one of the three access options:
  - User account with multi-factor VPN access to the system;
  - Ship the device directly to CrowdStrike,
  - Provide a point of contact to execute offensive software to establish remote access to the system (witting click or assumed breach start).
- Customer will work with CrowdStrike to ensure the system is configured with system settings, network connectivity, and applications in line with Customer's standard deployment.

Testing Activities

CrowdStrike will conduct the following activities:

- CrowdStrike will conduct a vulnerability and configuration assessment on one in-scope system as agreed by the parties (e.g., Windows, Linux, or Docker Image).
- Assessment activity will include the following focus areas:
  - Host Based (open ports, services, etc.);
  - Vulnerabilities or misconfigurations resulting in local privilege escalation, remote code execution, persistence, sensitive data disclosure; and
  - Overall endpoint protection, detection, and prevention capabilities.
- CrowdStrike will conduct unauthenticated and authenticated manual testing where possible;
- CrowdStrike will provide Customer a list of resources that contain possible exploitable vulnerabilities;
- CrowdStrike will coordinate with Customer before exploitation attempts;
- As applicable, CrowdStrike will analyze and document findings and recommendations to be included in the System Hardening Penetration Test Final Report.

Testing Location

CrowdStrike will perform work under this task remotely.

Status Meetings

CrowdStrike will provide Customer weekly summary status reports, or as otherwise mutually agreed.

Deliverables

CrowdStrike will:

- Document and deliver a System Hardening Penetration Test Final Report consisting of the following sections:
    - Executive Summary - a high-level overview of the security posture;
    - Key Findings Overview;
    - Assessment Findings Summary and Detail; and
    - Recommendations – specific actions or considerations to address documented issues.
- CrowdStrike will deliver one copy of the System Hardening Penetration Test Final Report to Principal Customer Technical Contact within ten business days following completion of the "System Hardening Penetration Test" activity, or as otherwise mutually agreed. Customer will have ten days to review and provide feedback on the draft report. If Customer has not provided feedback or comments within ten days after delivery, CrowdStrike will finalize the report.

Network Segmentation Testing

CrowdStrike will assess accessibility between given network segments within the Customer's network, to include what hosts and services are reachable. If requested by Customer, CrowdStrike will also assess if it is possible to exfiltrate fake personally identifiable information (PII), or other types of fake data, from the Customer environment to systems outside of the network.

The General Penetration Testing Notice applies to this service.

This Service may be provided by a third-party subcontractor. To the extent that such use of a subcontractor conflicts with the terms of the Agreement, Customer may be required to consent in writing to receive this Service.

Customer Activities

The Customer will perform the following activities:

- Customer will provide CrowdStrike with a point of contact that will ensure a system, typically a Linux virtual machine, is available within the appropriate network segment, which CrowdStrike can connect to via VPN or other secure connection method, install tools on, proxy traffic through, and use for segmentation testing. If an account needs to be provisioned this should be done ahead of the agreed upon testing start date. Customer may provide CrowdStrike with VPN and remote desktop access, SSH, or other access.

Testing Activities

CrowdStrike will conduct the following activities:

- **Segmentation Testing**. CrowdStrike will use common system administration and attacker tools to enumerate hosts and services that are reachable between given network segments. If requested by Customer, CrowdStrike will also assess if it is possible to exfiltrate fake personally identifiable information (PII), or other types of fake data, from the Customer environment to systems outside of the network, using common protocols such as FTP, SMB, SSH, HTTP, and HTTPS.

Testing Location

CrowdStrike will perform work under this task remotely.

Status Meetings

CrowdStrike will provide Customer regular written updates on the progress of the Services. Summary status reports will be provided weekly, prior to scheduled weekly status meetings.

Deliverables

CrowdStrike will:

- Document and deliver a Network Segmentation Testing Report consisting of the following sections:
  - Executive Summary - a high-level overview of the security posture;

- Key Findings Overview;
- Assessment Findings Summary and Detail; and
- Recommendations – specific actions or considerations to address documented issues.

- CrowdStrike will deliver one copy of the Network Segmentation Testing Final Report to Customer's Principal Customer Technical Contact within ten business days following completion of the "Network Segmentation Testing" activity, or as otherwise mutually agreed.

Optional Debrief

CrowdStrike will hold one remote debrief meeting with the Customer to review findings of the draft report, if requested by Customer.

Security Controls Validation

The purpose of this assessment is to verify security control remediation actions are effective and implemented properly through testing. This assessment is not intended to discover new issues or vulnerabilities, nor is it meant to be inclusive of all remediation recommendations identified as a result of a security event.

Activities

The Customer and CrowdStrike will mutually agree on the list of in-scope remediation items. In-scope remediation items will typically be associated with vulnerabilities or gaps in processes or technologies that can be assessed through targeted attack emulation or penetration testing activities.

Customer will:

- Provide CrowdStrike with a list of remediation items that need to be verified
- If required, provide CrowdStrike the level of network access required to test the in-scope remediation items

CrowdStrike will:

- Conduct hands-on technical testing to verify mitigations are in place and effective
- Assessment activities may include; web application testing, privilege escalation verification, lateral movement activities, and segmentation testing

Location

CrowdStrike will perform work under this task remotely.

Status Meetings

CrowdStrike will provide Customer weekly summary status reports, or as otherwise mutually agreed.

