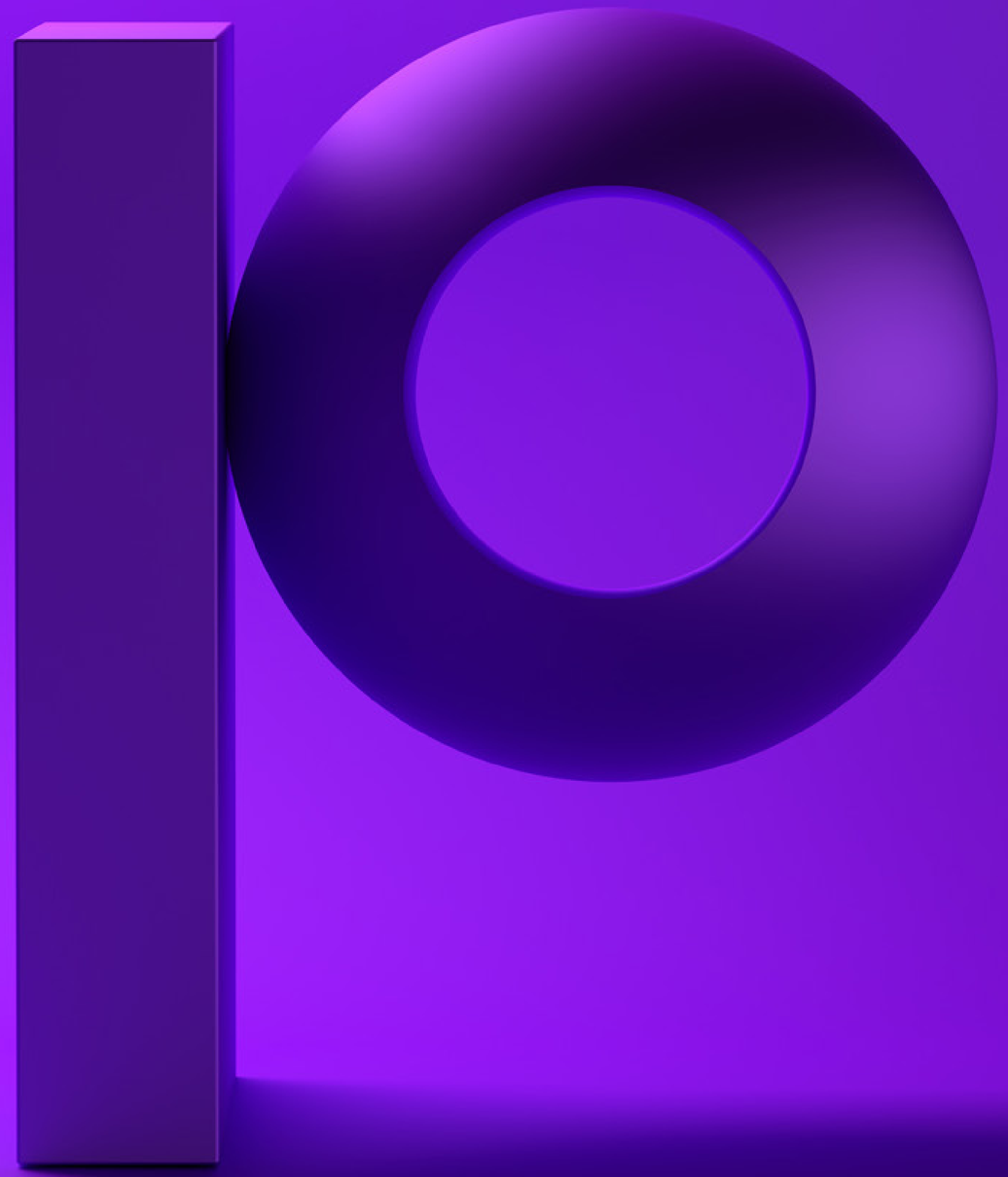
precisely

The Role of Mainframe Data in the Enterprise SIEM



Introduction

Security information and event management SIEM is an important function – and often a distinct department at many companies and government organizations. Security issues are top of mind for many CSOs (chief security officers) and CISOs (chief information security officers), but it affects many others in IT, including mainframe professionals. Let's take a look at what SIEM is, why it is relevant to you, and the state of the function and related areas.

Every week, the news reports about new data breaches at companies, individuals and government organizations continue. The frequent attacks underscore the importance of (and need for resourcing for) defensive and proactive countermeasures. As collecting, managing and analyzing both security information and security events has become more critical, SIEM solutions have become the preferred option for effectively managing the security challenges of today's environments.

SIEM software products and services utilize security management information and security events generated by IT infrastructure hardware and applications to provide real-time security threat identification, alerting and analysis. (see Figure 1). In addition to strengthening security, SIEM systems have also become essential for gathering and managing operational intelligence in large corporations and government organizations.

