



Product Brochure

MSSP SIEM

Mission critical cyber security analytics

▶ MSSP SIEM

Huntsman Security's MSSP SIEM supports you and your customers with a mission critical cyber security analytics application that deploys from a single SOC platform managed by your team. Our cost-effective SIEM offers multi-tenancy to support a diverse range of customers, with a complete cyber threat detection, incident management and reporting system.

Our next generation MSSP SIEM guards the systems holding your customers' sensitive data, IP, processes, contact and financial information, to protect against unauthorised access, attack and damage.

We also provide flexible commercial and licencing arrangements with OpEx/ subscription models for all our managed security service providers.

Why MSSPs choose Huntsman Security's Enterprise SIEM to **DETECT | ANALYSE | MANAGE** their customers cyber security:

A broad range of integrated SIEM capabilities that deliver significant functional efficiencies and a lower operating cost per customer. Key Features of Huntsman Security's MSSP SIEM:



COST-EFFECTIVE FOR MSSPS

It offers multi-tenancy for 250 to 50,000+ endpoints across multiple end-customers



SINGLE SOC PLATFORM

Eliminates the acquisition, support and resource training costs of multiple platforms, while still supporting a diverse range of customers



EASY NEW CUSTOMER ON-BOARDING

Utilising standardised yet flexible technology that enables the continuous development of new features



DEFENCE-GRADE CYBER SECURITY

For all organisation types and sizes



LIVE MITRE ATT&CK® THREAT HEATMAPS

With easy to access alerts and reporting



RESPONSIVE IN-STREAM PROCESSING

To reduce analyst workloads, simplify threat investigation and limit the time at risk



[Explore the features >](#)



[Register for a Demo >](#)

► Features

Huntsman Security's SIEM sits at the core of your Security Operations Centre (SOC) as a single, comprehensive, yet flexible multi-functional threat monitoring and response platform.

Live Interface & Visualisation

- ✓ **Real-time MITRE ATT&CK® heatmaps and threat summary**
GUI driven query interface to optimise investigation and save time
- ✓ **Configurable alert rules and behavioural models**
Allowing the detection of the widest range of threats – including APTs
- ✓ **Centralised management & coordination**
Alerting rules, event collection, queries and reports for reliable security governance
- ✓ **Lifecycle visibility of alerts, threats and incident information** for all stakeholders

Speed & Performance

- ✓ **Advanced, high speed in-stream event processing, analytics**
Responsive decision making – with capacity in excess 100,000 events per second
- ✓ **Behavioural anomaly detection**
Extend discovery beyond predefined patterns and signatures with machine-learning
- ✓ **Automatic collection and integration of multiple sources of Threat Intelligence**
For enrichment, threat verification and orchestration, to speed up resolution of incidents and reduce false positives
- ✓ **Accelerated capacity for cyber security decision making**
With multiple views of attack information by users or endpoints, to pinpoint an asset/user at risk and quickly tailor a defence

Workflow & Scalability

- ✓ **Simple, yet flexible**
Deployment options and scalable data storage architecture
- ✓ **Support for virtualisation**
Cloud and on-premise deployments
- ✓ **Optimised for detection**
Correlation and reporting OOTB – an extensive range of inbuilt alerts for attacks, technology types and compliance standards
- ✓ **Support for a wide range of data sources and technology platforms**
Hundreds of technologies supported natively + data stream or source can be configured
- ✓ **Broad range of pricing and licensing models**
To suit organisations of all sizes and complexity (inc. Capex and OpEx subscription pricing)



Register for a Demo >



▶ Explore MITRE ATT&CK®

MITRE ATT&CK® Summary Dashboard

Early warning systems to alert your SOC team to pending cyber-attacks are invaluable.

Huntsman Security's SIEM offers built-in high speed detection capabilities, matched to the MITRE ATT&CK® framework, that adds visibility and contextual information on pending attacks and their severity.



MITRE ATT&CK® Summary Dashboard



Explore the features >



Register for a Demo >



The value of Huntsman's Enterprise SIEM is evident in the vast number of sensitive/mission critical environments that use it, where the consequence of a breach can be measured in human lives.

