Huntsman
UNIFIED CONSOLE™

Modernise security –
Deliver enhanced intelligence

Huntsman®
Defence-Grade Security Platform

The Huntsman Unified Console™ will change the way heterogeneous SIEM environments are managed.

By overlaying existing SIEM solutions the **Huntsman Unified Console™** delivers advanced functionality including centralised alert information, comprehensive visualisation and security intelligence to multi-vendor SIEM deployments.

The Huntsman Unified Console™ delivers:

- A single aggregated security view to support centralised management, analysis, reporting and incident management for multiple information silos
- A modernised real-time security and compliance interface that spans disparate SIEM solutions to enable live GRC status dashboards, behavioural anomaly detection and threat intelligence capabilities

Huntsman Unified Console™ uses the Huntsman® Enterprise SIEM engine to seamlessly integrate existing SIEM solutions and visualise all downstream alerts and incidents from an up-to-the-minute management console to deliver:

- Operational and management dashboards
- Continuous compliance monitoring
- Real-time security intelligence
- Global alert coordination and response

FEATURES

- Single pane of glass for all security alert information
- Real-time alert correlation, true behaviour anomaly detection and machine profiling
- Advanced fully flexible live compliance and operations dashboards
- End-to-end Incident Management
- Out of the box reporting for compliance, auditors and business managers
- Multiple users with full role-based access control

BENEFITS

- Modernises and extends legacy SIEM deployments
- Real-time visibility of corporate security alerts
- Enterprise wide analysis and monitoring of alerts
- Simplify and automate collection of all security alert data
- Utilises existing investment and integrates with existing security and SIEM technologies
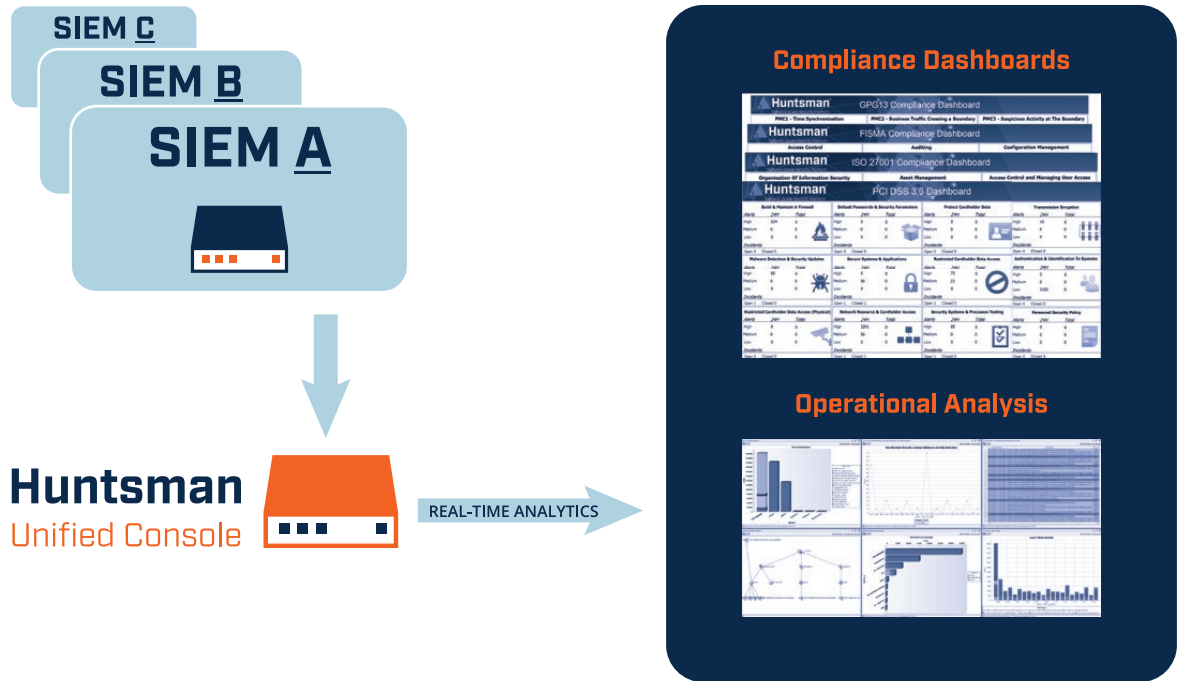
Huntsman®

- Huntsman® advanced analysis and performance
- Support for multiple downstream "legacy" SIEMs from multiple vendors
- Easy installation
- Simple architecture
- Utilisation of existing infrastructure
- Single security intelligence console

SIEM INTERCONNECTION

The **Huntsman Unified Console™** integrates with existing SIEM solutions through its capability to receive information from a legacy SIEM as a separate feed for processing and storage.

The level of detailed information received by **Huntsman Unified Console™** is dependent upon central information needs and the ability of the legacy SIEM to export relevant security information. Huntsman analyses and reports upon all alert information received from across all SIEM silos.

SIMPLE DEPLOYMENT

The **Huntsman Unified Console™** is simple and easy to deploy within any organisation. Existing SIEM components are configured as separate, aggregated data sources allowing information

outputs to be easily gathered for a single view from across otherwise unrelated environments.

Simple configuration details for each source SIEM mean that changes are quick and easy and there is no loss of data or disruption to existing services.

ALERT DATA STANDARDISATION

The **Huntsman Unified Console™** matches and links security alert data from different SIEM vendors and security silos.

Using predefined alert recognition profiles for each downstream SIEM, the Huntsman Unified Console™ is able to decode and recognise alerts from any source irrespective of the format it is delivered in, e.g. Syslog, SNMP, CSV, XML.

Huntsman®

CENTRALISED DASHBOARD

Huntsman Unified Console™ comes with operational and compliance dashboards out-of-the-box. Alert data from existing, downstream SIEMs can be monitored independently or unified as required for separate business units or domains or an enterprise wide view.

Operational dashboards display detailed or high-level security intelligence while compliance dashboards provide a real-time view of enterprise or business unit compliance against required security standards.

UNIFIED CONSOLE™ INTELLIGENCE PACK

With the optional Intelligence Pack, Unified Console customers can also utilise Huntsman's unique state-of-the-art Behavioural Anomaly Detection engine to analyse alert data, using activity profiles that have been automatically built within the machine learning engine, for trends, variations, anomalies and suspicious activity, locally or globally, in real-time.

The Intelligence Pack also includes the advanced Huntsman® Threat Intelligence capabilities which enable integration with a wide variety of external information sources, threat feeds, CERT advisories and data sources for early warning of known threats and the inclusion of that information for improved security decision making.

This enables advanced analysis and behaviour profiling to be performed across all security technologies and vendor solutions for an enterprise view of the prevailing status of security intelligence at any time.

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