DARKReading

SPONSORED BY ActZero

WHITE PAPER

Zombie SIEM: Dead but Lingering—and Eating Your Brain

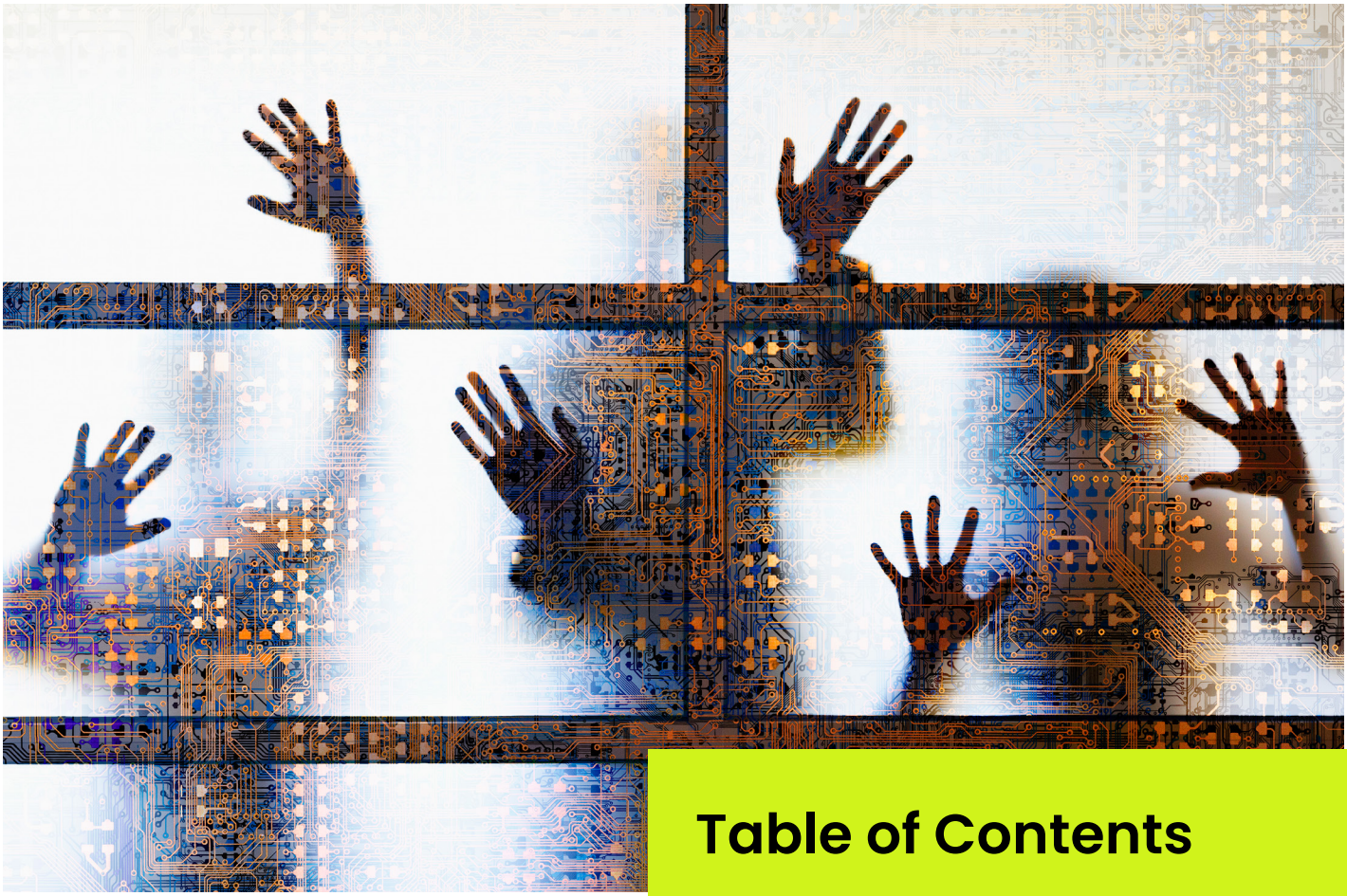

Table of Contents

Don't feel beholden to the SIEM zombie.

Introduction

Security information and event management (SIEM) systems stand as the standard platform upon which most security operations centers (SOC) run today. While SIEM certainly provides some semblance of centralization of security information, in many ways these systems hurt the cybersecurity cause more than they help it.