The mainframe SMF and log files you're familiar with are your mainframe's record for security-relevant information and events. The information they contain about what happened within your mainframe, who did what, who tried to do what, and so on, are critical for managing your organizations IT security. As powerful as they are, without access to your SMF and other logs, SIEM platforms simply cannot provide complete or effective security coverage. From a security management perspective, any component of IT which is not visible to the SIEM platform is a huge security hole, an unguarded open door that invites and enables cyber-attacks from without and within.

The Case for SIEM

An attack by an "insider" (i.e., employee or other person with authorized access to at least one system) is a very real concern for many organizations. It can no longer be assumed that the interview process and background check prove that someone is "safe" to have system access or that insider-based damage would be contained to just the system/s for which they were granted access. Among others, "SQL injection" and "Pass the Hash" attacks (where a low priority system is accessed and the attacker grabs the hash table to gain access elsewhere) are now common enough that they have nicknames. They may be utilized by current or former "insiders" familiar with the weaknesses within an organization's IT infrastructure.

Next to a compliance mandate (e.g., IRS Publication 1075, GDPR, PCI DSS, HIPAA/protected health information-related audits, etc.), suffering a damaging and/or embarrassing breach seems to be the biggest driver of new budget dollars for SIEM initiatives at many organizations.

While the stigma of a breach has lessened as more organizations are hit, it will still motivate a management team to take action with real dollars sooner than later and a SIEM solution is often a key part of the post-breach response.

As the SIEM platform market continues to grow, a number of software vendors are developing solutions and competing for a presence in this space. In a recent Magic Quadrant report for SIEM, the research and advisory firm Gartner stated that the need for early targeted attack detection and response is driving the expansion of new and existing SIEM deployments. From an awareness perspective, the news we see every day continues to provide ample publicity for SEIM adoption.

Consider all the potential internal and external points of "threat," and the full path a transaction or piece of data may take within your IT systems, and you get the picture. If you consider how many systems, servers and other machines (including a mainframe) that a simple ATM or mobile banking transaction touches, you can see how old silos within IT can no longer be tolerated from a security perspective.

While no solution can guarantee your organization is 100 percent safe, not doing what can be done, with readily available SIEM tools and your own company's machine data, can be viewed as professional negligence (or worse) by CSOs and CISOs. This fact is fueling the intense, growing interest in the category and substantial product development investments by SIEM solution vendors.

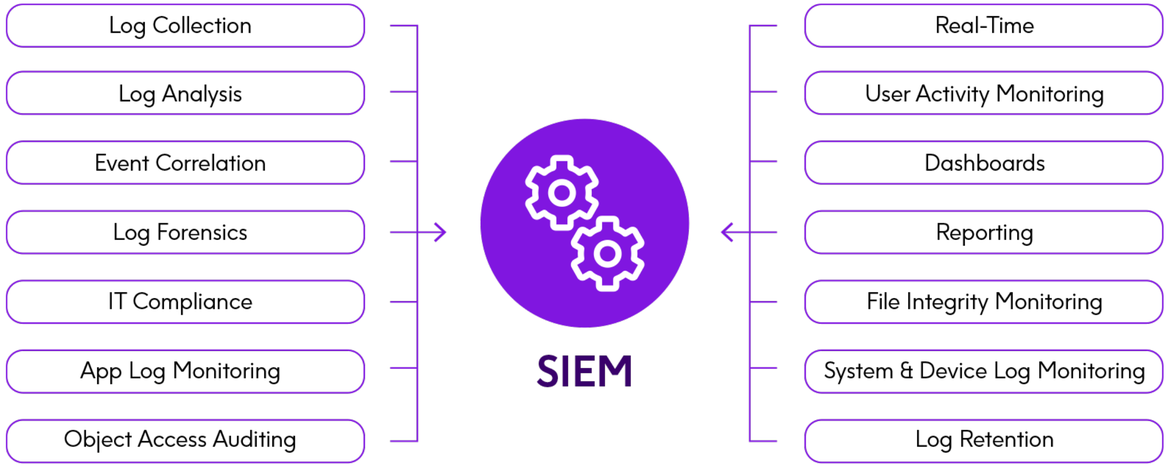


Figure 1

Effective SIEM requires that all the, event and "log" collection, search, visualization, and other security-specific activities traditionally done at a "silo" level, now must be integrated to include and correlate all relevant security information and security events from the entire enterprise, including especially all the SMF, log file and other security information generated by your business-critical mainframes. With proper IBM zOS security applied, your mainframe may well be nearly impenetrable. But from a SIEM implementation perspective, that is irrelevant.

