Surfacing Critical Cyber Threats Through Security Intelligence

A Reference Model for IT Security Practitioners

By:
Christopher Petersen
CTO & Co-Founder of LogRhythm

With a Foreword By:
Robert Lentz
Former CISO for the U.S. Department of Defense

IN MY 10 years as the CISO for the largest information enterprise in the world, the U.S. Department of Defense, we realized after numerous cyber incidents that leadership commitment was severely lacking and that victim organizations did not possess the tools, processes, staff, or mindset necessary to detect and respond to advanced intruders. Accordingly, we developed the Cyber Security Maturity Model to create a long term strategic commitment and an ability to measure tactical performance while institutionalizing a risk management culture.

The significant and successful cyber events of 2014 might well prove to be the cyber tipping point, where businesses and governments together finally acknowledge the fragility of their enterprises, the grave threat to national and economic security, and the need for executive-level oversight. 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.

"Harnessing the intelligence resident on your own network is absolutely essential in detecting today's sophisticated threats. Unfortunately, too many organizations are leaving it on the cutting room floor."

COL John Burger USA (Ret)
Chief, USCENTCOM Joint Cyber Center (2012-2014)

Robert Lentz

Former CISO for the U.S. Department of Defense

Introduction

It's almost quaint and more than a bit naive to look back on the days when an enterprise felt it could install a few firewalls and some anti-virus software and feel confident that the organization was well defended against cyber threats. Those days weren't so long ago, but much has changed in a few short years.

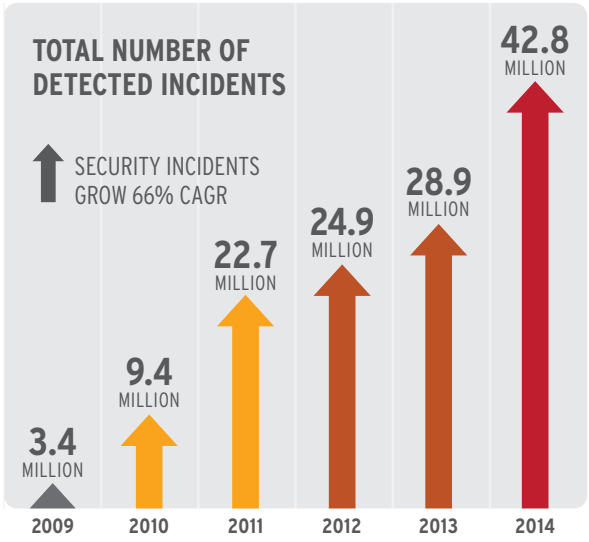
IT environments have become much more vulnerable as enterprise mobility, cloud services and "bring-your-own-everything" have broken down the defensible perimeter and added layers of complexity to securing the enterprise. At the same time, the nature of cyber threats has changed dramatically. Threat actors are well organized and well funded, and many of them are known to be supported by nation states. They have sophisticated technical skills which allow these actors to create custom malware for very specific targets, and they are relentless in pursuit of their objectives. Moreover, almost anyone with a malicious intent can purchase malware and rent botnets on the Dark Web, lowering the bar for criminal entities, nation states, and terrorists to use cyber as a weapon of choice towards their intended purpose.

The reality today is that for most organizations, if a motivated adversary wants to penetrate their network, they will get in.

Many organizations continue to focus their attention on identifying and blocking threats at the perimeter—or at least what's left of it. Unfortunately, prevention-centric strategies are failing and have failed in some of the largest attacks that have made recent headlines. Attackers are known to conduct reconnaissance to find a weakness in the armor. Attempting to prevent attacks is still important, but organizations must acknowledge that attacks that are stealthy by nature can be crafted to get past the preventive measures.

Cyber attacks now take place on an industrial scale. The 2015 Global State of Information Security Survey shows that the compound annual growth rate (CAGR) of detected security incidents has increased 66 percent year-over-year since 2009. (See Figure 1.) Survey respondents acknowledge detecting a total number of 42.8 million security incidents in 2014—an increase of 48 percent over incidents detected in 2013. That's the equivalent of 117,339 incoming attacks per day, every day, and that's only what has been detected and reported.[1] One cyber security company recently estimated that as many as 71 percent of compromises go undetected.[2]

Figure 1: The number of detected incidents keeps growing year after year



Source: PwC, The Global State of Information Security Survey 2015

In a relatively short time span, cyber security has become a major concern for government agencies, military branches, companies across every industry, financial institutions, law enforcement, and many regulators. The World Economic Forum says the theft of information and the intentional disruption of online or digital

[1] PwC, *The Global State of Information Security Survey 2015*, www.pwc.com/gsiss2015
[2] Trustwave Holdings, 2014 *Trustwave Global Security Report*, May 2014

processes are among the leading business risks that organizations face today. Research by BAE Systems confirms that notion: more than half of U.S. companies now regard the threat from cyber attacks as one of their top three business risks.[3]

The reality today is that for most organizations, if a motivated adversary wants to penetrate their network, they will get in. Practically speaking, organizations have to adopt the mindset of "If we are not compromised right now, we could be at any moment." They must work under the assumption that the network is untrusted and is already or soon to be compromised.

