RAPID7

BUYER'S GUIDE

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) SOLUTIONS

Practical advice for choosing your first (or next) SIEM

Introduction: Welcome to the New Frontier of SIEM Page 3

Chapter 1: Protecting Against Today's Threats Page 4

Chapter 2: SIEM for Threat Detection, Monitoring, and Incident Management Page 6

Chapter 3: Evaluating SIEM Solutions
- Data Collection Page 8
- Analytics Page 9
- Response Across the Incident Lifecycle Page 10

Chapter 4: Considering Managed Detection and Response Page 11

Chapter 5: Deploying a SIEM with Rapid Time-to-Value Page 12

Next Steps Page 13

About Rapid7 Page 14

Introduction:

WELCOME TO THE NEW FRONTIER OF SIEM

While security information and event management (SIEM) solutions have been around for the better part of two decades, modern SIEMs don't quite resemble their original, log management counterparts. As the security landscape has evolved, SIEMs have evolved as well (at least, some of them have).

The most effective, automated solutions today include user behavior analytics (UBA), attacker behavior analytics (ABA), deception technology (intruder traps), and other innovations to detect both known and unknown threats, provide comprehensive network visibility, and accelerate threat investigation and response.

While successful SIEM deployments measurably reduce risk, there's a big gotcha: SIEM deployment projects often fail. Even after all these years, too many organizations struggle to deploy a new SIEM, achieve rapid success, and deliver a return on investment. More often than not, it's because the chosen SIEM didn't align with the specific needs, maturity, and resources of the organization deploying it.

Whether your organization is currently SIEM-less, or you're exasperated and exhausted by your current SIEM, trying to negotiate the security products market to find the right SIEM solution for your organization can turn into a full-time job. (Which clearly is not an option because your full-time job is identifying and reducing risk across your company employees and information assets.)

This guide will help you rein in the SIEM evaluation effort by quickly introducing today's SIEM market, including what SIEM solutions can offer and how their capabilities can align and customize to your specific needs. You'll learn about the top three capabilities every SIEM must provide and the questions to ask vendors to understand how well they deliver on that functionality.

SIEM solutions drive growth in worldwide security spending

According to Gartner, security testing, IT outsourcing, and security information and event management (SIEM) solutions will be among the fastest-growing security subsegments driving growth in the infrastructure protection and security services segments. Worldwide spending on enterprise security is forecasted to reach $96 billion in 2018.[1]

[1]Gartner, "Gartner Forecasts Worldwide Security Spending Will Reach $96 Billion in 2018, Up 8 Percent from 2017," December 7, 2017.

01

PROTECTING AGAINST TODAY'S THREATS

While the good guys are using security solutions and best practices to gain the upper hand against cybercriminals, it can still be an arms race when it comes to emerging technologies. Take big data and artificial intelligence (AI) as one example. Like their white-hat counterparts, cybercriminals are starting to use machine learning and AI to mine big data for insights. In the case of cybercriminals, they are employing these technologies to help them hone their attacks and make them more successful.

For organizations that aren't keeping up with security advances, data breaches are still hitting hard, with tens of millions of personal, financial, and health records falling into the wrong hands every year. According to the Identity Theft Resource Center, 2017 hit a record high with 1,579 data breaches disclosed, a 45 percent increase compared to 2016.[2]

Spear phishing and social engineering continue to evolve. In its 2018 Data Breach Investigations Report, Verizon reports that phishing and pretexting are the two top tactics used in social engineering attacks.

Staying ahead of cybercriminals

Today's threat landscape is no doubt anxiety-provoking, but there are solutions available that help security teams stay ahead of cybercriminals. For instance, a SIEM solution that can centralize log and event data across a modern network can detect the stealthy behaviors that lead to breach, including account impersonation via stolen credentials and malicious lateral movement. By analyzing attacks seen across our Managed Detection and Response customers, Rapid7 research, and our incident response and pen test teams, we've found that attackers consistently attack three facets to gain unauthorized access to networks: (1) vulnerabilities, (2) misconfigurations, and (3) credentials.

