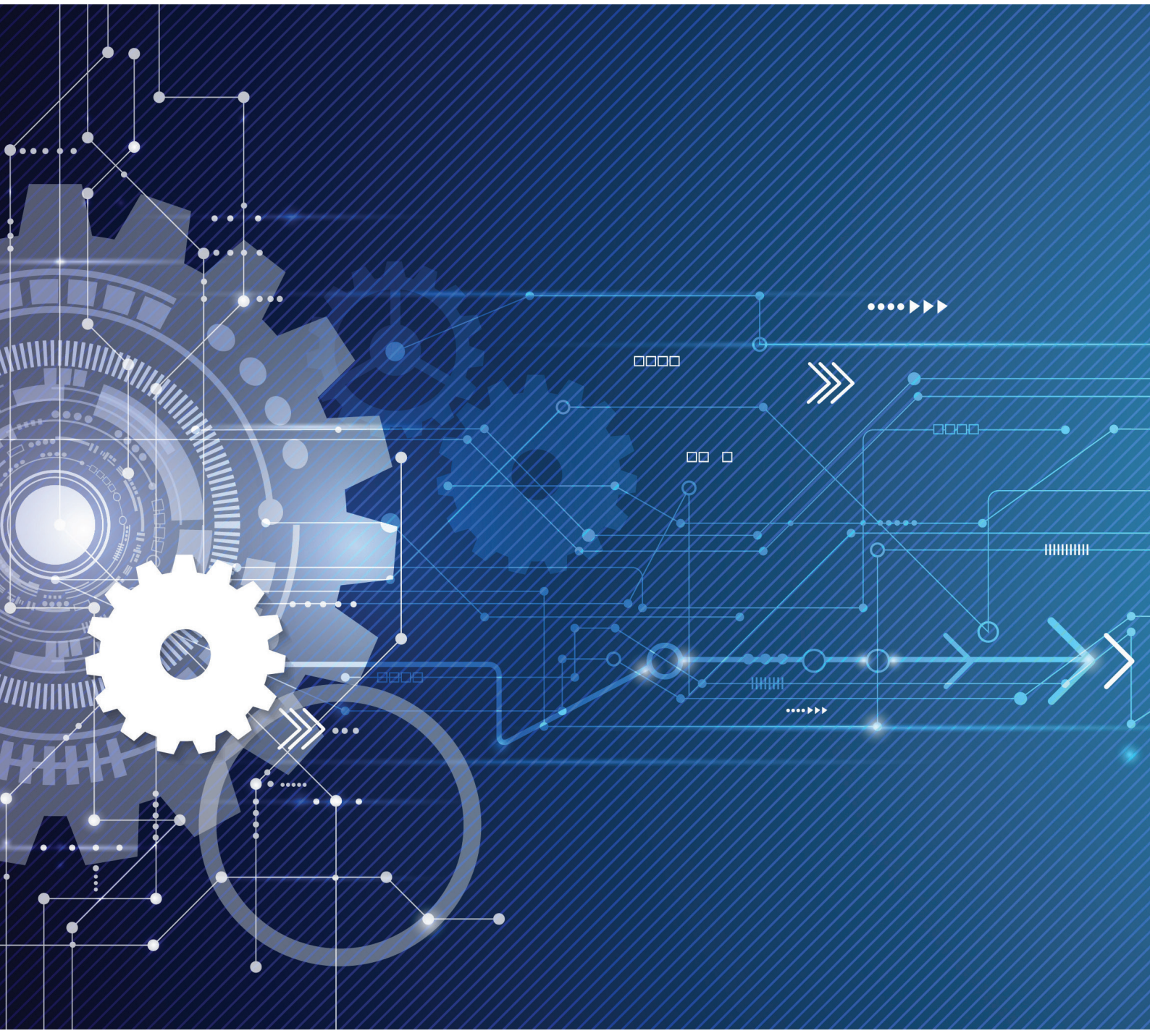
LogRhythm®
The Security Intelligence Company



