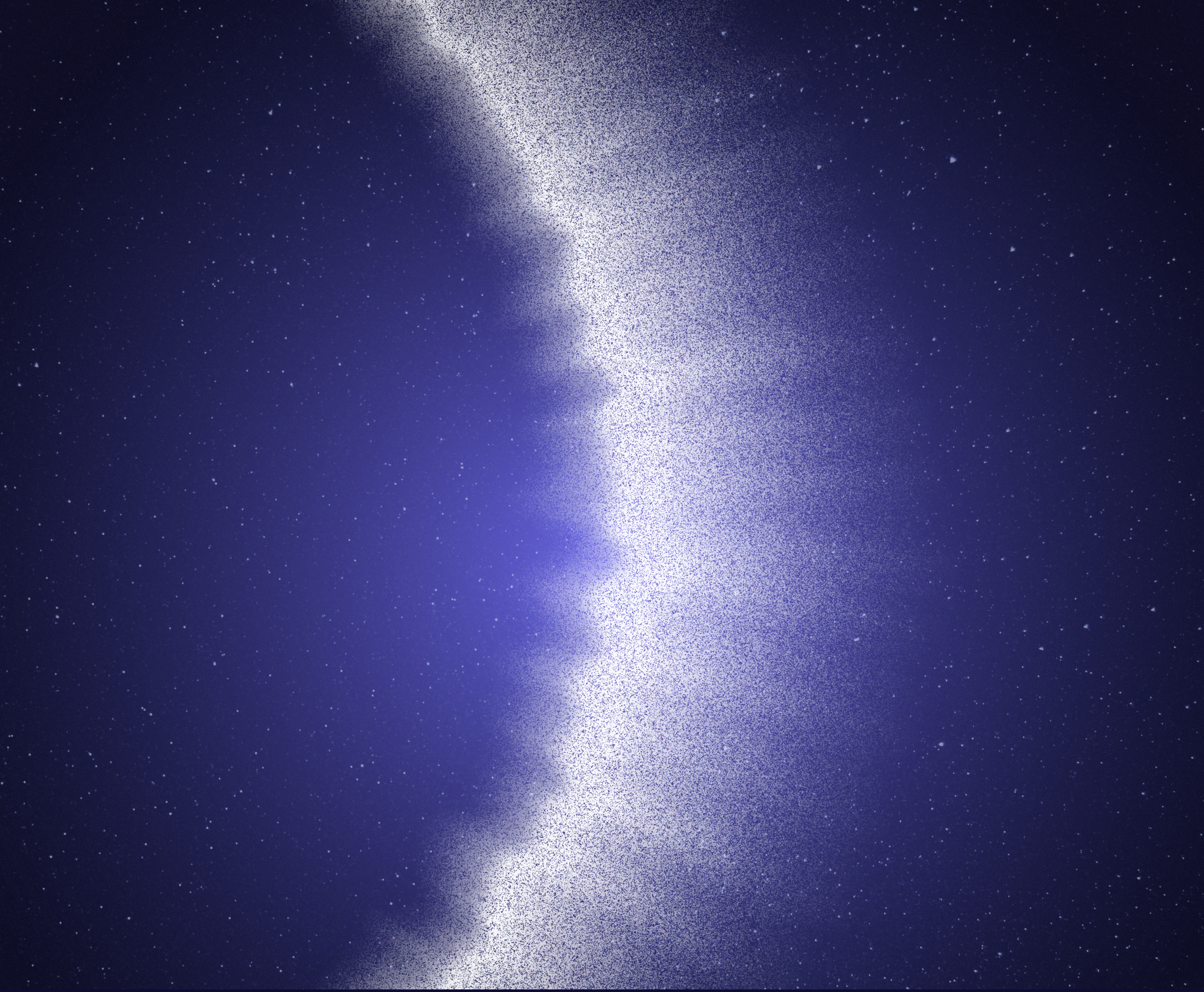


THE OVERWHELMED SOC: ARE YOUR ANALYST TEAMS BURNED OUT?

CENTRIPETAL

Security analysts are overwhelmed by a never-ending stream of security events generated from the network. Firewalls, Intrusion Detection Systems (IDS), servers, and Identity Access Systems (IAS) all produce high volumes of logs. These logs are further augmented by analysis from Endpoint Detection and Response (EDR) systems, network traffic tools, and vulnerability assessment tools. All of these events are funnelled into a Security Information and Event Management (SIEM) or Log Management Tool.

Despite the availability of tools designed to distill these logs into actionable security alerts, security analysts still face the daunting task of overseeing potentially millions of security events. Their goal is to identify and detect malicious activity amidst the vast volumes of data.

Even with increasingly advanced automation, a typical organization generates thousands of security alerts daily. Each of these alerts requires investigation by highly skilled but often exhausted security analysts. Wrestling, grappling and negotiating the sheer volume of alerts – while simultaneously trying to focus on other pertinent security requirements - results in alert fatigue.

Analysts, inundated with alerts, are becoming desensitized, leading to missed or overlooked threats. Many enterprises relate stories of analysts spending hours clearing false positives, deduplicating events and filtering through the noise. This is untenable, inefficient and ineffective use of expensive resources.

