Huntsman®
Defence-Grade Cyber Security

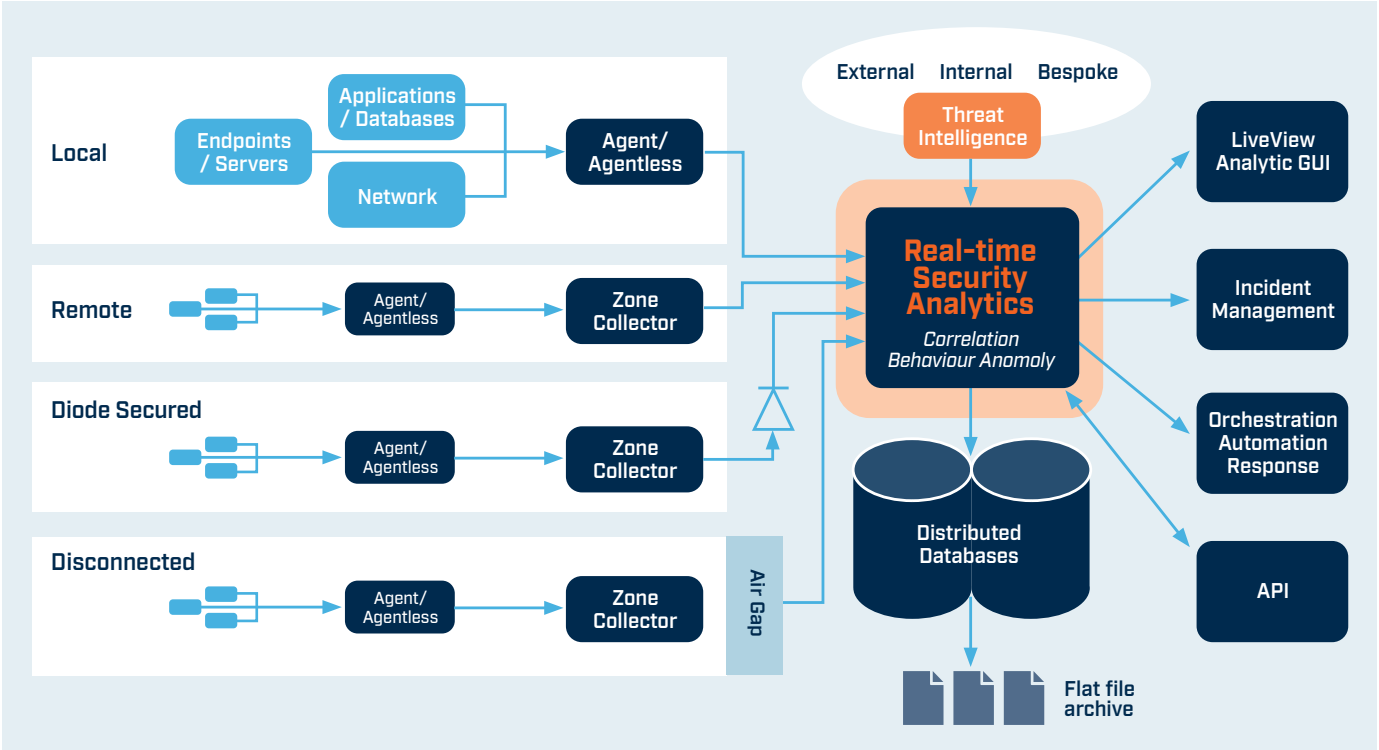
Enterprise SIEM for closed networks

Protective monitoring solution of choice for Government, Systems Integrators, MSSPs and high security environments

Huntsman SIEM is the chosen protective monitoring solution of UK government organisations at the highest security levels. It runs independently in closed networks **without** the need to rely on external resources or Internet connectivity to perform **any** function, including applying updates.

Designed as a software solution for use in highly secure networks, it easily adapts to accommodate bespoke log sources, unique architectures, and extreme requirements without the need for specialist skills.

Huntsman SIEM Architecture



HIGHLY FLEXIBLE DESIGN AND CONFIGURATION allows deployment within the most bespoke environments.

Easily customisable on-site, the SIEM:

- Can be deployed in any network architecture from the simplest to the most complex, whether distributed or multi-layered.
- Supports data collection from any readable source and specialist application, using any logging protocol.
- Fully supports custom log formats with the capability to perform pre-parsing actions on event data.
- Collects from network segments protected by data diodes or air gaps.