Attack Vector	Why You Need Visibility	How SIEM Helps
Vulnerabilities	In more than 250 engagements, penetration testers exploited at least one in-production vulnerability 84 percent of the time.	Detects behaviors (e.g. privilege escalation and lateral movement) that surround vulnerability exploitation.
Misconfigurations	At least one network misconfiguration was successfully abused 80 percent of the time in penetration tests. With an internal scope to the assessment, that figure rises to 96 percent of the time.	Highlights user and asset misconfigurations (e.g. unknown admins, shared accounts, and file integrity monitoring).
Credentials	In 53 percent of pen tests, at least one credential was successfully captured.	Identifies suspicious authentications and, if applicable, triggers investigation workflows.

Source: Rapid7, "Under the Hoodie: 2018"

[2]Identity Theft Resource Center, "2017 Annual Data Breach Year-End Review," 2018.

ASK YOURSELF:
Why a SIEM?

Understand what's driving your need for a SIEM by asking yourself these questions:

What were the results of your most recent penetration tests?

What were the results of your latest incident response plan test?

How would you rate the quality and effectiveness of your threat intelligence? This includes intel your team may curate from attacks on your network.

What does SIEM success look like? Watch our webcast on "Smashing the Mold: What to Expect from Modern SIEM."

02

SIEM FOR THREAT DETECTION, MONITORING, AND INCIDENT MANAGEMENT

Chances are good that you're in the market for a SIEM because you need to improve your organization's ability to detect common threats. You may also be looking for a SIEM that can provide improved security monitoring and visibility (especially across today's hybrid, multi-cloud environments). Finally, if compliance reporting is an important driver, a SIEM should be able to assist with dashboards and ensuring security policy is being enforced.

To support these top use cases, as well as others, SIEMs need to provide three core capabilities (all of which are explored in more detail in Chapter 3):

- **Data collection:**
  Collect and centralize data from across your environment and make it easily searchable
- **Analytics:**
  Identify risk and threats by analyzing the data using multiple techniques
- **Response:**
  Help you take action on the results, via orchestration and reporting

The real difference between SIEM solutions in the market today is how they implement each of these capabilities. Some focus more on the data collection and management, while others emphasize their analytics over response. Some deliver comprehensive functionality across all three areas.

Traditional SIEM pitfalls to avoid

- **Alert fatigue:** Meaningful context and prioritization will help you avoid alert tsunamis.
- **Reliance on rules:** Not all signs of intruder activity are found in log files. Make sure your SIEM uses additional detection technologies (e.g., honeypots and honey credentials) to supplement log-based detection rules.
- **Long, complex deployments:** Look for an intuitive solution with out-of-the-box analytics and pre-built detections. Better yet, choose a cloud-based solution to avoid hardware and software installation and management.
- **No insight into user behavior:** Insist on user behavior analytics to detect the misuse of stolen or weak credentials.
- **Too much time and money spent managing data:** Choose a solution that offers asset-based pricing to avoid data overage expense.
- **Limited visibility into cloud services:** With more and more organizations moving to cloud-based solutions such as a Microsoft Office 365, Salesforce, and others, your SIEM needs to integrate with and monitor your cloud services and IaaS.

Assess your SIEM readiness

To avoid a SIEM mismatch and disappointing results, you'll need to carefully evaluate each aspect of these three functions and determine, based on an honest assessment of your team's skills and resources, whether the solution will meet your organization's needs. Questions to consider:

- What is your team's current level of security maturity? Everything-but-the-kitchen-sink SIEM solutions can easily overwhelm your staff with functionality for which your organization doesn't need for success.
- Does your staff have the internal skill sets around writing log queries, investigating alerts, incident response, and feeding investigation findings back into preventative defenses? Lack of skills is a common problem for companies and a frequent reason behind SIEM project failures. This doesn't mean you can't deploy a SIEM, but a managed detection and response (MDR) service may be a better fit for your current needs.
- Do you have tested, scalable processes around threat detection and investigation? Many teams struggle to investigate all the alerts they receive because validation and early triage requires jumping between multiple tools and searching across raw logs. Consider a SIEM with orchestration and automation capabilities, or supported integrations with third-party SOAR/SAO vendors. You can then automate repetitive processes—which can include threat containment—and manage common tools (Active Directory, EDR, Firewall & NAC) from the SIEM itself.