A fundamental shift is beginning to take place in terms of the overall approach enterprises now have toward delivering cyber security to the organization. Given the notion that the computing environment might already be compromised, CISOs are directing a shift of processes and priorities toward detecting when those compromises occur and responding to them as quickly as possible. They know they can't spend all of their resources trying to build and maintain a seemingly impenetrable fortress that is now recognized as something that is painfully impossible to have.

Analyst firms are strongly advocating a rebalancing of the cyber security budget, shifting some funds from pure prevention to detection and response. Neil MacDonald, vice president, distinguished analyst and Gartner fellow emeritus at Gartner Inc., wrote, "In 2020, enterprise systems will be in a state of continuous compromise. They will be unable to prevent advanced targeted attacks from gaining a foothold on their systems. Unfortunately, most enterprise information security spending to date has focused on prevention, in a misguided attempt to prevent all attacks." He adds, "We believe the majority of information security spending will shift to support rapid detection and response capabilities, which are subsequently linked to protection systems to block further spread of the attack." MacDonald's report includes a key recommendation: "Invest in your incident response capabilities. Define and staff a process to quickly understand the scope and impact of a detected breach."[4]

In 2020, enterprise systems will be in a state of continuous compromise. They will be unable to prevent advanced targeted attacks from gaining a foothold on their systems.

This is not to suggest that threat prevention itself is obsolete. On the contrary, organizations should continue to buttress the network fortress to protect the IT infrastructure and the assets within, but they should also accept that those walls will eventually be scaled by the cyber equivalent of a marauder. The sooner the intruder can be detected and a response initiated, the less likely it is that the mission of the attack will be successful. Above all, organizations don't want the attacker to actually get to the data and exfiltrate it before they even know he is there.

[3] BAE Systems, *Business and the Cyber Threat: The Rise of Digital Criminality*, February 2014

[4] Neil MacDonald, Gartner, Inc., *Prevention is Futile in 2020: Protect Information Via Pervasive Monitoring and Collective Intelligence*, 30 May 2013

A Time of Great Risk: The Time Between Compromise and Mitigation

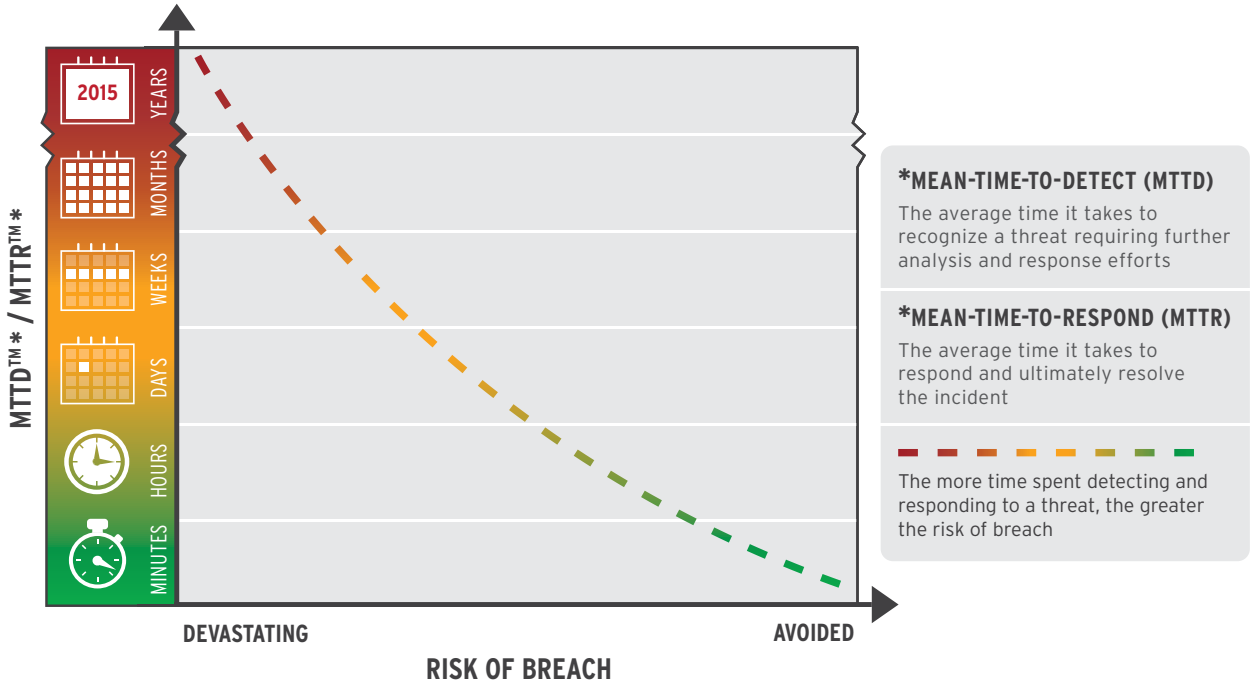
In most organizations today, threat detection is based on various security sensors that attempt to look for anomalous behavior or for known signatures of malicious activity. These sensors include firewalls, intrusion detection/prevention systems (IDS/IPS), application gateways, anti-virus/anti-malware, endpoint protection, and more. They operate at and provide visibility into all layers of the IT stack.