The Threat Lifecycle Management Framework

Prevent major data breaches by reducing time to detect and respond to threats

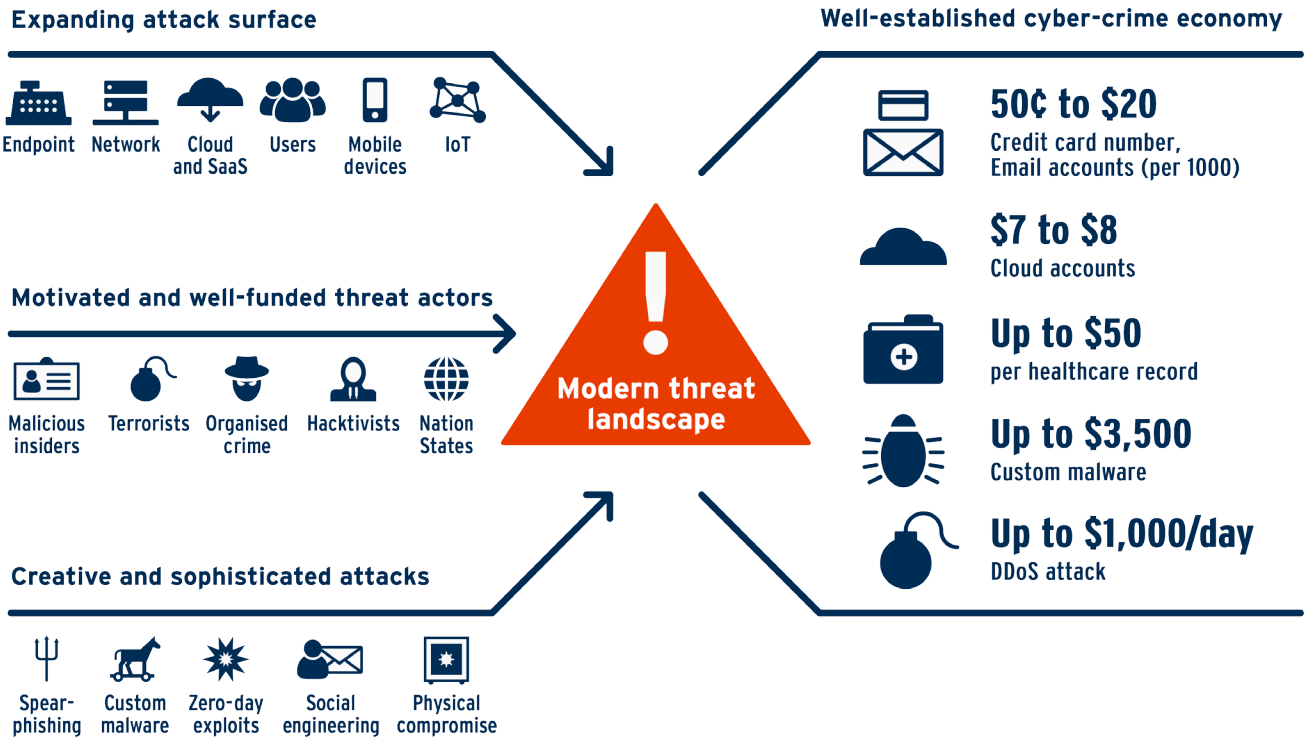
By: Chris Petersen
CTO & Co-Founder of LogRhythm

Table of Contents

Preface

Globally, sophisticated cyber-attacks are compromising organisations at an unprecedented rate and with devastating consequences. Modern attackers, including criminal organisations, ideological groups, nation states and other advanced threat actors are motivated by a wide range of objectives that include financial gain, industrial espionage, cyber-warfare, and terrorism. These attacks are often very expensive for compromised organisations, costing each company an average of USD $7.7M.[1]

The odds that your organisation will be compromised are high. In fact, a recent report indicates that 76 percent of surveyed organisations were compromised in 2015.[2] Against this backdrop, organisations increasingly expect that it's not *if* they will be compromised, but rather *when* will they be compromised.



The Modern Cyber Threat Pandemic [3]

> Regulatory fines, public relations costs, breach notification and protection costs, and other consequences of large-scale data breaches are well-understood. But the effects of a cyberattack can ripple for years, resulting in a wide range of "hidden" costs—many of which are intangible impacts tied to reputation damage, operational disruption or loss of proprietary information or other strategic assets.[4]
>
> -Deloitte, Beneath the Surface of a Cyberattack

[1] Ponemon 2015 Cost of Cyber Crime Study
[2] CyberEdge 2016 Cyberthreat Defense Report
[3] Symantec, Underground black market: Thriving trade in stolen data, malware, and attack service. November 20, 2015; Medscape, Stolen EHR Charts Sell for $50 Each on Black Market, April 28, 2014
[4] Deloitte, Beneath the Surface of a Cyberattack, 2016

