KB

THE BUSINESS VALUE OF A SECURITY MONITORING AND ANALYTICS PLATFORM

September 2018

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

ABERDEEN

As **security monitoring and analytics** initiatives mature, a **platform** approach reduces the **time** to *identify*, *investigate*, and *respond* to security-related incidents — and drives a significant reduction in **risk**.

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

Above and beyond the most obvious requirement for their enterprise computing infrastructure — i.e., to deliver the intended value to the business and its users — today's organizations are doing their best to address three simultaneous and closely interrelated objectives:

- Identify and assess security-related **risks**, and manage them to an acceptable level
- Achieve, sustain, and demonstrate **compliance** with policies and regulatory requirements
- Improve the **efficiency** and **cost-effectiveness** of ongoing operations, e.g., to provide greater flexibility and scale, at lower total annual cost

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

Unfortunately, Aberdeen's recent benchmark study of more than 360 organizations also found that most are neither fully secure nor fully compliant — despite their considerable level of investment. Over the last 12 months:

- About **3 out of 5 (58%)** enterprises experienced **at least one data breach** (median = 3).
- About **3 out of 4 (75%)** enterprises experienced **at least one non-compliance issue** (median = 3).
- A **median of 30%** of the overall **IT operations budget (OpEx)** is being allocated to the achievement and reporting / certification of compliance with data privacy and security requirements — making these resources unavailable for digital transformation or other strategic initiatives, at a potentially enormous *opportunity cost*.

Modern enterprises want their computing infrastructure to be secure, compliant, and well-managed. Aberdeen's research has consistently shown that the *order* of priority given to these three objectives is correlated with top performance.

Data breach: A confirmed incident of unauthorized access to any of the various types of enterprise data subject to compliance requirements, of any size.

Non-compliance issue: A finding / observation identified as an audit deficiency or other instance of non-compliance that is substantial enough to require remediation or a plan for remediation, i.e., an issue that cannot be deferred or ignored.

Some of the key activities for the respective segments of the secure, compliant, well-managed trifecta are summarized in Table 1.

Table 1: The Enterprise Computing Infrastructure of Top Performers 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 policies and regulatory requirements (*auditing and reporting*) • Report on status and posture for senior management, line-of-business owners, and other stakeholders (*dashboards*) • Report progress against an initial baseline and targeted metrics (*work progress*)	**Manage Security-Related Risks** • Monitor network activity, end-user activities, and privileged user activities • Monitor endpoints and back-end resources • Detect, investigate, and respond to anomalous behaviors, security incidents (attempts), and breaches (successful compromises) • Do forensic investigations of active threats • Detect and prevent 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., ISO, NIST, ITIL, COBIT) • Optimize efficiency of day-to-day management and administration (*automation*) • Optimize performance of networks and applications • Increase visibility / correlate with additional data sources

Source: Aberdeen, September 2018

It's common for companies to get started on security monitoring and analytics initiatives with an investment in **tools** that are typically used 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 simple compliance and reporting, to adopt a more strategic, proactive, **platform**-oriented approach to security monitoring and analytics. A platform approach helps enterprises to achieve better:

- **Integration** of data relevant to security, compliance, and operations — from a diverse range of sources
- **Visibility and intelligence** into a rapidly changing threat landscape, and an increasingly complex computing infrastructure
- **Analytics** — increasingly augmented by *artificial intelligence (AI)* and *machine learning (ML)* capabilities — to help operational staff prioritize and act on the most relevant information, and to help drive even greater value from the computing infrastructure that is enabling the business to achieve its strategic objectives

Tools vs. Platforms: In making a distinction between "tools" and "platforms" Aberdeen is simply reflecting a basic pattern of evolution, which can be seen in several solution categories:

- A mixed bag of lower-level **tools** for specialized IT staff
- Enterprise self-integration of **point solutions**
- Vendor-integration of **product suites**
- Vendor / ecosystem-integration of **platforms** for higher-level analysts (e.g., SOC)

