CROWDSTRIKE

CYBERSECURITY MATURITY ASSESSMENT

ANTICIPATE. IMPROVE. PREPARE.

The CrowdStrike ® Cybersecurity Maturity Assessment (CSMA) is unique in the security assessment arena. Rather than focusing solely on compliance or general information security principals, it provides an evaluation of an organization's maturity level in relation to its ability to prevent, detect, and respond to today's most advanced adversaries.

Many assessments in the marketplace evaluate whether your organization meets compliance requirements. Several even provide a focus on cybersecurity as opposed to general information security principles. CrowdStrike's assessment is unique because it focuses on one of CrowdStrike's core competencies: targeted attacks and the tactics, techniques, and procedures (TTPs) that allow these attacks to be successful. The CSMA is not simply a box-checking exercise. It involves in-depth conversations with real incident response (IR) professionals, who have decades of industry experience fighting against the world's most sophisticated nation-state adversaries, cyber criminals, and geopolitical cyber threats.

CrowdStrike understands that having an industry-recognized framework is important to many organizations when selecting their assessors. That's why CrowdStrike CSMA incorporates all functional areas of the NIST Cybersecurity Framework (CSF) and each of the CIS Top 20 Critical Security Controls. But CrowdStrike assessments go much further; they examine the quality and efficacy of your security program with the goal of evaluating your readiness to face the threat of a targeted attack. Leveraging the deep knowledge and experience of the CSMA team in dealing with advanced attackers, assessments identify the weak points that allow adversaries to compromise your environment or hamper your ability to respond effectively. To this end, an assessment will help you answer the following questions:

- **What are the gaps in my cybersecurity program across people, processes and technology?**
- **How mature is my organization today? What level of maturity should it strive for? How does it compare to the maturity level of others in my industry?**
- **What can I do to improve my organization's security posture? How should I prioritize those improvement opportunities?**

HOW CROWDSTRIKE DOES IT

CrowdStrike Services reviews your existing cybersecurity program to understand how prepared you are to deal with today's most sophisticated attacks. This review includes examining your relevant internal documentation and then meeting with individuals within your organization who understand how your security works in practice. Together, you and CrowdStrike develop a profile showing where your capabilities are strong, where you can improve, and how you can mature across six key cybersecurity areas.

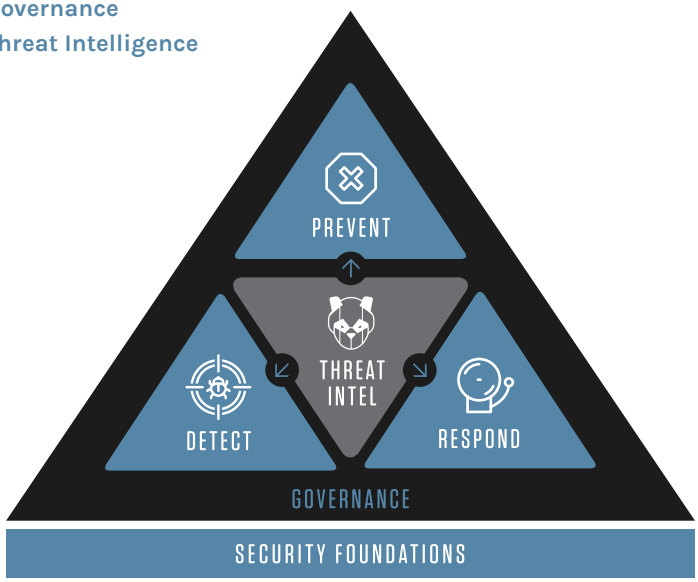
When onsite, the CrowdStrike CSMA team meets with your key staff members for about 30 to 45 minutes. Two CrowdStrike consultants perform these interviews, then spend their remaining time in interactive discussions with your security team, exploring areas that cause them the most concern.

These in-depth discussions allow the CSMA team to understand how your people, tools, and processes contribute to your current incident detection and response capabilities. They also show how security fits into the broader context of your organization's culture and operations.

ACTIONABLE GUIDANCE AND DELIVERABLES

The CrowdStrike CSMA methodology goes beyond the standard audit or information security assessment by strategically focusing on controls within areas that will assist you with your overall cybersecurity programs. These controls are placed into the following six categories:

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



Security Foundations include the basic blocking and tackling that all organizations must do to maintain a primary level of defense. Without these capabilities, even the most advanced cybersecurity program will fail:

- **Prevent** — considers all of the ways your organization can strategize to keep the adversary out
- **Detect** — identifies and ensures your organization's security infrastructure and processes include mechanisms to account for everything that gets through (and there will always be something that does)
- **Respond** — speaks to how efficiently your organization can respond once a threat is detected
- **Governance** — refers to the structure that supports the the three areas identified above and any existing threat intelligence capabilities within the organization

ACTIONABLE GUIDANCE INCLUDES:

- **An assessment of your organization's current maturity, a recommended target maturity, and a view into the range of maturities for others in your industry**
- **The CrowdStrike team's observations and findings from the documentation review and discussions**
- **A prioritization of recommended actions your organization should take to improve its cybersecurity maturity with a rating of each action's criticality, cost and implementation difficulty, integrated into a roadmap view of short-, medium-, and long-term implementation strategies**

ADD-ON SERVICES

CrowdStrike Services offers several options for add-on services to build on and customize the CSMA to better suit your organization's cybersecurity maturity needs.