Modern SIEMs suck up security information about as mindlessly as a B-movie zombie eats brains, and the shuffling victims they leave behind are security organizations that are left paralyzed by:

- a lack of meaningful analysis of security event information,
- shotgun detection mechanisms that leave a wake of alert fatigue, and
- considerable false positives that exacerbate the fatigue.

Today's SIEM platforms take considerable amounts of work from the security team to tune and integrate with new monitoring feeds, and the cost model for SIEM makes it such that it can't scale up telemetry without breaking the bank at most smaller organizations. If security leaders are truly honest, SIEM is a tool that has never quite worked the way it was supposed to, but one which has gotten its teeth deep enough into most organizations that everyone sticks with it out of habit. Organizations either live with the SIEM sunk cost under the assumption that this is as good as it is going to get, or seek to acquire a SIEM because that's what everyone else uses, too.

We'd argue, though, that MOST organizations don't actually need that big, expensive, complicated SIEM and that even if they've already invested in one they're continuing to spend money on hidden operational costs by sticking with it. The truth is there are better tools to do the things most organizations are trying to do with a SIEM. There are better ways that organizations can meet their log collection, detection, investigation and response needs.

In this paper we'll explain how:

- smaller organization moving beyond AV and Firewall can do so without sinking costs into SIEM
- mid-sized enterprises not seeing value from their existing SIEM solution can start to pivot in a way that will help their processes and their budgets.

How SIEMs are eating our brains (and budgets)

Many organizations use SIEMs to monitor telemetry across their environments for security and compliance. In theory, well-resourced organizations with the resident expertise to manage these tools properly can leverage SIEM's flexibility to support new types of tooling and operational monitoring requirements to effectively run their security organizations. But in practice it rarely happens that way.

SIEMs are a notorious resource drain if not managed extremely carefully. Simply piping more data into these systems doesn't automatically generate better results, though it does guarantee higher costs.

Brief history of the promises of siem

It's been the better part of two decades now since the SIEM category evolved as a mash-up between security information management's (SIM) log collection and centralized management capabilities with security event management's (SEM) event correlation and alerting functions. The promise of the combination was always that SIEM would offer a path toward not only comprehensive real-time monitoring but timely identification of the most risky security events so operators could act on small incidents before they turned into full-on breaches.

After all these years, SIEM still struggles to live up to all that potential sold by SIEM vendors.

After the initial introduction of SIEM's combined information and event capabilities, it became clear that scalability was going to be one of the first big roadblocks to reaching SIEM-driven security nirvana. The large volumes of log data streaming into the systems were causing traditional databases to creak, and so SIEM vendors moved toward big data architectures to push more data through.

But what ended up happening at that point is that there was so much data streaming through the SIEM that SOC personnel were drowned with a firehose of data crashing through their dashboards with no real way to figure out which droplets mixed in there were accurate, timely, relevant to what they needed to follow up on in any given moment.

This is where the push to SIEM as a security analytics platform came from. SIEM vendors came up with correlation capabilities and detection models that promised to do a better job linking log information together and providing a more comprehensive picture of incidents to security personnel. When those next SIEM revisions of correlation capabilities still frustrated operators, it became clear that just network information was not enough to track modern tactics, techniques and procedures (TTP), so SIEM would need to layer in endpoint data streams to really get visibility the SIEM needed. But no SIEM platform has truly been able to get that layer right. This is what led to the rise of the endpoint detection and response (EDR) category. While adding EDR to SIEM through integration is possible, it often layers

in insurmountable costs and complexity into the system. As a result, security analysts still struggle to gain value from the hopeful promise of SIEM.

Meantime, hope and promises at every stage of this evolution has pushed SIEM to become entrenched in many SOC environments and stipulated by numerous compliance regimes—in spite of all of the lackluster results over the years.

Alert fatigue and SIEM

Frankly, the ongoing problems of SIEM and its lingering pervasiveness across organizations of all sizes has rendered it as security's version of the walking dead.

The zombie SIEM's persistence in the industry comes down to a number of factors but one of the big ones is a common misunderstanding on the problem of alerts in the world of security detection and response. Specifically, that misunderstanding occurs when IT leadership thinks it needs security teams to scale their review of alerts to ensure they don't miss any potential indicators of compromise (IOCs). This pursuit of endless alerts is further exacerbated by security teams seeking all-seeing 'visibility' within the environment while ignoring the first principles of risk management.

