Huntsman
ANALYST PORTAL™

Threat detection to resolution in seconds.

Huntsman®
Defence-Grade Security Platform

THE CHALLENGE

Shortening the processing time from incident detection to resolution is one of the top priorities of any enterprise security team. Industry surveys, as well as breaches publicised in the media, highlight the importance of reducing the times from threat detection to resolution from months to days and even hours. This shortening of the risk window for any organisation is dependent upon faster more accurate threat detection and resolution.

The **Analyst Portal™** solves this problem by automating incident triage and investigation processes to enable threat verification and resolution in seconds. No more false positives to blunt your security efforts and delay your response to the threats that matter.

NEW THREAT ANALYSIS TECHNOLOGY

This unique technology will fundamentally change workflow efficiencies within your SOC operations.

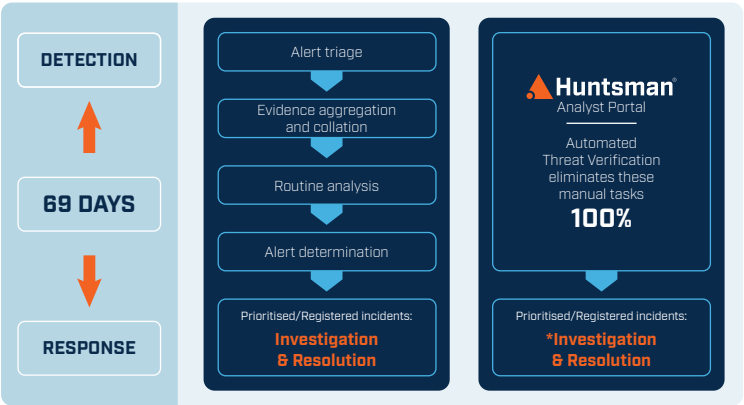
The **Huntsman Analyst Portal™** aggregates threat information from a range of sources including advanced cyber-security detection solutions, malware sandbox technologies, network infrastructure and end-points to give maximum context to an incident. Triage and investigation is significantly faster and more accurate.

This means highly focused threat verification and resolution. It also means that security teams can focus on the critical threats that matter rather than waste valuable time on those that don't. By automatically distinguishing a real alarm from all the noise the Analyst Portal brings significant workflow efficiencies for analyst investigation and incident resolution.

INTERPRETING DATA FROM SPECIALIST APPLICATIONS AND THE ATTACK TARGETS

Analyst Portal™ extracts the malware and attack information from detection technologies, specialist security solutions as well as comprehensive information from its host environment.

Analyst Portal™ automatically and in real time examines affected or suspected end points to determine where an attack is active, what the likely implications are, what host and network activities are occurring, and what other assets might be at risk.



***Analyst Portal**
Automated presentation of case files for all prioritised incidents. (drawn from end-to-end intelligence)

SPEED IS CRUCIAL

To shorten the time at risk, it is essential that threat information and evidence is captured in real-time and processed at high speed. The **Analyst Portal™** immediately gathers relevant data so analysts are not distracted by routine analysis activities. This enables the prompt resolution of benign threats and false positives so that incident investigation progress through the "alert queue" is more than 10 times faster than existing incident response techniques.

As a result, security analysts are provided with highly accurate information and can immediately resolve the real threats and putting the enterprise at risk.

AUTOMATION IS KEY

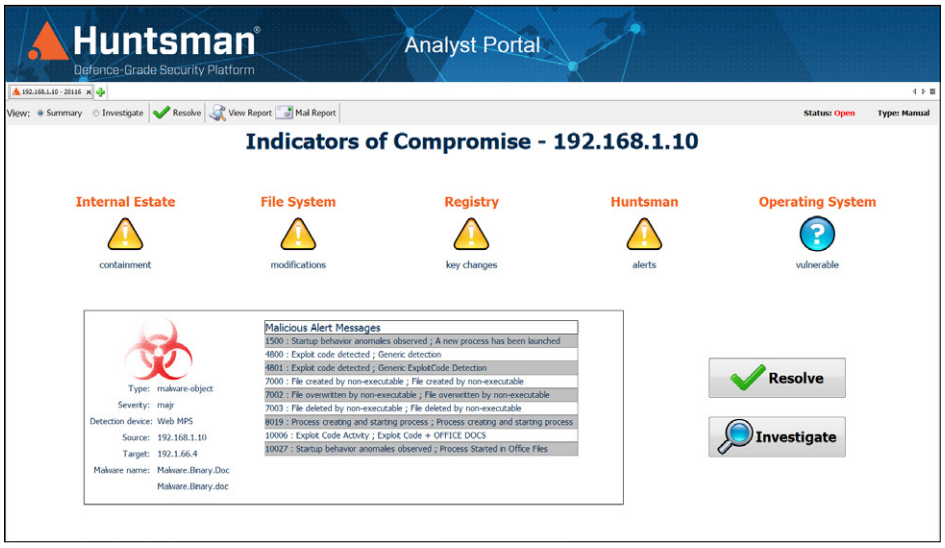
Automating security operations and analysis processes with the **Huntsman Analyst Portal™** directly benefits the process of threat management; from detection, investigation and validation to triage, incident response and resolution. This provides several clear benefits:

- Faster more accurate security decisions
- Dramatically increases the productivity of security teams
- Frees up analysts for in-depth analysis of serious events
- Allows less experienced security staff to operate more efficiently
- Reduces the time at risk for the enterprise

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 cyber-security solutions to identify, prove and resolve malware and unknowable threats

THREAT DASHBOARD



DATA-DRIVEN DECISION MAKING

The Huntsman Analyst Portal™ provides a comprehensive interface for analysts that delivers:

- Full incident management lifecycle support
- Automated evidential record and case history collection
- Full workflow automation for streamlined threat management

For every incident investigated by an analyst, the relevant evidence is automatically collated into an evidential case data file. This automation of routine pre-analysis and workflow saves significant SOC operations time and ensures that there is a complete and trusted record of incidents for in-depth investigation and compliance purposes.

BUILDING EXPERTISE INTO THE SYSTEM

The **Huntsman Analyst Portal™** provides all the evidence and the tools necessary for a thorough analyst investigation. For less experienced security staff, and to reduce SOC operational risks, a dashboard represents threats more simply and automatically guides operators through the workflow required to analyse, validate and mitigate real threats.

This means SOC operations and their capabilities are less vulnerable to the very real resource risks of highly skilled operators and can still provide effective threat detection and resolution, which results in less reliance on expensive experts and significant process automation for time and cost savings.

BENEFITS

- Reduces time at risk to seconds
- Delivers immediate value by automating routine investigation workflows to streamline SOC processes and free-up specialist analyst resources to focus on the most risky threats
- Dismisses benign threats and eliminates false positives to reduce analyst workloads and investigation overheads by up to 90%
- Enhanced corporate security capability by reducing the time at risk
- Significant ROI improvements from existing security investments and operations teams

A SYSTEM THAT DELIVERS

The **Huntsman Analyst Portal™** is unique in the speed and accuracy of its Automated Threat Resolution Management and in its ability to integrate specialist security solutions and services for the best possible security decisions.

It enhances the already high performance of the **Huntsman Enterprise SIEM** as part of a wider cyber-security platform; or can be deployed as a standalone solution or interface to third party security management solutions and SIEM systems.

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