Huntsman
Solutions Brochure

Huntsman®
Defence-Grade Security Platform

Huntsman Defence Grade Security Platform

Defence grade technology for military grade attacks

The **Huntsman Defence Grade Security Platform** is unique in its ability to deliver a modular set of integrated products that build to deliver an end to end Security Management solution that collects and contextualises security data in real time to automatically pinpoint the threats that matter and limit the time at risk for any enterprise.

Huntsman Security maintains its reputation for innovation by keeping pace with the rapidly changing security environment and developing solutions that continue to redefine the speed and accuracy of cyber threat resolution and reduce the time at risk.

REAL-TIME THREAT DETECTION

Using Huntsman's true **Behaviour Anomaly Detection (BAD)** capabilities you don't have to know what a threat looks like to detect it. Using automated machine learning Huntsman BAD allows you to pinpoint unknown and unknowable threats. These are the threats that are devised specifically to circumvent existing security solutions as they are simply invisible to rules or alert databases. BAD will:

- Automatically profile traffic, system and application activities in real time and use machine learning capabilities to understand what normal behaviour for your networks, systems, users and applications looks like.
- Identify deviations from this learned baseline in real-time using data analytic techniques.
- Achieve greater accuracy and speed of detection by contextualising alerts against internal or external sources of Threat Intelligence for real time actionable intelligence.

Incorporate internally and externally sourced threat information to add intelligence to the analysis process.
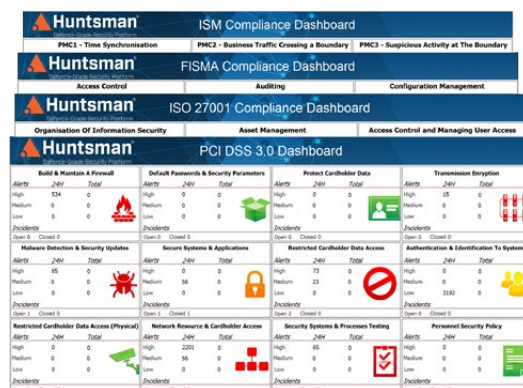

COMPLIANCE

Huntsman Enterprise SIEM incorporates comprehensive compliance packs, with defined query sets, alerts and reports for a range of compliance standards: ISM, DSD Top 4, ISO27001, FISMA/SP800-53, SOX and PCI-DSS are all included as standard. Compliance has traditionally been an activity that is verified or reported at specific times. Huntsman's real-time monitoring gives continuous "reporting" of compliance issues for immediate resolution and/or automated escalation and resolution when a breach occurs.

▲ Huntsman®

CYBER THREAT RESOLUTION IN SECONDS

Detecting a potential threat is where many security solutions finish and where the real work for the analyst begins. Analysts can be overwhelmed by the masses of threat information, many of which can be false positives. The problem is that it can take hours to investigate these threats. **Huntsman Analyst Portal™** removes the queue of detected but un-investigated threats by removing the noise and distinguishing in seconds between false positives and the smaller number of real threats, significantly reducing cost and time at risk.
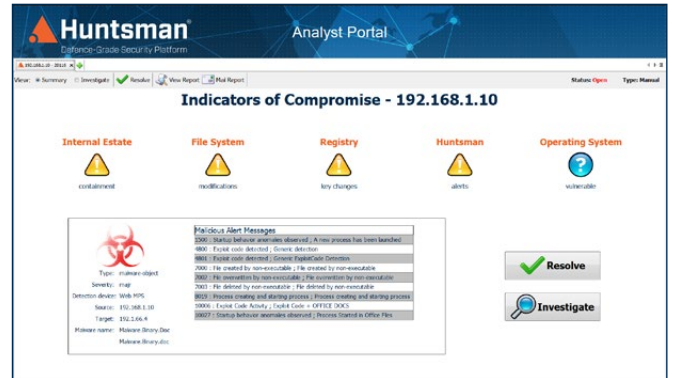
- It provides attack and situational awareness data, indicators of compromise, host and end-point infection information;
- This means your security team can quickly understand the reason, nature, origin and impact of an attack;
- Huntsman can also execute pre-defined responses or alert APIs to proactively avert attacks by quarantining systems, suspending access or increasing vigilance and monitoring levels on critical systems.

## The key to Cyber Resilience is instant detection and resolution

CONSOLIDATION AND MODERNISING OF LEGACY SIEMS

In large enterprises it is not uncommon to find several different SIEM solutions monitoring different network segments, divisions or regions. The result can be that it is impossible to get a single view of the compliance or risk status of the entire organisation. The same can be true for Managed Security Services Providers (MSSPs) who are monitoring a variety of legacy SIEM solutions on behalf of their customers.