Huntsman SIEM Architecture (cont'd)

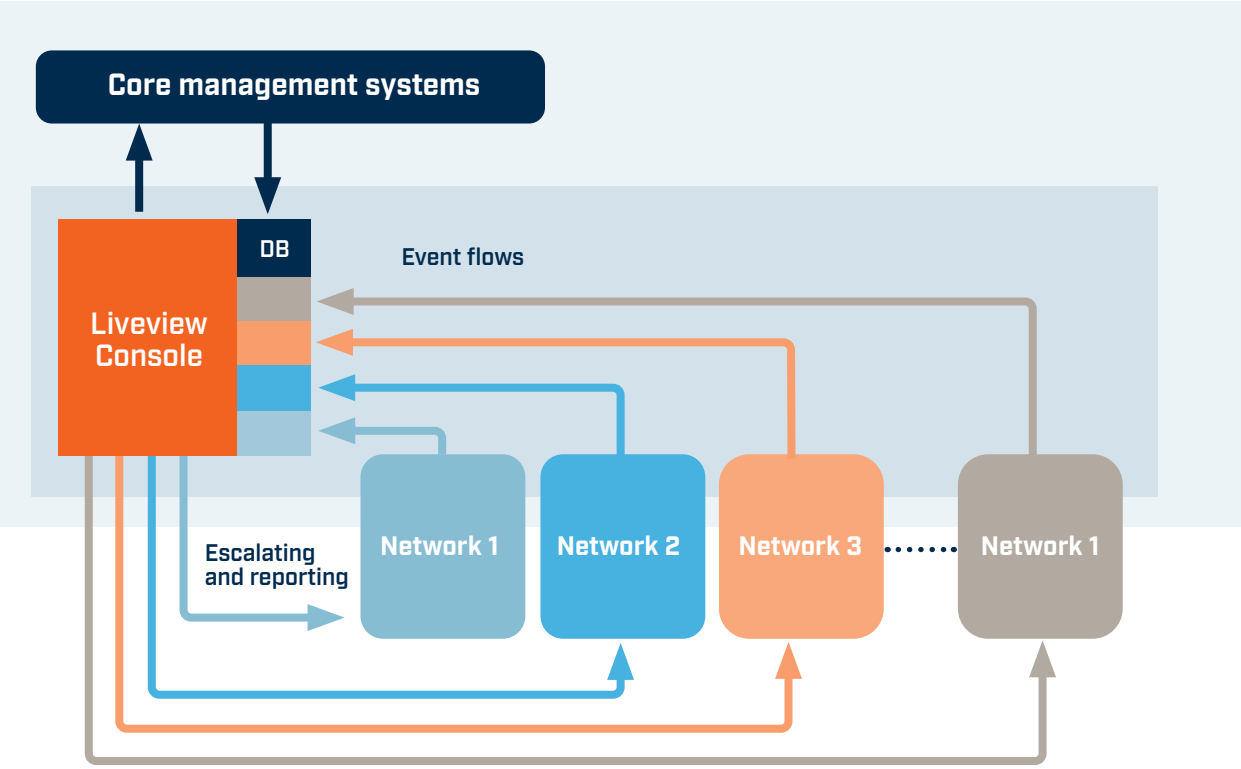
HIGH-SPEED IN-STREAM PROCESSING with a distributed architecture and **in-memory analytics**, to collect, process, analyse and alert upon events at a rate in excess of **130,000 events per second** (EPS). This dramatically reduces the time to detection and ensures performance is maintained even in high volume environments, avoiding risk of database contention.

Even under peak loads, Huntsman SIEM uses a Store and Forward design to ensure no data is lost whilst still allowing events to be collected and normalised.

MULTI-TENANCY is built into the core of the solution allowing data from different networks and security classifications to be collected and analysed on a single instance, but stored in separate, segregated data stores.

- Analysts only have to monitor one screen.
- Detection and alerting rules only need to be written once.
- Threat hunting across multiple networks.
- Custom detections and reporting for specific sources or networks as required.

Huntsman SIEM is a self-contained solution that does not require any Internet connectivity which makes it ideally suited for networks without external links .

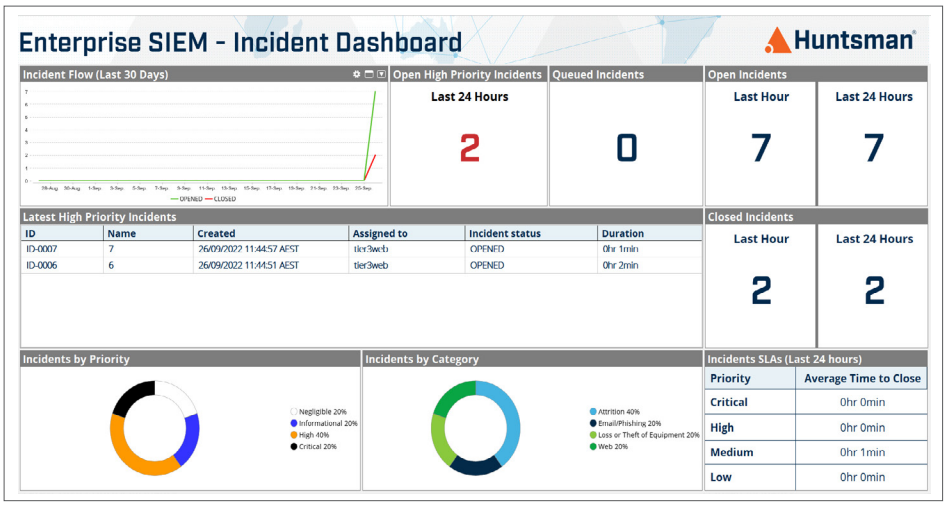


Huntsman SIEM multi-network segregation

Standard Features & Functionality

Huntsman SIEM provides an extensive array of features and functionality out of the box. Organisations can quickly achieve a strong baseline in Protective Monitoring and then easily supplement this with bespoke requirements and use cases.

