



Solving the SIEM Problem

Table of Contents

The Dawn of the SIEM Revolution	3
----------------------------------------------	----------

SIEM Solved Old Problems, but It Also Created New Ones

Too Much Data, Too Many False Positives	9
The Need For Expertise	11
Unpredictable Pricing Models	13

Resetting SIEM Requirements

Get Rid of the Data Lake Mentality	17
Rely on 24/7 Experts	18
Look for Sustainable Pricing Models	19

Challenging Traditional SIEM Models

Predictable Pricing. No Surprises	22
Works for Small Teams with Big Goals	24
Investigate and Stop Threats Sooner	25

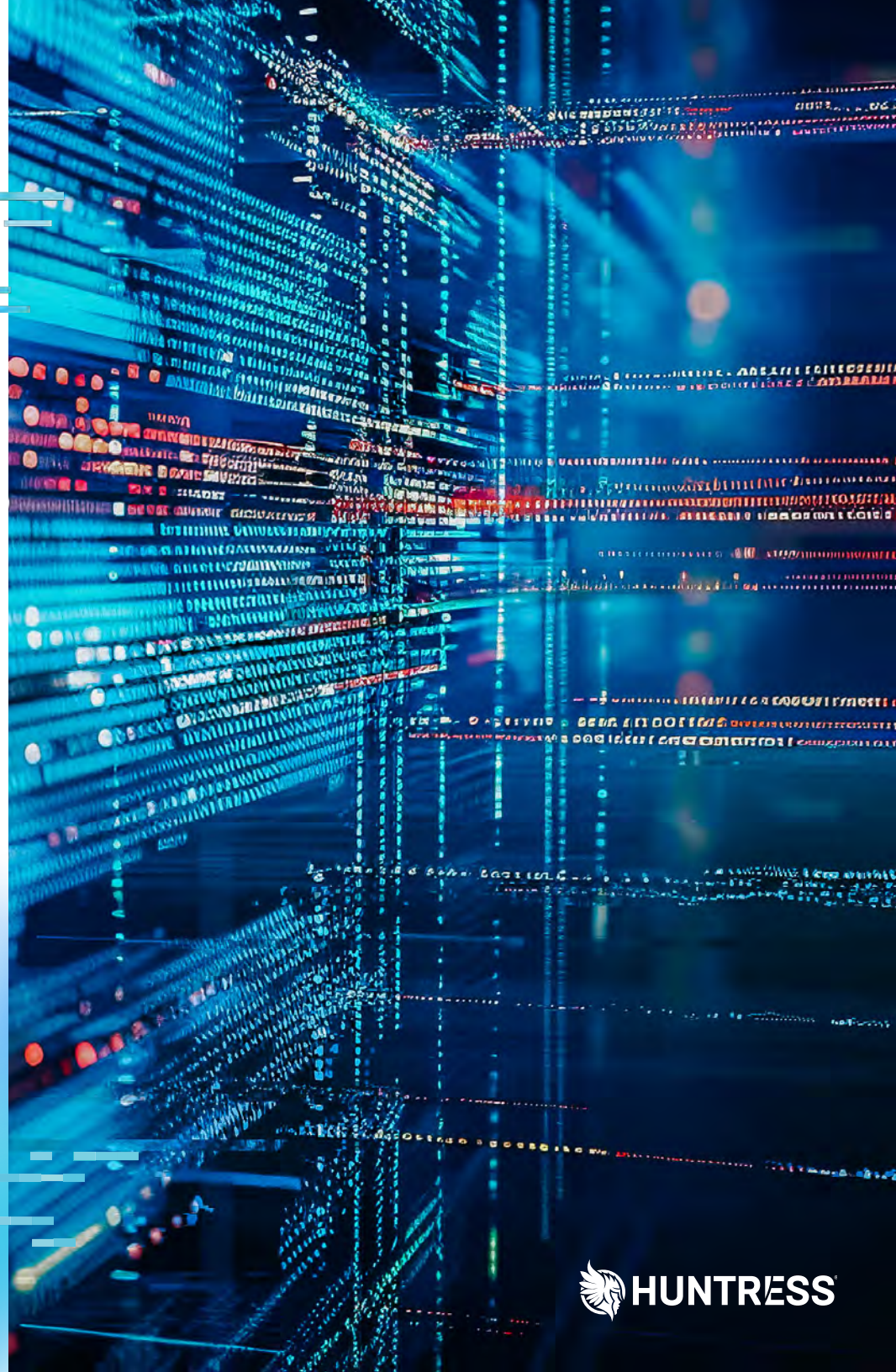
The Huntress Way	26
-------------------------------	-----------

The Dawn of the SIEM Revolution

If you've been in cybersecurity long enough, you've probably heard of "defense in depth" or the "security onion."