Detailed Roadmap: Builds on the CSMA assessment by reviewing CrowdStrike's recommendations in the context of your organization's priorities and existing plans, and develops a recommended sequence for implementing them. This includes a Gantt chart of the proposed roadmap and descriptions of how each recommendation affects your overall maturity and the factors involved in implementing them.

Detailed Roadmap + Health Checks: Builds on the detailed roadmap described above with quarterly reviews of your progress toward implementing your roadmap. The goal is to help you resolve any issues you encounter and revise the roadmap as necessary. Optionally, a CrowdStrike executive can brief your board on an annual basis to discuss the threat landscape and CrowdStrike Services' engagement with you over the course of the preceding year.

Technical Hygiene Assessment: This augments the CSMA's document review and in-person interviews with a hands-on technical assessment of your network. The CrowdStrike team manually tests software configurations and patching levels, access controls and permissions, network defense configurations, and more.

LEARN HOW CROWDSTRIKE STOPS BREACHES:

VISIT WWW.CROWDSTRIKE.COM/SERVICES

Speak to a representative to learn more about how CrowdStrike Services can help you prepare for and defend against targeted attacks.

LET'S DISCUSS YOUR NEEDS

Phone: 1.888.512.8906
Email: sales@crowdstrike.com
Web: http://www.crowdstrike.com/services

COMPARING THE CSMA TO NIST CSF AND THE CRITICAL SECURITY CONTROLS (CSC):

You may wonder why CrowdStrike doesn't leverage your industry standard of choice. The answer is straightforward: Those frameworks are intended to be building blocks — you choose what matters most to you and self-assess based on the gaps against the controls identified. There's no sense of prioritization or developing a roadmap to address the gaps in a meaningful way. These frameworks are also reliant on assessing the existence of certain controls, rather than the maturity of them.

The CrowdStrike CSMA looks at cybersecurity with an eye toward companies' capabilities for detecting, preventing, and responding to targeted attacks that have the most impact on your organization.

The CrowdStrike assessment:

- **Examines customer-specific threats**
- **Addresses the importance of having a mature function rather than just the existence of one**
- **Provides meaningful recommendations for improvement along a prioritized roadmap that is achievable**

COMMON INDUSTRY FRAMEWORKS ARE USEFUL AS A DIAGNOSTIC TOOL, BUT THE CROWDSTRIKE CSMA HELPS YOU BECOME OPERATIONAL.

The following chart maps CrowdStrike CSMA key focus areas to the functional categories found in the NIST CSF and CSC Top 20 frameworks. CSMA assessments go beyond these frameworks, but they also cover each of the topics addressed by them, and more.

CROWDSTRIKE CSMA	NIST CSF FUNCTIONS AND CATEGORIES					CSC
	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER	
SECURITY FOUNDATIONS						
Asset management and maintenance	AM	DS, IP, MA				1, 2
Data classification	AM	DS				
Testing and exercises	DP			IM	IM	20
Operational baselines	AM	IP	AE			
Backups		IP				10
PREVENTION						
Access controls		AC, PT				14, 15
Security architecture and segmentation		AC, DS				7, 9, 11, 12
Hardening		DS				3, 11
Patching and vulnerability management	RA	IP	CM			4
Account / Authentication management		AC				5, 16
Preventive technologies		DS, PT				7, 8, 13
Secure development		DS				18
DETECTION						
Log management and analysis		PT	AE	AN		6
Detection technologies			CM			8
Monitoring process			AE, CM, DP			
Proactive hunting						

CROWDSTRIKE CSMA	NIST CSF FUNCTIONS AND CATEGORIES					CSC
	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER	
RESPONSE						
Triage	AE		AE, DP	AN		
Plans and playbooks		IP		RP, CO	RC	19
Communications and escalation protocols			AE, DP	CO	CO	
Roles and responsibilities				CO		19
Forensic analysis				AN		
Containment and eradication				MI		19
Root cause and lessons learned				AN, MI	IM	
GOVERNANCE						
Plans, policies, and procedures	BE, GV					
Security culture		AT				
Awareness and training		AT				17
Risk management	GV, RM					
Executive management	BE, GV	AT				
THREAT INTELLIGENCE						
Risk identification	RA					
Strategic intelligence	RA, RM					
Operational intelligence	RA					
Intelligence sources	RA					

Please see page 19 of the **Framework for Improving Critical Infrastructure Cybersecurity** for further explanation of the Functions and Categories above.