

Modern attacks are specifically designed to **evade detection** by even the tightest security solutions.....

...how can you be sure you are not one of them?



Evidence is beginning to emerge which suggests that targeted attacks against individual organisation's are becoming commonplace.

How strong is your ICT security?

Conventional ICT security applications have their place in the protection system, but experience shows that few ICT managers are enhancing their security systems with a multi-faceted security application - one which oversees and controls existing security systems and which identifies suspicious activity as it occurs.

Research has shown that ICT managers are looking for a holistic approach to ICT security which draws together multiple defence technologies, using them as a resilient and coordinated defence to minimize their security exposure. Protection involves harnessing and integrating disparate security technologies to create an easily managed heterogeneous environment capable of safeguarding their enterprise and ICT assets,

It also needs to provide

- An accurate, integrated enterprise wide view of ICT assets and their usage
- Protection of customers' data and corporate Intellectual Property
- Analysis of existing legacy applications as well as new and emerging technologies
- Compliance analysis and reporting
- Alignment of ICT security and Operational needs of the business

What if:

- there was a way to collate, analyse and proactively manage abnormal behaviour across your enterprise environment, from one central control dashboard ?

Introducing:

Huntsman: Real-time Protection

Intelligence-lead, policy-driven, Huntsman enables you to protect yourself from regulatory and financial damage that can result from undetected security breaches. Huntsman monitors for all forms of unusual and unacceptable activity, and provides comprehensive operational risk and compliance analysis.

Reduce the cost of security incidents

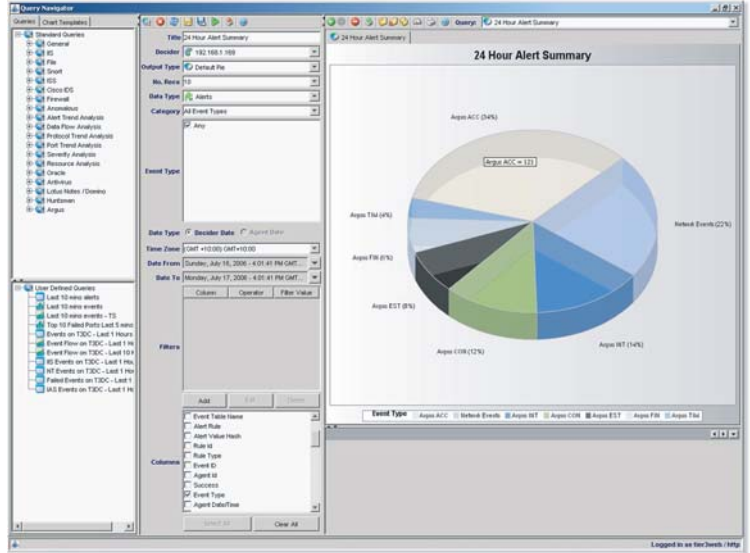
One of the greatest costs resulting from a security incident to an organisation is those associated with the cleanup and restoration of business services. The Huntsman *Guardian* when coupled with the analysis capabilities of the behavioural anomaly detection and correlation engines enables the efficient execution of preventative and remedial responses.

Future proof

Our patented heuristic behavioural-learning engine is not constrained by the need for fixed rules and constant updates. Any events in the enterprise that are unfamiliar are automatically assessed against your defined risk profile. Even the latest unknown threats or exploits designed to bypass existing security measures and target your enterprise can be detected using Huntsman.

Any platform, any application, any data source

Integrated threat management demands simple connectivity to network, server and application data sources. Huntsman has an easy to use "universal connector" that solves the problem of connection, management and control of diverse technologies to secure the enterprise from network to application



Integrate with systems management tools

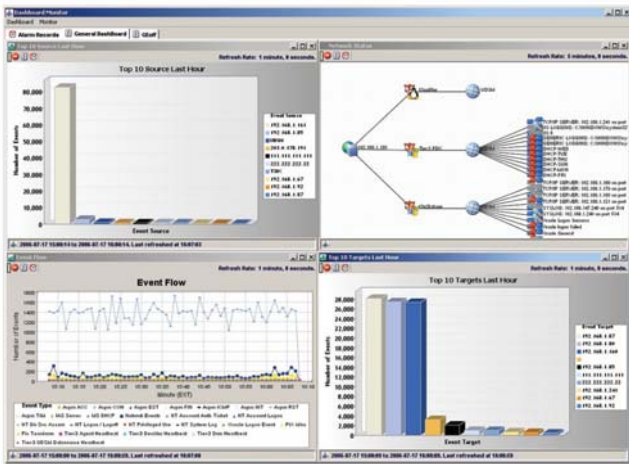
Centralised information drives collaboration between the Network Operations Centre staff and Security Operations Centre staff; bridging the NOC/SOC chasm and ensuring communication is shared, not isolated.

Interactive dashboard, centralised control

Develop a full audit trail, forensic event reconstruction, threshold monitoring, alerts and reporting. Create event drill-down with a full central dashboard providing a single point of access for systems monitoring and administration services.

Security and encryption

All components of the Huntsman system support industry standard encryption and authentication technologies and can be configured to support the highest levels of security. This ensures all data transported across the Huntsman framework remains secure.



Why Huntsman?

Multi Layered Anomaly Detection

The Huntsman Behavioural anomaly detection engine actively protects your network infrastructure ensuring business operation and availability as well as protecting against data theft from business applications such as databases, financial systems, intranets and more. Traditional rule or signature based systems by definition are only capable of detecting threats they have been programmed to identify. Whilst effective against known threats they offer little or no protection against the increasing danger of unknown threats.

The answer lies in being able to collect and manage events from across the enterprise, and then prioritise for remediation those which present an unacceptable or unfamiliar level of risk to stakeholders.

HUNTSMAN

Huntsman manages risks that threaten IT asset confidentiality, integrity and availability. Huntsman protects shareholder confidence, brand value and the bottom line.

To learn more about Huntsman's unique security protection, please contact www.tier-3.com