KB

HOW A PLATFORM APPROACH TO SECURITY MONITORING INITIATIVES ADDS VALUE: INTEGRATION, ORCHESTRATION, ANALYTICS, AUTOMATION AND THE NEED FOR SPEED

December 2020

Derek E. Brink, CISSP
Vice President and Research Fellow, Information Security and IT GRC

ABERDEEN

As **security monitoring** initiatives mature, a **platform** approach reduces the time to *detect*, *investigate*, *respond* to, and *recover* from security-related incidents — and drives a significant reduction in their business impact. Empirical evidence shows increasingly positive results, as well as the value of investing for additional improvements.

The Trifecta of Enterprise Computing Infrastructure: Keeping IT Secure, Compliant, and Well-Managed

For several years, Aberdeen has referred to a trifecta of operational objectives for enterprise computing infrastructure: to be **secure**, **compliant**, and **well-managed**. The term *trifecta* is used deliberately, because Aberdeen's research has consistently shown that the *order* of priority given to these three objectives is correlated with top performance:

1. To quickly detect, investigate, respond to, and recover from **security**-related incidents — and in doing so, to help manage the organization's security-related **risks** to an acceptable level
2. To cost-effectively achieve, sustain, and demonstrate ongoing **compliance** with enterprise policies and regulatory requirements
3. To continuously improve and mature the **flexibility** and **resilience** of ongoing operations — and in doing so, to provide the organization and its users with ever-better performance and scale, at lower total cost

Over time, top performers have continued to improve their operational capabilities to address these three simultaneous and closely interrelated objectives. Some of the key activities for the three respective segments of the secure, compliant, and well-managed trifecta are summarized in Table 1.

It's common for technical staff to get started on security monitoring initiatives with an investment in lower-level **tools**, which are typically used at first to help them with *forensic investigations* of anomalous activities — as well as after-the-fact *auditing* and *reporting* on compliance and work progress.

As these initiatives mature, however, the top performers are going beyond the use of tactical tools for investigations and reporting about what's already happened, to adopt a more strategic, proactive, **platform**-oriented approach.

Security incident: Any event that attempts to compromise the *confidentiality*, *integrity*, or *availability* of an enterprise computing asset.

Data breach: A security incident which results in the confirmed disclosure of an information asset to an unauthorized party.

In making a distinction between "tools" and "platforms," Aberdeen is reflecting a generalized pattern of evolution which can be observed in several security solution categories:

- From a mixed bag of lower-level **tools** for specialized technical staff
- To enterprise self-integration of **point solutions**
- To vendor-integration of **product suites**
- To vendor- and ecosystem-integration and orchestration of **platforms** across a wide variety of tools, point solutions, products, and services

Table 1: For the Top Performers, Enterprise Computing Infrastructure is Secure, Compliant, and Well-Managed — In That Order

2. Compliant	1. Secure	3. Well-Managed
After-the-Fact	**Real-Time**	**Forward-Looking**
Achieve and Sustain Compliance • Demonstrate compliance with enterprise policies and regulatory requirements (*auditing, reporting*) • Report on the current status and posture of enterprise computing infrastructure for senior management, line of business owners, and other key stakeholders (*dashboards*) • Report on progress over time against an initial baseline and targeted metrics (*"work progress"*)	**Manage Security-Related Threats** • Monitor network activity, user activities, and privileged user activities • Monitor endpoints and back-end resources • Detect, investigate, respond to, and recover from security incidents and anomalous behaviors • Do forensic investigations of active threat campaigns • Detect, prevent, and contain data loss	**Optimize Ongoing Operations** • Reduce the total annual cost of security, compliance, and ongoing operations • Implement selected industry standards and best practices (e.g., NIST, ISO, ITIL, COBIT) • Increase integration and visibility across multiple data sources and security tools (*orchestration*) • Optimize the efficiency, accuracy, and consistency of day-to-day playbooks and workflows (*automation*) • Optimize the performance of networks and applications

Source: Aberdeen, December 2020

A platform-oriented approach to security monitoring initiatives helps companies to achieve better:

- **Integration** and **orchestration** of information relevant to security, compliance, and operations — from a diverse range of data sources, systems, and applications throughout the extended enterprise