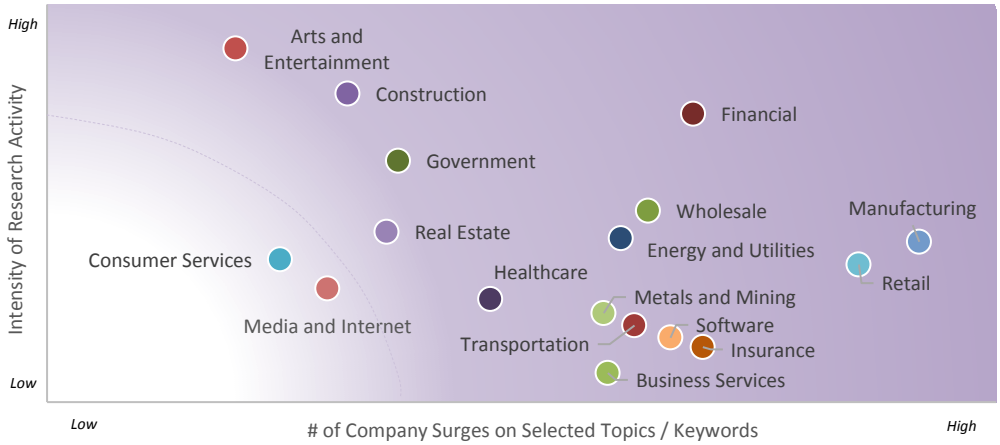
A *platform* approach to security monitoring and analytics helps companies make more complete use of the incredible volume of data that is already being generated by their existing computing infrastructure, for example:

- The *logs* that continuously record information about the events that take place throughout an organization's computing infrastructure — including network devices, servers, virtual machines, endpoints, operating systems, applications, and databases.
- The *log*, *information*, *event*, *flow*, and *session* data also being generated by the organization's existing 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 automates the collection, correlation, evaluation, and dissemination of insights into the "who, what, where, when, and how" of active attack campaigns, and allows analysts to spend more time being analysts.

Empirical Insights into Current Market Interest in Security Monitoring and Analytics: The Fortune 1000

To gain some fact-based insights into the current market interest in security monitoring and analytics platforms, Aberdeen analyzed the online research activities for selected topics / keywords by the Fortune 1000 over a six-week period in Q3 2018. Across virtually all industry sectors represented, both the *volume* and *intensity* of research activity on these topics was higher than the established baseline — indicating nearly universal high interest (Figure 1).

Figure 1: Online Research Activity on Security Monitoring, Security Analytics, AI, ML, SIEM in the Fortune 1000 During Q3 2018



Source: Adapted from Bombora Company Surge, Aberdeen, September 2018

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, and threat intelligence, and other data from a diverse range of sources.

Illustrative Solutions Landscape: Security Monitoring and Analytics

- **IBM Security** (*QRadar*)
- **MicroFocus** (*ArcSight ESM*)
- **McAfee** (*Enterprise Security Manager*)
- **Dell Technologies** (*RSA Security Analytics*)
- **AlienVault** (*Unified Security Manager*)
- **Trustwave** (*SIEM Enterprise*)
- **LogRhythm** *(Threat Lifecycle Platform)*
- **Splunk** *(Splunk Enterprise)*
- **Rapid7** *(InsightIDR)*

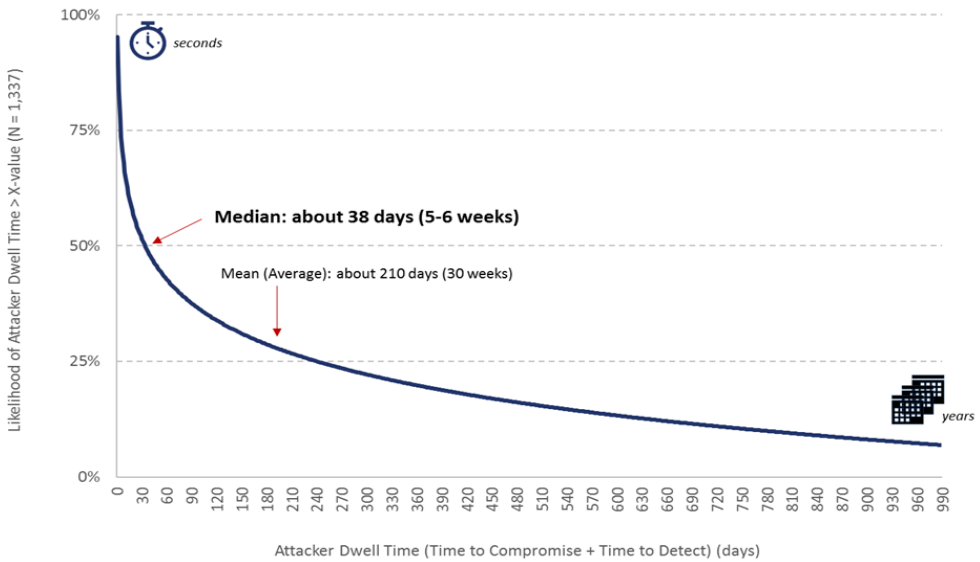
The Race Against Time: Why Integration, Visibility and Intelligence, and Analytics in InfoSec Matters

