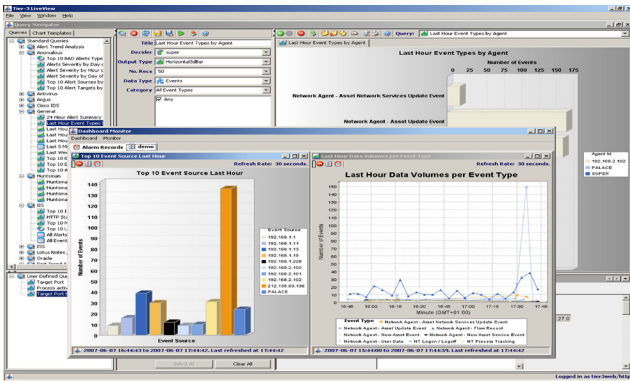


« Behavioural analysis

Huntsman 5.1



Supplier	Tier-3
Price	\$POA
Contact	www.tier-3.com

As security threats to networks become ever more sophisticated, there is a drive towards a more proactive stance and a demand for solutions that can identify unknown as well as known threats. Aimed firmly at the enterprise, Huntsman from Australian company Tier-3 is designed to provide these features and more, including risk management and compliance tools.

Tier-3's patented BAD (behavioural anomaly detection) engine keeps a close eye on the network in real-time and looks out for unusual behaviour. It identifies a multitude of threats, from distributed denial-of-service attacks to worms, while watching out for insider activity. The latter is a critical requirement for regulatory compliance as most security threats now issue from inside the network perimeter.

The Huntsman decision engine runs on a central system and provides functions such as data collection, reporting and threat analysis. It applies four stages of analysis to each event, including a correlation engine for user-defined patterns, a risk assessment and the application of the BAD engine. It requires an existing Oracle or SQL server database to store data. We had no problem getting Huntsman to work with SQL Server 2005.

The decision engine uses a guardian to carry out requests and actions defined in security policies. Next up is the universal data source monitor (UDSM), which provides data collection facilities. Its graphical interface allows it to be customised extensively and can function as a syslog server listener and supports a wide range of data sources, including TCP ports and databases.

The network agent monitors system activity and network traffic and, on Windows systems, runs as a service with administrative privileges. Agents can be used as network probes to collect traffic information, but you must install them locally on all systems if you want to gather detailed information about them. Huntsman can then record all user activities, for example file creation and deletion, applications run, websites visited and files downloaded. Huntsman offers a real-time forensics monitoring service. In comparison, products such as Guidance Software's EnCase (see SC June) are forensics investigators that analyse systems at a much lower level and can reconstruct deleted data on a user's hard disk.

Huntsman needs to baseline your network before it can get a feel for how things interact and what is acceptable activity. Systems with agents installed are also baselined and the information is used to determine client behaviour. These are all predefined activities,

but you can add custom policies that Huntsman will enforce. All communications between agents and the decision engine are encrypted by default to 128-bit AES standards, although you can request other schemes.

The action centres around the Huntsman LiveView console, which opens with the query navigator. You can run queries on any information the software can collect. Select a query, hit the play button and the output display will be updated with new information as it comes in. You can create custom queries, by choosing from events and alerts, select a category, apply filters and decide which columns you want displayed.

The depth of information on offer is equally impressive. Any events that require further investigation can be selected from the display and passed directly to the incident viewer, where you create a new incident and assign it to a Huntsman user. A case history is maintained where events and alerts associated with the incident are viewed, user comments added and, on closure, a reason can be provided for the status change.

The Huntsman configuration window serves to manage users, alerts and agents and enable the Guardian component. Guardian commands tie actions to any selected Huntsman event. Actions are script-based and can be applied to specific agents. We had no problems linking scripts with specific Guardians and liked that you can run the script to check that it works before going live.

The dashboard monitor provides an at-a-glance status of monitored items. A secure audit is kept of all



Reprints

activities that can be subjected to filters. At this price, you should expect topnotch reporting and Huntsman doesn't disappoint. All available query information can be turned into one-off or scheduled reports and exported to a wide range of formats.

Huntsman isn't something you deploy in a day. It will take a while to understand all of its intricacies. Once tailored to its environment, it is capable of providing a complete network security umbrella and can respond swiftly to known and unknown threats.

Dave Mitchell

SC MAGAZINE RATING	
Features	★★★★★
Performance	★★★★☆
Ease of use	★★★★☆
Documentation	★★★☆☆
Support	★★★★☆
Value for money	★★★☆☆
OVERALL RATING	★★★★☆

For Real-time monitoring of network and user activity, proactive responses to threats, licence based on CPU sockets, can be customised

Against A high starting price and a steep learning curve

Verdict A versatile enterprise-level network security solution that provides sophisticated real-time monitoring and that all-important first line of defence against zero-day attacks

Contact details:

HUNTSMAN

Tier-3 UK: +44 (0) 20 7664 7950
 Tier-3 Australia: +61 (0) 2 9419 3200
 Email: info@tier-3.com
 Website: www.tier-3.com