Moreover, the costs associated with storing and managing events are significant. This, combined with regulatory and compliance requirements around retention of data, are introducing considerable costs for even small security operations. While the overall intent behind the regulations is honorable and purposeful, the impact on businesses who are already crippled by cybersecurity costs is unsustainable.

A typical medium-sized business might see millions of security events per day - which could easily result in several hundred thousand alerts that a security team is expected to analyze.

Naturally they will focus on the highest priority alerts and implement strategies for automating remediation wherever possible. But there is an inherent risk that they will miss key indicators to malicious activity and adopt a ‘best effort’ approach based on the amount of time and resources available.

Unsurprisingly, teams are burned out.
They are exhausted, and potentially becoming disillusioned with the constant drudgery of monotonous event management, resulting in a lack of variety in their roles.

The current approach is not sustainable. Organizations need to look to a more preemptive solution, one that monitors and shields malicious traffic, or identifies sources of reconnaissance traffic and blocks them. That in turn, significantly reduces cyberattack traffic, which is crippling the organization in so many ways.

> "This morning I had zero alerts. I refreshed three times just to make sure. Sure enough we had no alerts thanks to Centripetal."
>
> Incident Response Analyst, Information Technology at a Pacific Gaming Casino

Alert Volumes

For even mid-sized businesses with a moderate cybersecurity infrastructure, the volume of alerts generated daily can be substantial.
Many organizations face the daunting task of processing tens of millions of events each day, leading to thousands of security alerts requiring prioritization and triage. While individual alerts are often dismissed as false positives or non-critical, a trained analyst can recognize patterns of activity that may indicate a more significant threat. However, as alert volumes rise beyond manageable levels, the effectiveness of analysts diminishes. Adding more analysts may seem like a solution, but it is rarely feasible in today's competitive market.

Event Storage Costs

Cybersecurity best practices require organizations to generate, store, and retain security event data across their networks. This data supports essential activities such as security analysis, incident reporting, and forensic investigations. Many organizations also face regulatory requirements mandating event retention for extended periods—anywhere from six months to three years—resulting in considerable costs that consume a significant portion of the cybersecurity budget.

Initial and operational expenses for a SIEM operation can be substantial. According to Blumira and Cybool, setup and integration of a SIEM can range from $70,000 to $440,000, with ongoing costs influenced by data volume, storage, and management. For example, analyzing 500GB/day can lead to expenses exceeding $525,000 annually. Some vendors may also use pricing models based on data ingestion or the number of endpoints, which can add variability and increase costs exponentially.

The volume of event data increases alert generation which in turn drives up costs for analysis tools, management services, storage infrastructure, and staffing. For many organizations, this becomes increasingly uncontrollable, costly and can impact profitability. The solution is not to eliminate valuable security insights, but rather to reduce unnecessary security events. Organizations need to adopt more innovative approaches, like leveraging contextualized cybersecurity threat intelligence, to improve results without escalating costs.

Artificial Intelligence (AI)

Organizations are turning to AI-based tools to address the alert overload problem. Automating repetitive, data-centric tasks is a natural application of AI, and event and alert management is a prime candidate for this technology. For AI to make effective decisions however, it must integrate global threat intelligence insights to triage alerts accurately..
The synergy of artificial intelligence and threat intelligence, applied in real-time, can significantly reduce alert volumes, freeing security analysts to focus on higher-value tasks.

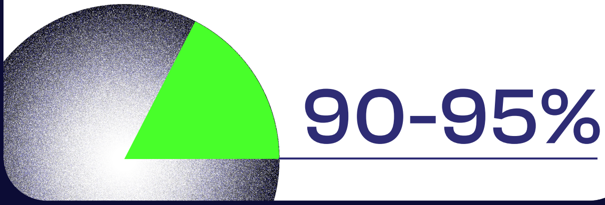
Event Saturation

Logging network events is both an industry best practice and a regulatory mandate. Although the volume and granularity of logged events vary, most organizations strive to capture sufficient data for threat hunting, forensic investigations, and incident reporting. However, managing, storing, and processing large volumes of event data can become burdensome.

While SIEM technologies offer powerful capabilities for event correlation and alerting, they are often costly due to the sheer volume of data they preside over. More data doesn't necessarily equate to greater protection and improved security posture.

Our experience indicates that by applying global threat intelligence to provide context to events and create meaningful alerts, effective decisions can be made. Automating and streamlining this process, with modern technologies can significantly reduce the alert volumes, ensuring the most critical ones are identified based on the risk they bring to the network.