In the bigger picture, improving integration, visibility and intelligence, and analytics with a platform approach to security monitoring and analytics initiatives is simply the *tactical means* to a *strategic end*. One significant source of business value from a platform approach is derived from **reducing the time** needed to identify, investigate, and respond to security-related incidents — from a status quo capability ranging from days to weeks, to an "after" capability ranging from minutes to hours.

The dimension of time has quietly become a central issue in the realm of information security. The incredible rate of change in computing infrastructure has led to such **complexity** in our networks and systems that most organizations struggle with the capabilities and resources to keep up. The required **regulatory** responses to these issues are literally years behind. We know that time can be the single biggest driver of business impact in scenarios involving **disruption of services**. We know that **user behaviors**, which can be carried out in an instant, are often the last line of defense.

We also know, from more than a decade of empirical investigations published in the Verizon Data Breach Investigations Report (DBIR) series, that attackers are quick to identify and exploit vulnerabilities to **gain access to enterprise systems**, and quick to **begin exfiltrating sensitive data** — while defenders are trying desperately to be faster to **detect**, **respond** to, and **recover** from successful compromises (see Figure 2).

Figure 2: Empirical Attacker Dwell Time for Confirmed Data Breaches



Source: Adapted from Verizon DBIR dataset, Aberdeen, September 2018

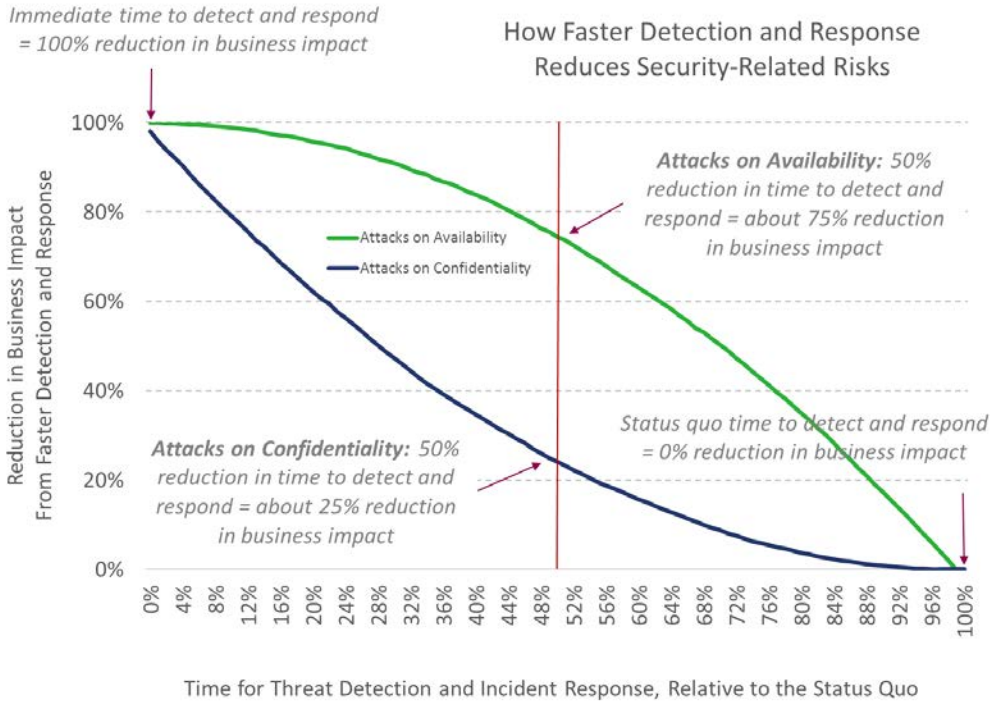
Based on the empirical investigations of **more than 1,300 confirmed data breaches** over the three-year period of 2014 to 2016, Figure 2 shows the distribution of *Attacker Dwell Time* — defined as the sum of *Attacker Time-to-Compromise* and *Defender Time-to-Detect* — which ranges from seconds to years. The **median** is **about 38 days**. To mitigate the risk of data breaches, defender performance using current approaches is simply too little, too late.