A new approach is required

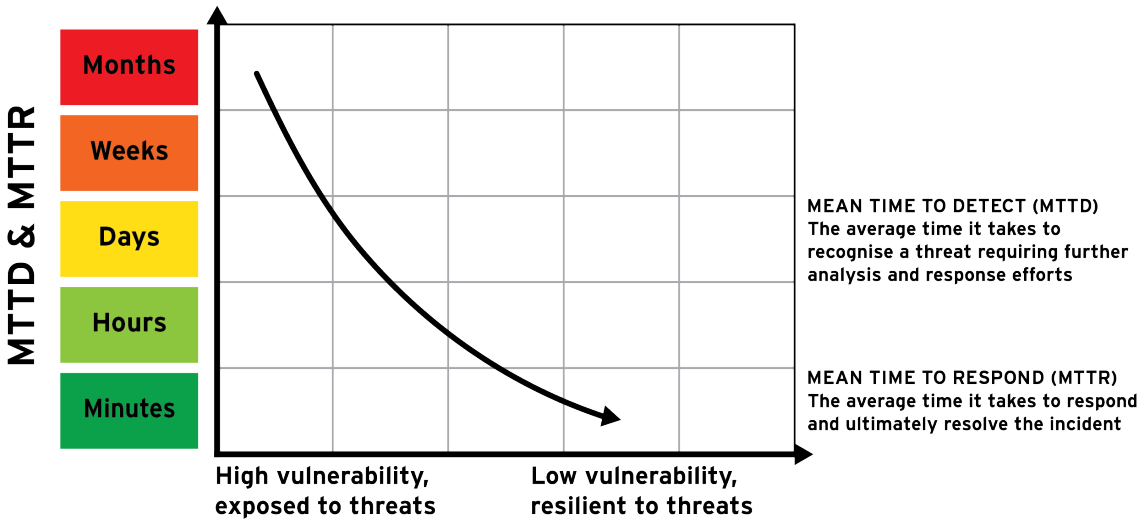
The traditional approach to cybersecurity has been to use a prevention-centric strategy focused on blocking attacks. While prevention-centric approaches do stop many threats, many of today's advanced and motivated threat actors are circumventing these defences with creative, stealthy, targeted, and persistent attacks that often go undetected for significant periods of time.

In addition, modern organisations are exposed through increasing interconnectedness—the growing use of cloud-based applications, the proliferation of mobile technologies, and the Internet of Things (IoT)—that blends the use of consumer and corporate technologies. The result is a rapidly growing attack surface that is increasingly difficult for your security and operational teams to protect without impacting the core business of your organisation.

In response to the shortcomings of prevention-centric security strategies and the challenges of securing an increasingly complex and open IT environment, many organisations are progressively shifting their resources and focusing towards strategies centered on threat detection and response. Gartner estimates that by 2020, 60 percent of enterprise information security budgets will be allocated for rapid detection and response approaches, up from less than 20 percent in 2015.[5] Security teams that are able to reduce their mean time to detect (MTTD) and mean time to respond (MTTR) can materially decrease their risk of experiencing a high-impact cyber incident or data breach.

Unfortunately, the growing complexity of IT and an increasingly hostile threat landscape has made it challenging to realise reductions in MTTD and MTTR. Most organisations are struggling to keep up with the volume of security alerts—many of them false positives or of low quality. This has created organisational "alarm fatigue" that inhibits security teams from identifying real threats that could lead to a damaging cyber-incident or data breach.

Security teams also often lack effective tools, automation, and processes for streamlining threat investigations and incident response. These challenges are evidenced when looking at recent data breaches. Too often, the time it took for the affected organisation to discover and respond to the data breach was measured in months, and in some cases years, with the average time to detection being 146 days in 2015.[6]



Faster detection and response reduces risk

Gartner estimates that by 2020, 60 percent of enterprise information security budgets will be allocated for rapid detection and response approaches, up from less than 20 percent in 2015.[5]

[5] Shift Cybersecurity Investment to Detection and Response, Gartner, 2016
[6] M-Trends 2016, Mandiant Consulting

The Cyber Attack Lifecycle

Fortunately, high-impact cyber incidents and data breaches can be largely avoided if you detect and respond quickly with end-to-end threat management processes. When a threat actor targets your environment, a process unfolds from initial intrusion through eventual data breach—if that threat actor is left undetected. The modern approach to cybersecurity requires a focus on reducing MTTD and MTTR where threats are detected and killed early in their lifecycle, thereby avoiding downstream consequences and costs.

The following graphic illustrates the Cyber Attack Lifecycle and the typical steps involved in a data breach.

Phase 1: Reconnaissance

The first stage in reconnaissance is identifying potential targets (companies or individuals) that satisfy the mission of the attackers (e.g. financial gain, targeted access to sensitive information, brand damage, etc.). Once the target or targets are identified, the attackers determine their best mode of entry.

They determine what defences you have in place, what web applications or other internet-accessible systems are in place, how to compromise external systems, and how to gain an initial foothold on an internal device. They choose their initial weapon based on what they discover during their reconnaissance, whether it is a zero-day exploit, a spear-phishing email campaign, physical compromise, bribing an employee, or some other means of launching their initial attack.