> "You've reduced our workload by 90-95%. Your technology significantly reduces the number of security alerts requiring our team's review, freeing them up to focus on strategic initiatives."
>
> Security Analyst, Healthcare Company, Ontario



Employee Churn

Alert fatigue often leads to dissatisfaction among cybersecurity analysts, impacting their job satisfaction and engagement. While cybersecurity roles can be highly rewarding, analysts thrive on engaging, dynamic work that challenges their skills and allows them to see the impact of their contributions. When their work is dominated by repetitive tasks and an endless stream of alerts, they may feel undervalued and unmotivated. Without opportunities for skill development in threat hunting or meaningful contributions to security outcomes, analysts are more likely to look for new roles elsewhere, especially given the high demand for cyber talent across industries. Retaining skilled professionals should be a priority for organizations, as the costs of recruiting and onboarding new talent can quickly escalate. Reducing alert fatigue and involving analysts in decisions around tools, processes, and intelligence strategies can boost morale and build stronger loyalty. When analysts have the right tools and support, they feel more empowered to protect the organization, leading to greater job satisfaction and lower turnover.

For example, reconnaissance traffic—which can constitute up to 90% of network noise—generates an overwhelming number of events.

Eliminating this traffic before it enters the network can dramatically reduce event and alert loads. Centripetal's CleanINTERNET® solution uses global threat intelligence to identify sources of reconnaissance traffic and block them, significantly reducing the alert load and limiting threat actors' visibility into network assets.

Increasing automation and leveraging AI in alert management also brings substantial value.

While numerous tools offer automated threat monitoring, businesses are understandably cautious about missing critical alerts that could be vital for attack detection and response. By leveraging threat intelligence at scale, **Centripetal's CleanINTERNET®** prioritizes security alerts based on business risk.

The CleanINTERNET® Advanced Threat Detection capabilities utilize AI and a range of sophisticated detection techniques to automate threat monitoring operations. Security analysts provide oversight, conduct further analysis as needed, and relay key insights to customers.

While reducing alert fatigue is a strategic goal, organizations must ensure that security coverage is not compromised. Broad tactics that reduce visibility into security threats can hinder threat detection and post-incident analysis.

Centripetal's CleanINTERNET® maintains full visibility into all events and provides a suite of tools that enable customers to analyze and inspect activity, supporting comprehensive threat management and response.

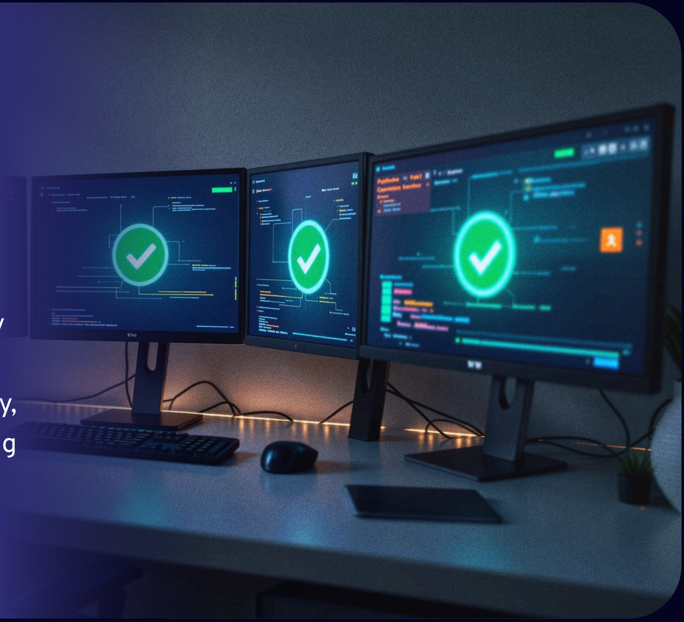
> “I did some spot checking on the firewall logs before Centripetal, 60 million before [the] appliance was implemented, down to 500,000 the other day.”
>
> Senior Cybersecurity Architect, Northeast Healthcare Provider

Centripetal changes the game in cybersecurity, enabling even small IT teams to be massively effective in preventing cyber attacks. Investment in CleanINTERNET® alleviates you and your teams from the many aspects of alert fatigue outlined above - alert overload, storage costs, event management, event saturation, AI and employee churn.

By lowering operational costs, enhancing visibility, and maintaining comprehensive threat protection, CleanINTERNET® provides a sustainable path forward for organizations looking to secure their networks without compromising quality or exhausting resources. As cybersecurity demands continue to rise, solutions like CleanINTERNET® stand as essential tools, enabling even small IT teams to make a significant impact in preventing cyber attacks and protecting valuable assets.

CleanINTERNET®

CleanINTERNET® is an intelligence-powered security solution using high performance computing technology, patented software algorithms and uniquely skilled security analysts to deliver a robust alternative protection strategy at significantly lower cost. CleanINTERNET® presents an alternative approach to cybersecurity, putting threat intelligence at the forefront, moving from reactive to proactive defense, and helping security teams be more efficient and effective.



Conclusion

Organizations need intelligent, proactive solutions to address the growing challenges of alert fatigue and event saturation. Centripetal’s CleanINTERNET® offers a transformative approach to cybersecurity, enabling companies to shift from reactive to proactive defense by leveraging real-time global threat intelligence,AI-driven insights, and robust automation.

This approach not only reduces the overwhelming volume of security alerts but also empowers security analysts to focus on high-priority threats, thereby improving the efficiency and effectiveness of security operations.

CENTRIPETAL

centripetal.ai