- Over 1,000 security and compliance queries and reports, plus associated dashboards.
- Support for hundreds of devices, applications, and log sources.
- Agent and agentless collection.
- Real-time audit collection, normalisation, analysis and alerting.
- Full alert handling and integrated incident manager.
- Automated response capability.
- Granular role-based access controls.



Easy to use interface for Threat Hunting with interactive drill-down for forensic analysis

No custom query language required

Advanced SIEM Features

Huntsman SIEM also includes advanced functionality that enables organisations to detect sophisticated attacks including insider threats, malicious nation-state activity, and targeted attacks. These have been specifically developed to support Defence and Government users.

MACHINE LEARNING monitors activity within the environment to detect abnormal behaviour by users or devices, such as inappropriate access to data, unusual communications between endpoints, and malware infections.

DYNAMIC DETECTION of important assets allows the automatic identification of sensitive systems and applications and adapts analysis rules to the changing environment without requiring manual configuration.

CONTEXT-BASED ANALYTICS using powerful **hierarchical Virtual Groups** enables asset, application, and user information to be included within analysis rules, and relevant alert priorities to be set based upon business value, criticality and context.

THREAT INTELLIGENCE in conjunction with contextual analytics, allows the detection of malicious events and activity based upon external, internal and bespoke information. Using Indicators of Compromise or user context, Huntsman SIEM alerts on unusual user actions or known malicious software, communications and endpoint behaviour.

NON-SEQUENTIAL EVENT HANDLING allows processing and analysis of data even when events are received out of sequence or are delayed so no alerts are missed.

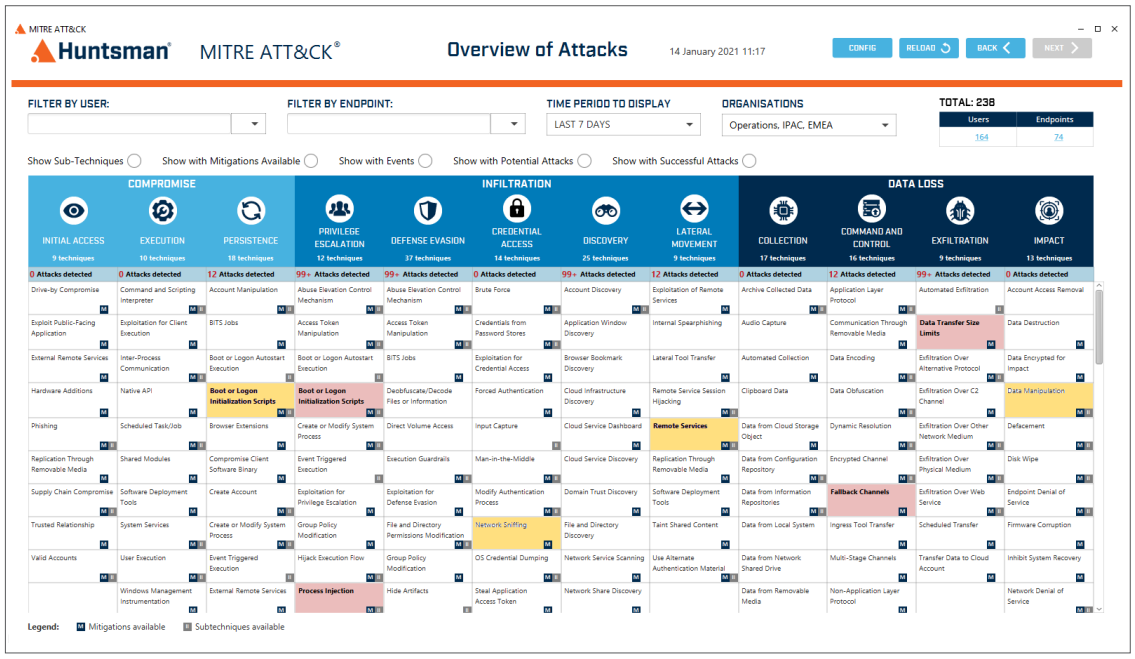
Huntsman®
Defence-Grade Cyber Security

MITRE ATT&CK®

Huntsman SIEM includes a MITRE ATT&CK® heatmap that shows events and alerts associated with their corresponding Techniques and provides analysts with a direct view of incidents.

Filtering of users, endpoints and networks allows the most important issues to be quickly focussed on to guide investigation and response efforts.

The built-in knowledgebase of MITRE's mitigations also enables analysts to review and implement strategies that limit and prevent attacks.



All Huntsman UK Government customers have achieved accreditation

Want to find out more?

Explore the FAQs >

Talk to an expert >

Huntsman®
Defence-Grade Cyber Security