These phrases suggest it's best to surround yourself with multiple layers of protection to prevent a cyberattack. While this is still solid advice, it also comes with its own set of problems.

Each layer requires products and services, which then need more management, personnel, and expertise. With these mounting complexities, IT had to find a way to consolidate logs onto one platform, parse the data, correlate against signatures and behaviors, and, after all that, notify someone about their findings.



Enter SIEM.

Security Information and Event Management, or SIEM for short, solved this problem by quickly ingesting data via agent-based syslog and API collection. Unlike traditional syslog and log management servers, however, SIEM could actually correlate events.

SIEM doesn't just collect log data, it generates actual events and alarms from that data. And by integrating intrusion detection engines like Snort or Suricata into SIEM, IT teams finally felt like they could have their "onion" and eat it too.



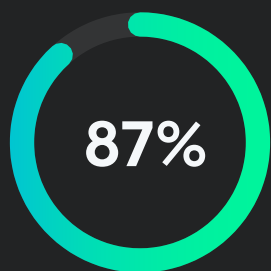
SIEM Solved Old Problems, but It Also Created New Ones

While SIEM solved the problem of disparate log sources, the actual execution was a different story. The advent of SIEM solved one set of issues and created a secondary set entirely.

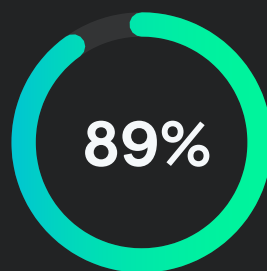
By nature, collecting and analyzing data from multiple sources creates "noise." This noise often happens because most SIEMs are treated as a giant data lake, and this needless data translates into false positives. The resulting headache, in turn, creates the second problem: the need for expertise.

While SIEMs can handle the workload of collecting and analyzing log data, you still need an in-house expert to generate the rules, refine them, and keep the SIEM operating smoothly. In-house expertise is also needed to triage and respond to alerts to neutralize threats.

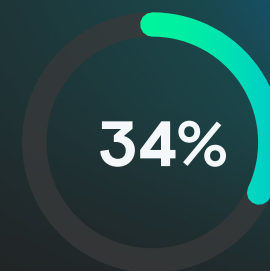
Apart from the salary expectations of a SIEM expert, the next big expense is the cost of log ingestion. For most companies, the status quo is to let their SIEM ingest all data sets without filtering because they don't know what data brings real security value. This leads to skyrocketing charges year over year. By looking at these problems, we get a clearer picture how quickly things can go wrong with SIEM.



of MITRE ATT&CK can be covered with existing data sources already ingested ¹



of organizations are being impacted by a security skills shortage in the labor market ²



of companies report a lack of budget as the major hurdle for maximizing value in SIEM ¹

Too Much Data, Too Many False Positives

Picture yourself standing in the middle of your favorite (or maybe not so favorite) tech conference, caught up in a whirlwind of conversations, flashing lights, and the neverending hum of activity. Trying to take it all in at once is like your SIEM collecting data points.

Now imagine having to report on your experience, but only pinpointing conversations spoken in French by speakers wearing blue jackets about their childhood pets: that's correlation. As difficult as that is, SIEMs are tasked with performing these actions every day.



With so much data flooding in, there's a high chance of false positives and data slipping through the cracks. That means users have to sift through mountains of irrelevant data that don't always apply to their detections.

Put simply, it's noisy. And today's SIEM users are desperate to filter out unnecessary noise.