Engagement Artifacts

CrowdStrike, as directed, will construct and deliver draft and final versions of a Security Controls Verification Assessment report, consisting of the following, as appropriate:

- Executive Summary – A high-level overview of the tested remediation items
- Assessment Findings – A list of remediation items, their status, and evidence of their status

CrowdStrike will deliver one copy of the Security Controls Verification Assessment report to your Point of Contact within ten business days following completion of the “Security Controls Verification Assessment” activity, or as otherwise mutually agreed. Customer will have ten days to review and provide feedback on the draft report. If Customer has not provided feedback or comments within ten days after delivery, CrowdStrike will finalize the report.

Assumptions

Testing will cover up to ten (10) remediation items.

Disclaimer

So long as CrowdStrike performs the Services in compliance with the express warranties set forth in the applicable Section of the Agreement, CrowdStrike disclaims responsibility for costs in connection with disruptions of and/or damage to Customer's or a third party's information systems and the information and data contained therein, including, but not limited to, denial of access to a legitimate system user, automatic shut-down of information systems caused by intrusion detection software or hardware, or failure of the information system resulting from the provision of the Services.

Penetration Testing Retest

The General Penetration Testing Notice applies to this service.

The purpose of this activity is to conduct a retest of high vulnerabilities identified during a penetration test performed by CrowdStrike within the previous six months. Such retest is designed to verify the success of the recommended remediation activities resulting from the original penetration test. For only the high vulnerabilities identified during the original penetration test, CrowdStrike will:

Activities

CrowdStrike will:

- Retest activities defined in previous test;
- Completion Criteria: This activity will be complete when CrowdStrike has delivered the Penetration Test Retest Final Report to your Point of Contact.

Deliverable Materials

The Penetration Test Retest Report is a document consisting of the following, as appropriate:

- Executive Summary - a high-level overview of the security posture;
- Key Findings Overview;
- Assessment Findings Summary and Detail; and
- CrowdStrike will deliver one copy of the Penetration Test Retest Final Report to your Point of Contact within ten business days following completion of the “Penetration Test Retest” activity, or as otherwise mutually agreed.

CROWDSTRIKE

Partner Services

Partner Services

Active Directory Security Assessment

The Active Directory Assessment Services are provided by a third-party subcontractor. To the extent that such use of a subcontractor conflicts with the terms of the Agreement, Customer may be required to consent in writing to receive this Service.

CrowdStrike will provide Active Directory security guidance that helps to make it more difficult for an attacker to gain access to the sensitive areas of the organization's network. This interactive assessment is meant to help answer questions about current and future project plans relating to Active Directory security to support both short-term and long-term planning. A signed Change Order is required to utilize this service.

Concept of Operations

- Evaluate Active Directory forest and domain configuration. This includes evaluating the current Domain and Forest functional levels and identification of security enhancements in the current and higher levels.
- Active Directory security misconfigurations are highlighted, and specific recommendation are provided.
- Active Directory trust configuration and security review.
- Active Directory administration groups review. This includes Enterprise Administrators, Administrators, Domain Administrators, custom delegation groups, and others as identified. Groups with logon rights to Domain Controllers are scrutinized and membership is expanded to gain a complete picture of the Active Directory administrators.
- Evaluate custom security groups with privileged access to Active Directory and their access rights identified.
- Review Group Policy security configuration for the domain and Domain Controllers.
- Review permissions for all Group Policy Objects (GPOs) and issues with the delegation of GPOs are noted along with recommended remediation.
- Evaluate Service Accounts with elevated permissions. Identification of Kerberos enabled services and their associated service accounts. Special focus on service accounts with domain-level administrator rights.
- Domain Controller management review including Operating System versions, patching, backup, server lifecycle management, and FSMO role holder locations.
- Enumerate security software and tools. This involves identifying the security components and their purpose and this information is used to identify potential gaps in defenses an attacker could leverage.
- Review Active Directory organizational unit (OU) permissions with a focus on top-level domain OUs. Additional Active Directory object permissions are reviewed to identify potential "backdoor" access which is not obvious based on group membership.

- Identify Domain Controller auditing configuration and determine what event IDs will flow to the central logging system (SIEM/Splunk). Provide recommendations for Domain Controller auditing and what specific event IDs should be sent to the central logging system in order to detect attacker activity.
- Provide broad recommendations for all Windows system auditing (specific event IDs) that should be forwarded to the central logging system (SIEM/Splunk).

Potential Engagement Artifacts

CrowdStrike may provide the following artifacts for this engagement:

- An executive summary of the key findings;
- Summary of the risk exposure to the organization;
- Detailed documentation of observations from the Active Directory analysis performed; and
- Recommendations for security and audit log settings.

Testing Notice

Additional Authorizations

The Principal Customer Technical Contact, or other customer designee(s), will be available as needed during the engagement to authorize CrowdStrike in writing or email to proceed, or not to proceed, regarding any aspect of the engagement.

Identification of Compromise

Identification of compromise is not part of normal testing activities. However, if CrowdStrike discovers indicators of compromise during testing activities CrowdStrike will halt all testing activities in the Customer's in-scope environment.

Disclaimer

So long as CrowdStrike and its subcontractors, if applicable, perform the Services in compliance with the warranties set forth in the Section entitled Warranties and Remedies in the Agreement, CrowdStrike and its subcontractors disclaim responsibility for costs in connection with disruptions of and/or damage to Customer's or a third party's information systems and the information and data contained therein, including, but not limited to, denial of access to a legitimate system user, automatic shut-down of information systems caused by intrusion detection software or hardware, or failure of the information system resulting from the provision of the Services.

