

# indeSIEM

UNIFIED EVENT CORRELATION AND RISK-MANAGEMENT FOR MODERN NETWORKS

## GET INTELLIGENT ABOUT SECURITY

Having a SIEM is essential - If you aren't monitoring your environment inside and out from a security perspective, how do you know how well your protections are working? Often SIEM systems are put in the 'too hard' or 'too expensive' bucket. A SIEM is crucial for proactive response and real-time alerts, post-incident forensics and a requirement for certain compliance standards.

Keeping your environment secure is increasingly complex and expensive, but it doesn't have to be. IndeSIEM is a comprehensive, fully managed SIEM-as-a-Service solution that provides centralised visibility and correlation across both your on-premises and cloud devices and systems.

IndeSIEM allows you to gain all the SIEM benefits, without the need for unnecessary capital investment, or the difficult recruitment and training required for these complex systems. Centrally hosted with virtual collector(s) in your environment means your credentials never leave your network, and event logs are encrypted before reaching the SIEM engine.

## Product Highlights



LOG COLLECTION, ANALYSIS  
AND RETENTION



EVENT CORRELATION



LOG FORENSICS



IT COMPLIANCE



CLOUD SYSTEM  
MONITORING



IDENTITY, DEVICE &  
LOCATION REPORTING



APPLICATION LOG  
MONITORING



OBJECT ACCESS  
AUDITING



REAL TIME ALERTING  
USER ACTIVITY MONITORING



DASHBOARDS



REPORTING



FILE INTEGRITY  
MONITORING

# indeSIEM

UNIFIED EVENT CORRELATION AND RISK-MANAGEMENT FOR MODERN NETWORKS

## Why Inde?

Put simply, Inde strive to hire the best, and we heavily invest in training to keep our experts at the top of their field. With IndeSIEM you can significantly improve your security posture, without the challenge of having to recruit and train specialized IT personnel in-house. Inde have experts across networking, cloud and application delivery which can translate events into meaningful analysis and remediation.

---

## Why IndeSIEM?

With more traditional SIEM platforms, the software licensing cost is just the beginning. After that you need expensive equipment to host the software – especially storage, which requires configuration, tuning, monitoring and maintenance. New on-premises and cloud systems need to be integrated, updated, and supported for the SIEM platform. IndeSIEM takes the hard work and ongoing management away, and it has a simple pricing structure.

# indeBLUE

IndeBLUE is the next step in intelligent security, especially when paired with IndeSIEM. Our team of security experts act as your defensive line, performing analysis of your organisation's information systems to actively detect attacks, collect forensic data, identify flaws, mitigate threats, and to make certain all security measures will continue to be effective long after implementation.

IndeBLUE will also provide proactive checks across your environment such as advising on new cloud security protections as they become available, network device firmware recommendations and new vulnerabilities found. IndeBLUE also includes ongoing complementary use of our advanced security scanner to scan your public endpoints, APIs and websites for threats, vulnerability and risks.

We strongly recommend each customer engage an external 'red team' to provide vulnerability and penetration testing. This serves to strengthen the defences and monitoring provided by our 'blue team'. IndeBLUE can be as little as 5 hours a month to provide proactive engagement and SIEM response to significantly enhance your security layers.

[WWW.INDE.NZ/INDEBLUE](http://WWW.INDE.NZ/INDEBLUE)