BitLyft
CYBERSECURITY

The Security Operations Maturity Model Quick Reference Guide for Education

The education sector comes bottom of the class when it comes to cybersecurity. A recent survey rated the sector last of the 17 sectors ranked.[1]

Educational institutions are targets for cyberattacks for many reasons. Most commonly, the motive is financial gain (70 percent). Eleven percent of attacks were "just for fun," and of the rest – almost one in five – were driven by espionage.[2] Whether it's personal information on students,[3] faculty, staff and alumni, or classified research, educational institutions are ripe for cyberattacks.

Educational institutions are a serious target for some very serious cybercriminals. As of March 2019, at least 27 U.S. universities have been targeted to obtain sensitive research on naval technologies.[4]

The first step to defending against such attacks is for an organization to assess its cybersecurity maturity. A complete, honest view of the entire organization's capabilities and weaknesses can then drive an informed discussion on next steps.

[1] 3 cybersecurity focus areas for education institutions in 2019, EdTech, Dec. 14, 2018
[2] Report: 7 in 10 Attempted Data Breaches in Education are Financially Motivated, Campus Technology, April 19, 2018
[3] Multiple Phishing Attacks Target Top Universities, Security Now, Oct. 26, 2018
[4] Significant Cyber Incidents, Center for Strategic and International Studies, Dec. 15, 2018

LogRhythm®
The Security Intelligence Company

The Security Operations Maturity Model

LogRhythm developed the Security Operations Maturity Model (SOMM) to assess an organization's current maturity and plan for improved maturity across time. Organizations should use this model as a basis to evaluate their current security operations maturity and develop a roadmap to achieve the level that is appropriate in the light of their resources, budget, and risk tolerance.

Improve Visibility
- Identify and eliminate blind spots
- See events across different systems/domains
- Accelerate threat investigation and incident response

Decrease Response Time
- Gain insight to make better decisions
- Be organizationally efficient
- Respond more quickly to threats

Quickly Identify Threats
- Detect threats earlier in the attack lifecycle
- Surface difficult-to-detect threats
- Reduce business impact

Centralized Forensic Visibility

Mean Time to Respond

Mean Time to Detect

SOMM
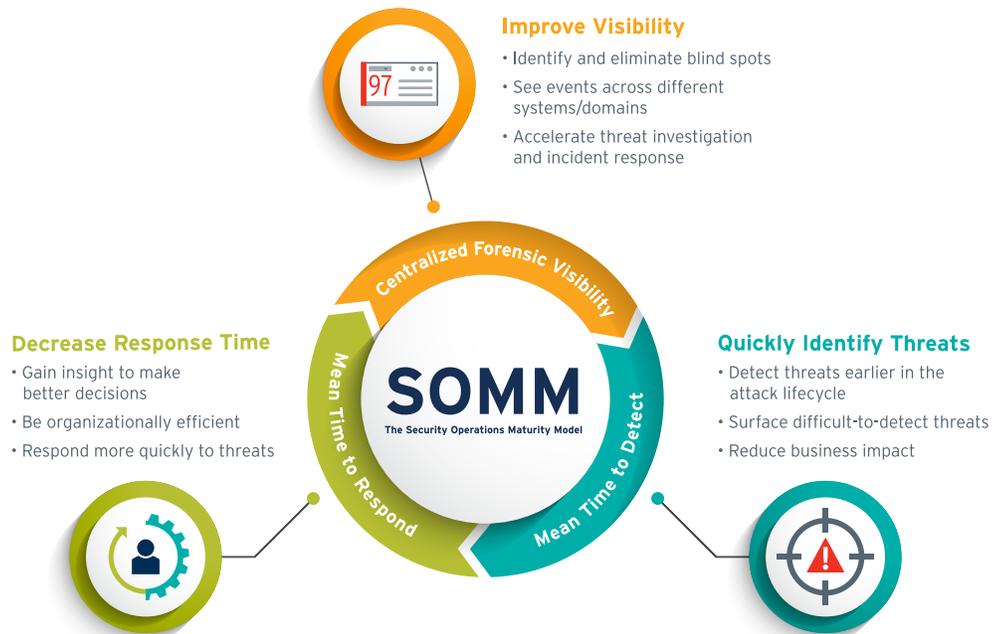The Security Operations Maturity Model

Figure 1. Reduced time to detect and respond to cyberthreats, and heightened visibility of your cyber environment are directly tied to security operations maturity

LogRhythm's model describes five levels of security operations maturity. Each level builds on the prior, adding additional technology and process improvements that strengthen the capabilities of an organization's security operation toward mean time to detect (MTTD) and mean time to respond (MTTR) reductions. Organizations can achieve lower MTTD and MTTR by using LogRhythm's Threat Lifecycle Management (TLM) framework — a set of critical capabilities that align technology, people, and process to support the principle programs of the security operations center (SOC).

