LogRhythm®
The Security Intelligence Company

SECURITY INTELLIGENCE & ANALYTICS IN THE PUBLIC SECTOR

Focus on the Mission at Hand

Table of Contents

Executive Summary

As state agencies, civilian agencies and military branches grow more dependent on systems and communications in cyberspace, defending the underlying infrastructure and information and the data it transports is absolutely essential to our nation's security and well-being. Cyber threats are constantly evolving, and agencies must operate under the assumption that a motivated adversary can and will infiltrate their network environments.

Enormous annual investments in cybersecurity strategies, products and services have resulted in an overly complex security infrastructure that sometimes fails to detect malicious intrusions in a timely manner. This is largely due to disjointed intelligence, alert overload and a dearth of skilled cybersecurity practitioners. A security intelligence and analytics platform can actually simplify an agency's approach to cybersecurity by unifying and analyzing disjointed threat data in order to surface the important threats and provide automated response capabilities.

The main objective of a security intelligence and analytics platform is to deliver the right information, at the right time, with the appropriate context, to the right people in order to significantly decrease the amount of time it takes to detect and respond to damaging cyber threats. Such a platform takes forensic data from existing security tools (i.e., log data from firewalls and user activities from behavioral analytics systems) and aggregates, correlates, and analyzes the information. This takes the burden off people who would otherwise need to perform these activities manually to find the threats that pose the biggest risk to the agency.

A security intelligence platform can help agencies by:

- Increasing the value of their investments in existing security technology
- Discovering and alerting on threats quickly so they can be blocked or stopped
- Increasing the agency's level of security intelligence maturity
- Meeting compliance requirements for applicable standards and regulations

By following best practices to simplify security intelligence, an agency reduces the burden on its security operations team and allows technology to do the work of surfacing and responding to cybersecurity threats.

The LogRhythm Security Intelligence and Analytics Platform empowers agencies to detect, respond to and neutralize emergent cyber threats, thus preventing damaging data breaches and other cyber incidents. The deep visibility and insight delivered by LogRhythm's platform empowers agencies to secure their environment and comply with regulatory requirements.

Introduction

Civilian, military and state agencies alike have grown dependent on a complex set of networks and communications that represent their own slice of cyberspace. Due to this dependency, these complex systems are part of the United States' national critical infrastructure. Defending this infrastructure – and more importantly, the information and data it transports and holds – is essential to our nation's security and well-being. A strong cyber defense has an impact on every agency's mission success.

The threats against this infrastructure are dynamic and constantly evolving. Some threats are quite advanced and persistent in their pursuits. Threat actors are well organized and well-funded, and many of them are known to be supported by nation states. Attackers relentlessly look for vulnerabilities to exploit and patiently wait for the right time to strike. They change their tactics quickly and more easily than agencies can update their defenses. For most agencies today, if motivated adversaries want to penetrate a network, they will.

While defensive strategies are still critically essential today, it's even more important to have the ability to find and associate the subtle signs that a computer system has been compromised—and to do so quickly to have the opportunity to disrupt the attack. The time between compromise and mitigation is a period of great risk for an agency.

Unfortunately, the time it takes to discover a compromise (known as mean time to detect, or MTTD) is often measured in weeks or months. The time it takes to process sufficient intelligence about the attack in order to respond to it (known as mean time to respond, or MTTR) is too often measured in days or even weeks. Given such a lengthy head start, the attackers most likely have already succeeded in their malicious mission.

The Federal government has already invested tens if not hundreds of billions of dollars in cybersecurity strategies, products, and services. All of this investment has led to an overly complex security infrastructure that exceeds the human capacity to operate and maintain it efficiently and effectively. Incident alerts numbering in the tens of thousands each day overwhelm the security operations (OPSEC) teams who cannot possibly investigate and respond to everything.

Across the board with the public sector, there are two pervasive issues that contribute to this complexity:

- the fact that security tools are, more often than not, deployed in silos, and
- a lack of trained InfoSec professions in the cybersecurity workforce.

Security tools, and the intelligence derived from them, are often deployed in silos.

These are all valuable tools in their own right, and a layered defense using multiple tactics is critically important, but the result is a complex security environment with disjointed intelligence and too many alerts to realistically evaluate and respond to. Too often, these products aren't integrated – meaning they can't exchange and correlate data – so there is little opportunity to connect the dots that would point to an intrusion. Too many individual dots create a fog that masks the signs of an attack.

