deepwatch + splunk>

WHITEPAPER

Choosing the Right SIEM for Managed Detection & Response Service

9 Key Considerations for Security Leaders

Executive Summary

SecOps teams can experience an immediate positive impact from incorporating an analytics-driven security and information management (SIEM) solution into their threat detection and response approach. This white paper creates a framework for understanding the key differences among the different types of SIEMs (e.g., open-source, legacy, and analytics-driven managed SIEM) and offers insight into the realities of SIEM capabilities, cost, and overall value, as well as the benefits of outsourcing SIEM management with a managed security service provider (MSSP). This white paper also offers guidance on choosing an MSSP's managed detection and response (MDR) services for an enterprise.

Highlights

[1] Not all SIEMs are created equal. Analytics-driven SIEMs offer 'big data' ingestion and analysis capabilities, forensics, integrated reports, hybrid operational environments, free text searches and dashboards, integration with existing IT operational tools and workflows, old and new data combination and analysis, raw data analysis, and no proprietary hardware.

[2] SIEM implementation costs aren't the whole picture. Implementation costs do not account for the total cost of ownership, such as staffing, upgrades, management, and maintenance.

[3] Legacy and open-source SIEMs may not be able to support the integration of existing products and platforms, scalability, or data maturity models. They also do not have a designated team and defined product roadmap to update and upgrade them over time to stay inline with or ahead of the ever changing threat landscape.

[4] Managing a SIEM solution in house requires critical staff experience and expertise that is often expensive and hard to come by in an environment where the cybersecurity skills gap presents tremendous hiring challenges.

[5] Choosing the right service, be it a managed SIEM service or an MDR service needs to include an analysis of the time to value, data scheme management, quick onboarding, and ease of use.

Table of Contents

Introduction

The world is a different place today than it was a few years ago and is a dramatically different place than it was just one year ago. The total number of breaches has increased by almost 70% since 2014. Ransomware payments were up by 33% between 2019 and 2020. Businesses are inundated with constant threats—with certain industries, like healthcare and finance, experiencing attacks at an unprecedented rate. Data types and sources are more diverse, deployment models have shifted noticeably, and the 'work from home' (WFH) model is becoming the norm. This means that how a security operations center (SOC) collects and analyzes data has changed, making the process of selecting the right security and information management (SIEM) solution increasingly important. SIEMs offer businesses significant compliance, threat intelligence, and attack detection benefits by automating the data collection, monitoring, correlation, and analysis process.

The New Security Paradigm and SIEM

With increasing threats, new and growing sources of data, and shifting working models, a SIEM solution can provide an organization with much needed, mission-critical support.

But not all SIEM solutions or managed security service providers are alike. And knowing what to prioritize for your business's current and future needs is critical when choosing a SIEM. Staffing capabilities, training, data analysis, flexibility, and scalability are just a few of the things to consider when selecting a SIEM tool. And all of these considerations are ultimately impacted by cost and time to value.

Today, companies need an efficient and adaptable way to monitor threats, develop infrastructure and capabilities to improve security intelligence, and respond more effectively to security events. The challenge for many organizations becomes not only how to integrate a SIEM into the existing infrastructure, but also how to evaluate the benefits of the potential SIEM solution within the context of capabilities, value, and cost. In this white paper, we'll explore some key considerations associated with choosing a high-quality, analytics-driven managed SIEM solution, including what features are critical to support scalability and how best to evaluate a SIEM's "true" cost and value.

TODAY'S SIEMS DELIVER CLOUD-BASED SECURITY

At one time, your SIEM processed active directory (AD) data from protected on-premise controllers. Today, cloud providers like Azure AD integrate with security products like Okta and Duo to protect data being delivered from cloud-native platforms directly into your SIEM.

Not All SIEM Solutions are Equal

The concept of a SIEM isn't new. They've evolved over the years to support the need for longer-term data storage and real-time monitoring. But as threats increase at unprecedented rates, as businesses shift from on premise to cloud, and as more users, data, devices, and infrastructure become connected, many organizations are discovering the need for real-time advanced analytics and machine learning, as well as the correlation requirements needed in an expanded IT and cloud environment. Legacy SIEM solutions are unable to keep up with the increasing requirements for advanced automation and machine learning, and open-source SIEMs often end up requiring more effort and costing more due to missing features, lack of support, internal staffing requirements, training, and do-it-yourself (DIY) build components.