- **Visibility** and **intelligence** into a rapidly changing threat and vulnerability landscape, across an increasingly dynamic and diverse enterprise computing infrastructure
- **Analytics**, which are increasingly augmented by *artificial intelligence (AI)* and *machine learning (ML)* capabilities, to help operational staff prioritize and act on the most relevant indicators
- **Automation** of the manual, repetitive, time-consuming, error-prone aspects of investigations and workflows — which frees up technical staff to focus on higher-value activities, and allows analysts to spend more time being analysts

A platform-oriented approach to security monitoring also helps companies to make more complete and effective use of the incredible volume of data that is continuously being generated by their computing infrastructure, including:

- The *logs* that continuously record information about the events that take place throughout an organization's computing infrastructure — including its network devices, servers, virtual machines, cloud service providers, endpoints, operating systems, applications, and databases.
- The *log*, *information*, *event*, *flow*, and *session* data also being generated by the organization's existing portfolio of security solutions — such as endpoint security software, intrusion detection and prevention systems, identity and access management systems, and a wide range of other potential sources.
- *Threat intelligence* from third-party sources — which ideally is part of an integrated, automated process of collection, correlation, evaluation, and dissemination of insights into the "who, what, where, when, and how" of active attack campaigns.

Some Empirical Evidence That We're Getting Better

Although security monitoring capabilities have organically evolved and matured over the past several years, Aberdeen's research has also shown that the pandemic of 2020 contributed to a more immediate and accelerated rate of change. For example, the mean percentage of resources allocated to *pre-incident* **"identify / protect"** capabilities upon entering 2020 shifted sharply, in the early months of the pandemic, towards adding more *post-incident* **"detect / respond / recover"** capabilities. This adjustment has helped organizations to cope with pivoting virtually overnight to support the new normal of employees, data, applications, and infrastructure in a predominantly **Work From Home / Work From Anywhere** model.

Log Management solutions are designed to address the process of generating, transmitting, aggregating, storing, and eventually disposing of log data.

Security Information and Event Management (SIEM) solutions are generally complementary to Log Management, in that they are designed to *ingest*, *interpret*, and *act* on security-related log, information, event, flow, session, threat intelligence, and other data from a diverse range of sources.

Security Orchestration, Automation, and Response (SOAR) is a more recent term used to describe the incorporation of complementary capabilities for threat and vulnerability management, incident response, and security operations into a platform-oriented approach.

Even so, empirical evidence supports the case that enterprise investments in more comprehensive security monitoring capabilities have provided increasingly positive results in recent years (see Table 2). For example:

- **Attacker dwell times** (the time from attacker compromise of enterprise resources, to defender detection) have been shortened from a global median of 99 days, to 56 days
- The ratio of attacker dwell times for **internal detections** of compromises, as compared to those for *external notifications* of compromises, have been reduced from 75% to 21% (i.e., internal detections have become significantly faster)
- The number of public **data breach** disclosures involving records (e.g., names, addresses, emails, social security numbers, payment card data, and so on) has declined year-over-year

Table 2: Enterprise Investments in Advanced Security Monitoring Capabilities Have Provided Increasingly Positive Results

Indicators of Security Monitoring Effectiveness	2016	2017	2018	2019
Global median attacker dwell times (days)	**99**	**101**	**78**	**56**
Ratio of attacker dwell times for internal detections vs external notifications	**74.8%**	**30.9%**	**27.4%**	**21.3%**
Number of public data breach disclosures involving records	**298**	**257**	**125**	**32**
Global median attacker time to data breach (days)				**21**

Source: Empirical data adapted from Mandiant *M-Trends* 2020 and PRC *Data Breach Chronology*, 2016-2019; Aberdeen, December 2020

