CROWDSTRIKE

CYBERSECURITY MATURITY ASSESSMENT

Taking a wide-angle look across your cybersecurity program

SPECIFIC GUIDANCE ON HOW TO IMPROVE YOUR CYBERSECURITY MATURITY

The CrowdStrike® Services Cybersecurity Maturity Assessment (CSMA) is designed to evaluate an organization's overall cybersecurity posture. The assessment provides a clear sense of how mature the organization's current capabilities are, how mature they should be to address the threats facing the organization, and how to get from the current to the target state.

The CrowdStrike CSMA is not a compliance exercise — it is focused on ensuring that the people, processes and technologies securing your organization are properly calibrated to defend against sophisticated modern attackers. While CrowdStrike incorporates all of the functional areas of the National Institute of Standards and Technology (NIST) Cybersecurity Framework and each of the Center for Internet Security (CIS) Top 20 Critical Security Controls, they are emphasized differently and incorporate other security functions that the CrowdStrike Services team sees as critical to mounting an effective defense. CrowdStrike's maturity model focuses on six key cybersecurity capabilities: security foundations, detection, prevention, response, governance and threat intelligence.

KEY BENEFITS

Identifies Weak Points: Proactively discovers gaps in your cybersecurity program that put your organization at greater risk

Focuses Improvement Efforts: Provides customized, detailed recommendations on how to improve your maturity

KEY CAPABILITIES

A HIGHLY SKILLED TEAM

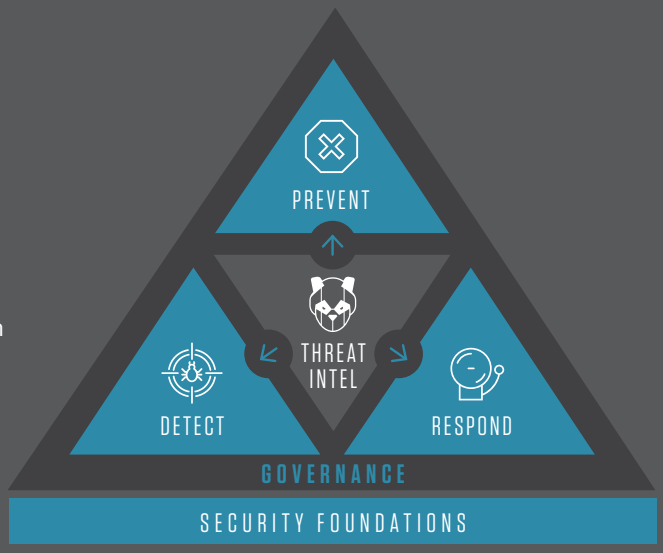
- The CrowdStrike Services team comprises seasoned security professionals with unrivalled expertise and firsthand insight into the cybersecurity programs of organizations across industries, sizes and geographies. The CrowdStrike team's deep knowledge of the tactics, techniques and procedures (TTPs) leveraged by today's most skilled adversaries grounds their assessment methodology in the areas likely to be exploited in the current threat landscape.

A TAILORED APPROACH

- By reviewing your organization's relevant internal cybersecurity documentation and interviewing your employees, the Services team seeks to assess how your existing cybersecurity program functions and also evaluate the risk profile of your organization. The team "right-sizes" its recommendations to reflect the unique risk factors and operational realities that your organization faces, ensuring that the targets set for you are attainable.
- Customers who want additional technical insights can deploy the CrowdStrike Falcon® platform. CrowdStrike consultants use it to enrich their assessment with technical data relevant to security hygiene. For example, they use the Falcon Spotlight™ module to identify unpatched vulnerabilities and the Falcon Discover™ module to identify unencrypted systems or user accounts with poor password hygiene.

CROWDSTRIKE'S CYBERSECURITY MATURITY MODEL

CrowdStrike developed its Cybersecurity Maturity Model as an alternative to box-checking, audit-focused security assessments. CrowdStrike uses this model to help customers answer an important question: How mature is an organization's ability to meet the threats posed by today's most advanced adversaries?