Phase 2: Initial compromise

The initial compromise is usually in the form of hackers bypassing your perimeter defences and, in one way or another, gaining access to your internal network through a compromised system or user account. Compromised systems might include your externally facing servers or end-user devices, such as laptops or desktops. Recent breaches have also included systems that were never traditionally considered as intrusion entry points, such as point-of-sale (POS) devices, medical devices, personal consumer devices, networked printers, and even IoT devices.

Phase 3: Command & control

The compromised device is used as a beachhead into your organisation. Typically, this involves the attacker surreptitiously downloading and installing a remote-access Trojan (RAT) so they can establish persistent, long-term, remote access to your environment. Once the RAT is in place, they can carefully plan and execute their next move using covert connections from attacker-controlled systems on the internet.

Phase 4: Lateral movement

Once the attacker has an established (persistent) connection to your internal network, they seek to compromise additional systems and user accounts. First, they take over the user account on the compromised system. This account helps them scan, discover, and compromise additional systems from which additional user accounts can be stolen. Because the attacker is often impersonating an authorised user, evidence of their existence can be hard to see.

Phase 5: Target attainment

At this stage in the lifecycle, the attacker typically has multiple remote access entry points and may have compromised hundreds (or even thousands) of your internal systems and user accounts. They have mapped out and deeply understand the aspects of your IT environment of highest interest to them. Ultimately, they are within reach of their target(s), and they are comfortable that they can complete their ultimate mission at the time of their choosing.

Phase 6: Exfiltration, corruption, and disruption

The final stage of the Cyber Attack Lifecycle is where cost to your business rises exponentially if the attack is not defeated. This is the stage where the attacker executes the final aspects of their mission, stealing intellectual property or other sensitive data, corrupting mission-critical systems, and generally disrupting the operations of your business. In the event of data theft, data is often transmitted via covert network communications across days, weeks, or even months. Attackers will also hide activity by using seemingly legitimate cloud-storage applications such as Dropbox and Google Drive to steal data.

Prevent high-impact cyber incidents through optimised Threat Lifecycle Management

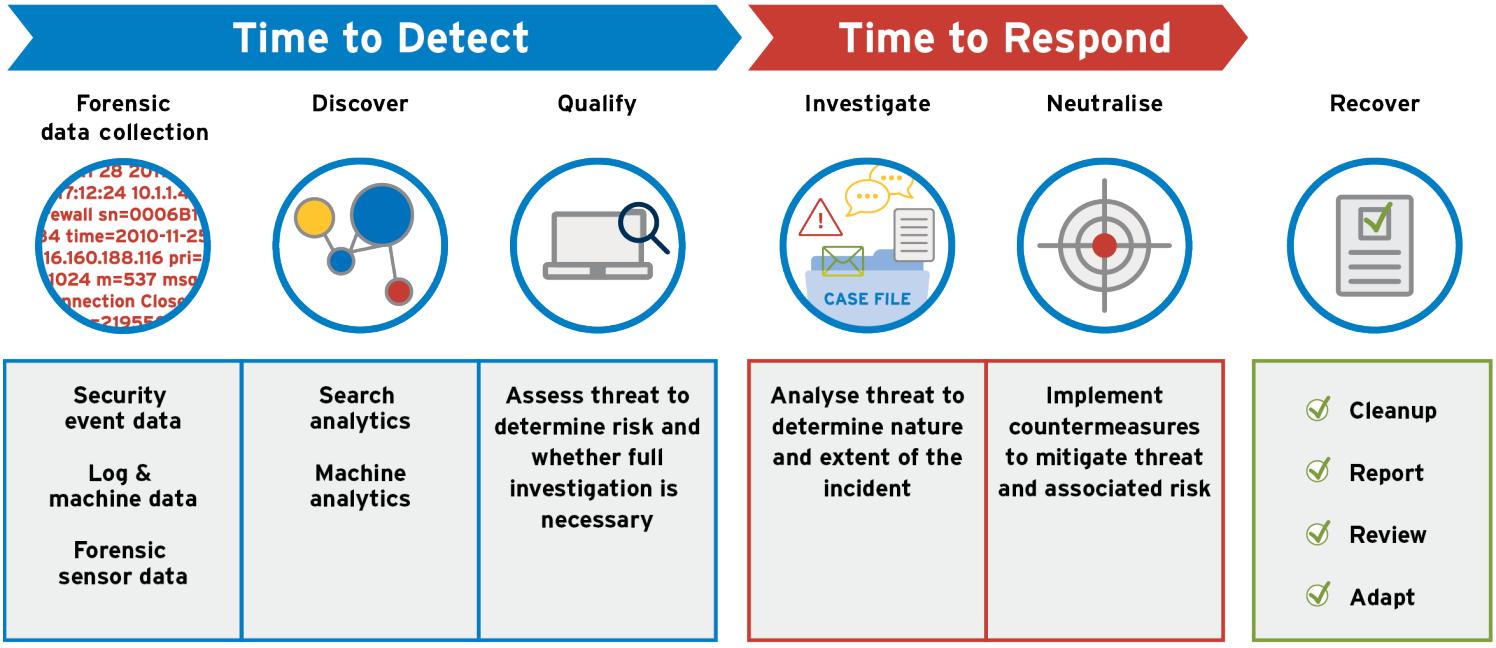
The ability to detect and respond to the threat early in the Cyber Attack Lifecycle is the key to protecting your company from large-scale impact. The earlier an attack is detected and mitigated, the less the ultimate cost to the business will be. If a compromised endpoint is quickly removed from the environment, the cost of cleaning up additional compromised systems due to successful lateral movement is avoided. If the attacker is detected while executing lateral movement, the cost of clean-up might be limited to 10 compromised systems vs. thousands (or ultimately having to deal with a class-action lawsuit resulting from a high-profile data breach).