The following table describes each level in further detail, identifying the key TLM technological and workflow/process capabilities that should be realized.

	TLM Capabilities	Organizational Characteristics	Risk Characteristics
LEVEL 0 Blind	• None	• Prevention-oriented (e.g., firewalls, antivirus, etc. in place) • Isolated logging based on technology and functional silos; no central logging visibility • Indicators of threat and compromise exist, they are not visible and threat hunting is not occurring to surface them • No formal incident response process; response due to individual heroic efforts	• Non-compliance • Blind to insider threats • Blind to external threats • Blind to advanced persistent threats (APTs) • Potentially stolen IP (if of interest to nation-states or cybercriminals)
LEVEL 1 Minimally Compliant	• Mandated log data and security event centralization • Mandated compliance-centric server forensics, such as file integrity monitoring and endpoint detection response (EDR) • Minimal compliance-mandated monitoring and response	• Compliance-driven investment or have identified a specific area of environment requiring protection • Compliance risks identified via report review; process to manage violations may or may not exist • Improved visibility into threats targeting the protected domain, but lacks people and process for effective threat evaluation and prioritization • No formal incident response process; response due to individual heroic efforts	• Significantly reduced compliance risk (depending on depth of audit) • Blind to most insider threats • Blind to most external threats • Blind to APTs • Potentially stolen IP (if of interest to nation-states or cybercriminals)
LEVEL 2 Securely Compliant	• Targeted log data and security event centralization • Targeted server and endpoint forensics • Targeted environmental risk characterization • Reactive and manual vulnerability intelligence workflow • Reactive and manual threat intelligence workflow • Basic machine analytics for correlation and alarm prioritization • Basic monitoring and response processes established	• Moving beyond minimal, "check box" compliance, seeking efficiencies and improved assurance • Have recognized organization is effectively blind to most threats; striving toward a material improvement that works to detect and respond to potential high-impact threats, focused on areas of highest risk • Have established formal processes and assigned responsibilities for monitoring and high-risk alarms • Have established basic, yet formal process for incident response	• Extremely resilient and highly effective compliance posture • Good visibility to insider threats, with some blind spots • Good visibility to external threats, with some blind spots • Mostly blind to APTs, but more likely to detect indicators and evidence of APTs • More resilient to cybercriminals, except those leveraging APT-type attacks or targeting blind spots • Highly vulnerable to nation-states

