Product Brochure

Next Gen SIEM Cloud

Secure Cloud Monitoring for CSPs

Huntsman®
Defence-Grade Cyber Security

View all customers from a single console

Next generation Security Monitoring for Cloud Service Providers

Huntsman Security's Next Gen SIEM Cloud is a highly dependable security platform that helps Cloud Service Providers (CSPs) deliver advanced, flexible and cost effective security monitoring and analytics services.

Providing high-value security oversight capabilities to cloud customers increases margins, improves service resilience, simplifies security management and accelerates revenue generation from new customers.

The technology is an ideal foundation for your Security Operations Centre (SOC). It operates quickly and autonomously, interfaces with all your systems and your customer's platforms and security controls. It works the way your security team and customers need it to.

Next Gen SIEM Cloud's multi-tenancy capability means cloud service providers can monitor all customer systems and conduct all security monitoring and reporting from a single console.

> "We need to maintain security of the infrastructure and provide security services and log information to customers. Everybody wants visibility of their security information."

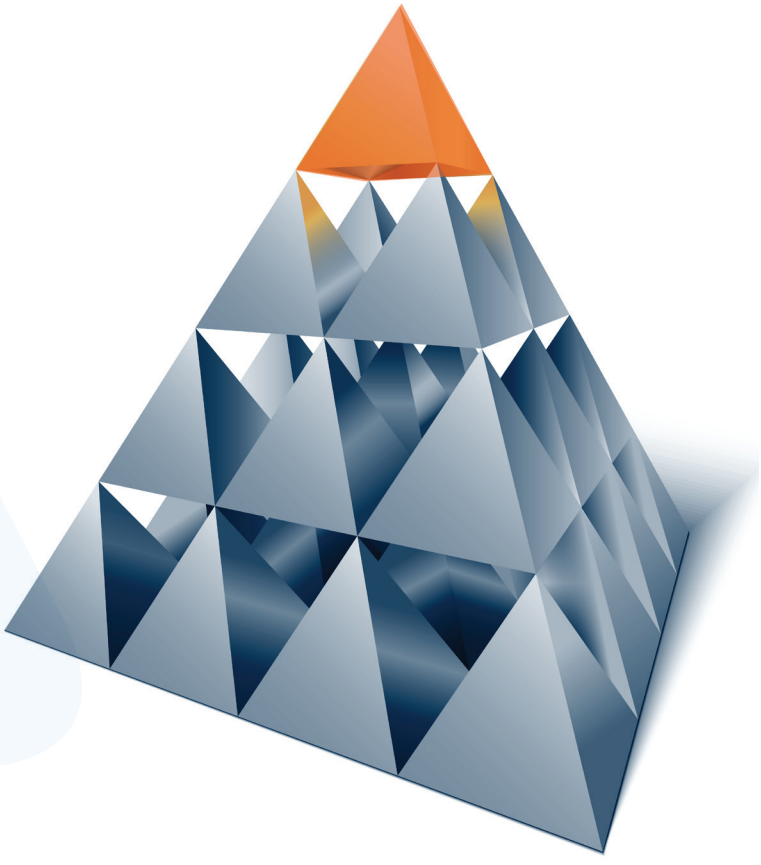
Huntsman®

What Next Gen SIEM Cloud delivers

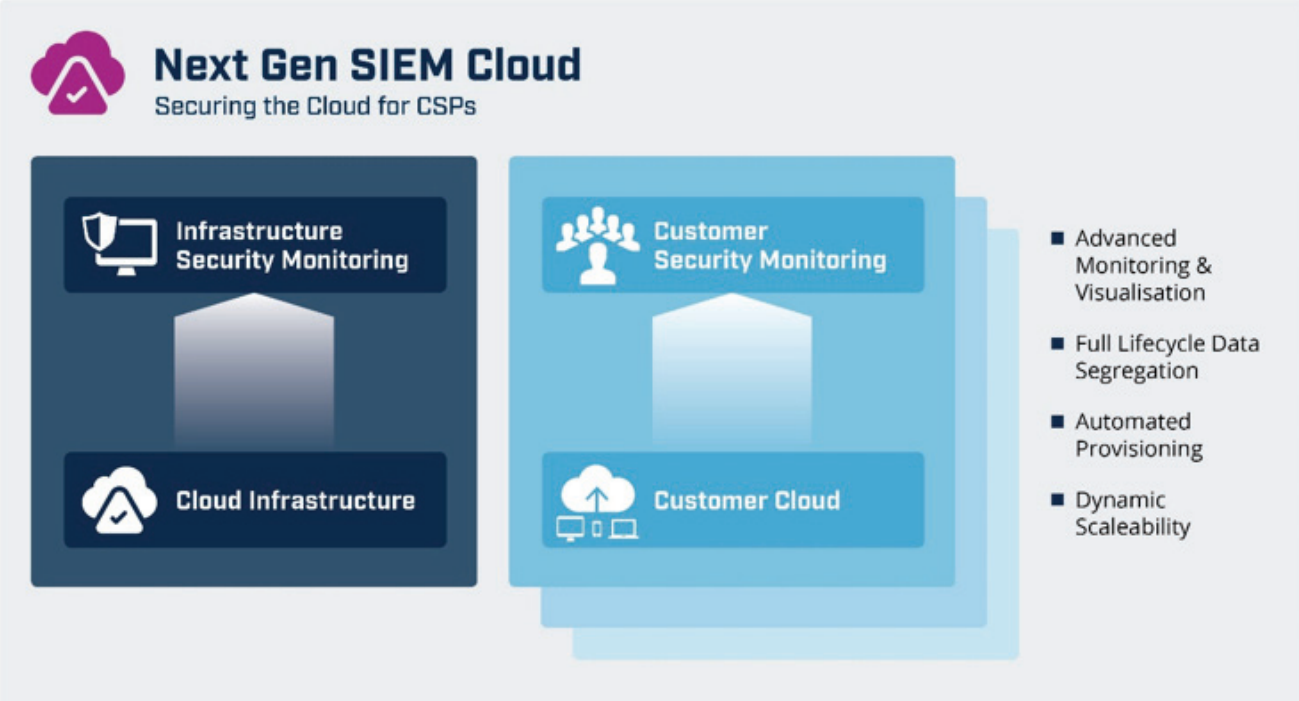
Huntsman Security's Next Gen SIEM Cloud has all the capability of Next Gen SIEM plus multi-tenancy. This enables cloud service providers to monitor both the cloud service infrastructure and provide value-added monitoring and security analytics services for customers.