To reduce your MTTD and MTTR, you must implement an end-to-end detection and response process—referred to as Threat Lifecycle Management (TLM) in this paper. To realise effective TLM, you must invest in people, process, and technology. More than ever, technology plays a critical role in realising cost-efficient reductions in MTTD and MTTR across the TLM workflow.

Threat Lifecycle Management overview

Threat Lifecycle Management is the fundamental workflow of the security operations center (SOC). Yet it is important to note that effective TLM does not require you to have or to build a 24/7 physical SOC. While for some organisations, a 24/7 SOC might be appropriate, for others, this is neither feasible nor warranted. Today, technology can enable effective TLM at the scale appropriate to your business, whether it be a virtual SOC with an effective staff of three, or a globally distributed 24/7 SOC with dedicated staff of 100.

Threat Lifecycle Management is a series of aligned security operations capabilities and processes that begins with the ability to "see" broadly and deeply across your IT environment, and ends with the ability to quickly mitigate and recover from a security incident. The next section describes the capabilities and processes that your organisation must invest in to implement effective TLM and realise reductions in MTTD and MTTR.



Threat Lifecycle Management

The phases of Threat Lifecycle Management

Phase 1: Forensic data collection

Before any threat can be detected, you must be able to see evidence of the attack within the IT environment. Because threats target all aspects of the IT infrastructure, the more you can see, the more ably you can detect. There are three principle types of data you should focus on, generally in the following priority:

1. Security event and alarm data

Most organisations have an array of security products to prevent a wide range of attacks from being successful. However, in some cases, these technologies can only warn an attack may be in process or has occurred. In these cases, events and alarms are generated. The challenge most organisations deal with is rapidly identifying which events or alarms to focus on, as tens of thousands might be generated on a daily basis. At the same time, this is typically the most valuable source of data your security team has for finding evidence of a successful attack.

2. Log and machine data

Log data can provide deeper visibility into your IT environment—recording on a per user, per system, per application, etc. basis—to illustrate who did what, when, and where. This rich set of data can support more effective and rapid investigations of suspected attacks. The ability to comprehend what is normal within the IT environment is also within this dataset—enabling machine analytics to detect behavioural anomalies that might indicate a more advanced attack is in progress.

3. Forensic sensor data

Once your organisation is effectively collecting their security and log data, forensic sensors can provide even deeper and broader visibility. Forensic sensors can fill visibility gaps when logs aren't available or the level of forensic detail is insufficient. There are two primary types of forensic sensors that might be employed:

- network forensic sensors that capture packets and flows, and
- endpoint forensic sensors (e.g., EDR agents) that can record with high fidelity all activity occurring on the monitored system.

Investment in forensic sensors can provide additional gains in investigative and incident response efficiencies. This data also enables more powerful and capable machine analytics-driven approaches for detecting the most sophisticated attacks.

Phase 2: Discover

Once visibility has been established, you now stand a chance at detecting and responding to threats. Discovery of potential threats is accomplished through a blend of search and machine analytics.

Search analytics

This type of analytics is performed by people and enabled by software. It includes things such as targeted hunting of threats by monitoring dashboards and leveraging search capabilities. It also includes reviewing reports to identify known exceptions. Search analytics is people intensive. Thus, while effective, it cannot be the sole (or even primary) method of analytics most organisations should employ.

Machine analytics

This type of analytics is performed by software using machine learning and other automated analysis techniques where outputs can be efficiently leveraged by people. Machine analytics is the future of a modern and efficient threat discovery capability.

According to Gartner, 25 percent of security products used for detection will have some form of machine learning built into them by 2018.[7] The goal of using machine analytics should be to help your organisation realise a "risk-based monitoring" strategy through the automatic identification and prioritisation of attacks and threats. This is critical for both detecting advanced threats via data science-driven approaches, as well as helping you orient your precious manual analytics capabilities to the areas of highest risk to the business.

