CHECKLIST

Turning Piles of Security Data Into Risk Management Insight

FortiSIEM Offers a Business-critical Insight and Shorter Time to Value

Organizations are seeking to address accelerating cyber crime with proactive threat detection and event response. However, they need more efficient ways to handle the deluge of event data generated by their security and network devices. FortiSIEM meets this need with a comprehensive security information and event management (SIEM) solution. An integral part of the Fortinet Security Fabric, FortiSIEM features automated workflows and integrated threat intelligence, helping organizations to improve their risk posture, even with lean security staffs.

Here Are 5 Reasons Why CISOs Should Consider FortiSIEM:

☑ Preconfiguration for shorter time to value

Eliminating the need for time-consuming integration efforts, FortiSIEM offers broad, out-of-the-box device support and a flexible ingestion engine that facilitates customization for region-specific or industry-specific security devices.

Built on a high-performance architecture, FortiSIEM readily scales to support businesses through all stages of growth. Because it is available as an all-in-one virtualized solution, FortiSIEM can be deployed anywhere, without the complexity of architecting a multi-component solution.

☑ High-fidelity, prioritized alerts

FortiSIEM incorporates several unique technologies for real-time event correlation and analysis. For example, the topology of the network provides valuable context for event analysis. Adding this information manually, however, can be time-consuming and error-prone. FortiSIEM features an intelligent infrastructure and application discovery engine, which automatically maps the physical and virtual infrastructure, both on-premises and in public and private clouds.

Further, dynamic user identity mapping correlates users with their network (IP) addresses and devices, while threat-intelligence services add context to alerts. This adds insight on top of the infrastructure view. Finally, patented technology enables distributed processing of information and enforcement of policies to speed detection and response times.

These features, together with robust rule sets and advanced analytics, enable FortiSIEM to prioritize threats, flagging those that require immediate attention.

☑ Automated incident mitigation

Applying the principles of security orchestration, automation, and response (SOAR), FortiSIEM enables organizations to respond to an incident automatically or alert a human operator. The decision depends on the event's level of risk and complexity, as well as the organization's comfort with automation. Whatever method is employed, response time is minimized due to seamless integration between FortiSIEM and the rest of the Fortinet Security Fabric, including Fabric-Ready Partner solutions and even a wide range of other third-party components.

☑ High-value business insights from a single pane of glass

Unlike typical SIEM solutions, FortiSIEM can present event information in a business context. For example, the SIEM dashboard can be configured to present the status of the company's ecommerce service, rather than the status of the individual devices (e.g., servers,

applications, networking equipment, security tools, etc.) that power that service. This enables the security team to monitor the availability as well as the security of the business.

Most importantly, a single staff member can oversee all SIEM activities from a central console and provide different role-based views and permissions to staff members or teams.

☑ Compliance-ready reporting

Integration unlocks automation across the entire kill chain—including SIEM, zero-touch deployment, and network access controls. Automating security processes enables security staff to extract themselves from daily log reviews and other manual processes and to focus on activities pivotal to the business. It also enables threat detection, prevention, and response in real time.

Conclusion

A powerful tool for organizations of all sizes, FortiSIEM shortens time to value, supports business growth, brings order to overwhelming volumes of security alerts, and lessens the burden on lean security teams. Highly reliable and easy to deploy, FortiSIEM offers CISOs a low-risk way to drive significant improvements in cybersecurity incident management.

October 18, 2019 2:59 AM

456963-0-0-EN

D:\Fortinet\Checklist\FortiSIEM Solution Selection\cl-turning-piles-of-security-data-into-risk-management-insight-v1