The technology delivers:

- Rapid deployment with delivery as a virtual machine
- Single view of the entire cloud estate and individual customer reporting
- Streamlined workflow in your security operations centre
- Robust data management, separation and access control mechanisms
- Threat awareness between and within customer networks – to detect threats more quickly and offer value-added services
- Highly flexible licensing models to suit the variable nature of cloud services
- Scalability to meet the evolving requirements of your business and your customers



Huntsman®



Next Gen SIEM Cloud explained

> "Scalable to high volume data processing and big data storage and analysis"

Next Gen SIEM Cloud – how it works

- Operates across a shared services environment with multi-tenancy capability and full scalability
- Support for all major virtualisation technologies
- Provides data segregation at both the database layer and administrative interface
- Supports all log and event sources, as well as databases, networks and applications for maximum flexibility
- Comprehensive threat Intelligence capabilities for intelligent detection and resolution using both external and pan-customer sources
- Automation of routine tasks, data gathering and reporting
- State-of-the-art query interface, data visibility and business intelligence
- Inbuilt compliance standard support
- Support for external cloud-based services at IaaS, PaaS or SaaS layers
- Data sovereignty control and management

Product Features	Next Gen SIEM	Next Gen SIEM Cloud
Data Collection and Anaylsis		
Continuous Monitoring	✓	✓
Real-time collection	✓	✓
Correlation and alerting	✓	✓
Behavioural Anomaly Detection / Machine learning engine	✓	✓
Network flow monitoring (Netflow/pcap)	✓	✓
Threat Intelligence (internal or 3rd party)	✓	✓
Reference tables of platforms, hosts, users for analysis	✓	✓
Unlimited/free agents	✓	✓
Original log file collection	✓	✓
File/Directory integrity monitoring	✓	✓
Reporting and Visibility		
Query/display interface	✓	✓
Operational dashboards	✓	✓
OOTB Compliance packs	✓	✓
GRC dashboards	✓	✓
Ad hoc and scheduled reports	✓	✓
Web-based “Business Intelligence” interface	✓	✓
Workflow and Automation		
Incident manager	✓	✓
Scripted/defined response (automatic or manual)	✓	✓
Alert tracking and workflow support	✓	✓
Management		
Role-based and granular access control	✓	✓
Full audit trail	✓	✓
Multi Tenancy		✓
Asset manager tool	✓	✓
High availability/Clustering	✓	✓
Multiple on-line data repositories	✓	✓
Automatic data backup, aging and archive	✓	✓
Support		
Phone/Email	✓	✓
Onsite	✓	✓

Want to find out more?

For a more detailed discussion on automating incident response, please contact the appropriate office listed below.

About Huntsman Security

Huntsman Security is the trading name of Tier-3 Pty Ltd. The technology's heritage lies in delivering a key foundation stone of the cyber security risk management, monitoring and response capability in some of the most secure and sensitive environments within the intelligence, defence and criminal justice networks across the world, where Huntsman Security solutions are deployed and accredited to the highest security levels.

HUNTSMAN | TIER-3 PTY LTD

ASIA PACIFIC

t: **+61 2 9419 3200**

e: **info@huntsmansecurity.com**

Level 2, 11 Help Street
Chatswood NSW 2067

EMEA

t: **+44 845 222 2010**

e: **ukinfo@huntsmansecurity.com**

7-10 Adam Street, Strand
London WC2N 6AA

NORTH ASIA

t: **+81 3 5953 8430**

e: **info@huntsmansecurity.com**

Awajicho Ekimae Building 5F
1-2-7 Kanda Sudacho
Chiyodaku, Tokyo 101-0041

huntsmansecurity.com linkedin.com/company/tier-3-pty-ltd twitter.com/Tier3huntsman