Qualitatively, with better integration, visibility and intelligence, and analytics to help see what's happening in their enterprise computing infrastructure, defenders can significantly shorten the time to detect, respond, and recover. But the objective of the security professional is not merely to demonstrate the *technical need*.

In their dual roles as both *subject-matter experts* and *trusted advisors*, the primary objective of the security professional is to help the organization's senior leaders **make better-informed business decisions about risk**. The *business case* that needs to be made is this: How does faster detection, effective response, and rapid recovery **reduce the risk** of attacks on the availability, confidentiality, and / or integrity of enterprise computing infrastructure, applications, and data?

Leveraging better *integration*, *visibility and intelligence*, and *analytics* from a platform approach to security monitoring and analytics initiatives reduces the time to identify, investigate, and respond to security-related incidents — which translates to a significant reduction in business impact.

Figure 3: Quantifying How Faster Detection and Response Reduces the Business Impact from Disruptions, Data Breaches



Source: Monte Carlo analysis; Aberdeen, September 2018

Quantitatively, Aberdeen has developed a simple *Monte Carlo* model to estimate the business value of faster detection and response compared to the status quo, in two areas (see Figure 3):

- **Reducing the business impact of non-availability:** For attacks on the *availability* of enterprise computing infrastructure, the business impact from a sustained disruption is presumed to grow from the time of compromise to the time of remediation. Incorporating this assumption into its Monte Carlo model, Aberdeen's analysis shows that *twice as fast* at detection and response compared to the status quo translates to *about 75% less business impact* — while *10 times faster* reduces the business impact by *more than 95%*.
- **Reducing the business impact of a data breach:** For attacks on the *confidentiality* of enterprise data, the business impact from a successful data breach is presumed to be greatest at the beginning of the exploit, when the records are first compromised. Incorporating this assumption into its Monte Carlo model, Aberdeen's analysis shows that *twice as fast* at detection and response compared to the status quo translates to *about 25% less business impact* — while *10 times faster* reduces the business impact by *about 75%*.

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

If a tools-based approach to integration and analysis of diverse data sources is done 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 InfoSec staff will be those who can successfully interpret the *implications* of the insights generated from security monitoring and analytics platforms — not only for staying secure, compliant, and well-managed, but also to proactively drive the optimizations from enterprise computing infrastructure that will help the business achieve its strategic objectives.

Quantifying the Business Value of Faster Detection and Response

For attacks on availability:

- 2x faster = 75% less impact
- 10x faster = 95% less impact

For attacks on confidentiality:

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

Summary and Key Takeaways

- A **platform**-oriented approach to security monitoring and analytics initiatives helps enterprises to achieve better:
    - **Integration** of data relevant to security, compliance, and operations — from a diverse range of sources
    - **Visibility and intelligence** into a rapidly changing threat landscape, and an increasingly complex computing infrastructure
    - **Analytics** — increasingly augmented by *AI* and *ML* capabilities — to help operational staff prioritize and act on the most relevant information, and to help drive even greater value from the computing infrastructure that is enabling the business to achieve its strategic objectives
- Demonstrating the **technical need** for faster detection and response is a legitimate part of the puzzle — but the big picture is incomplete without also making a **business case** for how faster detection and response reduces the organization's **risk**. To help make better-informed business decisions about risk, security professionals need to develop a solid understanding of both — and learn how to be more effective at communicating it to senior leaders.
- Quantitatively, Aberdeen has developed a simple *Monte Carlo* model to estimate the business value of faster detection and response compared to the status quo, in two areas:
    - **Reducing the business impact of non-availability:** *Twice as fast* at detection and response compared to the status quo translates to *about 75% less business impact* — while *10 times faster* reduces the business impact by *more than 95%*.
    - **Reducing the business impact of a data breach:** *Twice as fast* at detection and response compared to the status quo translates to *about 25% less business impact* — while *10 times faster* reduces the business impact by *about 75%*.

About Aberdeen Group

Since 1988, Aberdeen Group 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. The resulting research content is used by hundreds of thousands of business professionals to drive smarter decision-making and improve business strategies. Aberdeen Group is headquartered in Waltham, Massachusetts, USA.

17658