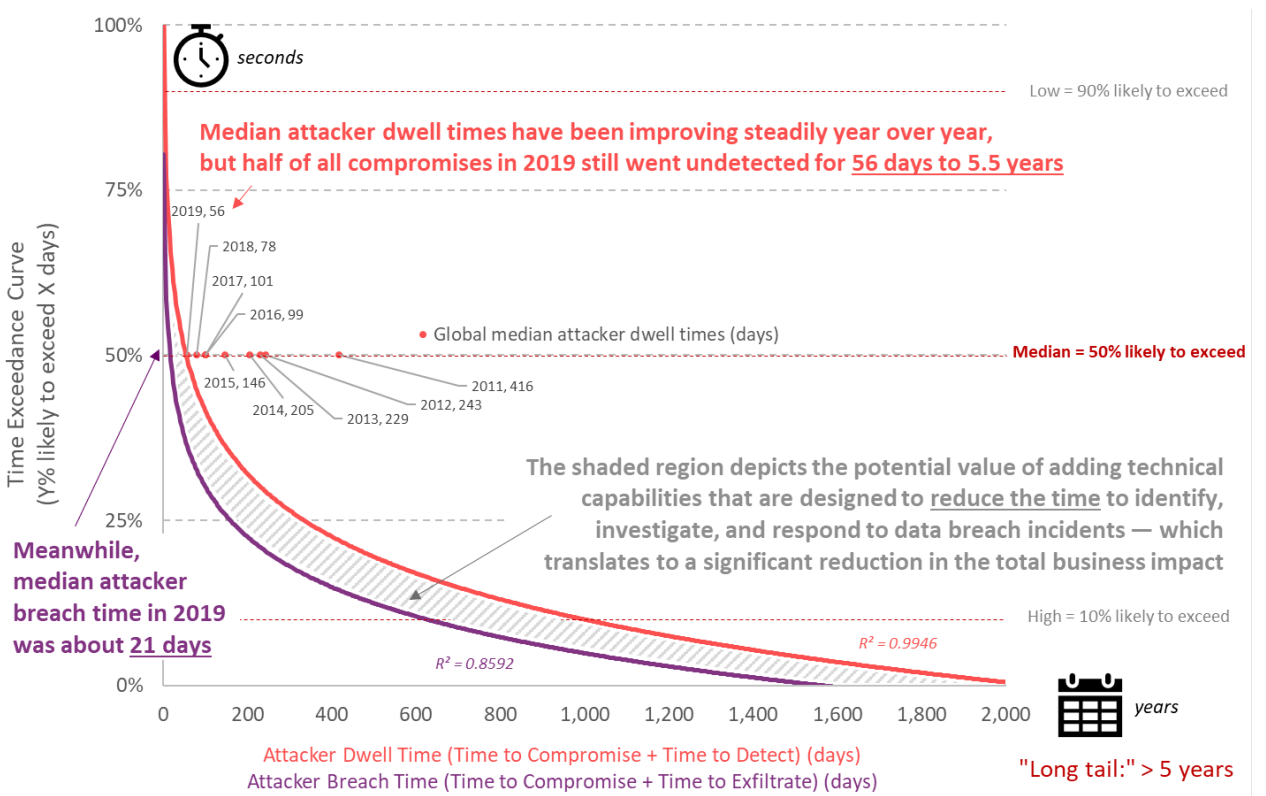
In spite of these improvements, however, additional progress is needed. For example, the **attacker breach time** (the time from attacker compromise to the successful exfiltration of enterprise data) was a global median of about 21 days in 2019 — a full *five weeks faster* than the global median of 56 days that it took for defenders to detect it. Clearly, defenders have the need for speed.

Some Empirical Evidence of the Need for Speed: Why Integration and Orchestration, Visibility and Intelligence, and Analytics and Automation Matters

The dimension of *time* has steadily become a central issue in the effectiveness of cyber security. For example:

- Computing infrastructure is complex and ever-evolving, and many organizations struggle to keep pace.
- Regulatory compliance requirements add still another level of complexity, while at the same time lagging behind the rate of change for the technology frontier.
- Time can be the single biggest driver of business impact, for incidents involving a disruption of services.
- Users routinely make real-time decisions about their actions and behaviors, which are often the last line of defense for security.
- As previously noted, the attackers are quick to identify and exploit vulnerabilities to gain access to enterprise systems, and quick to begin exfiltrating sensitive data — while the defenders are doggedly working to be faster at detecting, investigating, responding to, and recovering from successful compromises (see Figure 1).