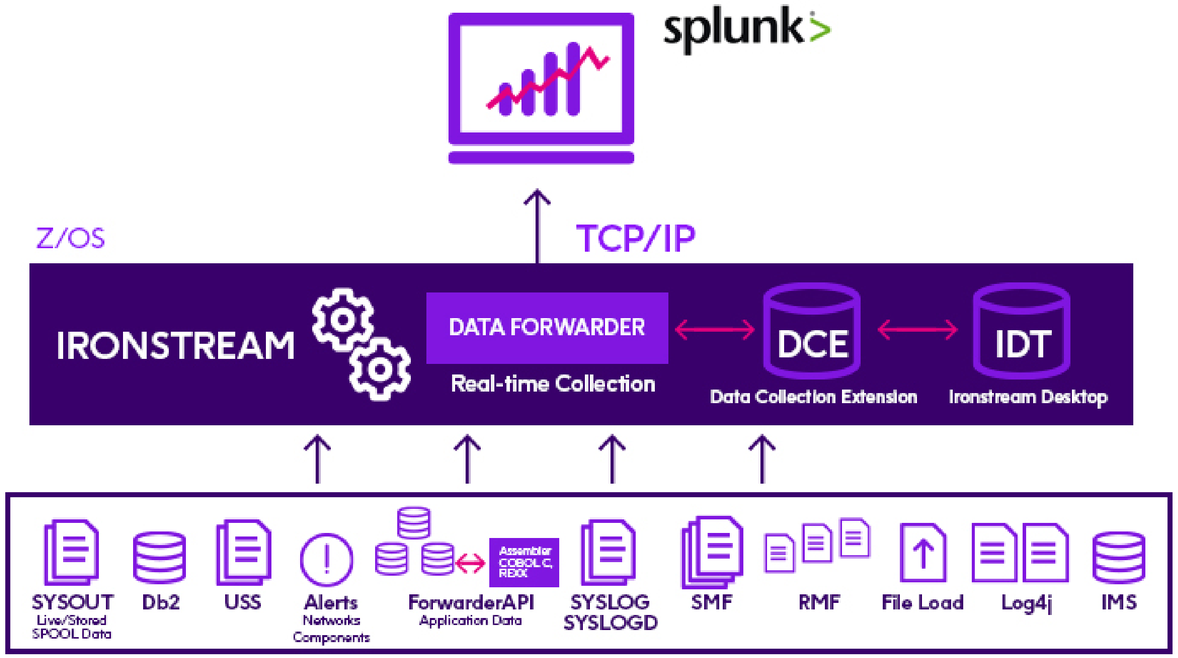
Mainframes are extremely high value targets for hackers. Experienced hackers, for example, will test multiple points of entry across an organization's IT landscape to find a weak spot, so even a failed log in attempt from a particular source, when correlated with others elsewhere across the company, looks much more suspicious viewed through an enterprise-wide SIEM lens. If mainframe log in attempts are not available to the SIEM system for analysis, the signature of a highly dangerous threat may be completely missed.

Integrating Mainframe into SIEM

With governments and companies across all industries under mounting pressure to better secure their data (and show how they're doing it), and financial services and insurance firms being required to pass more difficult and more frequent audits, SIEM solution adoption is increasing exponentially. Because your organization relies on mainframes to support critical business applications, these systems must be part of your SIEM solution for true enterprise-wide visibility of, and protection from, security threats. However, even leading SIEM platforms like Splunk don't natively support your mainframe, leaving a security blind spot that puts your organization at risk.

You need a comprehensive, single view of your entire IT infrastructure for early detection and threat response across all your systems. Unfortunately, integrating these legacy platforms into SIEM solutions can be extremely difficult. Legacy systems have a range of data sources and proprietary data formats that require specialized skills to integrate and analyze.

Precisely's Ironstream for Splunk solution provides automated, seamless forwarding of mainframe, as well as IBM i, machine data to Splunk to support your security and compliance initiatives. Ironstream continually collects security data from a wide range of IBM mainframe and IBM i sources, transforms it, and forwards it to Splunk in real-time. Once in Splunk, you're SIEM team is able to analyze the information in the context of your overall enterprise IT infrastructure.



Learn how Ironstream for Splunk can help your organization with its security and compliance mandates.

References

- Pass the Hash: https://en.wikipedia.org/wiki/Pass_the_hash
- IRS Publication 1075: https://www.irs.gov/pub/irs-pdf/p1075.pdf
- HIPAA: http://www.hhs.gov/hipaa/for-professionals/index.html
- DISA: http://disa.mil/
- Gartner Magic Quadrant for SIEM: http://www.splunk.com/goto/SIEM_MQ

precisely

Precisely is a global leader in data integrity, providing accuracy and consistency in data for 12,000 customers in more than 100 countries, including 90 percent of the Fortune 100. Precisely enables companies to integrate, verify, locate, and enrich their data to power better business decisions. To learn more, visit www.precisely.com.

www.precisely.com