Security Assessment for Microsoft Cloud

The Security Assessment for Microsoft Cloud Services are provided by a third-party subcontractor. To the extent that such use of a subcontractor conflicts with the terms of the Agreement, Customer may be required to consent in writing to receive this Service.

The assessment reviews your Microsoft Cloud tenant and identifies potential issues attackers could exploit. The configuration of your Office 365 & Azure Active Directory (AD) environment is analyzed to provide custom recommendations to better leverage features and controls available with your existing Microsoft Cloud subscription as well as others that are available. A signed Change Order is required to utilize this service.

Concept of Operations

The Microsoft Cloud Security Assessment involves review, analysis, and custom recommendations of the following:

- Current Azure AD tenant configuration
- Administration
- Privileged Roles and Accounts
- Azure AD PIM configuration (if applicable)
- Azure AD applications and permissions
- Azure AD Multi-Factor Authentication (MFA) configuration
- Conditional Access
- Azure AD Connect Configuration (based on tenant data)
- Exchange Online
    - Exchange Online configuration
    - Email security configuration
    - Exchange Online administration
    - Mailbox auditing
    - Mailbox permission

Potential Engagement Artifacts

CrowdStrike may provide the following artifacts for this engagement:

- An executive summary of the key findings;
- Summary of the risk exposure to the organization;
- Detailed documentation of observations from the Azure AD tenant analysis performed; and
- Recommendations for security settings.

Testing Notice

Additional Authorizations

The Principal Customer Technical Contact, or other customer designee(s), will be available as needed during the engagement to authorize CrowdStrike in writing or email to proceed, or not to proceed, regarding any aspect of the engagement.

Identification of Compromise

Identification of compromise is not part of normal testing activities. However, if CrowdStrike discovers indicators of compromise during testing activities CrowdStrike will halt all testing activities in the Customer's in-scope environment.

Disclaimer

So long as CrowdStrike and its subcontractors, if applicable, perform the Services in compliance with the warranties set forth in the Section entitled Warranties and Remedies in the Agreement, CrowdStrike and its subcontractors disclaim responsibility for costs in connection with disruptions of and/or damage to Customer's or a third party's information systems and the information and data contained therein, including, but not limited to, denial of access to a legitimate system user, automatic shut-down of information systems caused by intrusion detection software or hardware, or failure of the information system resulting from the provision of the Services.

Virtual Infrastructure Security Assessment

Virtual Infrastructure Security Assessment services are provided by a third-party subcontractor. To the extent that such use of a subcontractor conflicts with the terms of the Agreement, Customer may be required to consent in writing to receive this Service.

The Virtual Infrastructure Security Assessment involves the analysis of Customer's current VMware vSphere Virtual Infrastructure (vCenter & ESXi) configuration with a focus on Administration, Configuration, and Security Controls.

Concept of Operations

The Virtual Infrastructure Security Assessment involves analysis of the current vSphere virtual infrastructure configuration compared to security industry standard practices. This includes analysis and recommendations based on the assessment team's research and expertise as well as custom recommendations specific to customer environments meant to help improve the security posture of the virtual infrastructure. The assessment includes the following core activities:

- Review of the current virtual infrastructure configuration compared to industry standard practices. This review includes standard recommendations based on the assessment team's expertise and research as well as custom recommendations specific to Customer environment meant to help improve the security posture of the virtual infrastructure.
- Analysis and recommendations on how to leverage existing virtual infrastructure license levels for additional beneficial security controls.
- Review of the virtual infrastructure environment is currently managed as well as more secure administration recommendations.
- Review of network topology to ensure VMware security practices have been implemented.
- Auditing and logging configuration review and analysis provides a comparison of the existing logging configuration to security industry standard.

Potential Engagement Artifacts

CrowdStrike may provide the following artifacts for this engagement:

- An executive summary of the key findings;
- Detailed documentation of findings from the analysis performed; and
- Recommendations and supporting information for enhancing security settings.

Testing Notice

Additional Authorizations

The Principal Customer Technical Contact, or other customer designee(s), will be available as needed during the engagement to authorize CrowdStrike in writing or email to proceed, or not to proceed, regarding any aspect of the engagement.

Identification of Compromise

Identification of compromise is not part of normal testing activities. However, if CrowdStrike discovers indicators of compromise during testing activities CrowdStrike will halt all testing activities in the Customer's in-scope environment.

Disclaimer

So long as CrowdStrike and its subcontractors, if applicable, perform the Services in compliance with the warranties set forth in the Section entitled Warranties and Remedies in the Agreement, CrowdStrike and its subcontractors disclaim responsibility for costs in connection with disruptions of and/or damage to Customer's or a third party's information systems and the information and data contained therein, including, but not limited to, denial of access to a legitimate system user, automatic shut-down of information systems caused by intrusion detection software or hardware, or failure of the information system resulting from the provision of the Services.

OT/ICS Architecture Review (via Dragos)

Operational Technology (OT)/Industrial Control System (ICS) Architecture Review services are provided by CrowdStrike's third-party subcontractor, Dragos. To the extent that such use of a subcontractor conflicts with the terms of the Agreement, Customer may be required to consent in writing to receive this Service. Each Architecture Review is scoped on a per site basis.

During the OT/ICS Architecture Review, the assessment team will review the client's current detection and protection capabilities and propose activities and methods to mature the organization's security. The assessment team will use their knowledge of OT/ICS-focused adversaries and their tactics, techniques, and procedures (TTPs) to provide a real-world context to findings.

