Huntsman®
Defence-Grade Cyber Security

Huntsman SIEM

Deployment & Support FAQs

Experienced security architects and SOC professionals know that selecting a SIEM solution that satisfies in both the short and long term, involves much more than just the technical capabilities. Based on Huntsman Security's years of experience, here are some of the questions that repeatedly surface especially if the evaluating team has "been there before".

Licencing

How is the solution licensed?

Huntsman SIEM is licensed by events per second (EPS). Agents, high availability, multi-database support and incident management are all included within the licence.

What happens if the system is flooded with events and exceeds its licencing threshold?

By design, the software will continue to collect and analyse events and does not restrict access to data or functionality, even if the license threshold is exceeded. Huntsman SIEM uses 'store and forward' technology to ensure events continue to be collected and processed even during periods of high demand.

With distributed agent processing and in-stream analytics on the Huntsman SIEM platform, throughputs in excess of 130,000 EPS can be achieved using standard off the shelf hardware.

Deployment

What platforms and databases are supported?

The Huntsman server can be installed on Windows or Linux operating systems and supports Microsoft SQL Server and PostgreSQL database platforms. Agents can be installed on Windows, Linux and Solaris operating systems, and support the collection of data from any local or remote sources.

Can Huntsman SIEM be hosted in the Cloud?

Yes, Huntsman SIEM fully supports deployment within Cloud environments including AWS, Azure and Google Cloud Platforms.

Can we increase the size of the deployment as our network grows?

Yes, Huntsman SIEM's flexible architecture easily allows for the addition of new sources and network segments. The solution is easily scaled to meet the demands of an increase in the scope of protective monitoring whether that is simply an increase in the EPS, the number of devices being collected from, or the duration that data needs to be retained online.

What makes the deployment of a Huntsman SIEM faster than other solutions?

Unlike other SIEM solutions that simply provide a framework to build queries, reports, or dashboards, Huntsman SIEM **includes content out-of-the-box** that enables analysts and organisations to monitor, detect and report upon security issues from day one.

Huntsman SIEM ships with hundreds of alert and analysis rules, over 1,000 queries and reports, and dashboards showing operational, security and compliance data and alerts. This removes approximately 80% of the initial set-up and configuration time and customers find that they can perform baseline protective monitoring within a day.

Operation

What skills are required to operate Huntsman SIEM?

Huntsman SIEM has an intuitive interface that means operators do not have to be highly skilled in order to use the solution. Right-click drill-down options, selection list filtering, and menu based actions allow analysts to quickly perform investigations and root cause analysis. Huntsman SIEM does **not** use a proprietary query language and so analysts do not need to know what they are looking for before searching for it (no data scientists needed).

What skills are required to maintain Huntsman SIEM?

Huntsman SIEM includes automated database and systems maintenance tasks that mean very little intervention is required by systems operators or administrators. Huntsman customers report that the Total Cost of Ownership of the solution is negligible compared with alternative SIEMs.

What training do you provide?

Huntsman Security provides a 2-day training course for users that covers activities including threat hunting, incident management, reporting, and alert management. A 3-day Certified Administrator course provides system administrators with the skills necessary to manage, maintain and configure Huntsman SIEM to add new users, agents, event sources and detection rules.

Are Professional Services required to configure the solution?

No. Whilst some SIEMs are complex and require additional professional services in order to configure them, Huntsman SIEM is designed so that in-house analysts and IT staff can easily configure the solution as this is often a requirement of sensitive customers and Government organisations. However, engineering services are available to help with complex sources or where customers are short of security resources.

Support

Do you provide UK based support?

Yes, all customers have direct access to a UK support team, staffed by highly experienced security cleared engineers, which means 95% of support requests are resolved by the first point of contact. Engineers also have access to secured email services that permit the transfer of material up to Official-Sensitive to enable better support of our customers.

Support services are accessed via a dedicated email address and phone number and also include an annual health check.

User groups are held annually and regular newsletters are issued to customers around a range of pertinent security topics, new product releases and general information.

Do you have security cleared staff?

Yes, Huntsman Engineers in the UK are security cleared to either SC or DV allowing us to support customers with the highest security requirements.

How often do you release software enhancements?

A major software release occurs approximately every nine months with smaller updates released in the intervening months.

What if we want a product enhancement?

Customers have access to a named Technical Account Manager (TAM) who conducts account reviews on a regular basis and can handle requests for new product features.

General

Do you restrict the availability of the solution?

Yes. Whilst other solutions are sold all over the world Huntsman software is limited to the Five Eyes Alliance and those countries aligned to it.

Is GPG13 still relevant?

Although GPG13 is no longer used as a specific requirement it continues to be referenced and adopted by UK Government and other organisations as it provides an excellent template for rolling out protective monitoring. Huntsman Security continues to fully support GPG13 requirements through out-of-the-box dashboards, queries, analysis rules and reports.

All Huntsman customers who have deployed Huntsman SIEM and sought accreditation against GPG13, have achieved it.

Want to find out more?
Contact us to talk to one of our team today

t: 0845 222 2010 e: ukinfo@huntsmansecurity.com

Huntsman®