TAKING YOUR SIEM PLATFORM TO THE NEXT LEVEL, WITH MANAGED DETECTION AND RESPONSE

ABERDEEN GROUP | MICRO FOCUS | PALADION

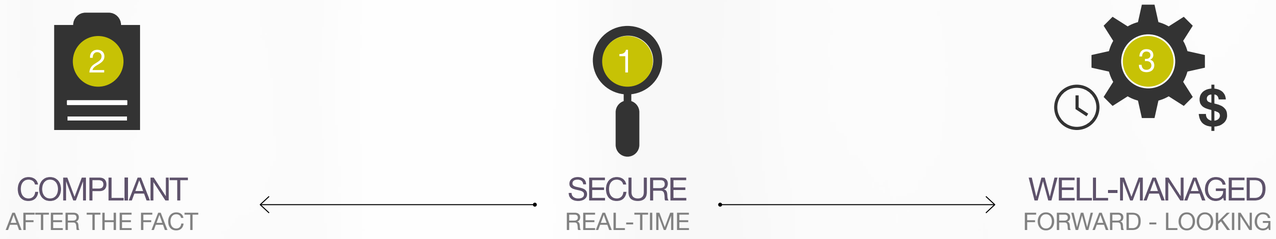
Executive Summary

To keep up with the complexity and compliance of their computing infrastructure, and to get ahead of the time advantage of the attackers, enterprise security operations centers need to build on the foundation of their existing SIEM platform with additional capabilities for active threat detection and faster incident response. Aberdeen Group's research quantifies the business value of time in these areas, and shows how market growth favors the use of specialized security service providers.

What Enterprises Want from Their SIEM Platform: Security, Compliance, and Operational Efficiency

In their quest to keep their computing infrastructure secure, compliant, and well-managed, many enterprises have gone beyond the use of tactical tools for simple compliance and reporting. Leaders have adopted a more proactive, platform-oriented approach to security monitoring and analytics, based on security information and event management (SIEM) solutions.

ABERDEEN'S RESEARCH HAS SHOWN THAT TOP PERFORMERS ARE
1) SECURE 2) COMPLIANT 3) WELL-MANAGED



Achieve and Sustain Compliance

- ▶ Demonstrate compliance with policies and regulatory requirements (auditing and reporting)
- ▶ Report on current 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, privileged user activities, and end-user activities
- ▶ Monitor endpoints and back-end resources
- ▶ Detect, investigate, and respond more quickly to suspicious behaviors, security incidents (attempts), and breaches (successful compromises)
- ▶ Conduct forensic investigations faster and more efficiently
- ▶ 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

Taking Your SIEM Platform to the Next Level, With Active Detection and Faster Response

Several forces are driving a significant shift in how enterprise security operations centers (SOCs) need to be run, which calls for taking your SIEM platform to the next level:

COMPLEXITY

The incredible rate of change in information technology infrastructure, which has led to much greater complexity in our networks, systems, and applications

COMPLIANCE

Regulatory and legal responses to these issues, and the intensifying requirements for demonstrating compliance

THREATS

Attackers who are increasingly sophisticated, focused, and successful

To keep up with complexity and compliance — and to get ahead of the current time advantage of the attackers —enterprise SOCs need to build on the foundation of their existing SIEM with additional capabilities such as advanced monitoring, advanced threat detection, accelerated investigation, and faster incidence response.

ADVANCED THREAT MONITORING

leverages the rules engines of the leading SIEM platforms, in combination with the specialized expertise and focus of full-time threat hunters, to make continuous improvements in use cases.

ADVANCED THREAT DETECTION

combines context-specific data with analytics and machine learning, to look for suspicious patterns and anomalies across a wider range of both historical and real-time data.

ACCELERATED INVESTIGATION

of suspected incidents makes use of increasingly automated triage, prioritization, and validation of alerts based on context-specific data — in addition to a final review and validation by human analysts.

FASTER RESPONSE

to incidents replaces purely ad hoc activities with common playbooks, analytical tools, incident management tools, and reporting — which liberates security analysts to spend less time doing research, and more time doing analysis.

Why Active Detection and Faster Response Matter: Quantifying the Business Value of Time

Reducing the total time needed to detect, investigate, respond, and remediate security-related incidents — from the status quo of weeks and months, to hours and days — can be a significant source of business value for the defenders. In Aberdeen's analysis, being twice as fast at detection and response, compared to the status quo, translates to:

30%

less business impact for attacks on the **confidentiality** of an information asset (i.e., a confirmed data breach)

70%

less business impact for attacks on the **availability** of enterprise resources (i.e., a confirmed disruption of normal operations)

ATTACK LIFECYCLE

Attackers identify vulnerabilities by doing reconnaissance of the target organization's networks, systems, and applications; implement and execute the exploits to selected vulnerabilities; and sometimes automate the exploits to run at scale. Additionally, attackers may also modify the exploits as the target organization happens to identify and eliminate the underlying vulnerabilities, staying one step ahead of the defenders.

IDENTIFY VULNERABILITIES ▶

IMPLEMENT EXPLOITS ▶

EXECUTE EXPLOITS ▶

AUTOMATE EXPLOITS ▶

MODIFY EXPLOITS ▶

DETECTION & RESPONSE LIFECYCLE

To identify anomalous behavior that signifies a potential attack, followed by assessment, containment, and remediation of the incident, and ultimately by the restoration of the infrastructure to its pre-incident state. In the worst-case scenario, the organization identifies all anomalous behavior only after exploits are already being run at full scale. In the best-case scenario, the organization identifies all anomalous behavior when the attacker is doing their initial reconnaissance.

◀ IDENTIFY ANOMALOUS BEHAVIOR

◀ ASSESS INCIDENTS

◀ CONTAIN INCIDENTS

◀ REMEDIATE INCIDENTS

◀ IMPLEMENT ADDITIONAL COUNTER MEASURES

Market Growth in Threat Detection and Incident Response Favors the Use of Specialized Security Service Providers

Many organizations lack the resources and the tactical focus to perform well at these activities, because their primary, strategic focus is naturally on running and growing their business — not on security, compliance, privacy, and risk. Even if an organization is capable, is it really better off doing this on its own — or would it be better off leveraging the expertise, scale, and scope of a specialized, third-party security service provider? In the classic business decision of "build or buy" (i.e., in-house, or outsourced) for active threat detection and faster incident response, Aberdeen's research shows that literally all the market growth favors the use of specialized security service providers.

In the category of security information and event management:

▶ PLANNED GROWTH FOR **IN-HOUSE** DEPLOYMENTS:

-3% (i.e., there is a deliberate move away from in-house installations)

▶ PLANNED GROWTH FOR **OUTSOURCED** DEPLOYMENTS:

150% (i.e., there is a deliberate shift towards the use of security service providers)

WATCH WEBINAR ➡

READ FULL REPORT ➡

16281

Created by Aberdeen Group. Brought to you by Paladion