Concept of Operations

The assessment team will work with key Customer stakeholders to develop a preliminary understanding of the existing network and security posture in relation to protection, detection, and response capabilities. The assessment team may also request to review documentation, network diagrams, packet capture, or other artifacts related to the Customer's ICS environment. Through documentation review and stakeholder interviews, the assessment team reviews the security posture of the network design for gaps. The assessment team will review customer provided PCAPS to inspect network traffic samples looking for vulnerabilities, indicators of compromise, threat behaviours, and insecure credentials practices. The team will then deliver prioritized tactical and strategic recommendations designed to strengthen the organization's ability to defend critical industrial control systems.

Potential Engagement Artifacts

At Customer's request, the assessment team may construct and provide a summary report based containing:

- Executive summary
- Methodologies used for analysis
- Findings with severity assignment
- Prioritized list of recommendations to address associated findings.

Testing Notice

Additional Authorizations

The Principal Customer Technical Contact, or other customer designee(s), will be available as needed during the engagement to authorize CrowdStrike in writing or email to proceed, or not to proceed, regarding any aspect of the engagement.

Identification of Compromise

Identification of compromise is not part of normal testing activities. However, if CrowdStrike discovers indicators of compromise during testing activities CrowdStrike will halt all testing activities in the Customer's in-scope environment.

Disclaimer

So long as CrowdStrike and its subcontractors, if applicable, perform the Services in compliance with the warranties set forth in the Section entitled Warranties and Remedies in the Agreement, CrowdStrike and its subcontractors disclaim responsibility for costs in connection with disruptions of and/or damage to Customer's or a third party's information systems and the information and data contained therein, including, but not limited to, denial of access to a legitimate system user, automatic shut-down of information systems caused by intrusion detection software or hardware, or failure of the information system resulting from the provision of the Services.

IR Plan Development

CrowdStrike will assist Customer by developing an Incident Response (IR) Plan. The IR Plan will incorporate currently relevant Customer IR procedures as well as industry best practice processes and methodologies.

This Service may be provided by a third-party subcontractor. To the extent that such use of a subcontractor conflicts with the terms of the Agreement, Customer may be required to consent in writing to receive this Service.

Project Planning Activities

- Draft project plan for delivery of services, including dependencies and project activities
- Align stakeholders on project objectives, deliverables, and requirements of project

Documentation and Configuration Review

Customer will provide, and CrowdStrike will review, Customer's documentation to understand Customer's security processes. CrowdStrike may request documentation including, but not limited to:

- Information Security policies, procedures, playbooks
- Incident Response policies, procedures, playbooks
- Information Security awareness and training materials
- Information Security organizational chart
- SIEM or monitoring and alerting process documentation
- List of forensic and incident response tools
- List of security prevention/detection tools
- Threat intelligence feed list
- Information Security roadmap, projects and/or initiatives
- Data classification and handling Policy
- Incident Response Communication Material (e.g., Call Tree, Contact List, Templates)
- Business Continuity & Disaster Recovery Plan
- Emergency / Crisis Management Plan
- Crisis Communication Plan
- Tier One Escalation Procedures (e.g., Service Desk, MSSP)
- Cyber Insurance Policy
- Third Party Retainers (e.g., DFIR, Legal, Public Relations, etc.)

Interviews

CrowdStrike will conduct interviews with Customer's key stakeholders to understand how security processes are conducted. Stakeholders may include:

- Information Security
- IT Risk and Compliance
- Enterprise Services
- Network Security
- SOC/NOC
- Executive Management
- Desktop Support/Help Desk
- IT Support / BC&DR
- Communications
- Legal
- Emergency / Crisis Management
- Data Protection / Privacy/Insurance (if applicable)
- Vulnerability Management

Additional meetings may be scheduled to facilitate follow up questions and additional areas of interest.

IR Plan Creation

CrowdStrike will leverage the information and knowledge gained during the documentation review and interviews to develop an IR Plan.

Location

CrowdStrike will perform work under this task remotely.

Status Meetings

CrowdStrike will provide Customer regular written updates on the progress of the Services. Summary status reports will be provided weekly, prior to scheduled weekly status meetings.

Deliverables

CrowdStrike will construct and deliver draft and final versions of the IR Plan, provided in a Word document. The IR Plan will include the following sections:

- Governance
- Definitions

- Incident Classification Criteria
- Roles and Responsibilities
- Communications Model
- IR Process by Phase
- Maintenance

CrowdStrike will construct and deliver supplemental templates related to the IR Plan including:

- Evidence Handling Templates
- Contact List Templates
- Communication Templates
- Incident Documentation Templates

IR Playbook Development

CrowdStrike will assist Customer in developing an Incident Response (IR) Playbook. The IR Playbook will incorporate currently relevant Customer IR procedures as well as industry best practice processes and methodologies.

This Service may be provided by a third-party subcontractor. To the extent that such use of a subcontractor conflicts with the terms of the Agreement, Customer may be required to consent in writing to receive this Service.

Documentation and Configuration Review

Customer will provide, and CrowdStrike will review, Customer's documentation to understand Customer's security processes. CrowdStrike may request documentation including, but not limited to:

- Information Security policies, procedures, playbooks
- Incident Response policies, procedures, playbooks
- Information Security awareness and training materials
- Information Security organizational chart
- SIEM or monitoring and alerting process documentation
- List of forensic and IR tools
- List of security prevention/detection tools
- Threat intelligence feed list
- Information Security roadmap, projects and/or initiatives

Interviews

CrowdStrike will conduct interviews with Customer's key stakeholders to understand how security processes are conducted. Stakeholders may include:

- Information Security
- IT Risk and Compliance
- Enterprise Services
- Network Security
- SOC/NOC
- Executive Management
- Desktop Support/Help Desk
- IT Support
- Communications

- Legal
- Emergency / Crisis Management
- Data Protection / Privacy/Insurance (if applicable)
- Vulnerability Management

Additional meetings may be scheduled to facilitate follow up questions and additional areas of interest.