These security sensors provide a continuous stream of threat-related events. In enterprise organizations, the stream might be better described as a fire hose that serves events at the rate of thousands or tens of thousands per hour. This intense stream of threat data effectively blinds a security team in a fog of noise. The team has so much to deal with that it can't identify the threats that really matter – let alone respond to them – in a timely manner.

Two key metrics for measuring the effectiveness of an organization's security capabilities are its Mean-Time-to-Detect™ (MTTD™) and its Mean-Time-to-Respond™ (MTTR™). The MTTD is the average amount of time it takes an organization to identify those threats that could potentially impact the organization—the ones that present an actual risk and which require further analysis and response efforts. The MTTR is the average amount of time it takes an organization to fully analyze the threat and mitigate any risk presented.

Unfortunately, many organizations operate in a mode where MTTD and MTTR would be measured in weeks or months. Enterprises whose networks have been compromised are at high risk during this time. If they are seeking to reduce their cyber security risk, they should minimally move these metrics into hours and days, and ideally to hours and minutes.

Figure 2: The impact of a breach is directly related to MTTD and MTTR



Research data from Trustwave illustrates the problem. The company looked at evidence gathered from 691 data breach investigations spread across industries and the world. Trustwave learned that 71 percent of compromise victims did not detect the breach themselves. Financial institutions, law enforcement agencies and other third parties are often the first to suspect that a company has experienced a security incident. In the breaches in this particular study, the MTTD was 87 days – nearly three full months – and the MTTR was a week. According to Trustwave, self-detection of a threat can shorten the timeline from detection to containment from 14 days down to one.[5]

The Security Intelligence Imperative

The way to bring visibility to the most important threats while clearing the fog of noise is with Security Intelligence (SI). Just as Business Intelligence has helped numerous organizations clear the fog of too many points of seemingly extraneous business data to find previously unknown business opportunities, Security Intelligence does much the same thing with threat information, enabling companies to clearly see the threats that matter. The main objective of Security Intelligence is to deliver the right information, at the right time, with the appropriate context, to significantly decrease the amount of time it takes to detect and respond to damaging cyber threats; in other words, to significantly improve an organization's MTTD and MTTR.

The main objective of Security Intelligence is to deliver the right information, at the right time, with the appropriate context, to significantly decrease the amount of time it takes to detect and respond to damaging cyber threats

There's no standard definition for Security Intelligence; it means different things to different companies. This composite definition helps to get us on the same page.

Security Intelligence is the ability to capture, correlate, visualize, and analyze forensic data in order to develop actionable insight to detect and mitigate threats that pose real harm to the organization, and to build a more proactive defense for the future. Users of Security Intelligence will shorten their Mean-Time-to-Detect and Mean-Time-to-Respond, extend the value of current security tools, and discover previously unseen threats through advanced machine analytics.

When threats are identified, whether via an enterprise's vast array of sensors or through machine analytics, the role of Security Intelligence is to deliver actionable insight into potentially damaging threats, with supporting forensic data and contextually rich intelligence. Security teams must be able to quickly evaluate threats to determine the level of risk as well as whether an incident has occurred. Ensuring that analysts have as much information as possible to make good decisions critically enables their efficiency and decision support processes.

Let's take a deeper dive into the key sub-processes that support the full threat detection and response process. An effective Security Intelligence platform ideally enables a streamlined workflow across each of the processes, delivering automation wherever possible. If an organization can optimize its efficiency in performing these critical steps in the detect/respond cycle, it can reduce its MTTD and MTTR and, more importantly, reduce its exposure to risk.

[5] Trustwave Holdings, 2014 *Trustwave Global Security Report*, May 2014

The End-to-End Threat Detection and Response Lifecycle™

Organizations that strive to seek reductions in MTTD and MTTR must optimize the end-to-end threat detection and response lifecycle. At each stage of the process, and in between, inefficiencies can exist that can dramatically impede an organization's overall effectiveness. However, organizations that are able to optimize the effectiveness of their security operations processes across each stage can realize profound improvements in MTTD and MTTR.