MITRE ATT&CK® heatmap highlights:

- Live dashboard that changes colour progressively, shows changes in tactics such as lateral movement and privilege escalation as they occur
- Equips analysts with an accurate picture of the state of alerts and detailed actions on how best to respond
- Multiple views of attack information by users or endpoints, to pinpoint an asset/user at risk, and quickly tailor responsive action
- Identifies patterns of intrusions and onward activity, to pre-empt subsequent stages
- Provides easy access to mitigations, for each stage of an attack, with a simple right click
- Provides context of alerts and stage(s) in the attack lifecycle, with a clear visual display based on users, endpoints or time windows
- Prioritises which alerts get attention, based on severity and volume of occurrences



MITRE ATT&CK® Active Heatmap



Explore the features >



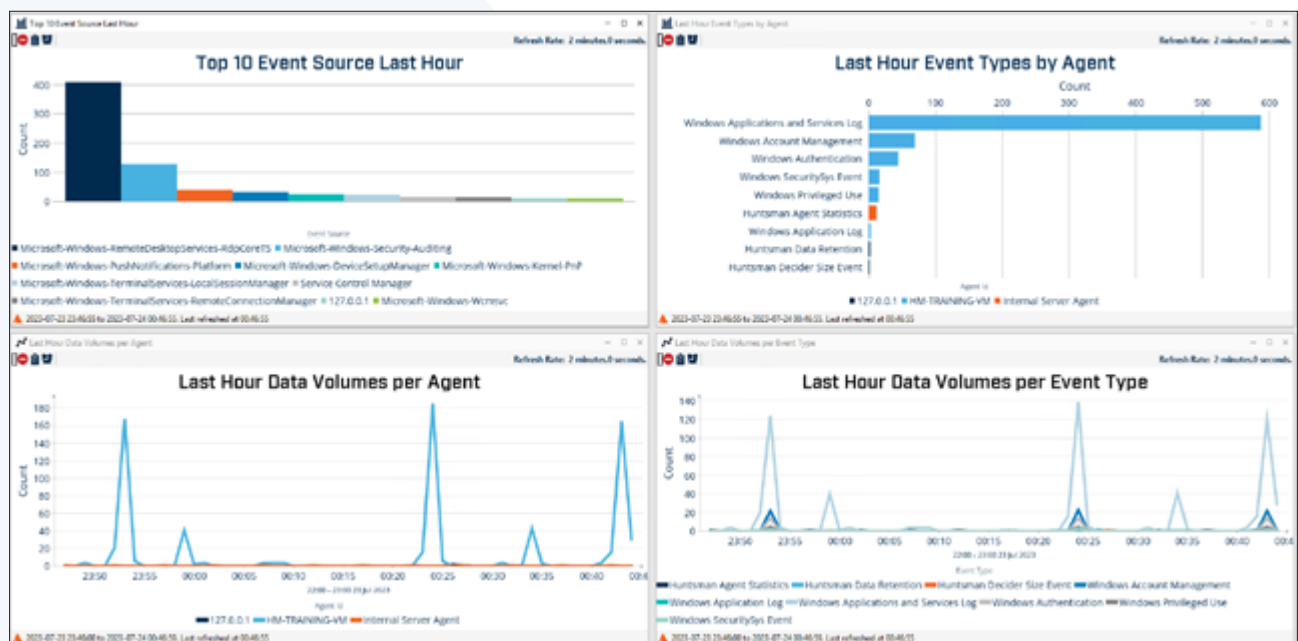
Register for a Demo >

Designed as the cornerstone of any Security Operations Centre - to **deploy into complex environments** and manage data across multiple end-customer tenants.

Reporting and Alerting

Visualisation of cyber-risk data is integral to the diagnostic process, and clarity of that information is also key to operational dashboard effectiveness and informed security reporting.

Any data set within the system can be easily translated into a report and automatically published to a relevant stakeholder in support of your compliance and reporting needs.



Live Dashboard



Explore the features >



Register for a Demo >



We provide **real time visibility of the state of your security operations** with live dashboards and alerts to **inform your response to attacks** and guide your team through investigation and resolution.

► Behaviour Anomaly Detection (BAD2)