	TLM Capabilities	Organizational Characteristics	Risk Characteristics
LEVEL 3 Vigilant	• Holistic log data and security event centralization • Holistic server and endpoint forensics • Targeted network forensics • IOC-based threat intelligence integrated into analytics and workflow • Holistic vulnerability integration with basic correlation and workflow integration • Advanced machine analytics for IOC- and TTP-based scenario analytics for known threat detection • Targeted machine analytics for anomaly detection (e.g., via behavioral analytics) • Formal and mature monitoring and response process with standard playbooks for most common threats • Functional physical or virtual SOC • Case management for threat investigation workflow • Targeted automation of investigation and mitigation workflowv • Basic MTTD/MTTR operational metrics	• Have recognized organization is blind to many high-impact threats • Have invested in the organizational processes and headcount to significantly improve ability to detect and respond to all classes of threats • Have invested in and established a formal security operations and incident response center (SOC) that is running effectively with trained staff • Are effectively monitoring alarms and have progressed into proactive threat hunting • Are leveraging automation to improve the efficiency and speed of threat investigation and incident response processes	• Extremely resilient and highly effective compliance posture • Great visibility into, and quickly responding to insider threats • Great visibility into, and quickly responding to external threats • Good visibility to APTs, but have blind spots • Very resilient to cybercriminals, except those leveraging APT-type attacks that target blind spots • Still vulnerable to nation-states, but much more likely to detect early and respond quickly
LEVEL 4 Resilient	• Holistic log data and security event centralization • Holistic server and endpoint forensics • Holistic network forensics • Industry specific IOC- and TTP-based threat intelligence integrated into analytics and workflows • Holistic vulnerability intelligence with advanced correlation and automation workflow integration • Advanced IOC- and TTP-based scenario machine analytics for known threat detection • Advanced machine analytics for holistic anomaly detection (e.g., via multi-vector AI/ML-based behavioral analytics) • Established, documented, and mature response processes with standard playbooks for advanced threats (e.g., APTs) • Established, functional 24/7 physical or virtual SOC • Cross-organizational case management collaboration and automation • Extensive automation of investigation and mitigation workflow • Fully autonomous automation, from qualification to mitigation, for common threats • Advanced MTTD/MTTR operational metrics and historical trending	• Are a high-value target for nation-states, cyber terrorists, and organized crime • Are continuously being attacked across all potential vectors: physical, logical, social • A disruption of service or breach is intolerable and represents organizational failure at the highest level • Takes a proactive stance toward threat management and security in general • Invests in best-in-class people, technology, and processes • Have 24/7 alarm monitoring with organizational and operational redundancies in place • Have extensive proactive capabilities for threat prediction and threat hunting • Have automated threat qualification, investigation, and response processes wherever possible	• Extremely resilient and highly efficient compliance posture • Seeing and quickly responding to all classes of threats • Seeing evidence of APTs early in the Cyberattack Lifecycle and are able to strategically manage their activities • Extremely resilient to all class of cybercriminals • Can withstand and defend against the most extreme nation-state-level adversary

7 Significant Metrics to Measure in Your SOC

To determine TLM operational effectiveness, financial services organizations should measure the following:

Alarm Time to Triage (TTT): Measures latency in your team's ability to inspect an alarm

Alarm Time to Qualify (TTQ): Measures the amount of time it takes your team to fully inspect and qualify an alarm

Threat Time to Investigate (TTI): Measures the amount of time it takes your team to investigate a qualified threat

Time to Mitigate (TTM): Measures the amount of time it takes your team to mitigate an incident and eliminate immediate risk to your business

Time to Recover (TTV): Measures the amount of time it takes your team to complete full recovery of an incident

Incident Time to Detect (TTD): Measures the amount of time it takes your team to confirm and qualify an incident

Incident Time to Response (TTR): Measures the amount of time it took a confirmed incident to have been investigated and mitigated

	TTT	TTQ	TTI	TTM	TTV	TTD	TTR	TLM Stage
Earliest Evidence						↑		Collect
Alarm Creation	↑	↑						Discover
Initial Inspection	↓					↓		Qualify
Case Creation		↓	↑				↑	Investigate
Elevate to Incident			↓	↑				Investigate
Mitigate				↓			↓	Neutralize
Recovery					↕			Recover

Figure 2. Seven key metrics for measuring the effectiveness of TLM

CONCLUSION

To reduce cyber risk and improve security posture, educational institutions must invest in realizing more mature levels of Threat Lifecyle Management—across their holistic IT and operating environments.

With their distributed administrative structure and multiple departments (often across several campuses), educational institutions can lose track of the exact shape of their networks. Students that hook up unauthorized devices make security even more difficult to manage. By bringing trained IT and cybersecurity staff to the table with a full assessment,[5] real lessons can be learned.

The LogRhythm Security Operations Maturity Model provides a roadmap for success by helping organizations make material reductions in detection and response times to profoundly decrease the risk of experiencing high-impact cybersecurity incidents. Don't learn the hard way.

[5] Elevating cybersecurity on the higher education leadership agenda, Deloitte Insights, Feb. 22, 2018

BitLyft
CYBERSECURITY

Founded in 2016, BitLyft Cybersecurity offers 24/7 network threat monitoring and intervention services. BitLyft's 'white glove' SOC-as-a-Service offering augments the LogRhythm NextGen SIEM Platform which combines advanced security analytics; user and entity behavior analytics (UEBA); network detection and response (NDR); and security orchestration, automation, and response (SOAR) in a single solution.

info@bitlyft.com // www.bitlyft.com // 517.220.0990