Organizations in the public sector are struggling with keeping trained personnel on staff due to the lack of trained InfoSec professionals in the workforce and frequent turnover.

This issue becomes more acute when teams spend time training a resource to become highly proficient, and then that resource leaves. This tends to happen frequently in the public sector because resources are working on a contract basis, or they go to the public sector for more attractive pay. New analysts coming in to fill the vacated roles need time to ramp up and gain similar expertise. In the meantime, the mission is jeopardized when the security team is a jack of all trades but a master of none.

With too much complexity and not enough trained people, it's crucial that DoD, civilian and state agencies simultaneously simplify and strengthen their approach to cybersecurity to be successful in their true missions and to stay a step ahead of cyber adversaries and nation states.

Making Security Intelligence a Standard Operating Procedure

You can simplify the complexity of your cybersecurity technology by surfacing visibility of the your most critical cyber threats with security intelligence and analytics. Security intelligence (SI) empowers your OPSEC team to capture, correlate, visualize and analyze forensic data in order to develop actionable insight to detect and mitigate threats that pose real harm so you can build a more proactive defense for the future.

A security intelligence and analytics platform is the overarching piece that unifies the disjointed threat data being captured or generated by your organization's various security devices. Evidence of the existence of threats can be found in log and machine data. Further visibility can be generated through endpoint and network monitoring and forensics.

When this rich data is surfaced, aggregated and correlated, and then examined using security analytics, threats and risks are clearly exposed. An effective SI platform enables a streamlined workflow across the threat detection and response lifecycle.

With intelligence and automation built into the SI platform, the burden on personnel is vastly reduced. Your agency can spend less time and money upskilling its OPSEC team members because the SI platform does the heavy lifting in terms of surfacing and qualifying the most serious threats that require investigation. The forensic information about these threats is put into context to facilitate the investigation and management by incident responders. And in many cases, automated incident response capabilities are delivered via intelligence-driven, highly integrated and automated workflows.

The expertise is built into the platform to mitigate the loss of knowledge that can result when inevitable turnover occurs in the workforce. As people rotate out of OPSEC jobs and new team members take their place, far less training and upskilling is required to get the new people to a high level of proficiency.

Using security intelligence as standard operating procedure (SOP) can help an agency detect, respond to and neutralize emergent cyber threats in less time and with fewer human resources, thus preventing damaging data breaches and cyber incidents.

Security Intelligence Simplifies the Cybersecurity Mission for Federal OPSEC Teams

There are numerous ways that an SI platform can help federal security teams. We highlight just a few of them here:

Increase the Value of Your Investment in Existing Security Technology

From the smallest of the civilian and state agencies to the behemoths of DHS and DoD, every agency and military branch has already made a tremendous investment in cybersecurity technologies, products and services. Many budget dollars over the past decade and longer have been dedicated toward preventative strategies to attempt to deter adversaries from penetrating the perimeter.

In recent years, some investments have shifted to detection capabilities on the assumption that attackers are already inside the network perimeter. In the case of insider threats, it's necessary to watch and analyze their behaviors for anomalous activities.

Despite tremendous investment, security gaps remain. Existing tools aren't integrated and don't share information. Small pieces of evidence might be found in different tools, and each tool might raise a low-level alert. But the aggregation of different tools creates an environment in which OPSEC teams are working from multiple monitors and dashboards—resulting in alarm fatigue and ineffective incident investigation when time to respond is most critical.

A security intelligence and analytics platform unifies these tools by aggregating forensic data. The forensic data includes captured log and machine data, generated forensic sensor data and event data. From this data, the SI platform builds a full picture of the security event.

Your agency can spend less time and money upskilling your OPSEC team members because the SI platform does the heavy lifting in terms of surfacing and qualifying the most serious threats that require investigation.

> The LogRhythm Security Intelligence Maturity Model offers a compelling framework to help organizations advance in their journey to combat advanced cyber attacks while simultaneously restoring confidence in the Internet.
>
> – Robert Lentz,
> Former CISO for the U.S. Department of Defense

Know the Unknown with Security Analytics

Security analytics enable your OPSEC team to detect attacks as quickly as possible so that they can be neutralized fast. It also provides crucial detailed information to reconstruct an attack, build a case for incident investigation and response, and use the data to help prevent a recurrence. This is done by collecting, correlating and analyzing a wide range of data. This entire process can be done by highly skilled people – the same people that are in very short supply today – or it can be automated with the use of security analytics tools.

