SIEM DATA PROTECTION

Steve Martinson, Advisory Services Consultant
Stephen Inocencio, PhD, VP Advisory Services

The SIEM Catalyst

The most frequently cited catalyst to the advent and growth of the Security Information and Event Management (SIEM) industry is the passing of HIPAA (Health Insurance Portability and Accountability Act) in the U.S. in 1996. Since then, organizations have been aware of the importance of enabling system/audit logging, aggregating data, and securely analyzing it in order to enable their business to better manage the needs of their clients, business partners, and external regulatory and compliance requirements. Besides protected health information (PHI) such as medical records, laboratory tests, and insurance information, similar aggregation and protection needs exist for educational information (e.g., enrollment records and transcripts), financial information (e.g., credit card numbers, banking information, tax forms, and credit reports), and sensitive corporate data (e.g., user passwords and system/endpoint information). As expected, along with long-standing controls frameworks like ISO 27002, other industry standards like the PCI DSS emerged soon after HIPAA's adoption that also emphasize the need for a properly managed SIEM that spans all critical assets and data.

Checking the Box or Usage Best Practices?

Despite nearly 25 years of increasing awareness of why SIEM is needed and intervening improvements in the technology and solutions that enable its capabilities, a general "check-the-box" mentality still exists wherein organizations acquire and implement a SIEM tool in order to satisfy an external driver. Companies continue to overlook the best practices related to information security management and governance and how the SIEM solution aligns to data protection and compliance efforts such as privileged account management (PAM), data loss protection (DLP), encryption of sensitive data, and foundational policies for data classification. With the addition of data privacy initiatives like the EU's General Data Protection Regulation (GDPR) and state-level legislation like the California Consumer Privacy Act (CCPA), the need to ensure that you document what you are doing with sensitive data, why, and the precautions taken to secure that data becomes a top priority for not only the CIO or the CISO but all of your key stakeholders, including the CEO. Businesses are accountable for protection of internal data and IP just as much as they are for protecting client data. Data leaks from within are just as dangerous (sometimes even more dangerous) then an external breach. Hence why it behooves security executives to better manage IP / data within the SIEM platform.

Where to Begin?

Most companies do not protect SIEM data, and that has led to risks and loss of IP. Starting with governance, organizations must have policies and standards in place that define the types and classes of data requiring protection and how they are protected, including SIEM data. Standards must be in place for:

- Robust access controls
- Exfiltration controls for both external channels and internal processes and users
- Encryption in transit and at rest
- Data retention and secure disposal

Protecting SIEM Data

Access control is a core tenet of proper security management that is associated with many layers of data protection. Managing internal, remote, and third-party access to SIEM data is no different than that of traditional data stores and repositories. If possible, the wholesale encryption of the SIEM repository would be best, but data access paths from multiple computing layers and sources coupled with data decryption routines often adds too much overhead that negatively impacts the user experience. However, since SIEM data is typically stored in a database, the hashing of specific data elements and use of lookup tables to replace the sensitive data fields with random IDs is a common method for controlling access by APIs and general users. Of course, the ability to be field-specific with security controls requires that the foundational sensitive data mapping be done. Fortunately, SIEM tools usually provide detailed database schemas that allow pinpoint alerting to be enabled.

For privileged user access and account management with SIEM data, most SIEM tools provide file integrity monitoring (FIM)-like access detection and reporting functions that enable you to detect log data change attempts no matter the source, whether originating inside or outside the data storage zones. Even before privileged access to SIEM data can be attempted, the many PAM password vaults available offer secure escrow of privileged accounts and passwords, controls on elevated task execution, privileged session recording, and robust reporting and alerting for all privileged user access. The ability to generate alerts on all access attempts to SIEM data that occur – whether via the prescribed application and programmatic methods or from direct connections or queries – provides the base level of DLP required by most IT security compliance and governance frameworks.

If your organization knows what its sensitive data elements are, where they reside – including all occurrences in consolidated log repositories – and understands the business use cases for accessing the SIEM data, the management of risk associated with that data is much more easily accomplished.

Contact GDT to discuss your options and which preventative measures are a best fit to protect your data today.