In all other facets of business, organisations compile management information about sales, revenue, costs etc. to enable informed prioritisation and decision making.

The **Huntsman Unified Console** links information from disparate legacy SIEM environments. Working with multiple SIEM solutions it enables managers, as well as analysts, to monitor, correlate, analyse and report standardised information from across the entire organisation without the need to change existing solutions, impact local processes or disrupt federated security technology management.
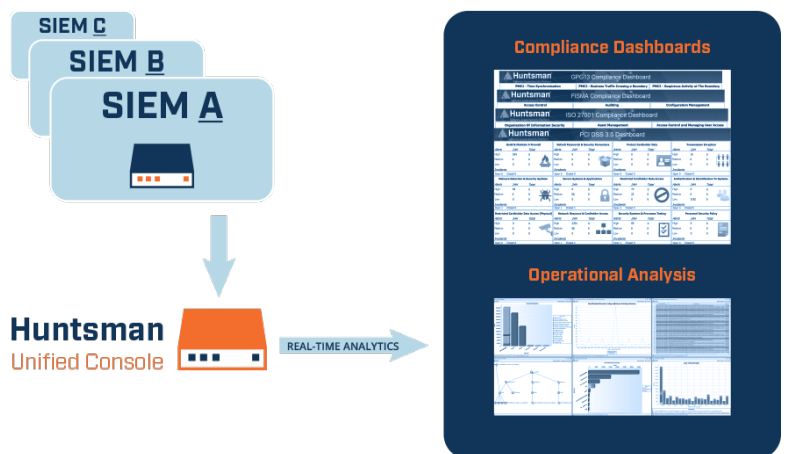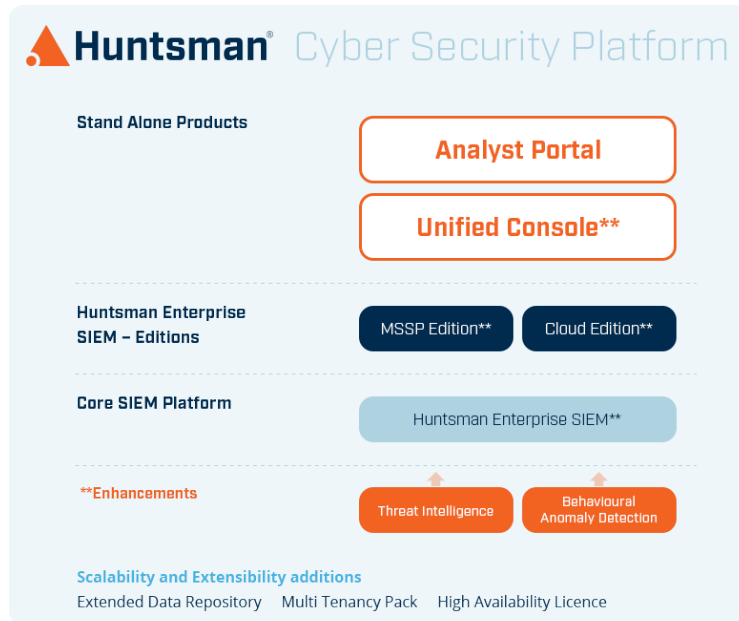
Huntsman®

HUNTSMAN ENTERPRISE SIEM

Huntsman Enterprise SIEM is at the core of the Huntsman Cyber Security Platform. The product delivers an intelligent security log, event and incident management solution that analyses and correlates events in real time to provide early detection of security threats and regulatory compliance issues.

Huntsman offers a single console view of all alerts, notifications and reports. Its drilldown dashboards permit rapid investigation for triage of issues that can then be fully analysed in conjunction with related events using the in-built incident management system or exported to a ticketing solution.

FOR SERVICE PROVIDERS, MSSPS AND CLOUD SERVICES...

Huntsman supports full multi-tenancy, offers highly flexible licence models to correspond with the commercial needs of service businesses and

delivers data sovereignty with advanced detection and resolution capabilities for the delivery of highly-optimised end-customer services and visibility.

ABOUT HUNTSMAN SECURITY

Huntsman Security is part 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 intelligence, defence and criminal justice networks across the five eyes community of Australia, Canada, New Zealand, United Kingdom and United States. Huntsman solutions are deployed and accredited within this community 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

100 Pall Mall, St James
London SW1Y 5NQ

North Asia

t: +81 3 5809 3188

e: info@huntsmansecurity.com

TUC Bldg. 7F, 2-16-5 Iwamoto-cho,
Chiyoda-ku, Tokyo 101-0032

Americas

toll free: 1-415-655-6807

e: usinfo@huntsmansecurity.com

Suite 400, 71 Stevenson Street
San Francisco California 94105

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