The Modern SIEM: Essential 'Analytics-driven' Components

To support security needs in a modern hybrid or cloud environment and turn data into actionable intelligence, there are several essential components that must be part of any SIEM solution:

- Real-time monitoring
- Incident response use case support
- User behavior monitoring
- Advanced analytics
- Advanced threat detection
- Threat intelligence ingestion
- Security content library

Additionally, an analytics-driven managed SIEM solution should include:

Big data capabilities—Can rapidly handle both data volume and variety.

Forensic adaptation—The SOC/SIEM team should be able to create rules and correlations based on investigations.

Integrated reporting—No separate database required.

Hybrid environment operation—Works in both cloud and on-premise environments.

Out-of-the-box reporting, free text searches, and dashboards—No requirement for customization.

Supports IT operations, use cases, ticketing, and case management workflows—Comprehensive support for the entire IT/security environment.

Ability to combine and analyze new and old data—SIEM can review old data and integrate it into analysis to produce new information.

Raw data analysis—Ability to analyze large amounts of raw data.

No proprietary hardware—No need to spend additional budget on infrastructure.

Not All SIEM Costs are Alike

The critical importance of a SIEM in today's cybersecurity world can't be overstated, which makes it necessary to fully understand the total cost of ownership (TCO), particularly those costs that are frequently overlooked.

Don't Make SIEM Costs All About the Initial Price

An initial lower price can make some SIEM solutions more attractive to businesses. However, there are critical differences between initial acquisition costs and the total cost of ownership. Often SIEM deployment costs seem low because they only reflect the actual initial implementation. Unfortunately, once deployment is complete, the SIEM may only offer the most basic features and will not include critical components, like DevOps support. SIEM solutions also require ongoing maintenance and updates, which increase the TCO.

Ultimately, many "less expensive" SIEM implementations end up costing businesses more in the long term, because initial costs do not reflect the addition of critical features and do not account for updates, management, and maintenance.

When comparing SIEM solutions and reviewing the total cost of ownership, consider these nine important questions:

Existing Products and Platforms—Does the SIEM solution support the products and platforms you already have in place? If not, you may find yourself paying more for customization, as well as covering high software development costs for custom technology integrations.

Scalability—Can the SIEM scale as your organization—and your data—grows? Very few organizations anticipate zero or negative growth in the future. More employees, devices, and customers, new software or infrastructure, and changing risk models can all impact your SIEM solution and its ability to integrate and analyze data. Therefore, it is critical that a SIEM solution be scalable. A company that opts for a basic SIEM in year one often finds itself spending significant amounts of money to upgrade or customize the solution just a few years later to support growth.

SIEM Solution/Provider Skillsets and Experience—Does the MSSP or MDR service provider require your security team to involve themselves with the minutiae of maintaining a complex SIEM platform? Or, do they have deep SIEM expertise? If you're working with a managed security service provider (MSSP) to outsource SIEM management and monitoring, make sure you understand roles, expectations, and the value you are getting from your investment. Ideally, you will have a strong partner that will let your in-house security team focus on their job.

Data Insight—Do you know how to prioritize the data sources to integrate into the SIEM? Not all data is equal and if you don't prioritize which data sources should get ingested, you'll waste time and money using your SIEM to evaluate and analyze data that isn't telling you the right story. A good example of data prioritization is logs. Many companies do not need to bring in Dynamic Host Configuration Protocol (DHCP) logs on day one. Instead, the focus should be on authentication logs, domain name system (DNS) logs, and firewall logs. Logs that are "chattier" or more complex can be stored in the syslog server for later forensics and analysis. An analytics-driven, managed SIEM solution/provider will have best practices and proven methodologies to help you prioritize data sources so you can get the most value out of your SIEM.

SIEM Staffing & Training Costs—Do you have staff who can manage the SIEM? And have you factored in the cost to manage it? While many open-source SIEM solutions are considerably less expensive, you're still going to pay for the DIY costs associated with adding the needed capabilities—and herein lies the rub. The cybersecurity skills gap is very real and presents a tremendous challenge to many organizations trying to hire talented professionals with the necessary skills and experience. Often, when companies do find the right person, salary and training costs may be considerable. And, unfortunately, even then there are still going to be costs associated with training on processes, networks, operations, and risks.