CORE SECURITY FUNCTIONS	ENABLING FUNCTIONS
Prevention: The tools and tactics to keep adversaries out and limit what actions an attacker with access can perform	**Security Foundations:** Fundamental IT management activities required to maintain a primary level of defense
Detection: Mechanisms to identify and assess attacks that are not prevented	**Governance:** Cultural factors, formal processes and risk management frameworks that support cybersecurity efforts
Response: Processes and methods to handle an attack once it is detected	**Threat Intelligence:** The use of information about threats to shape security strategy and operations

ACTIONABLE ANALYSIS AND FINDINGS

CrowdStrike recognizes that for a maturity assessment to be successful, the findings and analysis reports must be actionable. Reporting provided by CrowdStrike consultants may include:

A detailed report showing your organization's current and targeted maturity levels across each of the six key capabilities, as well as comparisons to organizations with similar risk profiles. The report also includes comprehensive recommendations that are prioritized and specify how to achieve the targeted maturity levels.

A brief executive summary report that summarizes the scope of the assessment, the primary strengths, areas for improvement and associated recommendations noted during the assessment.

Specific insights relating to the organization's technical hygiene based on data collected by the Falcon platform (optional).

CYBERSECURITY MATURITY ASSESSMENT

CrowdStrike CSMA	NIST Cybersecurity Framework Categories					CIS Critical Security Controls
	Identify	Protect	Detect	Respond	Recover	
Security Foundations						
Asset management and maintenance	AM	DS, IP, MA				1, 2
Configuration management	AM	DS, IP, MA				1, 2, 5
Identity and access management		AC				14, 16
Business continuity and disaster recovery		IP		RP, IM	RP	10, 20
Data architecture	AM, BE	DS				13
Patching and vulnerability management	RA	IP	CM	IM, MI	IM	3, 18
Prevention						
Data loss prevention	AM	DS, PT, IP	AE, DP			13
Email and browser security		PT				7
Privileged account management	AM	AC, AT				4, 14, 16
Access controls		AC, PT				14, 15
Network architecture and segmentation		AC, DS, PT				11, 12
Endpoint security and hardening		DS, IP, PT				5, 7, 8, 9
Detection						
Log management and analysis		PT	AE	AN		6
Detection technologies			AE, CM			7, 8
Monitoring process			AE, CM, DP	AN		6
Proactive hunting						
Response						
Triage and analysis			AE, DP	AN		6
Plans and playbooks		IP		RP, CO	RP	19
Exercises			DP			20
Communications and escalation protocols			AE, DP	CO	CO	
Roles and responsibilities				CO		19
Containment and eradication				MI		
Root cause and lessons learned				AN, IM	IM	
Governance						
Plans, policies and procedures	BE, GV	IP				
Security culture, awareness and training		AT				17
Risk management	GV, RA, RM					
Third-party risk management	SC	AT				
Planning and strategy						
Security organizational structure						
Executive management	BE, GV	AT				
Threat Intelligence						
Planning and direction						
Collection and processing	RA					
Ingestion and automation						
Analysis and production	RA					

NIST Cybersecurity Framework Categories

AC Access Control
AE Anomalies and Events
AM Asset Management
AN Analysis
AT Awareness and Training
BE Business Environment
CM Security Continuous Monitoring
CO Communications
DP Detection Processes
DS Data Security
GV Governance
IM Improvements
IP Information Protection
MA Maintenance
MI Mitigation
PT Protective Technology
RA Risk Assessment
RM Risk Management Strategy
RP Response Planning
SC Supply Chain

CIS Critical Security Controls

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

ABOUT CROWDSTRIKE SERVICES

CrowdStrike Services delivers Incident Response, Technical Assessments, Training, and Advisory Services that help you prepare to defend against advanced threats, respond to widespread attacks, and enhance your cybersecurity practices and controls.

We help our customers assess and enhance their cybersecurity posture, test their defenses against real-world attacks, respond to incidents, accelerate forensic investigations, and recover from a breach with speed and precision. Harnessing the power of our Security Cloud and the CrowdStrike Falcon® platform, we help you protect critical areas of enterprise risk and hunt for threats using adversary focused cyber threat intelligence to identify, track and prevent attacks from impacting your business and brand.

CrowdStrike: **We stop breaches.**

Learn more at **www.crowdstrike.com/services/**
Email: **services@crowdstrike.com**