leidos

# Cyber Defense Maturity Scorecard

## DEFINING CYBERSECURITY MATURITY ACROSS KEY DOMAINS

# Cyber Defense Maturity Scorecard

**DEFINING CYBERSECURITY MATURITY ACROSS KEY DOMAINS**

Continual disclosed and reported breaches provide testament to the evolving threat landscape elevating cybersecurity concerns all the way to the board room. Security executives tasked with preventing their organization from being the next victim headlining the news must evaluate the current state of their cybersecurity posture and then execute a sustainable plan to mature that posture.

## What does success look like?

We've outlined key considerations across thirteen key process areas with a description of an ideal 4.0 state for each domain.

| KEY PROCESS AREA CONSIDERATIONS | IDEAL STATE / LEVEL 4 |
|---|---|
| Organization and Mission<br>▸ How is the team organized?<br>▸ What is the organization's overall mission?<br>▸ Are there other drivers that either impact or enhance the overall mission?<br>▸ How is the threat landscape understood across the enterprise? | Security entities within the enterprise are established and the cybersecurity mission and vision is aligned to roles and responsibilities of personnel, securing the enterprise, and actively defending it. The threat landscape is understood by security stakeholders; and creating, understanding, analyzing, and leveraging threat intelligence of broad-based and sophisticated Advanced Persistent Threats (APTs) is executed to defend the enterprise against such threats. |
| Executive Support<br>▸ What type of leadership support exists for the security organization?<br>▸ How far up the organization does this support go?<br>▸ Is there sufficient funding to support the mission of the organization? | Management has a full understanding of the threats and how the associated risk affects the organization, driving elements of governance and risk management. Management has an established trust with the security organization and has empowered them to implement critical mitigations in real-time. Financial and technical support is aligned with mission and threat profile. There is adequate balance of business impact and security need. |

| KEY PROCESS AREA CONSIDERATIONS | IDEAL STATE / LEVEL 4 |
| --- | --- |
| Architecture and Engineering<br>▸ How is the perimeter protected?<br>▸ Are all entry points known and documented?<br>▸ What are the drivers for the perimeter protection strategy?<br>▸ Does the enterprise have a cloud strategy aligned to internal capabilities?<br>▸ Does architecture direct and implement a thorough network segmentation model?<br>▸ How are network and endpoint infrastructure baselines hardened and maintained? | The network and perimeter security strategy includes best practices and regulatory requirements driven by a holistic understanding of the adversary Tactics, Techniques, and Procedures (TTPs) and emerging threat intelligence. Organization possesses a comprehensive understanding of the network topology, boundaries, and security controls thorough documentation and technical mechanisms, providing observation of key network flows across the perimeter and throughout the enterprise. Perimeter devices are tightly integrated with enterprise log collection and management capabilities, policies and rule-based controls are dynamic and tailored to specific threats, and there is multi-level analysis of all cross-perimeter traffic flows. Foundational endpoint management practices and hardening are defined and operationalized for all systems and broad-based vulnerabilities are minimized to reduce threat vectors. For cloud footprints, parallel capabilities for detection and response are established and standardized under the enterprise framework. |
| Security Technology<br>▸ Are network malware detonation tools a part of security operations?<br>▸ How is network intrusion detection and prevention leveraged?<br>▸ Is Full Packet Capture used for historical network analysis?<br>▸ What capabilities are in place for email hygiene and malware analysis?<br>▸ How is web traffic controlled, both for inbound services and outbound connectivity?<br>▸ What are the drivers for the endpoint protection strategy?<br>▸ Who has admin access to the endpoints and host devices?<br>▸ What is the strategy for implementing protections? | Network, email, web, and endpoint security tools are deployed with visibility, detection, and prevention factors used to drive decisions. Security solutions protect both external connectivity and internal network segments from attackers. Assets are balanced between Commercial Off-the-Shelf (COTS) technology and custom capabilities to address broad-based and advanced attackers. |

