ZONES™

Case Study

Security Information & Event Management

Security FORTIFICATION | Authentication & Data Security

A medical system increases advanced threat visibility with SIEM real-time threat analysis.

The valuable PHI that healthcare organizations hold makes them prime targets for malware and other cyberattacks. With SIEM solutions, healthcare IT security teams get real-time, consolidated, and general views into security events, which can help keep sensitive patient data safe and secure and help prevent potential HIPAA violations. Recently, Zones nfrastructure,® the Services Company of Zones, helped a nationally recognized non-profit medical system improve its security posture, extending the value of the IT team, by implementing a leading-edge SIEM solution.

Challenge

- Gaining real-time analysis of security alerts generated by application and network hardware.

Solution

- Security Information and Event Management (SIEM) implementation.

Results

- Improved visibility to cyberattacks.
- Cut security incident response time.
- Reduced data breach and data loss risk.
- Ensured compliance with HIPAA standards and industry best practices.

ZONES

Security Information & Event Management

Case Study | Security FORTIFICATION | Authentication & Data Security

The Challenge

Entrusted with the security of patient health information (PHI) and operating in a highly regulated environment, the CISO of this regional medical system needed to implement the latest security technology combining advanced threat detection, basic security monitoring, digital forensics, and incident response capabilities. The organization's existing solution was multiple revisions out-of-date and required careful analysis and planning to re-implement without losing the data and existing integrations.

The Solution

After Identifying key weaknesses in existing policies, procedures and standards, Zones configured and implemented a leading-edge SIEM solution to enable the medical system's IT security team to improve their security efficacy through continuous visibility into threats and risks plus actionable analysis to guide their triage and speed investigations and the orchestration of security remediation. Key phases of the project included development of a comprehensive implementation framework, as well as data processor and data indexer implementation, file integrity management (FIM) agent implementation, staff training, and runbook documentation.

The Results

Leveraging SIEM technology, Zones simplified IT security for the healthcare provider by enabling improved threat visibility and reduced latency with real-time collection and analysis from host systems, security devices and network devices, combined with contextual information for threats, users, assets, and data. The organization's new SIEM solution provides long-term event and context data storage and analytics for scalability. As a result, this healthcare provider has improved its overall security posture, with the capability to more effectively protecting its patient's health data and help meet its HIPAA compliance requirements.

2018441_Security Information & Event Mgmt Case Study_180814