Threat detection typically begins the moment a threat is evidenced in forensic data. While it is true, threats can be identified before they become active, few organizations have the proactive threat intelligence and analysis capabilities to detect threats before they have begun to engage with the target environment.

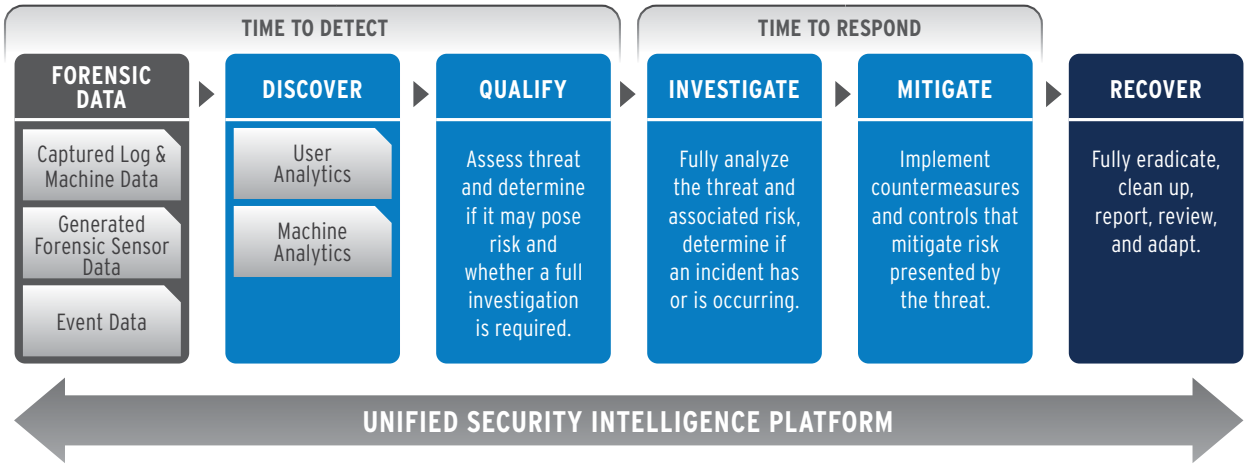
When a threat engages with the target environment, evidence will be left behind. This evidence will exist in forensic data that is collected or generated across the environment. The threat also may be detected by other security sensors. However, for most organizations, evidence of these threats gets lost in the noise. Separating the signal from the noise is the first step of the end-to-end threat detection and response process.

The response cycle begins the second a threat has been qualified as one that could present risk and requires further investigation. The cycle ends after a full investigation has been performed, and if the threat resulted in an incident, any risk to the organization has been mitigated. Organizations must collapse this response cycle from months to minutes if they are to avoid a damaging breach. Security Intelligence is the single largest enabler of collapsing this response cycle via:

- Centralized, full spectrum visibility around the threat and associated incident, delivered via powerful analytic tools
- Integrated workflows and collaboration capabilities that expedite the analysis and response process
- Automation in support of incident response processes and the deployment of countermeasures

Let's look at each of these process steps and what they entail.

Figure 3: The end-to-end threat detection and response lifecycle



Discover

As the first step in detection, discovery is the process of identifying those threats that could present risk; for example, seeing web traffic coming from a country the organization normally doesn't do business with. The traffic could be communication from a new international customer, or it could be attack traffic from a hacker in another country. At this stage, it's unknown whether it represents a threat or not.

The discovery process requires extracting those threats that require further analysis from the mass of forensic data. There are two principal types of analytics performed in support of discovering threats: user analytics and machine analytics.

User analytics are "person-based." That is, it's the work of individuals who are monitoring dashboards; manually evaluating trends, patterns and behaviors; and actively hunting for threats within the environment. This form of analytics scales based on the number of trained security staff an organization can afford to employ.

As the name implies, machine analytics are "machine-based." This form of analytics is delivered via software where captured forensic and event data is continuously monitored and analyzed. The primary function of machine analytics is twofold: first to detect threats that can only be seen via sophisticated analytic techniques, and second to prioritize threats detected by other technologies.

Qualify

Still part of the detection process, qualification is a critical step and involves further analyzing a threat to determine if it could present risk. When qualification is done well, threats representing risk are quickly identified as requiring additional analysis or response efforts. When qualification is done poorly, actual threats are missed, or teams spend the majority of their time chasing false positives.

The outcome of the qualification step is determining whether the discovered threat is a false positive; doesn't present risk and can be ignored; or likely presents risk and should be further investigated.

Investigate

If the outcome of the qualification process determines that a threat likely presents risk, the security team moves into the response process. It begins with conducting a deep investigation to understand the risk presented by the threat, and determining if an incident exists; in other words, if something bad has actually happened or is in the process of happening. The outcome of the investigation step is to conclusively determine whether the threat presents risk, if an incident has occurred, and if so, to initiate mitigation efforts.

