Huntsman

B.A.D.™

Behaviour Anomaly Detection

Huntsman®

Defence-Grade Security Platform

Huntsman® real-time Behaviour Anomaly Detection (BAD) technology includes the most advanced event stream processing engine available today.

The Huntsman® BAD engine uses patented machine-based learning techniques to deliver true behaviour-based profiling and detection, and is proven to detect threats that are not detected by standard rules and signatures.

Huntsman® enables your analysts to pinpoint and investigate real-time cyber-security attacks designed to circumvent traditional security controls, such as:

- Advanced Persistent Threats (APTs)
- Smart, customized and targeted malware
- Malicious or negligent insiders who abuse their access to put data or IP at risk
- Compliance breaches that require complex interrelated rule sets to be detected
- 'Unknown' and 'unknowable' external and internal threats that simply can't be second-guessed by analysts

Huntsman Behavioural Anomaly Detection is an add-on for the Huntsman Enterprise SIEM (including the Cloud and MSSP editions) and Unified Console.

FEATURES

- Passively establishes a dynamic baseline by automatically self-learning normal system behaviour to determine, by exception, unusual system activity and other indicators of compromise
- BAD techniques easily anticipate threats that can be quickly bounded to reveal malicious events more efficiently than by the continuous creation of rules to pinpoint a threat
- Adapts to authorised network changes, gradual trends, usage spikes and work patterns while still automatically distinguishing suspicious and risky outliers from normal events
- Connects seemingly unrelated events from multiple information silos across an enterprise to quickly determine any hidden or unexpected relationships between the data from disparate sources that might represent a threat or indicator of compromise
- Provides visual analysis so that metrics, key information and sensitivities can be tailored to meet precise profiling requirements

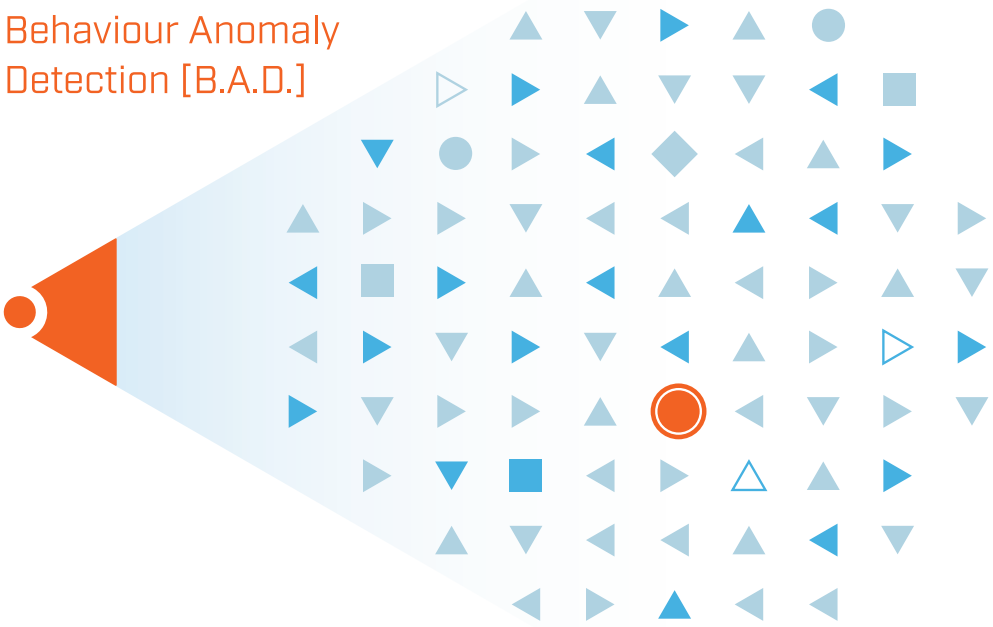
REAL-TIME THREAT DETECTION

Huntsman collects and processes data in real time – so all received events, activity and log data pass through its correlation and analytic engines "in stream", rather than being stored and/or indexed in a database for historical or periodic analysis.

This means real-time alerts are generated and directly despatched to operators, updating dashboard displays and triggering notifications so threats can be contained or averted and data losses can be stemmed.

Huntsman

Behaviour Anomaly Detection [B.A.D.]



THE ADVANTAGES OF 'TRUE' BEHAVIOUR ANOMALY DETECTION (BAD)

Huntsman's patented BAD technology establishes a dynamic, multi-dimensional baseline of normal user, system and network behaviour across the organisation.

It continuously monitors for activity that deviates from these learned patterns for early warnings of malicious intent.

After detecting these deviations, Huntsman immediately verifies them and alerts IT staff of abnormal activity.

Consequently, Huntsman eliminates the continuous job of writing new rules, alerts and scripts – a major advantage for any organisation.

BENEFITS

- Immediate visibility of anomalous situations within network, operating system and, uniquely, application layers
- Correlation of known threat intelligence and assets with behavioural data
- Autonomous BAD extends the detection of threats beyond the limits of pattern and signature-based security controls, to what you don't or can't know
- Ease of operation, reduces operational risk to limit uncertainty and operator error
- Integration with rules-based security solutions complement the analysis and insight into known and unknown threats

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