SOLUTION BRIEF

SIEM: Five Requirements that Solve the Bigger Business Issues

After more than a decade functioning in production environments, security information and event management (SIEM) solutions are now considered mature. Capabilities such as event collection, correlation, alerts, and demonstrating compliance with regulatory mandates are foundational, and most SIEM solutions address these needs. But the landscape is changing. Organizations face new threats such as targeted and persistent attacks; new trends like mobile, cloud, and virtualization; and shifting business priorities around customer acquisition, operational efficiencies, and cost savings. As a result, SIEM use cases require more advanced capabilities to solve bigger business issues.

McAfee spoke with SIEM users and asked them to tell us about their primary issues with SIEM. Here are their top five issues:

- Big Data security
- Situational awareness
- Real-time context
- Ease of management
- Integrated security

For SIEM to help usher in more effective security and risk management strategies—particularly as they relate to threat mitigation, embracing trends, and aligning with business priorities—these five issues must be addressed. Each issue is described here along with corresponding customer case studies and use cases.

1: Big Data Security

Big Data security can be extremely valuable—if you're able to use it. Legacy SIEM solutions weren't designed to integrate with such a broad number of endpoint, network, and data sources, nor intended to process such high event rates or maintain such long retention policies. As a result, relational databases and similar legacy SIEM shortcomings designed primarily with network-centric events in mind simply don't meet the security needs of today's dynamic IT infrastructures. They lack the speed, extensibility, and scalability to be effective and usable.

Case study: federal government

A large government agency was interested in applying advanced analytics to the Big Data security stored within its SIEM's multipetabyte relational database. But even simple reports took hours to render, and some took more than a day, making the agency's SIEM unusable for forensics.

By switching to McAfee® Enterprise Security Manager as its SIEM solution, the agency was able to expand the number and types of integrated devices—adding more data-centric and user-centric context to its analytics. The agency also increased event rates and stored data. Now, reports render in minutes, improving the entire approach to forensic analysis.

2: Situational Awareness

There was once a time when SIEM was simply a tool to correlate events across firewalls and intrusion detection systems, and then perhaps apply some vulnerability assessment data. Even today, there are some SIEMs that rely primarily on network flow data. While all of these sources are important, they need to be enriched with application, data context, and identity information. Without that, it takes more time and resources to understand and prioritize events with enough situational intelligence to be actionable and timely.

Case study: healthcare provider

A regional healthcare provider embraced the idea of "bring your own device" (BYOD) to increase staff agility by supporting personal tablets. Yet, because of past incidents, the provider was concerned about insider abuse. The healthcare provider's prior SIEM solution lacked the ability to understand which users were interacting with sensitive data regardless of the device—laptop, desktop, tablet, or virtual desktop.

Use Case: Big Data Security

- Expand data capture with more feeds from more sources
- Perform analytics and forensics on very large data sets
- Optimize for the speed and volume requirements of Big Data security
- Increase employee and process efficiencies

Use Case: Situational Awareness

- Enrich situational awareness with more identity solutions.
- Resolve who, when, how, where, and what.
- Understand how long, who else, and what else.
- Include BYOD assets, such as laptops and smartphones.

With McAfee Enterprise Security Manager, the healthcare provider connected with identity and mobility management, active directory, and LDAP products to gain user and device awareness. Because of integration with structured and unstructured data stores, such as native database support, as well as integration with data loss prevention (DLP) and database activity monitoring (DAM), there was more complete situational awareness and improved insider threat mitigation.

3: Real-Time Context

One of the earliest SIEM use cases was log management—collect, store, and query with a few extra bells and whistles. Logs are still a foundational component of SIEM, but today's SIEMs also need real-time context.

Examples of such context are McAfee Global Threat Intelligence (McAfee GTI) and McAfee Vulnerability Manager. McAfee GTI provides a real-time, cloud-based reputation service and McAfee Vulnerability Manager collects organizational information about asset vulnerabilities.

Case study: retailer

A Fortune 100 retailer without a production SIEM and no McAfee solutions conducted a proof-of-concept. Within the first week, the retailer discovered that more than 30% of the traffic attempting to enter its network was from malicious sources and/or contained malicious payloads.