Mitigate

By now it has been determined that there is a threat that presents real risk to the organization, and something must be done to reduce or eliminate that risk. The mitigation step is highly dependent on having sufficient knowledge about the root cause and impact of the threat as well as the knowledge and skills to do something about it. It is a time-sensitive step where security practitioners will benefit greatly by having an integrated and centralized view into all threat related activities, as well as streamlined cross-organizational collaboration capabilities, knowledge bases, and automated responses.

Recover

This final step could be considered "cleaning up the mess." Recovery involves performing post-mitigation efforts such as fully eradicating the threat from the environment, cleaning up any damage done, performing any required incident/breach notifications, and performing root cause analysis to learn from the incident in order to prevent it from happening again.

How MTTD and MTTR are Calculated

Looking at the five process steps – Discover, Qualify, Investigate, Mitigate, and Recover – it's easy to calculate the critical metrics of MTTD and MTTR.

MTTD is calculated as the time from when the threat was first evidenced (collected) in the environment to when it's discovered, plus the time between discovering the threat to determining its efficacy or dismissing it.

MTTR is calculated as the time from when a threat was qualified to when it was conclusively determined to present risk or it was dismissed, plus the time it took to mitigate the risk presented by the threat to an acceptable level.

The recovery stage, as defined above, isn't included in the MTTR metric. The critical measurement of response is considered to be the time it takes to determine risk exists and implement mitigations. The time required to implement full recovery procedures, while important, is a less critical metric in terms of understanding the overall effectiveness of the security operation towards achieving the most meaningful risk reduction.

The LogRhythm Security Intelligence Maturity Model™ (SIMM™)

Cyber security is a journey, not a destination. It takes time and resources to mature any significant organizational capability, and achieving significant reductions in MTTD and MTTR is no different. However, for organizations determined to reduce their cyber security risk posture, it is a capability that must be invested in.

Security Intelligence is the single most effective investment toward achieving reduced MTTD and MTTR.

Security Intelligence is the single most effective investment toward achieving reduced MTTD and MTTR. The LogRhythm Security Intelligence Maturity Model (SIMM) is designed to help organizations assess their current Security Intelligence capability and associated risk posture. This model also provides organizations a roadmap forward as they seek to continue improving their posture over time.

The model is focused on building and maturing an organization's detection and response capabilities as opposed to simply implementing more individual security products. However, technology-based solutions play a critical role in supporting and enabling the various stages of the process outlined above. Ideally the capabilities are delivered via an integrated and unified platform that supports the end-to-end threat detection and response process.

The critical capabilities that a Security Intelligence platform must deliver toward the goal of becoming impervious to cyber threats are:

