IBM Security

Six Myths of SIEM

IBM

Exploring the 6 myths of SIEM

Have you investigated SIEM solutions lately?
Because things have changed.

Rumor says SIEM solutions are unwieldy and complex — and therefore only for large organizations. True, some SIEMs fall into the enterprise-only bucket, but this myth overlooks the more progressive SIEM solutions designed for businesses of all sizes.

It's no secret the cybersecurity industry is facing a major skills shortage. Security solutions — or otherwise — must be designed to enable you to be effective at your job, despite your (likely) limited resources. When evaluating modern SIEM solutions, look for the opportunities to empower your security team and maximize the resources you do have.

We'll tackle the top six myths about SIEM and investigate what you should expect from a SIEM today.

Myth #1

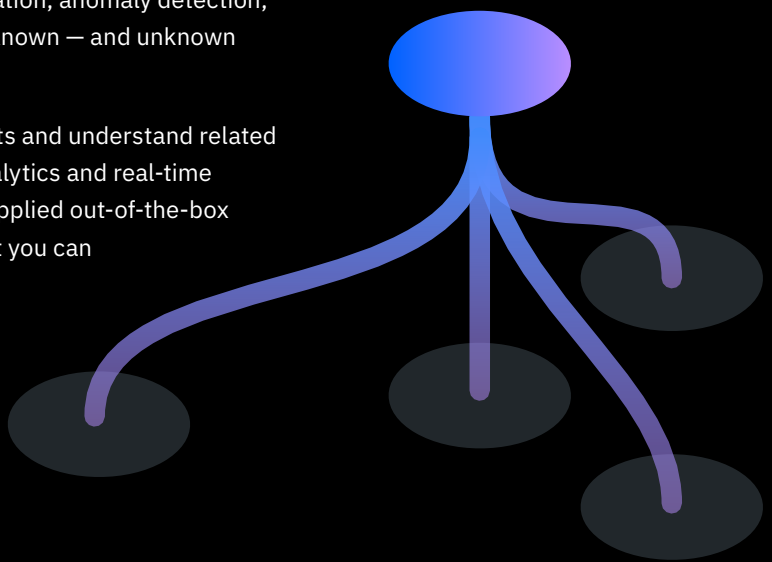
A SIEM can only detect known threats; it doesn't help with unknown threats.

SIEM solutions only use correlation to detect threats, and to write an effective correlation rule, you first need to know what to look for

Truth

Effective SIEMs use a combination of real-time correlation, anomaly detection, machine learning and behavior analytics to find both known — and unknown — threats.

They also use advanced correlation to connect the dots and understand related threat activities. When a combination of advanced analytics and real-time correlation are pre-built into your SIEM, they can be applied out-of-the-box to network, asset, user and application activity so that you can go well beyond just known threats to also identify anomalous activities that can indicate unknown threats.



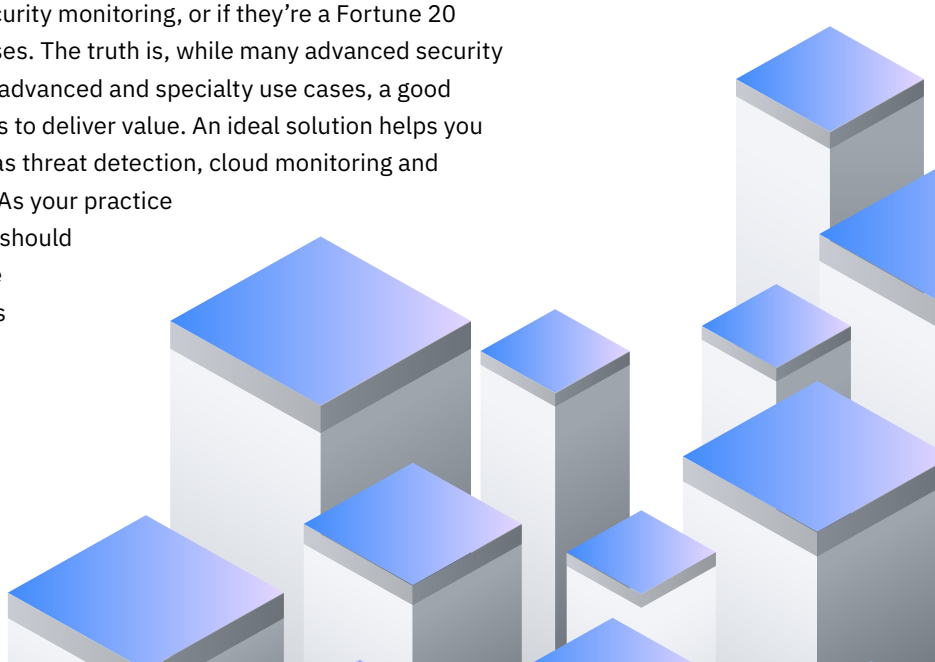
Myth #2

SIEMs are only for large enterprises with advanced security teams.