According to Gartner, 25 percent of security products used for detection will have some form of machine learning built into them by 2018.[7]

[7] The Fast Evolving State of Security Analytics 2016, Gartner

Phase 3: Qualify

Discovered threats must be quickly qualified to assess the potential impact to the business and the urgency of additional investigation and response efforts. The qualification process is manual and time intensive, while also being very time sensitive. An inefficient qualification process increases the level of human investment needed to evaluate them all but an efficient process allows you to analyse a greater number of alarms with less staff, while also positively affecting overall MTTD and MTTR.

False positives will happen. You need the tools to identify them quickly and accurately. Inefficient qualification could mean a true threat (aka "true positive") has been ignored for hours or days. Incorrect qualification could mean that you miss a critical threat and let it go unattended. Philosophically and practically, it is important to note that only qualified threats can truly be considered detected, otherwise it's simply noise—an alarm bell going off that nobody really hears.

Phase 4: Investigate

Once threats have been qualified, they need to be fully investigated to undeniably determine whether a security incident has occurred or is in progress. Rapid access to forensic data and intelligence on the threat is paramount. Automation of routine investigatory tasks and tools that facilitate cross-organisational collaboration is ideal for optimally reducing MTTR.

Ideally, a facility for keeping track of all active and past investigations is available. This can help ensure that forensic evidence is well-organised and is available to collaborators. It can also provide an account of who did what in support of investigation and response activities to measure organisational effectiveness and hold parties responsible for the tasks they own in the investigation.

Phase 5: Neutralise

When an incident is qualified, you must implement mitigations to reduce and eventually eliminate risk to the business. For some threats, such as ransomware or compromised privileged users, every second counts. To maximally reduce MTTR, easily accessible and updated incident response processes and playbooks, coupled with automation, is critically important. Similar to the Investigate stage, facilities that enable cross-organisational (e.g., IT, legal, HR) information sharing and collaboration are also important.

Phase 6: Recover

Once the incident has been neutralised and risk to the business is under control, full recovery efforts can commence. These efforts are less time critical, and they can take days or weeks depending on the scope of the incident. To recover effectively and on a timely basis, it is imperative your security team has access to all forensic information surrounding the investigation and incident response process. This includes ensuring that any changes made during incident response are tracked, audit trail information is captured, and the affected systems are updated and brought back online. Many recovery-related processes can benefit from automation. In addition, the recovery process should ideally include putting measures in place that leverage the gathered threat intelligence to detect if the threat returns or has left behind a back door.

How LogRhythm accelerates Threat Lifecycle Management

The responsibility of detecting and responding to threats that penetrate the perimeter or originate from within is typically borne by the security operations center (SOC). Regardless of whether an organisation employs a virtual SOC of three or a physical SOC of 30, how well this is executed is determined by the effectiveness of TLM. The TLM workflow is not novel; it is and has been the core foundation of SOC monitoring and response capabilities. The reason large data breaches still occur is because the TLM workflow is implemented poorly across a large number of diverse security systems, each offering different user interfaces, inadequate integration with other systems, and lacking automation in the areas of advanced security analytics and incident response. SOCs built on a foundation of poor TLM continue to suffer from alarm fatigue and operate with low human efficiency.

LogRhythm delivers Threat Lifecycle Management by bringing together historically disparate security solutions into one unified platform. The LogRhythm Security Intelligence and Analytics Platform gives the SOC a "single pane of glass" from which to evaluate alarms, investigate threats, and respond to incidents. LogRhythm's patented security analytics capabilities automate the detection and prioritisation of real threats. In addition, our platform provides mechanisms to orchestrate and automate the incident response workflow. The delivery of all TLM capabilities, with strong automation, in a unified platform, ensure your staff can work more efficiently to realise optimally reduced MTTD and MTTR.

10 Ways LogRhythm expedites delivery of TLM

1. Unbeatable forensic visibility

LogRhythm offers unparalleled forensic visibility by collecting the widest variety of machine data in real-time, including security events, audit logs, system and application logs, flow data, and more. Basically, if it logs, we can almost certainly collect it. In addition, purpose-built forensic sensors provide you with deeper visibility into network communications and endpoint activity. Central management and administration of all this data ensures a low total cost of ownership.

2. Machine Data Intelligence (MDI)

Simply put, nobody knows more about what log data means than us. Our Machine Data Intelligence (MDI) Fabric™ uniformly classifies, contextualises, and normalises data from over 750 different types of systems and devices.

LogRhythm Labs has spent a decade building our MDI knowledge base and is constantly at work adding new devices and updating existing devices via cloud-based delivery. Our ongoing investment in MDI, combined with our patented data-processing capabilities, lays the critical foundation for accurate security analytics and effective security automation.

