



Product Brochure

**B.A.D.**™

Behaviour Anomaly Detection

 **Huntsman**®  
Defence-Grade Cyber Security

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

“Huntsman® enables your analysts to pinpoint and investigate real-time cyber-security attack”

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 integral part of the Huntsman Enterprise SIEM (including the Cloud and MSSP editions).

### FEATURES

- Unique and powerful solution for automated real-time monitoring, investigation and resolution of enterprise security threats
- Automated collection and analysis of the relevant threat information necessary to resolve immediately verified threats and dismiss false positives
- Automated workflow to streamline the investigation process and quickly and accurately identify compromised IT assets resulting from an attack
- Integration with major cybersecurity solutions to identify, prove and resolve malware and unknowable threats

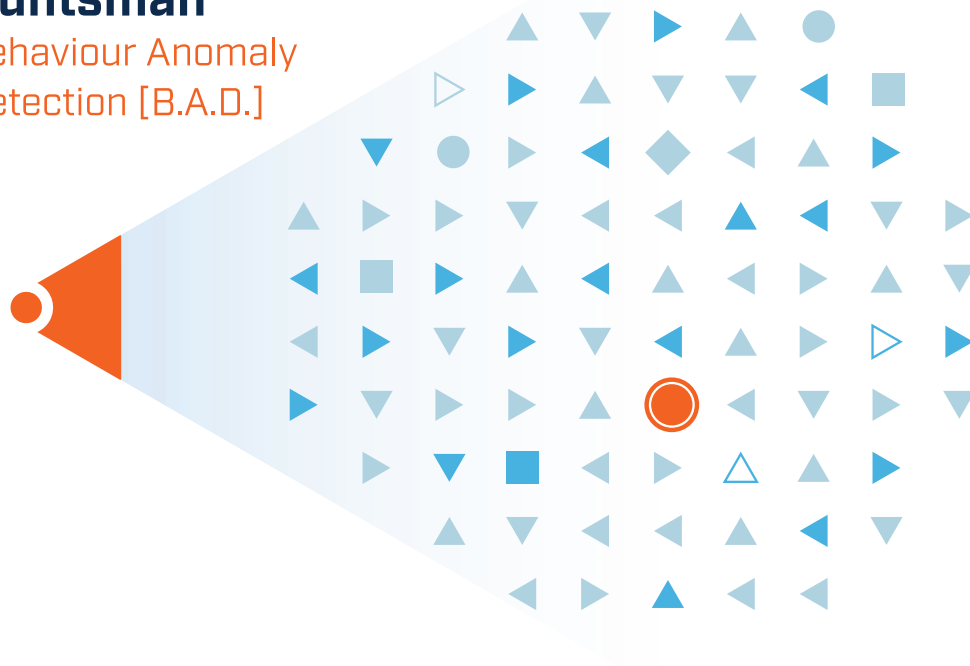
### ▶ Real-time threat detection

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](mailto:info@huntsmansecurity.com)

Level 2, 11 Help Street  
Chatswood NSW 2067

**EMEA**

t: **+44 845 222 2010**

e: [ukinfo@huntsmansecurity.com](mailto:ukinfo@huntsmansecurity.com)

7-10 Adam Street, Strand  
London WC2N 6AA

**NORTH ASIA**

t: **+81 3 5953 8430**

e: [info@huntsmansecurity.com](mailto:info@huntsmansecurity.com)

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

**AMERICAS**

toll free: **1-415-655-6807**

e: [usinfo@huntsmansecurity.com](mailto:usinfo@huntsmansecurity.com)

Suite 400, 71 Stevenson Street  
San Francisco California 94105



[huntsmansecurity.com](https://huntsmansecurity.com)



[linkedin.com/company/tier-3-pty-ltd](https://linkedin.com/company/tier-3-pty-ltd)



[twitter.com/Tier3huntsman](https://twitter.com/Tier3huntsman)