Conventional wisdom says because the best SIEM solutions on the market can scale to support the largest organizations, they're only intended for the largest organizations.

Truth

The best SIEM solutions address a wide variety of organizations, regardless of if they're a growing business just getting started with security monitoring, or if they're a Fortune 20 global enterprise in need of advanced use cases. The truth is, while many advanced security teams prefer all the bells whistles to support advanced and specialty use cases, a good SIEM doesn't require all the bells and whistles to deliver value. An ideal solution helps you to get started with standard use cases, such as threat detection, cloud monitoring and compliance reporting — right out-of-the-box. As your practice matures and your business grows, your SIEM should scale to support more environments, multiple geographies and advanced use cases, such as deep-packet inspection, DNS analytics and tightly integrated security orchestration, automation and response (SOAR).



Myth #3

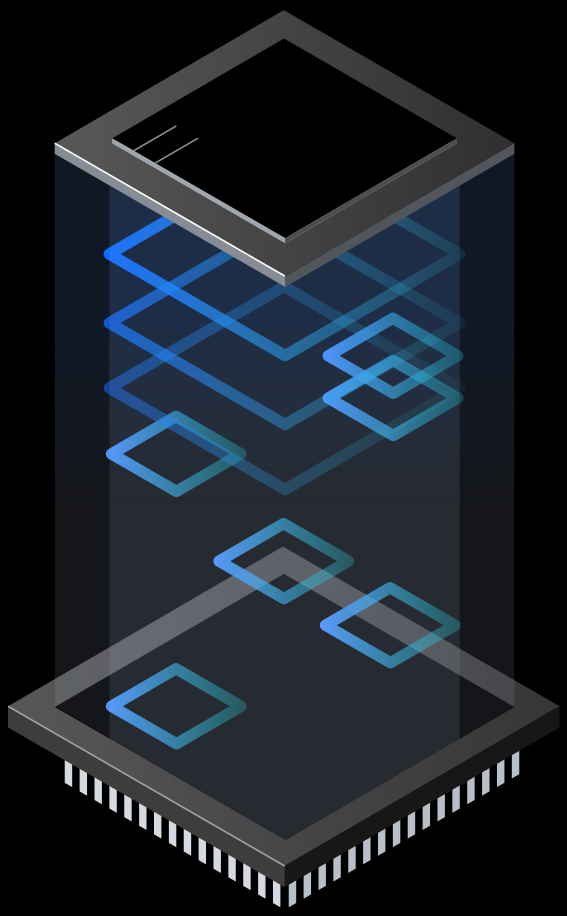
SIEMs require a great deal of data and the cost of collecting all that data is extremely high.

Because certain vendors in the market are known for becoming prohibitively expensive very quickly, some security teams assume that all SIEMs are also that way.

Truth

If you're considering vendors that charge based on the amount of data stored, it can get very expensive, very quickly. But different vendors price their solutions differently.

Before you commit to anything, think about what problem(s) you're trying to solve: Are you a retailer with payment card data to protect? Is your business migrating to Amazon Web Services and you need visibility into that new environment? The data that you collect for security purposes should help you to address your unique use cases. Don't be swayed into analyzing everything if you don't need to analyze everything. That said, if you've also got data-retention requirements, thanks to regulations or organizational policies, your SIEM vendor should be able to provide a low-cost option for storage, search and reporting only. By analyzing only what's important to your unique organization and sending the rest of your log and event data to low-cost storage, you can take on a SIEM project without it consuming your entire budget.



Myth #4

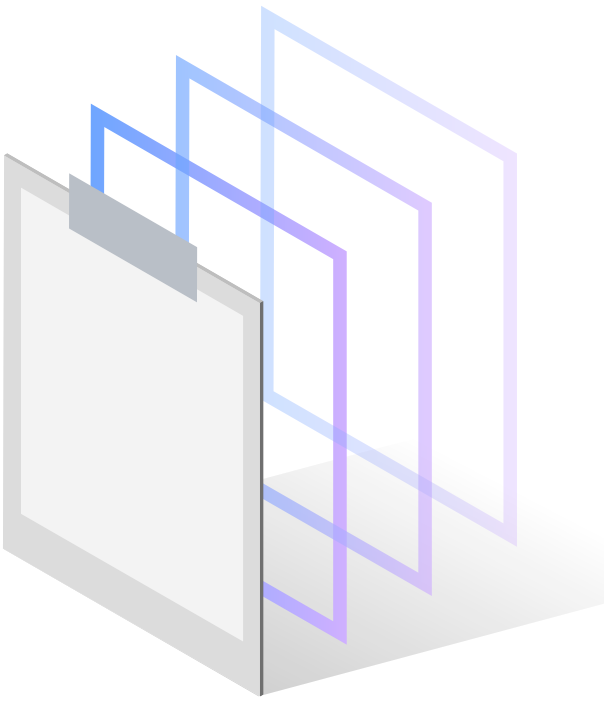
You need a team of full-time data scientists to make a SIEM effective.

They often say that to make a SIEM effective, you'll need a full-time data scientist (or a team of them) to build out all the rules and analytics from scratch.