3. Precision search, rapid decisions

Our Elasticsearch-based back-end empowers both contextual search and unstructured search. Unstructured search allows you to quickly and easily search data based on keyword criteria. Contextualised search criteria provides a more precise search experience, so you can get to the right data and right decisions, fast. Data is displayed in a powerful and intuitive UI, leveraging customisable analysis widgets.

4. Machine analytics technology

Our patented AI Engine technology employs a variety of sophisticated analytical techniques, including machine learning, behaviour profiling, statistical analysis and black/whitelisting. AI Engine detects threats that can only be seen via a centralised "big data" analytics approach. It also corroborates threats detected by other security sensors with relevant data from across your environment.

5. Holistic Security Analytics and User and Entity Behaviour Analytics

Only LogRhythm offers out-of-the-box analytics modules supporting user, network, and endpoint threat detection across your holistic attack surface. For instance, our User and Entity Behaviour Analytics (UEBA) module provides out-of-the box capabilities for rapidly detecting a wide range of user-based threats such as compromised accounts and privilege abuse. All analytics modules are developed & maintained by the LogRhythm Labs threat research team and are updated regularly through cloud updates. We provide these modules as part of a customer maintenance contract.

6. Threat intelligence operationalisation

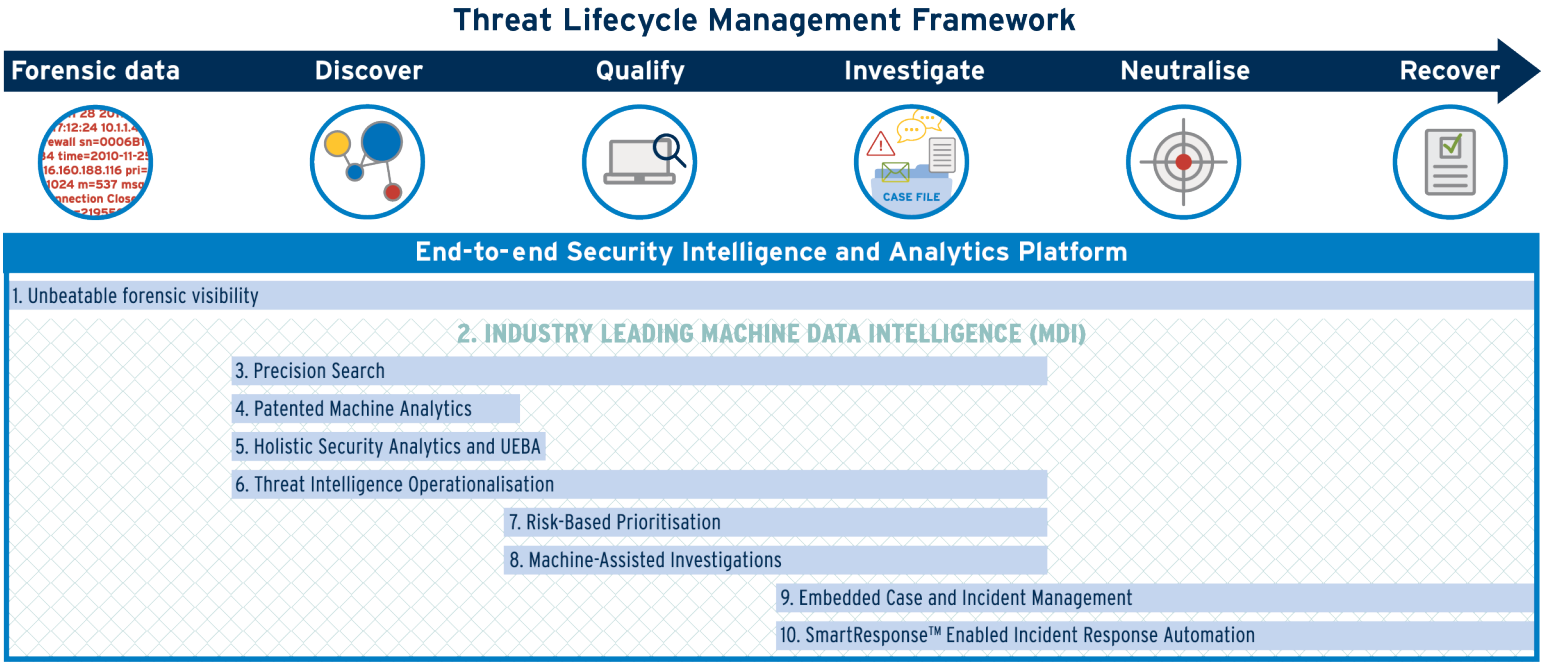
LogRhythm automatically and easily integrates with commercial, open-source, and industry-provided third-party threat intelligence feeds and services, operationalising actionable threat intelligence data (e.g., CrowdStrike, Malware Domains, STIX/TAXII). This intelligence can be used to alarm on known indicators of compromise, provide contextual data to existing alarms within the platform, and as a validation point to further qualify an alarm.