Using McAfee Enterprise Security Manager to correlate event information with McAfee GTI, the retailer quickly identified which assets were being targeted across all their store locations and data centers and came to a better understanding about the types of attacks targeting the organization. The McAfee SIEM solution determined the highest level of severity and then prioritized a response. SIEM paired with real-time context allowed for more rapid threat detection, prioritization, and remediation.

4: Ease of Management

Legacy SIEMs have very rigid architectures and lack a few essential capabilities. For example, they don't easily integrate with previously unsupported devices to make information usable. But a next-generation SIEM, on the other hand, is easy to customize and flexible enough to fit any given environment. This is exactly what makes a next-generation SIEM strategic for so many organizations.

Case study: utility company

A major utility company needed to employ security controls to prevent Stuxnet-like attacks from impacting the infrastructure and causing blackouts for millions of customers. With McAfee Enterprise Security Manager, the utility company achieved situational awareness across corporate IT, SCADA, and industrial control system (ICS) zones with native device, application, and protocol support.

Use Case: Real-Time Context

- Understand threats inside and outside the environment.
- Improve SIEM intelligence with real-time context.
- Reduce incident identification and response times.
- Identify and prioritize threats with additional security intelligence inputs.

Use Case: Ease of Management

- Deploy SIEM with dynamic whitelisting and hardware-assisted security to protect fixed-function devices.
- Simplify forensics with customizable drill downs.
- Integrate SIEM with firewall and intrusion prevention systems (IPS) for rapid incident response.
- Gain more life from legacy assets because of improved security.

The McAfee SIEM provided the customer with the tools to do their own custom integration with the SCADA and ICS devices. That in turn allowed correlation, anomaly detection, and trend analysis across all three zones. Beyond customized event collection, the customer quickly and easily built unique dashboards, reports, correlation rules, and alerts. This made SIEM an invaluable tool for security, demonstrating compliance with regulatory mandates, and asset availability—in other words, it kept the lights on.

5: Integrated Security

SIEM is an important component of any strategic security initiative, but it's still just one of many. Integration across security and compliance solutions delivers more together than just the individual solutions alone, while a non-integrated architecture creates complexity. Complexity is why security often remains largely tactical instead of becoming more strategic and aligned with business priorities.

Case study: financial services

A multinational banking customer owned a wealth of disparate products from various vendors. Some products were in production, but many were not regularly used or maintained because of limited resources. The bank determined that by leveraging SIEM in conjunction with integrated endpoint, network, and data controls, it could more effectively mitigate risk and reduce costs while also making security more business-relevant.

The bank reduced the number of vendors and gained economies of scale. It was able to decrease training costs and the number of agents, consoles, servers, and more. This also lowered contract costs and a multitude of associated expenses. Beyond cost savings, the bank ensured that all existing and future solutions were fully integrated with McAfee Enterprise Security Manager to ensure better controls and visibility to its security posture.

Key Considerations

- How important is the ability to easily handle the collection, storage, access, processing, and analytics challenges that Big Data security presents?
- Are your security stakeholders getting the information they need when they need it to make informed decisions and take timely actions?
- Does your security team have the real-time context it needs to identify risks and attacks before they can cause harm?
- What would be the security and resource impact if you used a SIEM with intuitive drill downs and easily customizable views?
- How would integration across your infrastructure improve your security, visibility, processes and responsiveness?

Use Case: Integrated Security

- Streamline security and operations work flow.
- Simplify complexity with automation and easy customization.
- Improve visibility and situational awareness with security solutions that work together.
- Deliver better security with intelligence and integration.

What worked in the previous decade with legacy SIEMs simply doesn't address today's requirements. With new requirements around Big Data, security intelligence, situational awareness, performance, usability, and integration, SIEM use cases have expanded. SIEM solutions should reduce complexity, not create it. Expect more from your SIEM.

Today, SIEMs need to operate as part of a larger, connected security framework where security and business priorities are aligned. SIEM plays an important role in making security more strategic and providing real business value.

To learn more about SIEM solutions from McAfee, please visit: **www.mcafee.com/SIEM**.

Integrated Security

McAfee provides a unified, integrated framework for hundreds of products, services, and partners to learn from each other, share context-specific data in real time, and act as a team to keep information and networks safe. Any organization can improve its security posture and minimize operational costs through the platform's innovative concepts, optimized processes, and practical savings.

McAfee™
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

61099brf_focus-5-siem_0514B
MAY 2014