Solution Brief

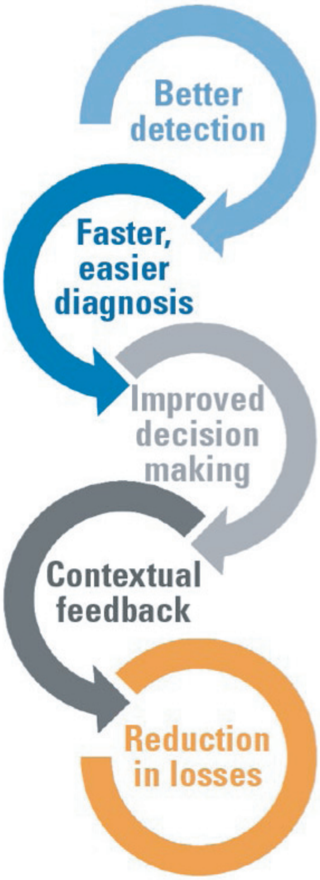
Threat Intelligence

How Huntsman Security leverages Threat Intelligence

Huntsman®

Defence-Grade Cyber Security

How to leverage Threat Intelligence using Huntsman Security's Next Gen SIEM



Performing contextual analysis, accessing multiple intelligence sources, drawing on inside knowledge and more.

What is 'Threat Intelligence'?

According to Gartner, Threat Intelligence is 'evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard'.

In simple terms, Threat Intelligence helps you interpret security events in the context of normal activity inside and outside of the enterprise. By looking for attack patterns identified via threat intelligence in your security monitoring/ analytics function, you can shorten the window between compromise and when you detect that compromise.

In 2014, Gartner coined the term Intelligence-aware Security Controls (IASC), and cited SIEM products as a core component to consolidate Machine Readable Threat intelligence (MRTI). Huntsman Security's Next Gen SIEM supports MRTI out-of-the-box, so its Threat Intelligence database can automatically update from available sources.

How can Threat Intelligence help?

This Solution Brief shows how to analyse Threat Intelligence gathered from a variety of sources to gain clearer insights into the current threat environment, using Huntsman Security's Next Gen SIEM.

An example of Threat Intelligence is the ability to detect a user accessing a permitted website, which has been compromised and is now distributing 'drive-by' malware downloads. A Threat Intelligence capability can flag compromised sites as soon as they're reported, and update Threat Intelligence data in real-time or on a regular schedule. Analysts can then configure an alert to detect attempts by users or a proxy to access the compromised web page. The alert can also trigger an action to capture data from the source system for subsequent analysis. In addition, analysts can block the traffic or quarantine the system.

Threat Intelligence needs to be deployed with care to ensure meaningful results. For instance, if threat intelligence draws only from a vendor's own customer deployments, the utility and value of such intelligence will be limited.

Choose your Threat Intelligence sources

Sources of Threat Intelligence may be internal and external, commercial (proprietary) or open source. External sources include security products and network appliance vendors, security associations and communities, MSSPs and cyber security consultancies. It's best to use intelligence from a number of sources, but it pays to limit them to those most pertinent to your business or industry.

Internal Sources	External Sources
Internal Threat Intelligence	**External Threat Intelligence**
• Sensitive systems/servers/networks • Departments/systems that hold IPR • Personal data systems (e.g. customer databases) • Web/externally accessible platforms • Admin/Privileged/Development users • Sensitive user lists (senior execs, R&D teams, Corp finance/M&A teams) • Status databases (staff locations, travel details, holiday booking systems) • Integration with physical systems (in/out building, which location) • Mappings of IP addresses to office locations	• Compromised web sites/URLs • Botnet memberships/spam sources • Known phishing senders • Phishing/attack emails subjects • Mappings between IP addresses and locations (Countries/Cities) • Countries/Locations/Network likely to originate attacks • Physical locations (risk of breaking/ compromise)
Contextual Threat Intelligence	**Community Threat Intelligence**
• Internal users who are under investigation • Servers/systems that are the subject of current incidents • External sources linked to incidents • Historical information and statistical/ correlated data over time • Time (local to target and source) • Numbers of things that have occurred • Input from other system management systems • Vulnerability information	• Patterns of attack on one customer system or silo which can be monitored for re-occurrence on others • Inter-customer or inter-silo information flows, traffic or connections • Known system vulnerabilities and in-the-wild exploits

Why context is critical

Additional context around events affords your security team deeper insights. Next Gen SIEM's 'Enhanced Threat Context' capability provides this, by monitoring Threat Intelligence repositories to build its own profile of event patterns and their relevance. By comparing these with a set of known, documented, recorded or anticipatable threats, our Next Gen SIEM can raise a contextual alert to enable early investigation of potential threats in real-time, rather than some period after the event.