| KEY PROCESS AREA CONSIDERATIONS | IDEAL STATE / LEVEL 4 |
|---|---|
| **Enterprise User Awareness**<br>▸ What user training and awareness programs exist?<br>▸ Are they general in nature or focused on specific threats?<br>▸ What metrics are captured from awareness and training initiatives? | In a mature, intelligence-enabled organization, training initiatives and campaigns include general awareness, compliance, and focused training based on observed attack activity. High-risk users receive specific training to help them identify potential adversarial activity and avoid risky behaviors. Finally, proactive testing of the user base is performed, producing metrics that gauge the training program's effectiveness at increasing user awareness and the overall security posture. |
| **Enterprise Visibility and Monitoring**<br>▸ How is network visibility achieved?<br>▸ Is the security team aware of all network boundaries and enclaves?<br>▸ What types of detections occur?<br>▸ What are the detections based on?<br>▸ Where do the indicators for these detections come from?<br>▸ Are the indicators used as-is or customized to the specific network topology?<br>▸ What occurs when a detection triggers?<br>▸ Is the action manual or automatic?<br>▸ What is done when a false positive detection occurs?<br>▸ What types of logs are kept?<br>▸ What is the retention policy?<br>▸ How are the logs managed?<br>▸ Who has immediate access to log data?<br>▸ Are the logs stored centrally or distributed?<br>▸ How are the logs correlated? | Enterprise has a log management strategy with comprehensive visibility into network and system assets. Use cases are defined for audit, compliance, and operations. Historical and real-time use cases specific to defending the enterprise are defined and prioritized. Visibility provides complete situational awareness of the enterprise networks and observes and tracks adversarial activity. Enterprise detection capabilities are identified, configured, and assessed based on emerging threat intelligence. Detections go beyond traditional alerts and include correlations between disparate technologies and external threat intelligence. Maturity of detection technologies and processes is measured via detailed metrics and proactive testing. Log and event data from security controls, infrastructure devices, endpoints, and applications are collected, aggregated in a central location, and correlated against threat intelligence feeds providing enhanced detection capabilities and detailed situational awareness. Event data is readily accessible to the team tasked with monitoring and responding to alerts, enabling rapid event reconstruction and historical analysis. |
| **Malware Analysis**<br>▸ Is malware analysis performed on suspected malware?<br>▸ Is the analysis performed in-house within the organization, outsourced to a different organization, or externally?<br>▸ What are the malware analysis capabilities of the analysts? | Malware analysis and reverse engineering is critical during incident investigations to understand fully the adversary's TTPs and intentions. Includes a malware analysis function whose primary responsibility is to derive intelligence by decomposing malware artifacts and populating the intelligence management system with all discovered intelligence and indicators of compromise. Malware analysts should be integrated with Investigation Teams but able to focus on the primary mission of extracting indicators from capture malware samples. |

| KEY PROCESS AREA CONSIDERATIONS | IDEAL STATE / LEVEL 4 |
| --- | --- |
| **Response and Mitigations**<br>▸ Is host based forensics performed on compromised assets?<br>▸ Is network-based forensics performed on compromised assets?<br>▸ Is the forensics performed in-house within the organization, outsourced to a different organization, or externally?<br>▸ What are the forensics capabilities of the analysts?<br>▸ What types of mitigations are used?<br>▸ Where and how are the mitigations used?<br>▸ Are the mitigations customized and/or configured to the specific network topology?<br>▸ Once a mitigation is put in place, are there periodic reviews to see if it is still applicable or useful? | Proactive incident response plays a critical part in event investigations and actions taken as a result. Execute consistent processes and procedures tailored to attack vectors and the organization's threat exposure producing a significant opportunity for application and extraction of threat intelligence. Extract indicators from compromised assets and network flows to leverage network and host-based forensics, in conjunction with a structured analysis framework, allows analysts to fully decompose the attack and gain insight into the adversary's TTPs and intent. Enterprise mitigations and countermeasures are identified, selected, and assessed based on emerging threat intelligence, and thorough understanding of the adversary. Threat intelligence framework is leveraged to proactively implement mitigations before attacks occur and ensure mitigations against each step of the adversary's attack. Effectiveness of these mitigations is measured via detailed metrics and proactive testing. Mitigation processes include analysis of opportunities to increase situational awareness and produce further threat intelligence. |
| **Analysis Process and Skills**<br>▸ Is there a consistent methodology that is followed when performing computer network defense?<br>▸ What is the process?<br>▸ What occurs after an adversary is stopped?<br>▸ What information is collected from successful intrusions?<br>▸ Do the analysts know and understand the individual adversaries?<br>▸ Do the analysts follow an analysis methodology?<br>▸ Do the analysts understand the topology of the network being defended? | Common and specialty skill sets are balanced across the team, aligned to the core functions of security operations, including threat monitoring, network and system forensics, incident response, threat intelligence specialization, malware reverse engineering, signature creation, coding and scripting, etc. Analysis is performed within an established analysis framework, which facilitates threat intelligence through the discovery and documentation of each stage of the adversary's TTPs observed during an incident. A formalized analysis process is followed by each member of the Detection and Response Team and continues after the adversary has been stopped. Each analyst fully understands the organization's threat intelligence mission and leverages a common framework during analysis activities. A common understanding of adversary TTPs is shared among the team and evolves through production and dissemination of threat intelligence. Each analyst is able to gather, document, and communicate incident data to the team and partners, and possesses a strong understanding of the enterprise and how specific threats affect risk. |