IR Playbook Creation

CrowdStrike will leverage the information and knowledge gained during the documentation review and interviews to develop stand-alone Incident Response Playbook(s) which are limited to the following scenario(s):

- Account Takeover (Elevation of Privilege) and Account Takeover (Root Access)
- Data Compromise (Accidental Data Release)
- Data Compromise (Data Theft)
- Denial of Service (and DDoS)
- Escalation and Triage
- Insider Threat
- Lost or Stolen Device
- Malware
- Network Compromise
- Phishing
- Ransomware
- Third-Party Compromise

Location

CrowdStrike will perform work under this task remotely.

Status Meetings

CrowdStrike will provide Customer regular updates on the progress of the Services. Brief updates will be provided on a schedule as agreed between Customer and CrowdStrike. Summary written status reports will be provided weekly.

Deliverables

CrowdStrike will construct and deliver draft and final versions of the separate Incident Response Playbook(s) as identified in an Authorization Form or other signed writing.

Mobile Application Penetration Testing

The Mobile Application Penetration Testing services are provided by a third-party subcontractor. To the extent that such use of a subcontractor conflicts with the terms of the Agreement, Customer may be required to consent in writing to receive this Service.

CrowdStrike will perform mobile application penetration testing to attempt to discover exploitable vulnerabilities, assess data integrity, and gain access to sensitive data.

The General Penetration Testing Notice applies to this service.

Testing Activities

CrowdStrike will conduct the following activities:

- Perform mobile application vulnerability discovery and exploitation of mutually (CrowdStrike and Customer) agreed upon mobile applications (iOS and Android only) and their associated platforms;
- Perform authenticated and unauthenticated mobile application testing focusing on OWASP Mobile Top 10 security issues;
- As applicable, analyze, and document its findings and recommendations to be included in the Mobile Application Penetration Testing Report.

Assumptions

- If the in-scope resources exceed scoped amount (defined in the Testing Activities), CrowdStrike may request additional hours.
- CrowdStrike will not attempt lateral movement. Activities will only progress to the point of demonstrating remote command line access, if possible.
- Code review, API fuzzing, and denial of service testing are not included in these testing activities.
- Mobile application testing will focus on mobile application on a mobile device, as opposed to testing a web app from a mobile browser app.
- Testing may be conducted using an emulator or by installing the mobile app on a physical device. If a specific model of physical device is required for testing, this will be provided by customer.
- Client will provide the binary for the application (APK and/or IPA). If client does not provide the binary, testing will be conducted on the versions from the App Store or Play Store, in the production environment.

Testing Location

CrowdStrike will perform work under this task remotely.

Status Meetings

CrowdStrike will provide Customer weekly summary status reports, or as otherwise mutually agreed.

Deliverables

CrowdStrike will:

- Document and deliver a Mobile Application Penetration Testing Report consisting of the following sections:
  - Executive Summary - a high-level overview of the security posture
  - Key Findings Overview
  - Assessment Findings Summary and Detail
  - Recommendations – specific actions or considerations to address documented issues
- CrowdStrike will deliver one copy of the Mobile Application Penetration Testing Final Report to Principal Customer Technical Contact within ten business days following completion of the "Mobile Application Penetration Testing" activity, or as otherwise mutually agreed. Customer will have ten days to review and provide feedback on the draft report. If Customer has not provided feedback or comments within ten days after delivery, CrowdStrike will finalize the report.

CROWDSTRIKE

Endpoint Recovery Services

Endpoint Recovery Services

CrowdStrike will assist Customer with the detection, analysis, and remediation of know security incidents and enable recovery.

Concept of Operations

CrowdStrike, as part of a fixed 30-day service engagement, will assist the Customer with recovery and remediation from a suspected computer security incident. Recovery objectives and outcomes provided by CrowdStrike will focus on the analysis of Falcon detections and Real Time Response (RTR) to mitigate and prevent active/ongoing attacks, remediate Threat Actor persistence and malicious artifacts, and provide monitoring for the service term to ensure effective eradication of the Threat Actor.

America Region: All Endpoint Recovery Services' activities will be performed Monday—Friday between the hours of 9:00 am to 5:00 pm US Eastern Time.

EMEA Region: All Endpoint Recovery Services' activities will be performed Monday—Friday between the hours of 9:00 am to 5:00 pm GMT.

APJ Region: All Endpoint Recovery Services' activities will be performed Monday—Friday between the hours of 9:00 am to 5:00 pm AEST.

