CONTINENT8 technologies

SIEM & SOC

secure8

SECURE | SIEM & SOC

Discover the Threats Hidden in Your Data

Maximise Security while Minimising Your Effort: A Security Incident and Event Management (SIEM) platform is the foundation of your cyber defence strategy. However, due to the constant maintenance and tuning required while deploying a highly trained 24x7 team to investigate security alerts in a timely manner, it's extremely difficult to do it well.

Continent 8 delivers a comprehensive solution to the challenges of managing and monitoring a world-class SIEM. With an advanced SIEM built on the ELK Stack, Continent 8 provides real-time intelligence into your logs and event data by leveraging threat intelligence, custom rules, machine learning and advanced behavioural analysis to identify security threats while scaling to handle any volume. The Continent 8 team of security experts will customise the SIEM to fit your unique business requirements and security policies. From following your playbooks to customising dashboards to integrating into your ticketing system, our team has you covered.

Centralised Visibility

Eliminate blind spots by viewing or correlating data across endpoints, networks, cloud and much more. Rapidly build custom dashboards and reports to meet the needs of individual users, large groups or customers. Embed charts into your business applications for real-time visibility. Intuitively incorporate geographic mapping into your data to better understand location-based trends.

Eliminate Alert Fatigue

If you've managed a SIEM before, then you've likely dealt with alert fatigue. A seemingly non-stop stream of false positives that can't be easily separated from the real threats. That's exactly what our team of 24x7 security experts does on your behalf. Continent 8 will consistently optimise the platform by correlating event logs, data flows and threat intel to minimise false positives while investigating all of the anomalous behaviour and alerts that remain. The result: A dramatic reduction in the mean-time to detect threats and only a handful of alerts that require real action.

Custom-Tailored Solution

We follow your direction, not the other way around. We customise our playbooks, case management, escalation rules, dashboards, reports and more to align with your compliance requirements and security policies.

Fully Managed SIEM Solution:
24x7 SOC monitoring, platform tuning and investigation of alerts and anomalous behaviours

Advanced Threat Detection:
Machine Learning and Advanced Behavioural Analysis learns the typical behaviours of your data to flag anomalies

Integrated Threat Feeds:
Automated and integrated threat insights to stay ahead of evolving and high impact threats

GET IN TOUCH
sales@continent8.com

Asia: +65 3165 4649
Europe: +44 1624 694625

Latin America: +54 11 5168 5637
North America: +1 514 461 5120

CONTINENT8.COM/SECURE

FACEBOOK TWITTER LINKEDIN YOUTUBE

CONTINENT8 technologies

SIEM & SOC

secure8

SECURE | SIEM & SOC

Monitoring, Detection & Responding to Critical Threats

Customer-Defined Dashboards

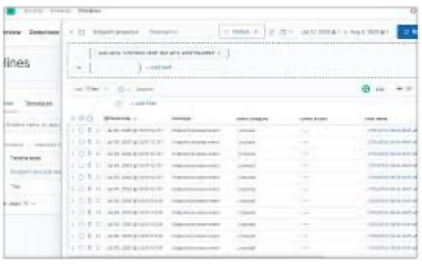
Dashboards aren't always one-size fits all. That's why we customise them or create new ones to fit your needs. After all, dashboards are an integral part of any SIEM solution to help you in visualising the security incident and event log data throughout your infrastructure or to just keep up with regulatory requirements like PCI or SOX.

Investigation Timeline

A timeline depicts the operational events underlying a security incident in sequential orders. Data from multiple indices can be added to a timeline to help in visualising complex threats. It's a vital tool for our security experts to follow the movement of threats in your infrastructure and an easy way for you to validate the threat before remediation.

Maps with Multiple Layers & Indices

Embed maps in dashboards or view them independently. Depict how your data sits relative to physical features like international borders or business-specific features like sales regions. You can plot individual documents or use aggregations to plot any data set, regardless of size.



Third-Party Validation

PCI-DSS and HIPPA Compliant. Pre and post-execution validation from AV Comparatives, NSS Labs, VirusTotal, Forrester, SE Labs, and MITRE. Participation in MITRE's program for public testing, submitting to MITRE researchers for independent testing against targeted attacks.