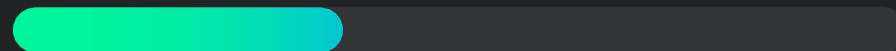
51% of SIEM users consider their SIEM not to be fully effective ³



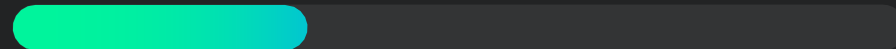
50% of SIEM users are not happy with their current SIEM vendor ³



37% of SIEM users described SIEM as having too many false positives ³



30% of SIEM users described SIEM as too complex ³



The Need For Real Expertise



Expertise isn't something you can fake—you either have it or you don't. There are no exceptions. So when it comes to SIEM, this unfortunate truth leaves you with two options: keep your expertise in-house or outsource it.

SIEM started with a DIY-based approach. Companies would purchase a SIEM, train their internal teams, and manage everything in-house. But the truth is threat research, correlation building, and standard maintenance are very complex. This meant real SIEM experts quickly became expensive and hard to retain, and DIY SIEM became a luxury only the biggest enterprises could afford.

This pushed many smaller businesses to outsource their SIEMs through managed detection and response (MDR) service providers.

SIEM management now fell under the MDR service provider's purview but opened businesses up to various pricing models. While both approaches have pros and cons, the more common model for most small businesses has defaulted to outsourcing—but at what cost?

Unpredictable Pricing Models

If given the choice between paying a loan with an interest rate that fluctuates daily or a set percentage, which would you choose? Most, if not everyone, would always choose the set interest rate each time. Unfortunately, SIEM customers don't normally get this predictability.

Consumers are often billed according to the amount of data their infrastructure ingests. Since most companies don't know how much log data they generate daily, this creates an unfavorable situation for them.



Imagine paying interest on that loan, but the rate can balloon higher depending on the day.

Worse yet, the cost can never go down. This describes the problem with SIEM pricing across most of the industry. Unpredictable pricing models mean you could face nasty surprises should your infrastructure needs increase or spike temporarily.

Licensing Type	Data Predictability	Cost Reliability
Events per second (EPS)	Low	Low
Gigabytes volume per day	Low	Low
Server/asset count-based	High	High
User-based	High	High
Hybrid data ingested/asset count	Medium	Medium



Resetting SIEM Requirements

With all the issues SIEM users face, it's easy to see why the market feels disillusioned.

SIEM has been out of reach for most businesses.

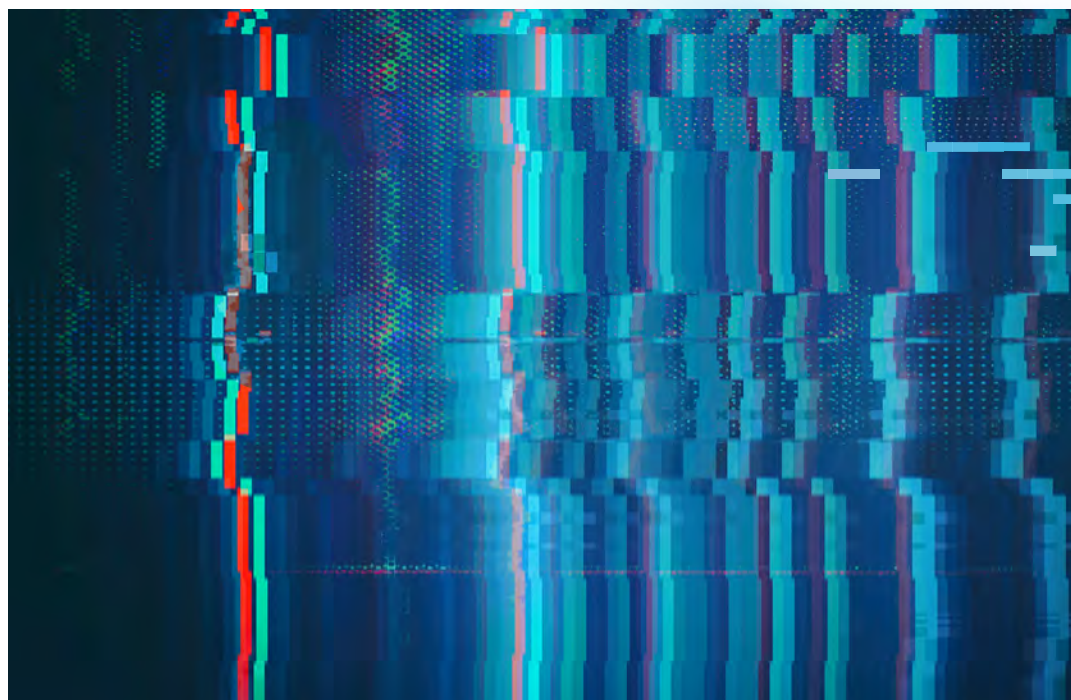
From its initial design to its current iteration, most SIEMs are tailored for big enterprises, leaving under-resourced companies to force-fit their security needs to a system that doesn't cater to them. While the problems facing SIEM can seem daunting, there are ways to solve them. Organizations need to demand more from SIEM vendors.