SIEM Fine Tuning—Do you have in-house security analysts who can tune and maintain the SIEM? Another component of SIEM costs that are often overlooked are the costs associated with ongoing management and maintenance. Excessive and inappropriate data sources can lead to alert overload and alert fatigue. But it takes time and staff power to constantly monitor SIEM inputs and evaluate and fine-tune alerts to the point that your SOC is getting what it needs to ensure the right level of protection and security.

Choosing a Managed Detection & Response (MDR) Service

When deciding on a SIEM approach to support MDR, there are a few things to consider from a cost/value perspective.

Time to Value—The ability to rapidly install a SIEM and have it begin providing insight as quickly as possible is crucial. If you need to begin to provide value to your organization or your customers immediately, then a quick SIEM install is preferred. Upgrades to legacy SIEMs and open-source SIEMs are going to take more time and cost more. A managed SIEM solution will provide time to value more quickly.

Data Schema—With extensive amounts of data, it becomes critical to centralize and normalize information without the complexity of having to fully understand and manage the data model itself. Upgrades to legacy SIEMs and open-source SIEM installations require you to understand the data scheme and how it is ingested and indexed. An MSSP providing a managed SIEM service will manage the data schema components for you.

Quick Onboarding—When working with an MSSP to manage your SIEM, your business should be able to onboard the SIEM as quickly as possible to minimize costs and to ensure the system is providing the value expected.

Ease of Use/Minimal Training—A managed SIEM solution should enable a fast ramp up of analysts and engineers thereby avoiding costs associated with excessive training times. The SIEM solution should also include free text search, auto suggestions, and search history preferences to facilitate ease of use.

THE BENEFITS OF OUTSOURCING

Contrary to expectations, outsourcing SOC operations and working with an analytics-driven managed SIEM solution can save an organization up to 80% of the cost associated with building and managing these things in house.

deepwatch and Splunk: The Winning Solution for Managed Detection & Response (MDR) Service

To ensure the SIEM solution we use with all deepwatch customers meets their necessary requirements, we sought customer feedback and engaged in rigorous testing. We chose Splunk—and only Splunk—as our SIEM platform to deliver managed detection and response (MDR) services. Splunk offers the modern capabilities our customers want and need, such as unmatched big data capabilities, raw data analysis, hybrid deployment options, and integrated reporting. In addition, to provide even more comprehensive security solutions for our customers, we fully integrated Splunk into our Cloud SecOps Platform and our Security Orchestration Automation and Response (SOAR) technology for reliable security event monitoring and response.

Why Splunk Cloud and deepwatch

Splunk Cloud and deepwatch is truly a partnership that brings out the best in one another. So how did this powerful union come to be and what does it mean for customers?

Read More

The deepwatch/Splunk partnership offers:

Flexibility and Time to Value

The Splunk platform is mature and designed specifically to support a vast range of customer data sources for the ingestion of cyber threat intelligence. The context-rich alerts enable deepwatch security analysts to triage, escalate, and respond to customer security events quickly. Because Splunk has built-in capabilities, our customers see significantly faster time to value.

Threat Intelligence and Threat Protection at Scale

deepwatch is able to crowdsource threat intelligence across a broad range of customers to identify new threats by running the data through analysis, and then distributing the information to our customers automatically. When a new threat is found, we are able to anonymously collect indicators of compromise (IoCs) from one customer, aggregate the information, and distribute the threat intelligence and response actions to all customers in near real-time. This scaling ability gives customers a breadth and depth of threat intelligence and protection that would not be possible on their own. In fact, you will typically find the most accurate, relevant, and actionable cyber threat intelligence within your own network data, not via open source intelligence (OSINT) feeds.

Customizable and Rapid Customer Onboarding

We understand that while every customer is different, the need to launch new security measures quickly and effectively is critical, regardless of a company's industry, risks, or size. The Splunk solution offers deepwatch the ability to customize each SIEM deployment to ensure it meets every customers' unique requirements, use cases, and operational environments. By the same token, because of Splunk's built-in flexibility, as well as components like free text search and an easy-to-use interface, analysts do not need to spend extra time learning a new query language or searching IP addresses to get context if there is a threat within the customer network.

Scalability and Consistent Data Usability and Availability

deepwatch leverages Splunk's scalability, high availability, and disaster recovery capabilities to ensure rapid data ingestion and coverage, as well as consistent MDR customer service delivery and data portability. Also important to note: deepwatch customers own all of their data, always.