IT stakeholders stop thinking critically about what they're trying to measure or which indicators matter most based on business priorities or risk thresholds, and instead "turn on all the signals" for alerting. That lack of prioritization ultimately contributes greatly to the alert fatigue problem and dooms SIEM success from the start.

Alerts should never be confounded with visibility or telemetry. In the shift to ML/AI, alerts aren't what feed correlation. Machine learning models need raw security data and not alerts streaming via every different kind of security tool. For example, an ML model would not be able to use alerts from an AV solution and tie it to other alerts from another system. It would need to have the AV information converted to metadata to avoid over-storage and limits to searches, correlation, and enrichment.

Simply consuming all the alerts not only doesn't work to pick out the biggest risks, but it's cost-prohibitive at scale.

Why SIEM doesn't work for modern IR

To dig further into why the alert-centric mentality has cursed SIEM into its current ineffective role in the modern cybersecurity organization, it would be beneficial to explore the mismatch of SIEM functionality with the steps of modern incident response (IR).

As we've already established, EDR arose as a category to fill in the gap for endpoint data that SIEM was long unable to fulfill in the collection phase of IR. More fundamentally, the problem in the collection phase is that with or with or without endpoint data the SIEM model measures its success not on enrichment of data but on the volume of data it can handle. SIEM vendors make money based on data volume and so

they are less interested in tuning their pipelines to get metadata sources to work well in context of one another or as enrichment of one another, but instead to optimize how much data can be stored. This has greatly limited the amount of innovation that SIEM vendors have done in the collection phase.

Meanwhile, when it comes to detection and response SIEM platforms have tried to bolt-on machine learning capabilities for correlation and searches of information. But the reality is that while today's SIEMs do offer the potential for teams to do solid data science work within them, a lot of it is of the DIY nature. SIEMs provide all the raw materials to utilize machine learning, but teams must often know which models to use, how to tune them, and they've got to do significant on-going work optimizing both the data sets and the models to gain significant value from them.

More disconcerting is that the machine learning capabilities of SIEMs today remain mired in single-variable analysis. They are unable to crunch security data in the context of numerous data dimensions. Modern cyber attackers tend to simultaneously go after numerous attack targets at once and also chain together TTPs to achieve their objectives. This means that detecting specific patterns requires models that can better contextualize data on the fly. SIEM's inability to do multivariate analysis severely hampers the effectiveness of detection models.

This deficiency cascades into the response stage of IR because an ML model that doesn't work very well can't be trusted to automate many actions or orchestrate workflows. In fact, this lack of ability by SIEM arguably is what led to the rise of the security orchestration, automation, and response (SOAR) category—which is still notoriously inaccessible in use by other than the most mature large enterprises.

SIEM's spiraling cost models

Hypothetically, to make SIEM work the way it's always been promised, a security organization needs three ingredients for success:

- Infinite tuning
- A wide and deep set of data sources—especially from the endpoint
- Multivariate analysis.

Another reason why SIEM manages to stick around neither dead nor alive in modern security organizations is that achieving those three success factors would eat a security budget alive through SIEM's data-based pricing model.

The modern managed SIEM solutions' business model charges by the volume of data submitted. This leaves it cost prohibitive to include most endpoint data—especially over the length of time required by security analysts. This cost problem works at odds with that desire for increased security visibility and data collection necessary to appropriately feed data science models such as multivariate analysis. Data costs skyrocket as telemetry scales and SIEM

vendors are not financially incentivized to change the situation anytime soon.

That's just the start of how SIEM's spiraling cost models are crushing modern security budgets. A typical security leader must also factor in the hidden costs involved, particularly labor costs involved in running the SIEM.

Not only does it take significant labor for analysts to glean decision-making information from the SIEM, but simply tending to the care and feeding of the platform and its daily operation takes a lot of time.

The reality is that the modern security workforce has been paralyzed with endless wheel spinning caused by the problems within their SIEM. Often an organization is spending twice as much on labor to pull value out of a SIEM that the organization has already sunk as a cost. And they're frequently sinking more money into the prospect with endless SIEM refreshes chasing the next round of promises that SIEM's champions foist on the market.

Is it time to kill the zombie?

Ultimately the goal of the security department isn't to run the most efficient SIEM on the planet—it's to achieve superior detection and response results.

Organizations do that by gathering most relevant telemetry across their network, cloud, and endpoints.

Why doesn't SIEM just do those things?

Some would argue this was the goal of SIEM all along, so why has it never been able to do these things on its own?