Get Rid of the Data Lake Mentality

SIEMs are notorious for creating a lot of noise due to the sheer amount of data they take in. To solve this, SIEM vendors often give companies a tuning period from two weeks to six months. Sadly, this increases time-to-value, making SIEM an even less affordable choice for businesses. This approach leads to a few questions: can this filtering and tuning be done earlier in the ingestion process? If so, how and to what extent?

A novel approach would be to filter out the unnecessary noise as close to the source as possible, eliminating the need for tuning in the first place.



Rely on 24/7 Experts

No one will argue how complex SIEM can be. In fact, managing it goes far beyond just the detection and notification of SIEM products. To manage SIEM effectively, you need to take into account the following:

- ✓ Deployment of the SIEM platform (appliance or agent)
- ✓ Adding collection and normalization of new log sources
- ✓ Patching of SIEM agents or the appliance in use
- ✓ Updating threat intelligence feeds
- ✓ Tuning correlation signatures
- ✓ Creating canned reports
- ✓ Shipping log and trend data into dashboard-based widgets

That's why it's critical to establish a solid partnership with a SIEM provider that can consider all of these areas.

Look for Sustainable Pricing Models

Too often, SIEM pricing favors the provider. The more log data ingested, the bigger your data lake gets and the higher your storage costs climb. Plus, temporary data spikes or long-term increases can make it tough to predict your budget for SIEM or result in reaching a cap that limits the ingestion of new data.

Pricing can only be predictable if you can anticipate log collection or limit the amount of stored data. Various pricing models have attempted to adjust for data spikes by charging per data ingested, per user, or per endpoint.