Figure 1: Attacker Dwell Times for Confirmed Data Breaches Ranged from <1 Day to >5 Years in 2019, With a Global Median of 56 days — But the Median Time to a Successful Data Breach Was Just 21 days



Source: Empirical data adapted from FireEye *M-Trends* 2020 and Verizon *DBIR* 2019; Aberdeen, December 2020

In the bigger picture: improving **integration** and **orchestration**, **visibility** and **intelligence**, and **analytics** and **automation** with a *platform* approach to security monitoring initiatives is simply the tactical means to a strategic end. In Figure 1, the shaded region depicts the potential value of adding technical capabilities that are designed to **reduce the time** to identify, investigate, and respond to data breach incidents — which translates to a significant reduction in the total business impact.

To quantify the business value of faster detection and response compared to that of the status quo, Aberdeen developed a simple *Monte Carlo* analysis. Assuming that the business impact of a data breach is greatest at the beginning of the exploit, when the data is first compromised, Aberdeen's analysis estimates that *twice as fast* at detection and response compared to the status quo translates to *about 25% less business impact* — while *ten times faster* reduces the business impact by *about 75%*.

Quantifying the business value of faster detection and response, compared to that of the status quo:

- 2x faster = 25% less impact
- 10x faster = 75% less impact

Looking Forward: From Secure, Compliant, and Well-Managed, to Driving More Business Value

If a tools-based approach to security monitoring initiatives is undertaken merely to investigate what has already happened, or to generate static reports to satisfy the next auditor, the organization is missing out on the opportunity to *interpret the data* and *identify the actions needed* to extract additional business value from its enterprise computing infrastructure.

Looking forward, the most valuable IT and cyber security staff will be those who can successfully interpret the *implications* of the insights generated from security monitoring platforms — not only for staying secure, compliant, and well-managed, but also to proactively drive the *optimizations* in the enterprise computing infrastructure that will help the business to achieve its strategic objectives.

Summary and Key Takeaways

- A **platform**-oriented approach to security monitoring initiatives helps enterprises to achieve better:
    - **Integration** and **orchestration** of information relevant to security, compliance, and operations — from a diverse range of data sources, systems, and applications throughout the extended enterprise
    - **Visibility and intelligence** into a rapidly changing threat and vulnerability landscape, across an increasingly dynamic and diverse enterprise computing infrastructure

- **Analytics**, which are increasingly augmented by *artificial intelligence (AI)* and *machine learning (ML)* capabilities, to help operational staff prioritize and act on the most relevant indicators
- **Automation** of the manual, repetitive, time-consuming, error-prone aspects of investigations and workflows — which frees up technical staff to focus on higher-value activities, and allows analysts to spend more time being analysts

- Empirical evidence supports the case that enterprise investments in advanced security monitoring capabilities have provided increasingly positive results in recent years:
  - **Attacker dwell times** (the time from attacker compromise of enterprise resources, to defender detection) have been shortened from a global median of 99 days, to 56 days
  - The ratio of attacker dwell times for **internal detections** of compromises, as compared to those for *external notifications* of compromises, have been reduced from 75% to 21% (i.e., internal detections are significantly faster)
  - The number of public **data breach** disclosures involving records (e.g., names, addresses, emails, social security numbers, payment card data, and so on) has declined year-over-year
- Even so, additional progress is needed. For example, the **attacker breach time** (the time from attacker compromise to the successful exfiltration of enterprise data) was a global median of about 21 days in 2019 — a full *five weeks faster* than the global median of 56 days that it took for defenders to detect it. Clearly, defenders have the need for speed.
- To quantify the business value of faster detection and response compared to that of the status quo, Aberdeen developed a simple *Monte Carlo* analysis. Assuming that the business impact of a data breach is greatest at the beginning of the exploit, when the data is first compromised:
  - Aberdeen's analysis estimates that *twice as fast* at detection and response compared to the status quo translates to *about 25% less business impact* — while *ten times faster* reduces the business impact by *about 75%*.

About Aberdeen

Since 1988, Aberdeen has published research that helps businesses worldwide to improve their performance. Our analysts derive fact-based, vendor-neutral insights from a proprietary analytical framework which identifies Best-in-Class organizations from primary research conducted with industry practitioners. Aberdeen provides intent-based marketing and sales solutions that deliver performance improvements in advertising click-through rates and sales pipelines, resulting in a measurable return on investment. Aberdeen is headquartered in Waltham, Massachusetts, USA.

18264