Typical Service Timeline and Phases

Containment and Prevention

- Timeframe: First 24-72 hours
- Objectives:
  - Support Falcon deployment, if needed, and provide Falcon prevention policy recommendations and support aligned to;
  - Disrupt active attacks, lateral movement, and eliminate the Threat Actor's hands-on-keyboard within the environment

Active Recovery

- Timeframe: 72-96 hours
- Objectives:
  - Analyze Falcon detections, and EAM and RTR data to implement attack countermeasures and custom IOAs
  - Use Falcon data and RTR queries to identify remediation plan and scope
  - Use RTR to execute remediation plan across all impacted endpoints to eliminate, including but not limited to:
    - Active malware
    - Threat Actor persistence

- Additional attack artifacts

Monitoring

- Timeframe: Post Active Recovery until the end of the 30-day Service term
- Objectives:
  - Monitor customer environment for re-emergence or continuation of Threat Actor behavior
  - Validate completeness of remediation

Reporting (If requested)

- Timeframe: Post engagement
- Objectives:
  - Provide a report outlining recovery actions

Potential Engagement Artifacts

CrowdStrike may provide the following artifacts for this engagement, if requested:

- Periodic (typically weekly or twice-weekly) status reports to provide updates on completed and ongoing activities and identified challenges
- A final report with executive summary, technical details of significant findings, and summary recommendations
- A technical datasheet or appendix including all findings and actions related to recovery and remediation details

CROWDSTRIKE

Exhibit A
Authorization Form

Exhibit A – Authorization Form

CrowdStrike Services Authorization

Authorization Order

This is an Authorization from Customer for CrowdStrike to draw down the Retainer for Services purchased by Customer pursuant to an [SOW/Order] by performing the Services set forth below. This is documenting the specific Services to be performed pursuant to the terms of such [SOW/Order] and the Professional Services Catalog available here[3]. This Authorization requires no signatures (except as noted). Services described below shall begin on a mutually agreed upon date.

Request Date:	**x**
Customer Company Name:	**Account Name**
Law Firm Name:	
SOW or Order Effective Date:	**x**
Customer Contact (Name, Phone, Email):	NAME **Contact Full Name** TITLE **Contact Title** PHONE **Contact Phone Number** EMAIL **Contact Email**
Service Type: (As defined in the Catalog)	**x**
Minimum hours to be drawn down from Retainer (Minimums are estimates only and may be exceeded in accordance with the SOW/Order)	**x**
CrowdStrike Tools Fee (Provided on a per month basis)	**x**
Authorization Effective Date:	**x**

[3] http://www.crowdstrike.com/ServicesCatalog

CROWDSTRIKE

Exhibit B Privileged Engagement Letter (PEL)

Exhibit B – Privileged Engagement Letter (PEL)

[DATE]

CrowdStrike, Inc. (“CrowdStrike”)
150 Mathilda Place, Suite 300
Sunnyvale, California 94086

Re: Privileged Engagement

Dear CrowdStrike:

[Name of Firm] (“Counsel”) is providing legal advice in connection with a privileged investigation of a potential security incident (“Incident”) for [Name of Client] (“Client” or “Customer”). In furtherance of this investigation, Counsel engages CrowdStrike to work under our direction and to assist with formulating our legal analysis and recommendations and perform the services set forth on Schedule A (the “Services”) under the terms of this privileged engagement letter including all attached schedules (collectively, the “Privileged Engagement Letter” or “PEL”).

All Engagement Artifacts (defined in Schedule A) developed by CrowdStrike in the course of performing the Services are done so under the direction of Counsel in anticipation of litigation and/or regulatory obligations and inquiries. CrowdStrike understands that communications with Counsel and Client regarding the investigation of the Incident will be confidential and used to assist Counsel to provide legal advice to Client. Therefore, CrowdStrike agrees: (i) to treat such Engagement Artifacts and such communications as Confidential Information, and that the Services, Engagement Artifacts and such communications are to the extent afforded to under applicable state and federal law in the United States, subject to the attorney-client privilege, attorney work product doctrine, and/or consulting expert privilege. In furtherance thereof, CrowdStrike shall mark all Engagement Artifacts and communications in connection with this PEL with the following headers: (i) Engagement Artifacts: “Privileged & Confidential – Prepared at the Direction of Counsel” and (ii) such communications: "Privileged & Confidential – Attorney-Client Communication – At the Direction of Counsel".
This PEL may be executed in counterparts, each of which will be considered an original but all of which together will constitute one agreement. Any signature delivered by electronic means shall be treated for all purposes as an original. Each of the parties below represents and warrants that the signatory is duly authorized to execute and deliver this PEL (including all Schedules which are incorporated in herein) and agrees to be bound hereby. This PEL is entered into by the parties as of the date signed by the last party (“Effective Date”).

Firm: _____
By: _____
Name: _____
Title: _____
Date: _____

By executing this PEL, Client and CrowdStrike also agree to the terms and conditions incorporated by reference into Schedule A.

Client: _____
By: _____
Name: _____
Title: _____
Date: _____

CrowdStrike, Inc.
By: _____
Name: _____
Title:_____
Date:_____

SCHEDULE A
DESCRIPTION OF SERVICES

Firm Contact Email	**[Firm Email]**
Customer Technical Contact Email	**[Customer Email]**
Payor Accounts Payable Email (T&M only)	**[A/P Email-if applicable]**
Payor Accounts Payable Phone Number (T&M only)	**[A/P Phone-if applicable]**

This Schedule A is incorporated by reference into and subject to the PEL. In addition to the PEL, Client and CrowdStrike agree that this Schedule A is also subject to the CrowdStrike Terms and Conditions located here[4] (the "Terms"). Capitalized terms used in this Schedule but not defined herein shall have the meaning set forth in the PEL or the Terms. Nothing in this Schedule A shall be construed as an amendment of the PEL or the Terms but is merely a supplement thereto. In the event of any inconsistency between this Schedule A and the PEL or the Terms, the PEL and then the Terms shall prevail.