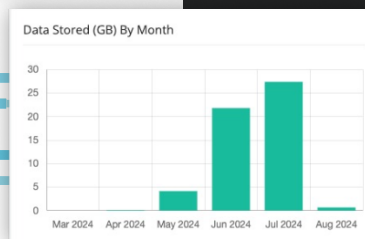
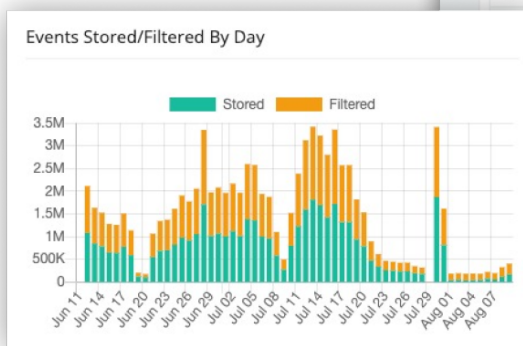
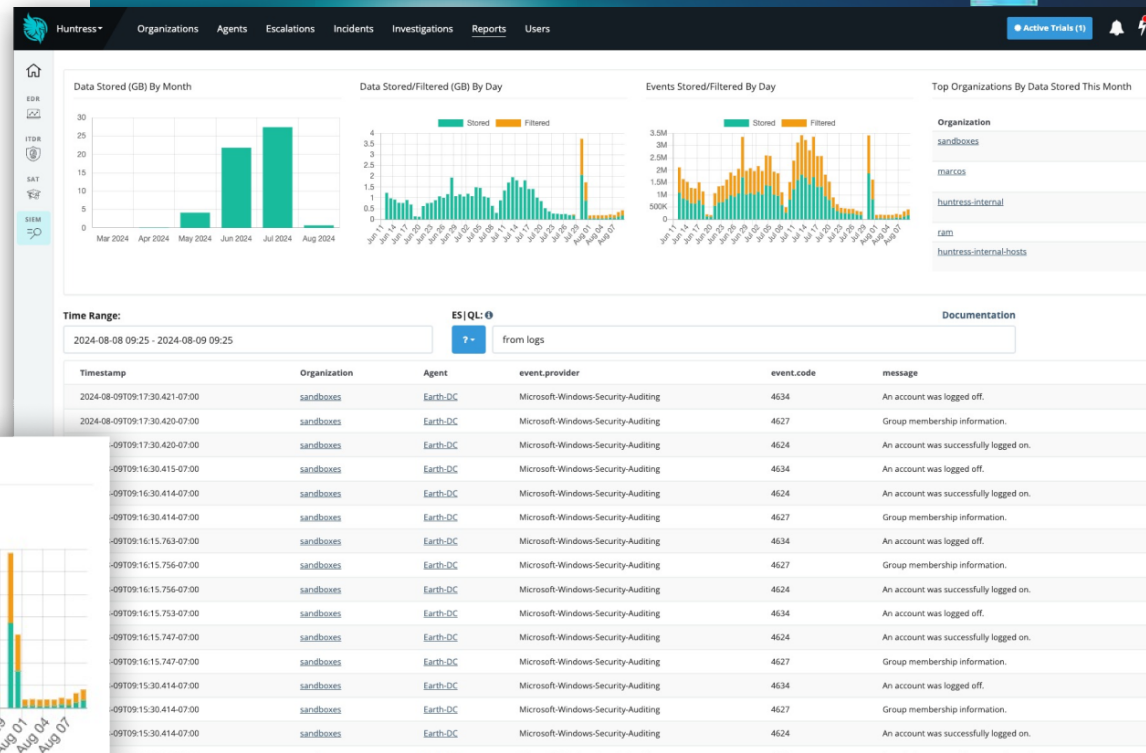
One of the newer methods to address this problem is now to reduce the amount of data to critical security content and collect across data sources, with an eye toward smart pooling of data allowances to ensure data is averaged out and you don't consistently hit volume limits.



Challenging Traditional SIEM Models

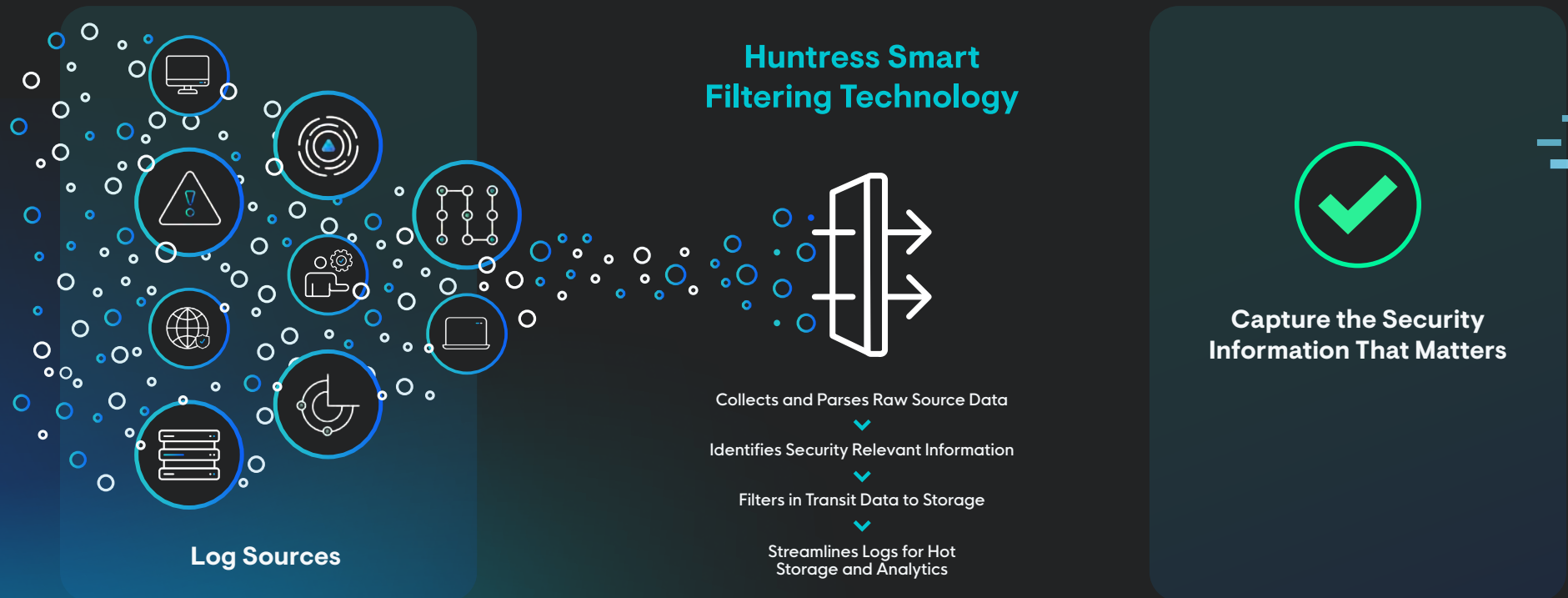
Huntress levels the playing field by redefining how SIEM should work, making it possible for all businesses to get the benefits of SIEM. We've designed our Managed SIEM platform to tackle the common challenges everyday consumers face. Keeping in mind the lessons of the past, we're moving forward with a SIEM platform that's purpose-built to make SIEM accessible for first-timers who felt it was out of reach before.


