Threat Intelligence
Using Huntsman®
OVERVIEW

Huntsman®
Defence-Grade Security Platform

Threat Intelligence using Huntsman.

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

In simple terms, Threat Intelligence helps organisations interpret security events in the context of normal activity inside and outside of the enterprise. Securosis describes the key advantage this way: '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.'

HOW CAN THREAT INTELLIGENCE HELP?

As an example, Threat Intelligence can flag compromised sites and malicious network addresses as soon as they are reported. Analysts can then configure alerts to detect attempts by users or a proxy to access the compromised page or to detect traffic to known risky locations. Alerts can also trigger actions to capture data from the source system or network for subsequent analysis. In addition, analysts can block the traffic or quarantine the system.

CHOOSE YOUR THREAT INTELLIGENCE SOURCES

Threat Intelligence may be internal and external, commercial (proprietary) or open source. It is best to use threat intelligence feeds from a number of sources, but it pays to limit them to those most pertinent to your business or industry.

Internal Threat Intelligence

- Sensitive systems/servers/networks
- Web/externally accessible platforms
- Admin/Privileged/Development users
- Sensitive user lists
- Integration with physical systems

External Threat Intelligence

- Compromised web sites/URLs
- Botnet memberships/spam sources
- Known phishing senders
- Mappings between IP addresses and locations

Contextual Threat Intelligence

- Systems that are the subject of current incidents
- External sources linked to incidents
- Input from other system management systems
- Vulnerability information

Community Threat Intelligence

- Patterns of attack on one system which then reoccurs on others
- Inter-customer or inter-silo information flows, traffic or connections

© 2014 Tier-3 Pty Ltd, All rights reserved

WHY CONTEXT IS CRITICAL

Additional context around events affords your security team deeper insights. Huntsman's 'Enhanced Threat Context' capability provides this, by monitoring Threat Intelligence repositories to build its own profile of event patterns, indicators of compromise and their relevance.

Huntsman's patented Behaviour Anomaly Detection (BAD) can add vital insight by detecting a sudden surge in traffic to an external IP address. Analysts can then use Threat Intelligence to identify the destination IP address and pinpoint its city/country location with Huntsman.

HOW TO 'SHORTEN THE WINDOW'

Huntsman'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.
- Faster Diagnosis and less time wasted.
- Faster decision-making with more context.
- Better view of endpoint security.
- Faster response.
- Prevention of loss or damage.
- IT Security Intelligence.

In short, Huntsman 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.

WHY CHOOSE HUNTSMAN FOR THREAT INTELLIGENCE

1. Far more than SIEM - Huntsman is a flexible, modular and highly scalable Security Risk Platform.
2. Specific Threat Intelligence capabilities - Huntsman supports advanced SIEM capabilities with specific Threat Intelligence.
3. Advanced Automation to aid investigation - Huntsman can trigger pre-defined actions that allow the automatic look-up of information immediately an alert is generated.
4. Much more than integration - Huntsman not only integrates with many third party intelligence solutions but also analyses and interprets their intelligence.

Huntsman's enterprise cyber security solution 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.

Huntsman 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.

© 2014 Tier-3 Pty Ltd, All rights reserved

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

100 Pall Mall, St James
London SW1Y 5NQ

North Asia

t: +81 3 5809 3188
e: info@huntsmansecurity.com

TUC Bldg. 7F, 2-16-5 Iwamoto-cho,
Chiyoda-ku, Tokyo 101-0032

Americas

toll free: 1-415-655-6807
e: usinfo@huntsmansecurity.com

Suite 400, 71 Stevenson Street
San Francisco California 94105

huntsmansecurity.com

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

twitter.com/Tier3huntsman

© 2014. All rights reserved. Huntsman is a registered Trademark of Tier-3 Pty Ltd Tier-3 Pty Ltd