CrowdStrike's objective in the investigation is to assist Counsel in providing legal advice to Customer by answering Counsel's questions related to a potential security incident, such as:

- Did a threat actor gain access to Customer systems
- How the threat actor gained access to the systems
- The earliest and most recent dates of threat actor activity
- Whether and how the threat actor moved laterally in the Customer environment
- Whether there is any evidence the threat actor accessed or exfiltrated Customer data, and if so, what data was accessed or exfiltrated
- Whether the threat actors persist or whether they have been evicted from the Customer environment

Scope of Work

At the direction of Counsel, a CrowdStrike Privileged Investigations Team will assist Counsel with responding to a suspected computer security incident by performing the following phases of work:

Phase 1 – Incident Response Triage

CrowdStrike shall, as needed:

- Analyze data, including but not limited to:
  - Forensic images of disk and/or memory from systems of interest;
  - Data collected by CrowdStrike Tools (defined in section entitled CrowdStrike Tools) (defined below);
  - Live response data from suspected systems of interest;
  - Logs from computer systems, including network traffic, firewalls, DNS and DHCP servers, authentication servers, VPN or remote access servers, and system logs;
  - Documentation of system and network architecture, tools and capabilities;
  - How the incident was detected;

[4] https://www.crowdstrike.com/terms-conditions/

    - Malware, attack tools, malicious software or documents, adversary tactics or other Threat Actor Data;
- Provide, assist with the deployment of, and use CrowdStrike Tools as well as use existing Client tools to gather data for analysis;
- Perform this analysis on or off Client's site;
- Provide a summary of incident triage, with recommended next steps and effort estimates.

Phase 2 – Investigation

CrowdStrike shall, as needed:

- Determine compromised or accessed systems, develop a timeline of attacker activity, investigate the likely attack vector, and what data and user accounts may have been compromised or accessed;
- Use CrowdStrike Tools, as directed, to perform tactical actions, including but not limited to, advanced information gathering (e.g., suspicious or unknown file collection) removing malware, terminating processes, and removing or modifying a malicious Windows registry key or value;
- Provide network analysis services;
    - Provide to Client for use during the engagement Falcon Network tools (defined below in the section entitled *CrowdStrike Tools***)** that monitor network traffic near Internet egress designated by Client;
    - Help Client's staff position and connect Falcon Network hardware (if any) to Client's network;
    - Collect and analyze network traffic.

Status Reporting

During all phases, CrowdStrike will:

- As requested, provide daily status updates verbally or by email, including information about activities performed, findings and their criticality, and plans for upcoming work; and
- As requested, provide written weekly summary updates, reviewing tasks, issues and progress, and advising of the status of work and the budget.

Strategic Recommendations

If requested to do so by Counsel, CrowdStrike may produce recommendations for long-term continuous security posture improvement.

Engagement Artifacts

If directed by Counsel, CrowdStrike shall construct and present draft and final reports containing findings and observations ("Engagement Artifacts" or "Deliverables"). A report is initially delivered in a draft format then discussed with Counsel and Client. The draft report is then revised and delivered as a final report if Counsel has not requested revisions or provided questions regarding the report in 10 business days.

Term and Change Management

Engagement Term

Work will begin on a mutually agreed upon date and no fewer than 40 hours will be charged. This Schedule A expires on the earlier of the completion of the engagement[5] or one year from the Effective Date. If new or additional Services are requested by Counsel after completion or expiration, a new mutually agreed upon Schedule must be established.

Change Management

CrowdStrike will notify the Payor (specified below) via email if any of the hourly estimates listed below will be exceeded. Payor is responsible for fees in excess of the estimate without the need for approvals beyond this signed PEL so long as all hours billed are within the scope of work described in the PEL (including Schedule A). Any change to the scope of Services will be agreed upon in writing by the parties in advance of the change and any additional fees associated therewith.

Pricing

Fees

CrowdStrike will charge [Client or Counsel [SELECT ONE] ("Payor") at the rate of USD XXX per consultant per hour for work that is performed within this PEL.

Service	Estimated LOE*	Structure	Estimated Cost
Incident Response** Estimate for initial Incident Triage	x hours	Time and Materials	Debited from Retainer
Tools Fee for Falcon Forensics*** -X month(s) at USD XXX per month	XX,XXX endpoints	Per Month Basis	USD X,000
Total: (Expenses billed at actuals)			**USD XX,XXX**

* The Level of Effort ("LOE") estimates provided for Professional Services performed on a Time and Material basis are estimates only and not a guaranteed time of completion.
** Actual Level of Effort ("LOE") will be updated based on Incident Response Triage. The LOE hours listed above will be leveraged for Services indicated herein, however, CrowdStrike's ability to perform all of these activities under the initial number of hours estimated is dependent on the level of complexity and scope of the breach.
*** CrowdStrike Tools fee(s) shall be incurred on a per month basis beginning on the Schedule A Effective Date.

[5] **The "completion of the engagement" date will be specified in an email from CrowdStrike at the conclusion of the Services.**

Travel & Expenses

CrowdStrike will charge actual expense amounts as incurred and will provide access to copies of receipts for those amounts upon request. CrowdStrike will not travel unless coordinated with Counsel and Customer. Travel expenses shall be reimbursed as follows: coach class airfare for flight times of 4 hours or less, economy plus for flight times between 4 and 8 hours, and business class airfare for flight times of more than 8 hours or for urgent international travel in support of Incident Response Services; moderate class lodging; full size rental car; ground transportation including taxi or similar transportation services, parking or mileage; visa, work permit or similar fees; meal allowance of USD 125 per person per day. Time spent traveling will be charged at USD 225 per person per hour. Travel time estimates are not included in Services time estimates.