That's Huntress Managed SIEM.



Predictable Pricing. No Surprises.

SIEM shouldn't just be about collecting data—it should be about making good use of it. We're shifting the mindset from collecting everything to honing in on what really matters to a SOC analyst who needs to stop threats cold. With our Smart Filtering engine, we're revolutionizing how logs are captured to do just that.





Smart Filtering takes the typical log data and filters twice—once as close to the source as possible and again on our backend. This eliminates the day-to-day noise common with SIEM, letting us quickly pinpoint the data that delivers actionable insights. We capture and retain only the most critical, security-relevant information by analyzing data from essential security tools and sources. This focused collection lets you zero in on valuable insights without drowning in data, keeping security notifications streamlined and effective. The added benefit? We keep pricing predictable throughout the year and slash costs without compromising security visibility.

Works for Small Teams with Big Goals

SIEMs are notorious for burying under-resourced teams with a relentless stream of tasks, leaving the platform either underused or never deployed in the first place.

Huntress Managed SIEM is unmatched in ease of use because it's backed by our experts, who oversee your deployment, tuning, and monitoring.

We've got your back 24/7— during late nights, weekends, and holidays. Our SOC has eyes on your environment to detect, investigate, respond, and hunt for specific tradecraft that would otherwise go unnoticed. We do everything from constant monitoring to fine-tuning and configuration that keep things running smoothly. You get the credit. That's how it should be.



Investigate and Stop Threats Sooner



One big benefit for organizations that adopt Huntress Managed SIEM is the ability to “shift left” in their detection and response strategy by spotting and neutralizing threats earlier in the attack chain.

For example, in one recent attack, deploying SIEM would have allowed the Huntress SOC to identify a threat actor 19 hours faster than relying on EDR alone. This extra time to catch and contain threat actors earlier in the attack path means organizations can respond faster to credential theft and reduce the risk of business downtime.

This type of security isn't just for enterprise-level budgets. We've made it accessible for growing businesses everywhere.

The Huntress Way

Like most things in life, it's much easier to find the right fit for you rather than mold yourself to fit something else. Cybersecurity is no different.

Huntress is challenging old SIEM models and solving common problems.

By rethinking the outdated paradigms of traditional SIEMs, we're bringing enterprise-grade security to businesses of all sizes, helping protect their digital assets effectively and affordably. Our approach isn't just an improvement—it's a necessary evolution in SIEM technology.

Huntress Managed SIEM makes powerful threat hunting and robust compliance support accessible to everyone without the big budget, big team, or big headaches that come with traditional SIEMs.

Cut costs, not corners

Start your trial and stick it to attackers with
Huntress Managed SIEM, purpose-built for
our expert SOC to keep you safe 24/7.

Sources:

¹ Cardinal Ops 2024 SIEM Report

² ESG SOC Market Trends Report

³ 2022 Cybersecurity Insiders SIEM Report

X in YouTube f