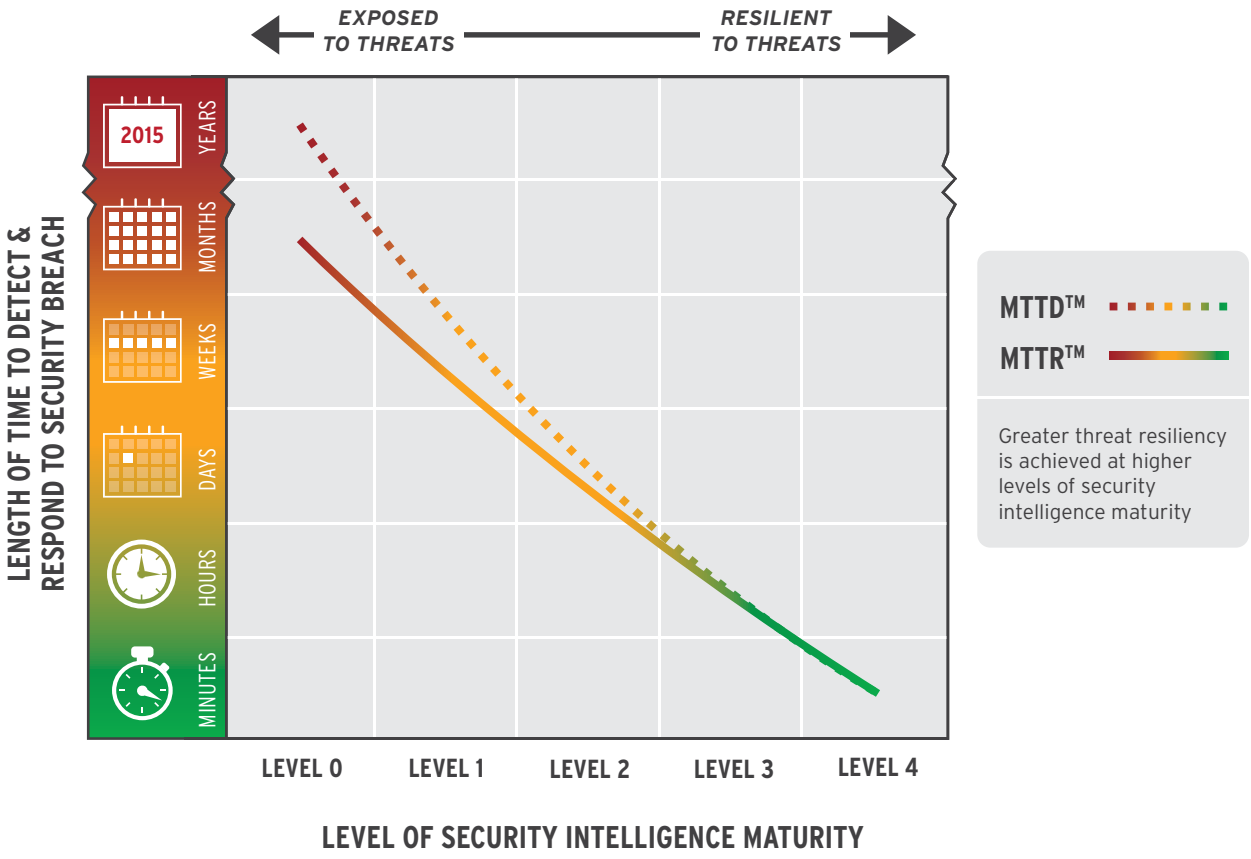
- Provide centralized, real-time acquisition of all forensic log and machine data generated across the complete IT environment
- Provide sensors that constantly, or on demand, acquire additional forensic data from endpoints, servers, and networks, holistically or targeted to areas of highest risk
- Uniformly process all acquired data into a highly classified and contextualized form, unlocking the intelligence contained in machine data and optimally preparing for downstream analytics
- Deliver state-of-the art machine-based analytics that can continuously and automatically surface risks and advanced threats via:
  - Access to 100 percent of acquired forensic data
  - Application of hybrid analytics techniques from correlation to behavioral modeling to machine learning
  - Intelligent prioritization of threats via contextual, risk based corroboration
- Deliver real-time visibility into highest risk incidents requiring further investigation and ongoing management by incident responders
- Deliver powerful search-based analytic tools that provide responders a 360-degree view around incidents via centralized access to forensic data in both raw and a fully contextualized form

- Deliver optimally orchestrated and automated incident response capabilities via intelligence driven, highly integrated workflows
- Deliver dashboards and reports that provide upper management key indicators of risk and active incidents within the environment

The LogRhythm Security Intelligence Maturity Model, fully detailed in the upcoming table, is comprised of multiple levels, beginning with Level 0 where there are essentially no SI capabilities and the organization is quite exposed to risk, and progressing to Level 4, with full SI capabilities that support an extremely resilient and highly efficient security posture.

As an organization progresses up the maturity model, its MTTD and MTTR and the associated timeframe of greatest risk grow smaller as illustrated in Figure 4.

Figure 4: MTTD and MTTD shrink as Security Intelligence capabilities grow more mature



The LogRhythm SIMM (see enclosed table) illustrates how increasing and maturing SI capabilities reduce an organization's risk posture.

Matrix Security Intelligence Maturity Model™

		SECURITY INTELLIGENCE CAPABILITIES	ORGANIZATIONAL CHARACTERISTICS	RISK CHARACTERISTICS
LEVEL 0 **BLIND**	**MTTD** MONTHS **MTTR** WEEKS OR MONTHS	• None	• Prevention oriented mindset. Have firewalls, A/V, etc. • Isolated logging based on technology and functional silos, but no central logging visibility • Indicators of threat and compromise exist, but nobody is looking and/or they are lost in the noise • No formal incident response process, comes down to individual "heroic efforts"	• Compliance risk • Blind to insider threats • Blind to external threats • Blind to APTs • If have IP of interest to nation-states or cyber criminals, likely stolen"
LEVEL 1 **MINIMALLY COMPLIANT**	**MTTD** WEEKS OR MONTHS **MTTR** WEEKS	• Targeted Log Management and SIEM • Targeted Server Forensics (e.g., File Integrity Monitoring) • Minimal, mandated, compliance oriented monitoring & response.	• Often have a compliance mandate driving investment or alternatively have identified a specific area of their environment to better protect • Compliance risks identified via report review, although risk exists if reports not reviewed and processes don't exist for managing compliance violations • Improved visibility into threats targeting the protected domain, but still lack the people and processes to effectively evaluate and prioritize threats • No formal incident response process, still comes down to individual "heroic" efforts. However, better enabled to respond to incidents affecting the protected environment	• Significantly reduced compliance risk, however, depends on the depth of audit • Blind to most insider threats • Blind to most external threats • Blind to APTs • If have IP of interest to nation-states or cyber criminals, likely stolen
LEVEL 2 **SECURELY COMPLIANT**	**MTTD** HOURS OR DAYS **MTTR** HOURS OR DAYS	• Holistic Log Management • Broader, Risk Aligned Server Forensics • Targeted environmental risk characterization • Targeted Vulnerability Intelligence • Targeted Threat Intelligence • Targeted Machine Analytics • Some monitoring and response processes established.	• Want to move beyond the minimal "check box" compliance approach, seeking efficiencies and improved assurance • Have recognized are effectively blind to most threats and want to see a material improvement towards detecting and responding to potential high impact threats, focused on areas of highest risk • Have established formal processes and assigned responsibilities for monitoring high risk alarms • Have established basic, yet formal processes for responding to incidents	• Extremely resilient and highly efficient compliance posture • Seeing insider threats • Seeing external threats • Still mostly blind to APTs, but more likely to detect indicators and evidence of • Much more resilient to cyber criminals, but still vulnerable to those leveraging APT type capabilities • Still highly vulnerable to nation-states