Legal Request Fees

In the event CrowdStrike is legally required to respond to a request for information, and/or provide documents or testimony in connection with the Services as part of: (a) a legal proceeding to which the Client is a party and CrowdStrike is not; or (b) a government or regulatory investigation of the Client, the Client shall: (i) pay all of CrowdStrike's reasonable and actual out of pocket legal fees and expenses (as evidenced by reasonably detailed invoices) in connection therewith, and (ii) pay the hourly rate set forth in this PEL (if no hourly rate is stated, then CrowdStrike's then-current hourly rate) for CrowdStrike's Services consultants' actual hours worked in responding to such requirement, including, time spent preparing for, and participating in, depositions and other testimony.

Taxes

Payor agrees to be responsible for the collection, remittance and reporting of all Value Added Taxes or similar taxes related to this PEL if work is performed outside the United States. Payor is not responsible for any income tax liability incurred by CrowdStrike.

If Payor is claiming a governmental exemption from sales tax, Payor must provide an official purchase order, or other documentation demonstrating direct payment from Payor's agency, and CrowdStrike will confirm whether or not such an exemption is applicable in Payor's particular jurisdiction. Purchases by individuals and reimbursed to them by a federal, state or local government do not qualify for a sales tax exemption.

Payment and Invoicing

Services shall be debited from Retainer Order effective Month Day, Year. CrowdStrike will invoice Payor at the end of each calendar month for: (i) fees associated with any additional time and materials overage hours, (ii) CrowdStrike Tools fees and/or Post-Engagement Data Retention fees, if any, (iii) travel time, if any, and (iv) actual expense amounts, all incurred in arrears. At the conclusion of the Services, remaining hours (if any) will be drawn down from the Retainer Order to the Payor in order to meet a minimum of forty (40) hours to be charged under this PEL.

Post-Engagement Data Retention Fees

If Counsel directs CrowdStrike in writing to retain evidence/data beyond standard retention periods, Payor shall pay the Post-Engagement Data Retention fees set forth in the table below.

Post-Engagement Data Retention Fee(s) Table

Evidence/Data	If retention period is longer than…	Fees per month (or any portion thereof)
Physical Evidence (e.g., removable media, hard drives)	90 days from the completion of the engagement[2]	USD 500.00 per physical evidence device
Virtual Evidence (e.g., system images, memory capture) and Falcon Forensics Collector data	90 days from the completion of the engagement[2]	USD 25.00 per GB (or any portion thereof)

CrowdStrike Tools

Definition

CrowdStrike may use tools while performing the Services (the "CrowdStrike Tools"). CrowdStrike Falcon is not subject to the tools fees as defined in this PEL. Data collected by CrowdStrike Tools is encrypted and stored in the United States or European Union and viewed by personnel in locations that include, but are not limited to, the United States, Canada, United Kingdom, the European Union, New Zealand and Australia.

Falcon Forensics

CrowdStrike personnel may use the Falcon Forensics tool to collect specific data points relevant to the investigation based upon their expertise and knowledge of specific actors/threats. The following are some of the functions performed by Falcon Forensics: directory parsing, handles dump, file hashing, network data dump, detailed process listing, strings extraction, services enumeration, drivers enumeration, environment variables dump, jobs and task enumeration, users and group enumeration.

Falcon Horizon & CrowdStrike Cloud Collectors

CrowdStrike personnel may use Falcon Horizon, a cloud security posture management and detection application, and the CrowdStrike Cloud Collectors, a cloud data collection toolset, to collect and analyze cloud service plane-related information in order to help identify adversary tradecraft and activity.

Falcon Network

CrowdStrike may utilize a threat-specific network monitoring tool referred to as Falcon Network to identify potential outbound malicious communications. CrowdStrike's threat signatures focus on targeted attackers, advanced persistent threats, organized crime and hacktivist groups. Falcon Network is connected to a network egress location and passively captures suspicious traffic in a packet capture library (PCAP). CrowdStrike will not capture any data or signatures other than those necessary to perform the Services. Falcon Network utilizes Corelight and proprietary configurations and tools to maintain a stealth packet capture capability.

CrowdStrike Falcon

CrowdStrike personnel may use CrowdStrike Falcon, a cloud-managed end point detection and response application. CrowdStrike Falcon is comprised of two core components, the cloud-based application and the on-premise device sensor application (Falcon Sensor). CrowdStrike Falcon leverages the lightweight Falcon Sensor that shadows, captures, and correlates low-level operating system events, including, but not limited to: machine event data, executed scripts, code, systems files, log files, DLL files; login data, usernames, binary files, file names, tasks, resource information, commands, protocol identifiers, Internet protocol addresses, URLs, network data, and/or other executable code and metadata. To the extent such data is aggregated and/or anonymous it is referred to as Execution Profile/Metric Data. Execution Profile/Metric Data, similar to Threat Actor Data, is used for collective security purposes and is not considered Client Confidential Information. The analysis of the collected data helps identify the adversary tradecraft and activity as opposed to focusing on malware signatures, indicators of compromise, exploits, and vulnerabilities, used in older information security technology. CrowdStrike uses Execution Profile/Metric Data to analyze, characterize, attribute, warn of, and/or respond to threats against you and others, and to analyze trends and to optimize the functionality of CrowdStrike's products and services. CrowdStrike Falcon is equipped with remediation functionality, including but not limited to advanced information gathering (e.g., suspicious or unknown file collection) actions such as executing scripts and executables, deleting a file, terminating processes, and deleting or modifying Windows registry key or value. CrowdStrike provides automatic updates to CrowdStrike Falcon.

CROWDSTRIKE

Thank you