Security analytics tools are a complement to existing security controls and applications, and they are an important part of an SI platform. These tools perform sophisticated activities such as advanced correlation, statistical analysis, behavioral profiling, machine learning, and forensic analysis. Vast amounts of raw data are the input to the analytical engines that search for and find needles in the haystack.

Insights are then fed back into security controls quickly via automaton to help protect the agency. For example, these tools could close ports on a firewall, implement a specific rule on the intrusion prevention system, block access from certain IP addresses, remove a device from the network, and so on.

Security analytics tools also provide analysis environments for forensic evaluations and attack reconstructions, allowing your team to study the attack methods that were used and the vulnerabilities that were exploited to breach your systems. Armed with this knowledge, your organization can fortify its weaknesses to prevent a similar attack.

Climbing the Ladder of Security Intelligence Maturity

When Robert Lentz was the Chief Information Security Officer for the DoD, his team created a Cyber Security Maturity Model to build a long-term strategic commitment to the tools, processes, staff and mindset necessary to detect and respond to advanced intruders. The model also provided the ability to measure tactical performance while institutionalizing a risk-management culture. The DoD maturity model has been adapted for widespread use as the LogRhythm Security Intelligence Maturity Model (SIMM).

The LogRhythm SIMM is designed to help agencies assess their current security intelligence capabilities and associated risk posture. The model also provides a roadmap as agencies seek to continue improving their security posture over time. The SIMM maps five levels of an organization-wide security posture, from Level 0 where an agency has virtually no security intelligence capabilities, up to Level 4, where the agency has the well-rounded capabilities to be resilient in the face of the most extreme adversary.

The model is focused on building and maturing an agency's detection and response capabilities rather than simply implementing more security products. Technology-based solutions play a critical role in supporting and enabling the various stages of the maturing model. At Level 4, the capabilities of an integrated and unified security intelligence and analytics platform support an end-to-end threat lifecycle management process.

Meet Federal Compliance Requirements

Federal oversight is tightening the noose around compliance with cybersecurity standards and government regulations. Whether it's FISMA, HIPAA, NERC-CIP, the NIST Risk Management Framework (RMF), NIST 800-53, or any other standard or regulation, compliance is compulsory. It can be a challenge to verify and demonstrate true compliance, but the penalties for non-compliance can be harsh.

A well-designed SI platform incorporates the controls and proof points that are prescribed by all major cybersecurity standards and government regulations. Ideally, an agency can simply choose which regulations apply, and the platform implements the controls and provides on-demand reports that verify compliance status. This results in an extremely resilient and highly efficient compliance posture.

Seven Ways to Simplify Security Intelligence so Your Team Can Work Smarter, Not Harder

An agency that makes use of security intelligence and analytics takes a burden off its OPSEC team and allows technology to do much of the work. Powerful machine analytics can make associations among traces of evidence and identify security events much more quickly and efficiently than humans can. Automation enables you to respond to an incident in seconds, minutes or hours, not days.

With automated incident response, your team won't be taxed with manual processes. Instead, they can run with approval-based automated operations so your analysts can review the situation before countermeasures are executed, while at the same time greatly reducing MTTR. Here are seven best practices for getting SI technology to work harder, so people can work smarter:

1. Centralize visibility and management of the entire IT environment in one platform.

Your team must have visibility across your entire IT environment and be able to manage all of its security controls through one console (i.e., "a single pane of glass") with dashboard visibility into all security tools. Think of the total environment as a hub-and-spoke configuration, with the SI platform as the hub and all other security tools as the spokes.

2. Monitor everything with an IP address.

You must consider that anything and everything with an IP address is vulnerable to attack. This includes not just endpoint devices and servers, but also badge readers, SCADA systems, medical devices, HVAC and environmental systems, video cameras, mobile devices, and any other type of device that is addressable from the outside world.

3. Understand "normal" behavior in order to detect "abnormal" behavior.

Over time, an IT environment establishes a pattern of normal activity, not only by people, but also by anything that operates or communicates on the network. Activity outside the range of what is normal could be indicative of malicious activity. A good SI platform should establish a baseline of normal behavior so that outlier activity can be identified and flagged for investigation. Sophisticated behavioral analytics can help to detect aberrations.