Continued on page 11

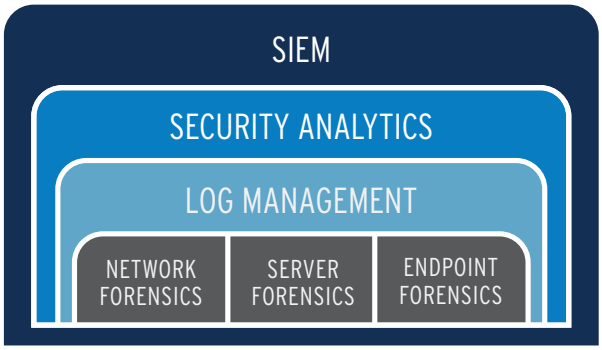
Matrix Security Intelligence Maturity Model *continued*

		SECURITY INTELLIGENCE CAPABILITIES	ORGANIZATIONAL CHARACTERISTICS	RISK CHARACTERISTICS
LEVEL 3 **VIGILANT**	**MTTD** HOURS **MTTR** HOURS	• Holistic Server Forensics • Targeted Network Forensics • Targeted Endpoint Forensics • Multi-vector, commercial grade, Threat Intelligence • Holistic Vulnerability Intelligence • Targeted Behavioral Analytics • Fully established and mature monitoring and response processes • Functional SOC established • Targeted IR Orchestration and Automated Response	• Have recognized are still blind to many high impact threats that could cause material harm to the organization • Have invested in the organizational processes and required people 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 capability that is running effectively with trained staff • Have begun to automate incident response processes and countermeasures • Are actively hunting for risk in the environment via dashboards and search	• Extremely resilient and highly efficient compliance posture • Seeing and quickly responding to insider threats • Seeing and quickly responding to external threats • Seeing evidence of APTs early in their lifecycle but may have trouble attributing activity to an actor/intent • Very resilient to cyber criminals, even those leveraging APT type capabilities • Still vulnerable to nation-states, but can reactively defend against
LEVEL 4 **RESILIENT**	**MTTD** MINUTES **MTTR** MINUTES	• Holistic Network, Server and Endpoint Forensics • Holistic environmental risk characterization • Holistic, Multi-Vector Machine Analytics • Proactive Threat Intelligence • Proactive Vulnerability Intelligence • Holistic IR Orchestration and Automated Response • Functional 24 x 7 SOC • Cyber Range Practice	• Are a high value target for nation-states, cyber terrorists, and organized crime • Are continuously being attacked across all possible vectors: physical, logical, social • A disruption of service or breach is intolerable and represents organizational failure of the highest level • Take a proactive stance towards threat management, and security in general • Invest in best-in-class people, technology, and processes • Have eyes on the data, eyes towards emerging threats, 24/7 • Have automated response processes and countermeasures wherever possible	• Extremely resilient and highly efficient compliance posture • Seeing and quickly responding to all classes of threats • Seeing evidence of APTs early in their lifecycle and able to manage their activities • Can withstand and defend against the most extreme nation-state level adversary

The LogRhythm Unified Platform Approach

LogRhythm's unified platform approach (Figure 5) ensures that all the aforementioned critical capabilities of Security Intelligence are delivered via an integrated product suite, where all components are designed to elegantly and efficiently work as a whole. For organizations seeking ideal MTTD and MTTR, this is critical. While the full suite of capabilities will be leveraged by organizations seeking to reach higher levels of maturity, customers starting their journey toward SI maturity can start with specific products and build on their investment over time.