ASK YOURSELF: **What are your objectives for adopting a SIEM?**

The top use cases for SIEMs include: threat detection, monitoring and visibility, compliance reporting, and incident response management. However, there are many more. Before beginning your search for a SIEM, you should clearly identify your most important use cases and how you want to use a SIEM to support them. This will help you focus your efforts on only those solutions that clearly fit your needs, while tuning out the noise of a crowded marketplace.

03

EVALUATING SIEM SOLUTIONS

Let's look at each of the three core SIEM capabilities in more detail. Within each area, you'll find a list of questions to ask SIEM vendors to drill down into how the vendor implements the capability and why that's important.

Data Collection

The foundation of every SIEM is data collection; this aspect hasn't changed since SIEMs were introduced. What has changed is how the SIEM goes about it.

The SIEM you choose should help you manage all of the rich data generated by security programs, letting you centralize, search, and visualize all of your event and log data, and track authentication for all users across assets and services, including cloud-based services.

To avoid security blind spots, a SIEM solution should be able to monitor your entire network, including endpoints that aren't on-premises. Be wary of pricing models that are based on the quantity of data processed or indexed, which can discourage companies from adding important data sources. To reliably detect attacks, the SIEM solution needs to collect all of the activity that's happening on your network. Limiting data sources to save money can seriously impede the SIEM's ability to find threats.

ASK VENDORS:

How thorough is the vendor's data collection? SIEMs with a focus on detecting threats understand the importance of collecting data from across your entire environment, including data from integrated, or modular, endpoint detection and response (EDR) agents. Integrations with cloud services are standard in many SIEMs today, but make sure the vendor supports the services your company uses.

Is the vendor collecting data to support User Behavior Analytics (UBA)? A SIEM is the only security tool with a real shot at exposing malicious lateral movement and the use of stolen credentials by collecting data across your environment (e.g. Active Directory). You don't need a SIEM to make your firewall logs more searchable—you need a SIEM to detect threats you'd otherwise miss. That's why it's critical that your SIEM collects the right data to automatically identify risky users and external adversaries.

Where will the data be stored? The fewer full-time resources you have available to commit to security operations, the more you should consider a cloud-based (software-as-a-service) solution for your SIEM. While on-premises deployments require hardware and software management and upgrades to keep up with data growth, a cloud-based SIEM handles all the data storage, management, and security for you, with the reassurance that your event data stays out of attackers' hands.

Analytics

While traditional SIEM solutions deliver basic, rule-based analytics for correlating information at a network level, today's SIEM needs to provide advanced analytic capabilities to better detect threats, including multi-stage attacks and anomalous user behavior. Advanced analytics minimize false positives, prioritize alerts based on risk, and reduce the total number of alerts that analysts must investigate.

ASK VENDORS:

Does the SIEM help detect gaps across the MITRE ATT&CK framework?[3] If an attacker has internal access to your network, can the SIEM help you reliably detect the use of compromised credentials? Ask the vendor to show you how its solution provides detection capabilities across the ATT&CK framework.

How do the SIEM solution's detections evolve in response to emerging threats? With a monolithic, legacy SIEM, new detections need to be created by the vendor, deployed to the on-premises SIEM, potentially turned on by the analyst team, matched against relevant data, and then conceptually understood by the SOC analyst when it's triggered. This creates lag time and multiple points of failure that could lead to a missed threat. The benefit of a cloud-based SIEM is that the vendor can continuously update detections, keeping pace as attacker behavior evolves, with no additional effort or delay on your part to update the software.

Does the solution provide high-fidelity alerts and make it easy to investigate them? Instead of a mountain of false positives, SIEM solutions that generate high-fidelity alerts deliver a low volume of true positives that you can act on immediately. To determine this, ask the vendor how it tunes its detections and provides suppression of false positives. At the same time, make sure that you can also tune pre-built SIEM analytics to your environment. One way to do this is to ask for a proof of concept with the SIEM vendor and run attack simulation to test the solution's detections.

How will the investigative features in the SIEM make my analysts more efficient? Look for easy pivots into log and endpoint data, straightforward integrations into your existing workflows (whether that be via ticketing or chat systems), and containment and orchestration features so you're able to take direct action to contain or obtain forensic data around a threat.

Thinking of building your own SIEM?