The technology's ability to build a broader 'Enhanced Threat Context' leverages its other capability Behaviour Anomaly Detection (BAD). An example of the way BAD can add vital context is by detecting a sudden surge in traffic to an external IP address.

As soon as BAD alerts security staff to the abnormal behaviour, they can use Threat Intelligence to identify the destination IP address and pinpoint its city/country location. The analysts now have much more information to work with in evaluating the seriousness of the incident.

How to 'Shorten the Window'

Huntsman Security Next Gen SIEM's Threat Intelligence and Enhanced Contextual Analysis capabilities raise the effectiveness and responsiveness of your security team in a number of crucial areas:

- Faster and more accurate detection of security incidents. Working in real-time, our Next Gen SIEM enables faster and more accurate decisions about the significance of events, discrete alerts, correlated alerts spanning multiple events, contextual alerts derived from time/situation/system status, and deviations from normal behaviour.
- Faster diagnosis and less time wasted. By presenting analysts with fewer alerts that have been triaged by context and risk, and more accurate alerts due to reduced false positives and background 'noise', our Next Gen SIEM lets the security team focus on the serious threats.
- Faster decision-making with more context and more relevant detail. By providing the status of affected systems and their users, and up-to-date threat intelligence; analysts don't have to spend time piecing together intelligence from multiple repositories.
- Faster response to incidents by creating useful feedback loops from internal systems or controls that provide real-time and localised 'threat context'. This helps security staff detect and stop the spread of attacks and 'kill chains' as they occur, rather than following a 'cold trail' during a post mortem long after the event.
- Prevention of loss or damage due to early detection, investigation and resolution. With better threat intelligence, rogue users can be intercepted, information flows can be halted and personal data or IP can be secured before it is compromised, threatened or lost.

In short, Huntsman Security's Next Gen SIEM enables your security team to make faster decisions, to reduce the time and cost to investigate and resolve incidents, and to reduce the scale and cost of breaches should they occur.

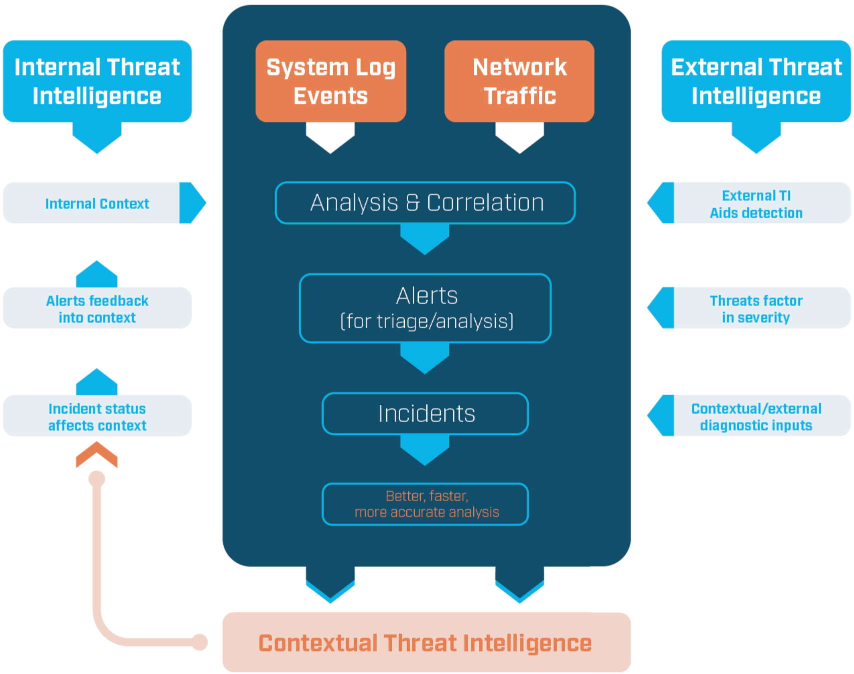

Internal Threat Intelligence
System Log Events
Network Traffic
External Threat Intelligence
Internal Context
Analysis & Correlation
External TI Aids detection
Alerts feedback into context
Alerts (for triage/analysis)
Threats factor in severity
Incident status affects context
Incidents
Contextual/external diagnostic inputs
Better, faster, more accurate analysis
Contextual Threat Intelligence

Figure 1: How Huntsman Security's Next Gen SIEM leverages Threat Intelligence

Why choose Huntsman Security for Threat Intelligence

1. Far more than SIEM

Huntsman Security's Nex Gen SIEM is a flexible, modular and highly scalable Security Risk Platform that delivers:

- Next generation SIEM capability;
- Rapid, real-time 'in-stream' data ingestion, not post-storage database monitoring;
- Full event correlation and Behavioural Anomaly Detection; and
- Scalable distributed database for immediate access to long term, high volume data sets across multiple repositories, for resilience, load sharing and archiving.