| KEY PROCESS AREA CONSIDERATIONS | IDEAL STATE / LEVEL 4 |
| --- | --- |
| **Defender Operations**<br>▸ What types of capabilities are in place to drive automation and orchestration?<br>▸ Are network defender tools and data isolated and controlled from the rest of the enterprise?<br>▸ How is the network defense team structured?<br>▸ Are there formally defined analyst roles, responsibilities, and onboarding plans to support analyst training and growth?<br>▸ Are there longer term security projects and initiatives that cross sub-organizational boundaries?<br>▸ How are these initiatives identified, funded, and managed?<br>▸ How are the initiatives aligned to the current threat? | 24x7 dedicated monitoring and response analysts who fulfill the mission of computer network defense. Analysts work collaboratively with other teams through defined communications to support foundational and advanced capabilities necessary to provide an agile response to the ever-changing threat. This includes external partnerships to bi-directionally share cyber best practices and threat intelligence. Cybersecurity workforce management focused on establishing and maintaining onboarding plans, training and growth plans, procedures, and workflows to build up and maintain cybersecurity talent. To effectively deploy large-scale security capabilities across the enterprise aligned with emerging threats and recognized gaps, organizations must include a mechanism for capturing, tracking, and communicating enterprise security strategies and initiatives. Roadmaps, projects, and proposed capabilities are evaluated and prioritized against intelligence of attack trends, adversary TTPs, and identified weaknesses in the enterprise security posture. Process is formalized, documented, and accessible so each member of the team can understand the current posture and make informed decisions and recommendations. |
| **Intelligence Management**<br>▸ What type of intelligence is received from internal and external sources?<br>▸ How is received intelligence tagged/labeled?<br>▸ How is intelligence searched?<br>▸ How is the intelligence information managed?<br>▸ How is the intelligence utilized?<br>▸ What type of collaboration occurs:<br>» …within the organization?<br>» …with industry peers?<br>» ...with government and/or intelligence community?<br>▸ What types of information sharing agreements are in place?<br>▸ What tools exist to help facilitate sharing? | Assimilate both internal and external intelligence in a central repository that is easily searchable and accessible by the security team. Analysts can fuse intelligence from disparate incidents into Campaigns that identify broader actor trends. Utilizes available metadata to gain intelligence. Utilizes internal and partner intelligence and detections beyond what has already occurred to predict what may happen and build additional defenses. Significant internal and external collaboration resulting in detailed situational awareness. Established collaboration agreements and personal relationships to gain intelligence that can be fused with internal data. An industry leader that is sought out for opinion and analysis. Tools, technology, and facilities that enable effective collaboration among team members and with the rest of the organization. Structured framework to ensure pertinent information is exchanged and captured. |

| KEY PROCESS AREA CONSIDERATIONS | IDEAL STATE / LEVEL 4 |
| --- | --- |
| Metrics and Measuring Success<br>▸ What types of metrics are captured?<br>▸ What analysis is performed on the metrics?<br>▸ How are the metrics and analysis used?<br>▸ How well do the metrics and analysis reflect what is happening with the system? | Uses metrics to understand the effectiveness of deployed detections and mitigations and to identify gaps in the security posture. Metrics are meaningful at all levels of the security organization and provide alignment of defenses with emerging threats, identify opportunity for efficiency and provide validation of security investment. A matrix that tracks effectiveness of deployed mitigations against specific known adversary TTPs only becomes possible once an organization advances maturity in many of the other domains measured in this assessment. |
| Supporting Programs<br>▸ How are assets identified, tracked, and decommissioned as part of a system development lifecycle?<br>▸ Is a comprehensive vulnerability management program in place to identify, track, and remediate weaknesses within the organization?<br>▸ What security testing programs or policies exist?<br>▸ Does a dedicated insider risk program exist?<br>▸ Does physical security defenses integrate with logical network strategies? | Foundational security programs are crucial to the success of securing the enterprise, so defending the enterprise is more effective and focused. Dedicated entities and programs have direct correlations with cybersecurity including areas such as asset management, vulnerability management, assessments and security testing, insider risk, and physical security. |

Above and beyond industry best practices and compliance-driven security programs, our Unified Enterprise Defense framework has proven successful and been adopted by network defenders around the globe. An evaluation like no other, the Leidos Cyber Defense Maturity Evaluation considers the “how” rather than the “what,” helping organizations engineer and align themselves to defend, sustain, and outpace evolving attackers. Talk to a cybersecurity expert today!

**FOR MORE INFORMATION**

855-56-CYBER / cyber.security@leidos.com
cyber.leidos.com



XX-LH-V0