Truth

If you can't (or don't want to) find and pay for a team of data scientists who also happen to understand security, look for a vendor that provides pre-packaged content out-of-the-box.

Some vendors take the approach that since the solution will likely be customized anyway, why not start with a blank slate? In practice, security teams today simply don't have the resources to take on such a massive project that requires such specialized skills. With any SIEM solution, you'll need to provide it with information about your network, but after that's done, you should be able to take advantage of pre-written rules, analytics and correlation policies to start detecting threats right away. You shouldn't have to start with a blank slate. And if you're still worried, many SIEM vendors partner with managed security service providers (MSSPs) so you can get all the benefits of a progressive SIEM with the added benefit of having a helping hand from security operations experts.



Myth #5

A log management stack can provide the same visibility as a SIEM

Creative marketing by log management and data lake vendors would have you believe that log management solutions are superior to SIEM for finding and investigating threats

Truth

Log management tools can accomplish compliance and audit use cases but fall short in real-time analysis and alerting.

Log management was a solution to a decade old problem - companies needed solutions to comply with audits for Sarbanes Oxley (SOX), Payment Card Industry (PCI) and other industry regulations. Log management stacks have made a resurgence in recent years due to lofty claims of petabyte search and indexing, however a lack of real-time analytics puts a disproportionate amount of manual detection responsibilities – whether it be querying, pivoting, or threat hunting - on your already limited staff.

Most SIEM providers provide a log management layer or data lake as part of the solution for aggregation, parsing and storage. Often times, the log management layer can be licensed separately from SIEM, enabling teams to establish a security data lake with a cost-effective and predictable host-based pricing model. The incremental value of SIEM is in the out-of-the-box analytics (real-time correlation, machine learning, etc). that perform the heavy lifting for monitoring and detection. Simply put – log management is not a SIEM on its own, but a feature of a SIEM.

Myth #6

SIEMs are difficult to integrate with other solutions in my environment.

SIEMs have a reputation for being difficult to integrate with other solutions, even though they rely upon data from other solutions to provide value

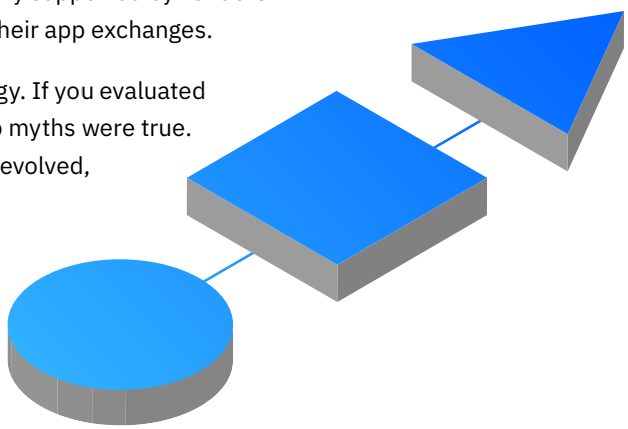
Truth

Leading SIEM solutions must be easy to integrate — and thankfully, many are.

The early SIEMs that came to market a decade ago and failed to evolve with changing needs and evolving technology are difficult to integrate. However, those players have either died out entirely or are struggling significantly now. The leading solutions today offer hundreds of out-of-the-box integrations with commercial IT and OT technologies, and they offer simple connectors to integrate with and parse logs from custom applications. If you're curious about what integrations exist — and are fully supported by vendors — check out the different vendors' customer support websites or browse their app exchanges.

The stereotypes that exist today tend to be based on outdated technology. If you evaluated a SIEM solution ten years ago — or even five years ago — many of the top myths were true. But, to the same extent that the technology and threat landscapes have evolved, so have SIEMs.

If you're struggling to detect threats or make sense of the logs in your log manager, today may be the day to take another look at SIEM solutions and discover for yourself how much they have changed.



About IBM Security QRadar

Manage defenses against growing threats with IBM Security QRadar, the market-leading security information and event management (SIEM) solution. Evolve and scale security operations through integrated visibility, detection, investigation, and response. Gain complete visibility into your environment and apply advanced analytics to prioritize your most critical threats. With QRadar, you can scale rapidly with out of the box support for thousands of security use cases and integrations. Detect threats in real time with advanced analytics and threat intelligence embedded with deep expertise from years of protecting Fortune 100 companies. QRadar can help you accelerate compliance and manage regulatory risk with support for GDPR, ISO 27001, HIPAA and more. Leverage IBM Watson to force multiply security teams with AI-driven investigations that prioritize and automate triage - resulting in an up to 60x improvement in speed of investigation. Finally, respond to threats faster and more efficiently with orchestration and automation, case management and dynamic playbooks provided by tight integration with IBM Security SOAR.

To learn more, contact your IBM Business Partner:

Sweet Spot International

403-461-6227 | swifthillb@sweetspotint.onmicrosoft.com

https://saas-ssi.com/

IBM Security

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
September 2020

IBM