7. Risk-Based Prioritisation (RBP)
Whether threats are detected by another security product or via LogRhythm's AI Engine, our RBP algorithm uses environmental risk characteristics and threat context to assign a 100-point score to all alarms. The algorithm provides out-of-the box prioritisation, but it can also be tuned over time based on unique organisational needs. This helps you quickly adopt a risk-based monitoring strategy, reducing alarm fatigue and effectively focusing your teams' time where it matters most.

8. Machine-assisted investigations
When investigating alarms, ensuring that your analysts are looking at the "right" data is of critical importance to investigatory efficiency and accuracy. In addition, knowing what to search for can be challenging when analysing complex threat actor scenarios or behavioural abnormalities. For every alarm LogRhythm generates, there is a machine-assisted drill down that automatically returns the data of highest forensic interest, helping ensure you are looking at the right data for fastest decision support.

9. Embedded case and incident management
LogRhythm has a fully integrated case and incident management system that allows security analysts to collaborate efficiently and securely. Case management provides a full audit history and real-time dashboard of all active investigations and incidents. Adding an alarm to a case is as simple as one-click, helping ensure suspected threats are promptly tracked. An evidence locker centralises all forensic data associated with your active investigations. For organisations with existing IT ticketing and orchestration systems, LogRhythm offers an API for bidirectional integration.

10. SmartResponse™ enabled incident response automation
LogRhythm's SmartResponse plug-ins allow for proactive mitigation of threats by automating routine investigatory actions (e.g., scan server, dump memory) as well as incident response countermeasures (e.g., disable user, quarantine endpoint). SmartResponse actions are automatically associated with specific alarms creating pre-staged automation playbooks. Actions can be initiated without human interaction or can require single- or multi-party approval. Out-of-the-box functionality enables rapid adoption, and you can easily develop your own plug-ins to support custom workflows and playbooks.



LogRhythm's unified approach provides lower total cost of ownership and achieves better results

LogRhythm's unified Security Intelligence and Analytics Platform provides the technology foundation necessary to realise a highly efficient security operation across the entire threat lifecycle. Only a unified approach ensures that information, people, and processes are ideally aligned toward the objective of maximally reducing MTTD and MTTR. Some of the principal cost benefits resulting from our unified approach:

- Reduced costs associated with integrating multiple third-party systems through APIs
- Reduced data storage and infrastructure costs associated with shipping copies of data across disparate systems
- Fewer products and UIs to learn and manage across the TLM workflow reducing analyst "swivel head" inefficiencies

Conclusion

You can lessen your organisation's risk of experiencing a damaging cyber incident or data breach by investing in effective Threat Lifecycle Management. Although internal and external threats will exist, the key to managing their impact within your environment and reducing the likelihood of costly consequences is through faster detection and response capabilities.

Highly effective and efficient workflows that use automation where possible will help your organisation gain human efficiencies and optimal TLM. Machine-driven security analytics must play an increasingly significant role, delivering human operators accurate, actionable intelligence on real threats. You must also invest in incident response orchestration capabilities that automate routine investigative tasks and countermeasures.

While TLM can be realised via a combination of disparate systems, overall effectiveness then becomes dependent on complex API-level integrations and the speed in which you can navigate across multiple product interfaces. In contrast, LogRhythm has steadily invested towards being the platform leader in Threat Lifecycle Management. We firmly believe that TLM is optimally delivered via a collection of seamlessly integrated capabilities, that elegantly fuse technology, people and process through automation and an incredible user experience.

To learn more about how our unified platform approach can help you optimally reduce your MTTD and MTTR, visit LogRhythm.com.

LogRhythm®

About LogRhythm

LogRhythm, a leader in security intelligence and analytics, empowers organisations around the globe to rapidly detect, respond to and neutralise damaging cyber threats. The company's patented award-winning platform uniquely unifies next-generation SIEM, log management, network and endpoint monitoring, User and Entity Behaviour Analytics (UEBA), security automation and orchestration 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 recognised as a market leader. The company has been positioned as a Leader in Gartner's SIEM Magic Quadrant report for five consecutive years, named a 'Champion' in Info-Tech Research Group's 2014-15 SIEM Vendor Landscape report, received SC Labs 'Recommended' 5-Star rating for SIEM and UTM for 2016 and earned Frost & Sullivan's 2015 Global Security Information and Event Management (SIEM) Enabling Technology Leadership Award. LogRhythm is headquartered in Boulder, Colorado, with operations throughout North and South America, Europe and the Asia Pacific region.