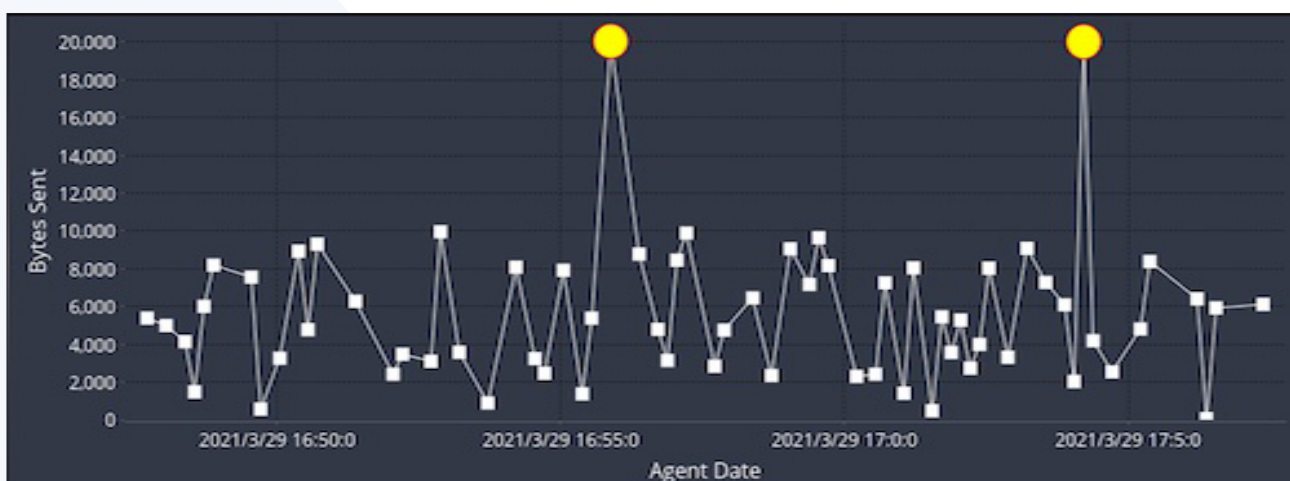
Huntsman Security's patented Behaviour Anomaly Detection (BAD2) engine is integrated into its SIEM to provide real-time machine learning capabilities to detect unknown threats.

Huntsman Security's SIEM analyses activity, based on the organisation's risks, threats and vulnerabilities, to learn normal patterns of behaviour and activity. Armed with activity baselines, it detects threats or suspicious activity that differs from expected behaviour.

Huntsman Security's SIEM can detect:

- Higher/unusual volumes of network session or user traffic on a per user or per host basis
- Volumes of events such as file accesses or other activity on hosts/workstations
- Changes in the usage profile of application servers or query operations on databases
- Changes in the frequency or prevalence of operations – up or down

By dynamically profiling multiple variables with sophisticated in-stream behavioural algorithms, the detection engine adapts to changes and trends over time; either adjusting and relearning “normal” values or using fixed/pre-set baselines, depending on the nature of the environment and risk.



Behavioural Analysis - Network Data Transfer Anomaly



[Explore the features >](#)



[Register for a Demo >](#)



It incorporates **best practice security and compliance**, and is deployed in the some of the most highly accredited security environments in the world including: UK GPG13 and Australian ISM

▶ Threat verification and automation

Huntsman Security's SIEM provides extensive automated response script and command execution capabilities, (Guardian Response). Additionally, we provide the option to include our integrated Security Orchestration, Automation and Response (SOAR) technology.

Guardian scripts can automatically initiate complex automated responses, including:

- Asynchronously seek data to enrich the investigation process, therefore reducing operator workload and limiting the time between detection and response
- Verify security alerts in seconds, automatically seeking supportive contextual data to distinguish between real threats and false positives
- Support the threat response process of security analysts through the delivery of a case file of all available and relevant threat information, or launch specific machine-automated actions in response to trigger events

Once an alert has been legitimised as both serious and genuine, the system can be configured to take actions to mitigate risks such as (i) threat containment at a network level; (ii) initiate perimeter/Wi-Fi connection termination; (iii) isolate or suspend a user account based on malicious user activity.

Huntsman®
Defence-Grade Security Platform

Analyst Portal

Views: Summary Investigate Resolve View Report Mail Report

Status: Open Types: Manual

Indicators of Compromise - 192.168.1.10

Internal Estate	File System	Registry	Huntsman	Operating System
containment	modifications	key changes	alerts	vulnerable

Type: malware-object
Severity: major
Detection device: Web MPS
Source: 192.168.1.10
Target: 192.166.4
Malware name: Malware.Binary.Doc
Malware: Binary.doc

Malicious Alert Messages

1500 : Startup behavior anomalies observed ; A new process has been launched
4000 : Exploit code detected ; Generic detection
4801 : Exploit code detected ; Generic ExploitCode Detection
7000 : File created by non-executable ; File created by non-executable
7002 : File overwritten by non-executable ; File overwritten by non-executable
7003 : File deleted by non-executable ; File deleted by non-executable
8019 : Process creating and starting process ; Process creating and starting process
10006 : Exploit Code Activity ; Exploit Code → OFFICE DOCS
10027 : Startup behavior anomalies observed ; Process Started in Office Files

Resolve

Investigate

Automated Threat Verification



Explore the features >



Register for a Demo >



Offering processing capacity in excess 100,000 events per second, rapid resolution through extensive internal and external threat intelligence, and **in-built security and compliance best practice**