Some organizations go the route of attempting to build their own SIEM to analyze log data using open source tools. However, even though open source software is essentially free, the upfront and ongoing investment in engineering and maintaining an in-house SIEM solution using open source can be significant, with considerable technical debt and risk.

Before you embark on a do-it-yourself initiative, ask whether you can invest sustaining cycles across your team to build something that probably isn't as full-featured as you need it to be.

[3]MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's lifecycle and the platforms they are known to target. You can learn more at: https://attack.mitre.org/wiki/Main_Page.

Response Across the Incident Lifecycle

To make the most of your SIEM choice, it should be able to both adapt to your existing processes, as well as accelerate response via security orchestration and automation (SOAR or SAO). Your processes will depend on your use cases, with different processes required for threat detection compared to compliance reporting.

For example, let's look at the process of incident response by stages, as defined by the SANS Institute:

Preparation

This stage is where you prepare your team to handle an incident at a moment's notice. It includes everything from setting policies and procedures to making sure your team has the tools it needs to respond, including a SIEM.

ASK YOURSELF: Does the SIEM provide full visibility into your environment (including context on vulnerabilities and your endpoints)?

Identification

Is it an incident? This phase is all around identifying and assessing potential threats. A high-fidelity alert generated by the SIEM could be the first evidence of an incident happening.

ASK YOURSELF: Can the SIEM help you detect the most likely threats your organization will face, with a combination of pre-built detections and the ability to tune and write custom rules?

Containment

This is where you work to limit the damage of a threat and prevent further compromise. A SIEM can help you quickly understand the scope of the incident and confirm that containment counter-measures were successful.

ASK YOURSELF: Once you've identified a threat, are you able to contain threats directly from the SIEM?

Eradication

At this point, the focus is on removal of the threat. A SIEM can help you validate that the threat has been eradicated properly from affected systems.

ASK YOURSELF: Does the SIEM provide investigation workflows, case management, and integrations with IT service tools to enable your team to collaborate using the same information, with visibility into "who is doing what?"

Recovery

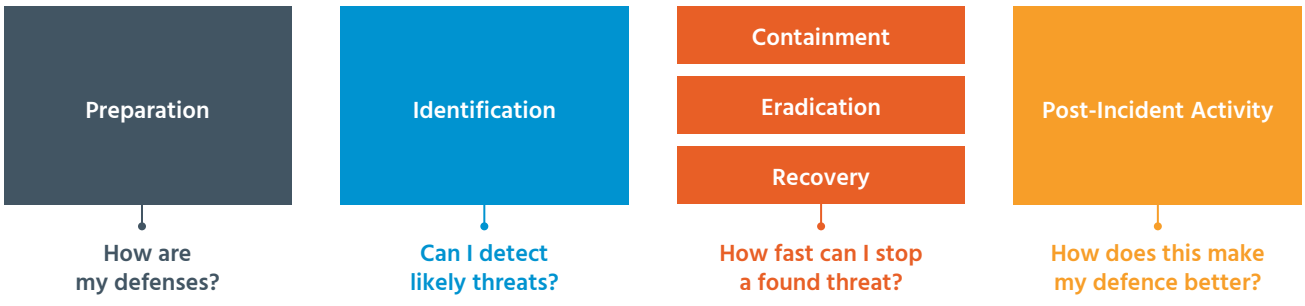
Once systems are back into production, you can use a SIEM to monitor that they aren't being re-infected or compromised.

ASK YOURSELF: Can the SIEM identify "normal" user behavior by creating a baseline for typical asset and user activity across your environment?

Post-Incident Activity/Lessons Learned

With the incident over, it's time to use lessons learned to improve your team's response and document the incident for future reference. Your SIEM should support tuning to help you use the insight from an incident to improve your security posture.

ASK YOURSELF: Does the SIEM have the ability to add threat intelligence gleaned from investigations to inform future detection efforts?



The Incident Response Process

Source: SANS Institute, the Incident Handler's Handbook

04

CONSIDERING MANAGED DETECTION AND RESPONSE

It's a rare (and usually extremely large) organization that has unlimited security resources, time, and budget. For nearly everyone else, constraints are a constant reality. If your organization is too resource-constrained—whether across people, budget, and/or skills—to deploy a SIEM, a managed service might be the best alternative.