Figure 5: The LogRhythm Security Intelligence Product Suite



The Principal Benefits of LogRhythm's Unified Approach

The Principal Benefits of LogRhythm's Unified Approach

LogRhythm's unified SI approach delivers organizations the technology foundation to realize a highly efficient security operation across all stages of the detection and response process. Only a unified approach ensures that information, people, and processes are ideally aligned toward the objective of reducing MTTD and MTTR. Following are some of the key principal benefits realized via this approach:

Comprehensive Big Data Analytics

When deployed, LogRhythm has incredible visibility across the IT environment from a data acquisition standpoint. This visibility is leveraged via Security Analytics capabilities to conclusively detect threats via big data analytics approaches. Security Analytics delivered outside an integrated architecture approach introduces complexity, latency and increased cost of ownership. These issues often result in data gaps. LogRhythm has taken an integrated approach to ensure the Security Analytics capability has optimal access to all acquired forensic data, in real-time, with lowest cost of ownership possible.

Holistic Contextual Analytics

Context is critical in support of effective analytics and incident response efforts. Security Information and Event Management (SIEM) traditionally provides a rich store of environmental context such as host and network risk ratings, lists of privileged user accounts, known vulnerabilities, etc. This context is critical when trying to effectively surface and qualify threats requiring highest attention. LogRhythm's integrated approach ensures context is configured once and maintained everywhere. This greatly helps ensure more accurate analytics and swifter incident response efforts, while reducing ongoing total cost of ownership.

Globally Prioritized Threat Management

Detecting threats is the easy part; discovering those that matter is the hard part. Security teams need a consolidated view of threats across their global landscape. Additionally, threats must be intelligently prioritized so end-user analysis cycles are spent effectively. LogRhythm's comprehensive big data analytics, combined with holistic context, allows the system to not only detect a unique class of threats, but to prioritize those that are detected by LogRhythm and other technologies, all in a consolidated global view. This is imperative to achieving low MTTD and is critically enabled via LogRhythm's unified platform approach.

Streamlined Incident Response

When threats are discovered, the clock begins ticking. How fast incident responders can access relevant forensic data and context critically impacts the amount of time required to investigate each threat. As threats are investigated, a subset will be identified as incidents requiring a full response. LogRhythm's unified approach ensures that forensic data associated with an incident is readily and immediately available to responders and automatic response capabilities.

When forensic data is tightly coupled with the system responsible for orchestrating and automating incident response, response times are exponentially more efficient—especially when cross organizational workflow is required. To the contrary, when forensic data is decoupled, automatic responses become constrained, and incident responders have to scramble and hunt through disjointed disparate systems. Cross-organizational collaboration becomes manual and slow. All the while, the clock continues to tick.

Conclusion

As organizations evolve their Security Intelligence maturity, the realized reduction in MTTD and MTTR significantly reduces the risk of experiencing a damaging cyber incident. Of course, each organization needs to assess for itself the appropriate level of maturity based on its own risk tolerances.

As organizations evolve their Security Intelligence maturity, the realized reduction in MTTD and MTTR significantly reduces the risk of experiencing a damaging cyber incident.

Fortunately, organizations with limited budget and higher risk tolerances can achieve significant improvements in capability by moving towards a Level 2 posture. For organizations with more cyber security resources and much lower risk tolerances, moving towards Level 3 or even Level 4 might be appropriate.

LogRhythm's unified platform approach and flexible product architecture allow an organization to adopt and mature capabilities over time, comfortable in the fact that subsequent investments will build on previous steps along the maturity model. LogRhthym's goal is to ensure that enterprises have a partner able to provide the integrated technology building blocks, and associated services, to most effectively and efficiently realize their Security Intelligence objectives so they can best protect themselves from damaging cyber threats.

About LogRhythm

LogRhythm, the leader in security intelligence and analytics, empowers organizations around the globe to rapidly detect, respond to and neutralize damaging cyber threats. The company's patented and award-winning platform uniquely unifies next-generation SIEM, log management, network and endpoint forensics, and advanced security analytics. In addition to protecting customers from the risks associated with cyber threats, LogRhythm provides unparalleled compliance automation and assurance, and enhanced IT intelligence.

LogRhythm is consistently recognized as a market leader. The company has been positioned as a Leader in Gartner's SIEM Magic Quadrant report for three consecutive years, named a "Champion" in Info-Tech Research Group's 2014-15 SIEM Vendor Landscape report and ranked Best-in-Class (No. 1) in DCIG's 2014-15 SIEM Appliance Buyer's Guide. In addition, LogRhythm has received Frost & Sullivan's SIEM Global Market Penetration Leadership Award and been named a Top Workplace by the Denver Post.

To download or forward the complement to this paper, **The Cyber Threat Risk – Oversight Guidance for CEOs and Boards**, go to: www.logrhythm.com\SIMM-CEO.

LogRhythm™
The Security Intelligence Company

LR_SIMM_CISO_01.15

LogRhythm™