2. Specific Threat Intelligence capabilities

Huntsman Security's Next Gen SIEM supports these advanced capabilities with specific Threat Intelligence that allows:

- Groups of systems to be defined based on role, risk or context;
- Data pertaining to these groups to be collated in a concerted way;
- Creation and incorporation of internal and external Threat Intelligence resources;
- Specific rules to be applied to higher risk networks, sites, systems or business units;
- Definition of communities to highlight sets of systems with common technologies, roles or risk profiles based on organisational, technical or contextual factors such as: role, type, platforms, location, sensitivity or security status;
- The creation of interfaces to internal contextual systems, for example, the physical tracking of users entering or exiting a building.

3. Advanced automation to aid investigation

In addition, the technology can trigger pre-defined actions that allow the automatic look-up of information immediately an alert is generated. This can be configured to allow:

- Retrieval of information based on alert fields or cross-reference in local databases;
- Enrichment of log data at the point of alert detection;
- Gathering of incident data based on the user, system or network connection;
- Event/alert streams to be fed into other solutions as inputs for ticketing, system management or escalation;
- Watch lists to be defined to track the frequency of defined events on specific systems or groups of users to logically group data for easy analysis or reporting;
- Exchange of alert data between instances - or to/from support and ticketing systems, or to/from network or systems management solutions.

Huntsman Security's Next Gen SIEM helps analysts investigate complex scenarios, for example, for systems or users that are suspected of being the subject, target or origin of an attack. Analysts can easily determine what else is happening on a system under investigation and whether, or not, an incident is contained or spreading.

With the relevant usernames, hostnames and IP addresses defined within the next generation SIEM specific triggers can be set to raise high severity alerts for any suspicious activities that relate to those systems or users.

4. Much more than integration

Our Next Gen SIEM integrates with third party intelligence solutions, including technologies like:

- Deep Packet Inspection;
- Data Mining;
- Predictive Analytics;
- Event Visualisation;
- Vulnerability Scanning; and
- Policy Compliance Monitoring.

It also analyses and interprets the intelligence of third-party solutions by alerting on anomalies and returning specific alerts to those specialist solutions for amended vigilance, policy or specific filtering.

Summing up

Threat Intelligence is critical for effective cyber security, especially in the current landscape of increasingly diverse and stealthy threats. The wide-spread use of cloud services, smart mobile devices and the BYOD trend pose even more challenges for security analysts who are in short supply, and for their teams who are being asked to deliver more with less.

The Huntsman Security Next Gen SIEM can assist your security teams to:

- Increase the speed of their detection and diagnosis;
- Ensure that relevant information is available to investigators, immediately;
- Inspect threat repositories to improve their risk perception;
- Detect, diagnose and make informed decisions more quickly and accurately;
- Reduce losses or the costs due to incidents through a better understanding of the nature of an incident and when it occurs.

In addition, our Next Gen SIEM supports machine-readable Threat Intelligence, and 'learns' automatically as that intelligence updates the system. This provides a comprehensive and dynamic threat update loop for a rapid and continuously informed decision-making process. With its ability to collect and contextualiseThreat Intelligence from internal, external, contextual and community sources, the technology provides your security team with unparalleled speed and accuracy of detection, diagnosis and decision-making. All of which are vital for rapid response and threat mitigation.

About Huntsman Security

Huntsman Security is the trading name of Tier-3 Pty Ltd. The technology's heritage lies in delivering a key foundation stone of the cyber security risk management, monitoring and response capability in some of the most secure and sensitive environments within the intelligence, defence and criminal justice networks across the world, where Huntsman Security solutions are deployed and accredited to the highest security levels.

Huntsman®

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

7-10 Adam Street, Strand
London WC2N 6AA

NORTH ASIA

t: +81 3 5953 8430

e: info@huntsmansecurity.com

Awajicho Ekimae Building 5F
1-2-7 Kanda Sudacho
Chiyodaku, Tokyo 101-0041

huntsmansecurity.com linkedin.com/company/tier-3-pty-ltd