Unlike a managed security service provider (MSSP) that monitors network security controls and sends alerts to you when anomalies are identified, but does not investigate or respond to threats, a managed detection and response (MDR) service acts as an extension of your security team, providing round-the-clock detection, as well as response. Using a turnkey approach, an MDR service helps your team detect and remediate threats, especially targeted advanced threats and insider threats.

If your organization lacks the resources or the expertise to support all of your SIEM use cases, consider managed, where you can get the combination of centralized log management backed by 24/7 monitoring by an experienced security partner.

ASK VENDORS:

Does the service employ user behavior analytics (UBA)? UBA is the only reliable method to detecting the use of stolen credentials and insider threats.

Does the service have a threat hunting methodology? Through the combination of layered analytics and threat hunting, security experts working on your behalf can identify unknown threats and incidents faster.

Does the MDR service offer 24/7/365 support? In the event of a security incident, you should be able to rely on the vendor to provide technical security expertise and breach response. The constant contact with your team as you work toward response and remediation is essential.

05

DEPLOYING A SIEM WITH RAPID TIME-TO-VALUE

While traditional SIEMs have been prone to project failure because of their complexity, a new breed of SIEM is changing that. Rapid7 InsightIDR is intuitive, easy-to-use, fast-to-deploy, always up-to-date, and adaptable.

It's a cloud-based solution focused on helping you detect and respond to threats as quickly as possible. Customers not only deploy in hours, but they find immediate value by identifying dangerous misconfigurations and user behavior.

Here's how the Rapid7 Insight platform helps across your incident response lifecycle:

- **Attacker Behavior Analytics:** InsightIDR comes with threat intelligence (to find behaviors, not static indicators) baked in. It's curated and maintained by our global security operations centers (SOCs) and threat intel team so you can stay ahead of emerging threats without any action from your end.
- **Containment:** You won't just find out about threats, you can take direct action to stop the spread of a threat. This includes managing existing EDR tools to kill a process or quarantine an asset. You also have the ability to take action on directory services, firewalls, and network access control tools all from within InsightIDR.
- **Expertise:** Rapid7 analysts are available to monitor your network 24/7 with our Managed Detection and Response service, IR (incident response) plan development, attack simulation, and IR retainers to make sure you're responding to threats with confidence. Rapid7 Managed Detection and Response is an extension of your security team and combines our InsightIDR technology and proprietary tools with real-time threat intelligence and world-class analysts to monitor your network around the clock. The best part? Their expertise and findings feed directly into InsightIDR, so all Rapid7 customers can benefit.

What Our Customers Are Saying

"Splunk and similar solutions just collect the logs ... but I want to know if something strange or irregular is happening, which InsightIDR tells me. It was the best solution to provide the intelligence I need for a reasonable price."

– Benjamin Nawrath, Energie Sudbayern [Read the case study >]

"[InsightIDR] was easy to implement and has provided tremendous value since day 1. With a single solution, we are now able to have visibility and monitoring of almost every asset on our network."

– IT System and Security Administrator, via Gartner Peer Insights
[Read the review >]

"One of things that I really like about InsightIDR is that the capabilities to blend a purely responsive incident management approach and a proactive hunting approach are there within the tool."

– Christopher Calvert, Visier
[Watch the testimonial >]

Next steps

Choosing the right SIEM has never been more important for the security of your business or organization. Letting your use cases, team skillsets, resource constraints, and risk exposure guide your selection is the best way to achieve sustainable, scalable success.

To learn more about how Rapid7 InsightIDR can be the SIEM solution you've been looking for, or to start a **free 30-day trial**, visit

rapid7.com/insightidr

Looking for **24/7/365** monitoring and threat hunting? Enlist our Managed Detection and Response team to be your army of cyber guardians. To learn more, visit

rapid7.com/MDR

ABOUT RAPID7

Rapid7 powers the practice of SecOps by delivering shared visibility, analytics, and automation that unites security, IT, and DevOps teams. The Rapid7 Insight platform empowers these teams to jointly manage and reduce risk, detect and contain attackers, and analyze and optimize operations. Rapid7 technology, services, and research drive vulnerability management, application security, incident detection and response (SIEM), orchestration and automation, and log management for more than 7,100 organizations across more than 120 countries, including 55% of the Fortune 100.

To learn more about Rapid7, visit www.rapid7.com.