First of all, as we've explained above the SIEM vendors are not financially incented to make it so. In fact, we'd argue that so many of cybersecurity's new product categories have arisen to make up for the deficiencies in SIEM. That includes EDR and SOAR.

Secondly, the machine learning capabilities of SIEM are bolted on rather than native. They require constant attention from human analysts to tweak models. Additionally the level of ML analysis SIEMs are capable of still aren't able to truly account for the number of dimensions necessary to get truly accurate detection of attacks today. Detection must be able to handle multivariate analysis of IOCs in context of a number of data dimensions and SIEM products today are still stuck with single-variable analysis models.

What a SIEM killer looks like

In the age of advancing analytics and machine learning, improved data management, and maturing data science both outside of and within security—this is imminently doable using a SIEM and a collection of other specialized security platforms. But cobbling solutions together to glean value out of SIEM is also something that requires a rockstar security team only accessible to the biggest enterprises. Achieving similar results would also be prohibitively expensive to do via Managed SIEM.

Fortunately, there is a way to kill the zombie SIEM as we know it. In order to gather and analyze relevant telemetry across all of an organization's threat vectors without breaking the bank, many organizations are sidestepping SIEM in favor of viable alternatives.

Chief among them are managed detection and response (MDR) services, which focus on the highest fidelity logs containing information that will be most

THE COMPLIANCE FACTOR

When organizations are considering forgoing SIEM for MDR, one of the most common questions to come up is 'What about compliance?' While a lot of compliance requirements have been crafted with SIEM in mind, at the end of the day what auditors care about is capabilities of an organization's security stack. Namely, how well does that stack maintain compliant log data and how well does it enable detection and response. In both cases, MDR does that very well and should be able to pass muster under scrutiny by the auditors.

indicative of today's attack patterns. MDR moves beyond single variable analysis enabled by SIEM solutions. It is fueled by a lake of data that extends beyond any single environment, while gathering intelligence about what is "normal" for your specific environment. The architecture is well-suited for multi-variate analysis. And detection is done without forcing the user to consume the whole lake in the process.

When MDR is powered by an extended detection and response (XDR) platform that can perform SIEM-lite log management capabilities to store and handle relevant sources of raw data, small to medium organizations can either circumvent the necessity for SIEM or replace a SIEM that simply isn't reaping the SOC very good ROI.

The MDR model is determined by success in detection, not by the sheer volume of security data that the platform can handle. As such, innovation in detection remains dynamic in the MDR space. This is supported by the fact that MDR is ultimately a service that's run by people who are always working to stay a step ahead of the next attack TTPs.

Just as in the B-movies where humans tend to beat the zombies with the help of some kind of war machine, MDR defeats traditional SIEM with its human + machine capabilities. MDR services utilize machine learning platforms—powered by the most advanced data science—and then layers human cybersecurity expertise on top of that to continually train those models based on how attackers change their TTPs over time. The data science team and security engineering team of an MDR provider, paired with their own custom-built technology is what puts MDR over the top compared to SIEM's straight technology approach.

Unlike other forms of machine learning, security machine learning requires constant tweaks to work. That's because attack patterns don't stay static—and so the models for detection must be constantly changed based on that, not to mention on the changing ways that IT infrastructure operates, which is similarly dynamic. When the machine can't find a new type of attack, An MDR provider's cadre of experts is constantly innovating to create more detections that will apply in more places. This will echo out to the quality of responses that its IR teams are able to run.

How can ActZero help?

Don't feel beholden to the SIEM zombie. Small and mid-sized organizations can finally achieve the promises of SIEM without the headaches or the costs by turning to MDR alternatives.

As an MDR provider, ActZero's guiding philosophy is to free up security teams to focus on higher value tasks by taking the burden of detection and response off of them. We have invested heavily to build intelligence and automation that eliminates the burdens of log ingestion and monitoring while still providing them with the flexibility to address a broad set of security, compliance and operational management requirements. ActZero delivers this as a very simple to consume service that efficiently ingests, analyzes and delivers both visibility and response without adding to IT security workloads.

That means we've freed up those IT Security teams to spend their time on more valuable things, and that means we're delivering the security outcomes they expect. Our dashboard enables customers to select the data sources, the amount of data, and storage duration that is most relevant to their business, and that is required by their specific compliance frameworks.

Want to see ActZero's MDR in action? Check them out now at **actzero.ai**.