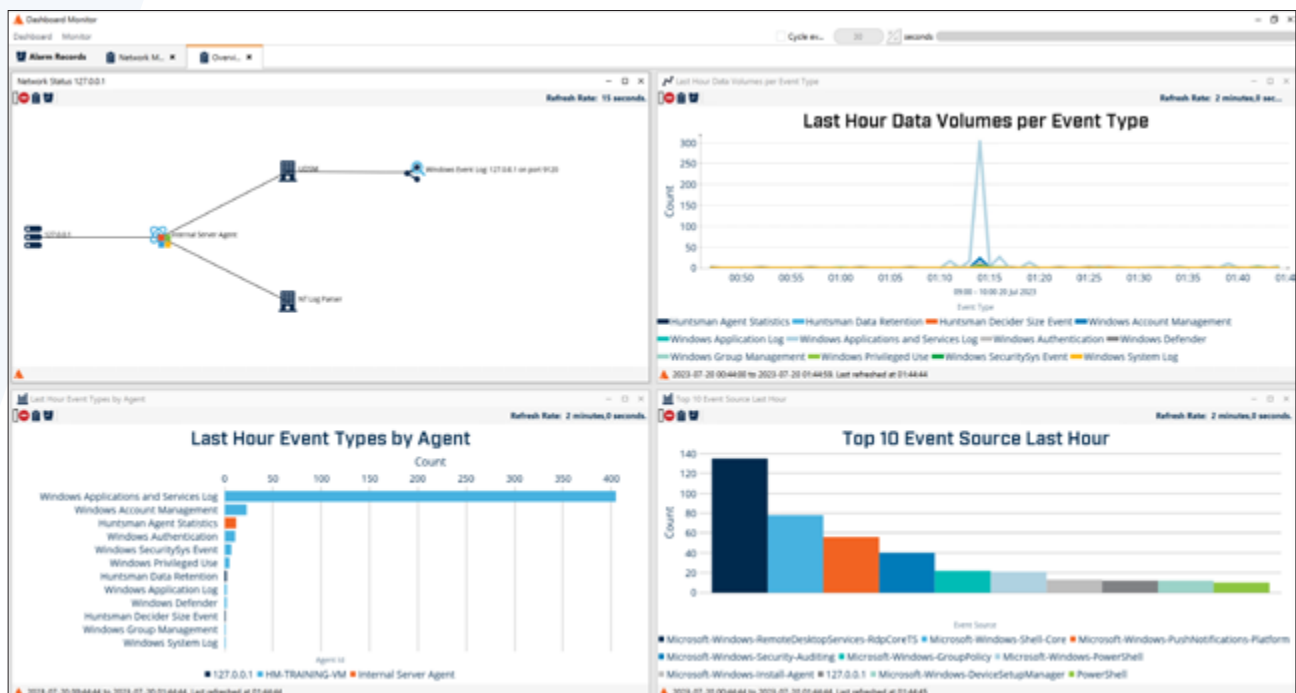
▶ Managing alerts and incidents

Detecting a threat and generating an alert is only the first stage of the security operations process.

Huntsman Security's SIEM provides complete support for the alert triage, investigation and response lifecycle.

Key alert and incident features of Huntsman Security's SIEM:

- Threat verification automatically gathers evidence to enrich alert data and eliminate false positives
- Alert tagging, to aid triage and classification with customisable statuses
- Clearly pinpointing an asset or user at risk, through multiple views of attack information by users or endpoints. This simplifies and accelerates critical cyber security decisions and response actions.
- Incident management, screens for tracking, as issues are opened, investigated and closed
- Incident history and root cause reporting



Alert Classification Dashboard



Explore the features >



Register for a Demo >



Our SIEM's in-built incident management solution allows serious problems, comprising multiple alerts, events, data sets and multiple stages of investigation to be handled and reported with ease and efficiency.



Incident Summary

Register for a Demo

Register for a 15-minute demonstration of our SIEM

[Register](#)



Want to find out more?

Register for a 15-minute demonstration of our SIEM

[Register](#)

Or contact your local Huntsman Security office (listed below) to talk to one of our team today.

▶ About Huntsman Security

Since 1999, Huntsman Security has been on the cutting-edge of cyber security software development, serving some of the most sensitive and secure intelligence, defence and criminal justice environments in the world.



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

GINZA EAST SQUARE 4F
3-12-7 Kyobashi Chuoku, Tokyo
Japan 104-003



huntsmansecurity.com



linkedin.com/company/tier-3-pty-ltd



twitter.com/Tier3huntsman