4. Perform continuous analysis and correlation of all activity observed in the environment.

Individual pieces of evidence might not mean much until they are correlated against other data points and analyzed for meaning. An advanced intelligence rules engine can analyze and correlate all of the security intelligence and determine when events are important enough to alert the SOC.

5. Automatically assemble forensic data so humans don't have to.

Forensic data represents the vital clues of what is happening and has happened in the environment. This data comes from multiple sources, sometimes over long spans of time. Manually assembling this data is time consuming and cumbersome. Allow the SI platform to assemble all of this information automatically and present it in a way that will speed up the human response to a security event.

6. Automate incident response.

There are some situations where a response can be automated in order to mitigate a threat quickly; for example, to take a device off the network if it is found to have a virus, or to insert a firewall rule to block a malicious IP address. Develop a process to automate responses according to your organization's preferred policies. Automation can give your team efficient workflows and a flexible approval process to reduce the manual burden on your workforce, while at the same time reducing time to respond to an incident.

7. Share threat intelligence with other agencies.

If threats are hitting one agency, chances are they are hitting others too. DHS is a conduit for sharing threat intelligence among Federal agencies and military branches.

How LogRhythm Can Help

LogRhythm empowers agencies to detect, respond to and neutralize emergent cyber threats, preventing damaging data breaches and cyber incidents.

LogRhythm takes a unified platform approach to security intelligence and analytics that provides the technology foundation to realize a highly efficient security operation across all stages of the threat lifecycle. The LogRhythm Security Intelligence and Analytics Platform is built as an integrated product suite, where all components are designed to effectively and efficiently work as a whole.

While the full suite of capabilities will be leveraged by those agencies seeking to reach the higher levels of security intelligence maturity, those agencies that are just starting their journey toward SI maturity can start with specific products and build on their investment over time. The security technologies that already exist in an agency's IT environment can be incorporated into the platform through product integrations and data exchanges.

The LogRhythm Security Intelligence and Analytics Platform integrates:

- Next-generation SIEM and log management
- Endpoint forensics, with registry and file integrity monitoring
- Network forensics, with application identification and full packet capture
- Behavioral analytics for holistic threat detection (users, networks and endpoints)
- End-to-end incident response orchestration workflows to support team collaboration
- Smart**Response**™ automation framework

LogRhythm addresses today's most sophisticated cyber threats. The platform attains full visibility by aggregating log and machine data with network and endpoint data. LogRhythm's patented machine analytics technology continually performs real-time analysis on this environmental activity, helping identify previously unknown threats. When a threat is detected, analysts can quickly qualify and investigate it by pivoting and drilling down into rich forensic data. The platform's collaborative incident response orchestration and patented Smart Response**™ automation framework help security teams efficiently perform threat lifecycle management.**

The deep visibility and understanding delivered by LogRhythm's Security Intelligence and Analytics Platform empowers agencies to secure their environment and comply with regulatory requirements.

Conclusion

Cyber threats pose a risk to agencies accomplishing their designated missions. It's not possible to prevent all threats from affecting an agency's IT environment. This makes threat detection and response capabilities an essential requirement. Security intelligence and analytics, delivered through a unified platform, is the best approach to threat detection and response.

Contact the LogRhythm Federal Team to schedule a demonstration of the LogRhythm Security Intelligence and Analytics Platform and learn how this solution can protect your agency from a world of rapidly evolving cyber threats.

DefenseTeam@LogRhythm.com

Glossary of Acronyms

A/V	anti-virus
DHS:	Department of Homeland Security
DLP:	data loss prevent system
DoD:	Department of Defense
FISMA:	the Federal Information Security Management Act
HIPAA:	the Health Insurance Portability and Accountability Act
HVAC:	heating, ventilation and air conditioning
IDS:	intrusion detection system
InfoSec:	information security
IPS:	intrusion prevention system
IT:	information technology
MTTD:	mean time to detect
MTTR:	mean time to respond
NERC-CIP:	the North American Electric Reliability Corporation Critical Infrastructure Protection regulation
NIST:	National Institute of Standards and Technology
RMF:	Risk Management Framework
SCADA:	supervisory control and data acquisition
SI:	security intelligence
SIEM:	security information and event management
SIMM:	Security Intelligence Maturity Model
SOC:	security operations center
SOP:	standard operating procedure
UBA:	user behavioral analysis