Integration with the deepwatch Cloud

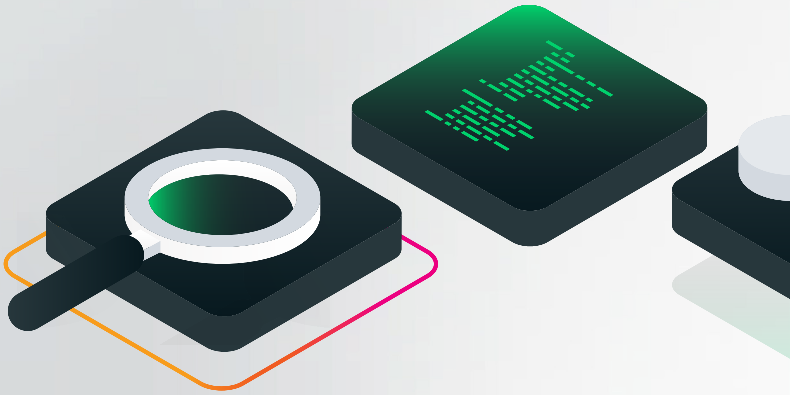
Splunk integrates with the deepwatch cloud SecOps platform for customers that want an out-of-the-box, turn-key solution. In addition, Splunk offers a native SaaS platform that can be deployed on premise for customers that need to keep their data in a traditional data center. The deepwatch cloud SecOps platform also includes a large ecosystem and the capability to plug into most popular product APIs.

Ability to Normalize Data Standards

Because the Splunk data models are standardized (through Splunk's Common Information Model), the system has the flexibility to facilitate different customer endpoints. This normalizes data and standardizes analytics at the highest level, instead of at the sensor points. It also gives deepwatch the ability to send Splunk raw data continuously and engage in free text search while also identifying important components, such as IP address, username, etc.

Integration of the MITRE ATT&CK® Framework

The deepwatch MDR service integrates the MITRE ATT&CK® framework to support the creation of threat models and methodologies specific to a customer's business and industry, all while leveraging the superior data management capabilities of Splunk. The deepwatch Splunk engineering team aligns every security use case with the framework. The framework enables deepwatch to address four important concerns: adversary behaviors, unique threat lifecycle models, applicability of real-world threats to individual business environments, and consistent and common taxonomy to identify tactics, techniques, and procedures (TTPs). deepwatch threat hunters also meet with customers on a monthly basis to review the ATT&CK framework and select specific TTPs from it in order to prioritize their hunting efforts.



Conclusion

In today's security landscape, where zero-day threats, nation state attacks, and lurking ransomware signals are risks that have to be managed, an effective security operations program requires an analytics-driven SIEM solution combined with a 24/7 managed detection and response service. While in the short term, upgrading a legacy SIEM or implementing an open-source SIEM tool may seem like the most cost-effective option, these solutions do not account for the mission critical components necessary to support around-the-clock security operations and longer term growth. An MDR service that leverages SIEM, capabilities such as 'big data' ingestion and analysis, forensics, hybrid operational environments, and integration with existing IT tools and workflows, will measurably lower risk and protect your organization against advanced and emerging threats.

To maximize the effectiveness of security operations, businesses need to approach SIEM adoption by looking at the total cost of ownership, which includes inputs like time to value, staffing, upgrades, management, and maintenance. A managed detection and response provider with deep SIEM expertise empowers their customer's in-house security team to oversee and respond to threats without having to constantly manage and monitor the SIEM. This allows more time for staff to concentrate on other facets of their organization's security and risk program.

About deepwatch

deepwatch secures enterprises via its unique, highly automated cloud based SOC platform backed by a world class team of experts that protect your network and digital assets 24/7/365. deepwatch extends your team and proactively improves your cybersecurity posture via our proprietary maturity model. deepwatch's managed security services are trusted by leading global organizations.

About Splunk + deepwatch

deepwatch is an Elite Tier Splunk MSP with a large team of experienced Splunk engineers. deepwatch is Splunk's #1 MSSP in terms of the amount of data we manage across our customers. Splunk customers trust deepwatch as a true extension of their security team. Whether you have an existing Splunk license or you are looking to get started with Splunk, deepwatch can help.

let's talk