Cyber Risk Reduction:

Why Automated Threat Verification is key

Huntsman®

Defence-Grade Security Platform

Automated threat verification: The new stage between detection and resolution

Alarmingly, recent findings indicate that organisations are increasingly exposed to cyber security risk for longer periods of time. This is despite ongoing investment in deployments of up-to-date threat intelligence platforms and teams of highly skilled security experts. It's little wonder that industry experts are calling for a new weapon to close the gap between threat detection and resolution. Automated threat verification promises to do just that, filling an important hole in the incident management process.

HOW BIG IS THIS PROBLEM?

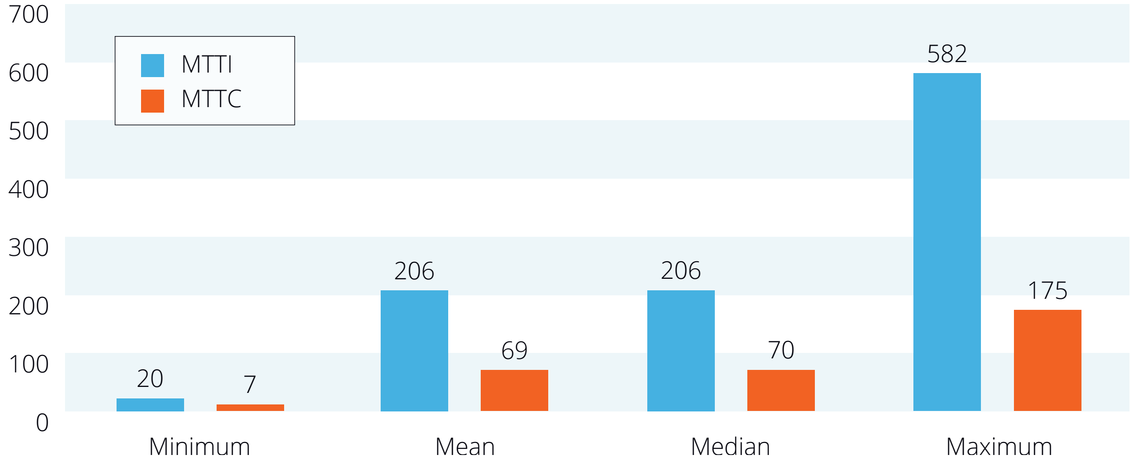
A recent study by Ponemon Institute found that malicious attacks take an average of 256 days to identify, and data breaches caused by human error an average of 158 days *(2015 Cost of Data Breach Study: Global Analysis, Ponemon Institute, May 2015)*.

The study also provides data on the mean time to identify (MTTI) and mean time to contain (MTTC) data breaches:

- MTTI 206 days (range of 20 to 582 days)
- MTTC 69 days (range of 7 to 175 days)

Figure 17. Mean time to identify and contain data breach incidents (in days)

Consolidated view (n = 350)



Source: Ponemon Institute, 2015

Unsurprisingly, the Ponemon study also found that the cost to an organisation goes up in parallel with the time at risk.

Meanwhile, Forrester Research pulled no punches in a recent report. It stated that [security and risk professionals] "lack threat intelligence and analytics to anticipate, prevent, and mitigate threats. Not only do S&R professionals lack an understanding of the emerging threats to their digital businesses, they lack the ability to identify and address the high-risk vulnerabilities across their environment, and they can't detect the intrusions and data exfiltrations that are already in progress." *(Defend Your Digital Business From Cyberattacks Using Forrester's Zero Trust Model, Forrester Research, September 23, 2015)*

SO, WHAT IS GOING ON?

One of the main reasons it takes so long to address a malicious threat is that most threat detection platforms flag large volumes of unusual events for investigation, including benign alerts – otherwise known as false positives. It can take security experts hundreds of hours to collect and sort through an overload of information to detect an actual threat when they should really be turning valuable skills to the urgent task of threat resolution. It is a process that has been likened to sifting through a full sack of mail. And for highly skilled security experts, the often mundane process can hold a similarly low level of satisfaction.

As Gartner's Anton Chuvakin says in a recent blog: "Everybody whines that organizations have too many alerts, even the makers of the tools that produce alerts. Everybody! Everybody!! Everybody!!!" (Five Basic Forgotten Security Alert Truths, Gartner, September 25, 2015)

This situation is well summed up by Peter Woollacott, CEO and co-founder of cybersecurity specialist, Huntsman Security, developers of threat detection and verification platforms for some of the world's most demanding defence grade environments.

"There has never been more security intelligence available to support cybersecurity specialists," says Woollacott. "The problem, however, is that the current manual processing of machine-generated information means security specialists are struggling to isolate the real threats from the noise. In environments that can generate billions of events per day, current human solutions can't scale."

Woollacott is not alone in thinking this way. In another recent blog, Chuvakin writes:

"So, detection [D] gives you alerts, indications, ambiguous end user reports, other weak signals about possible attacker activities, mixed in with copious amounts of noise. On the other hand, response [R] – such as formally declaring an incident – requires clarity and not ambiguity, as the CIRT team is imbued with their super-powers during the actual live response. How and when you transition from D to R really matters.

"... this between-D-and-R stage is what enables you to actually stop the attacker before the damage is done. Yes, D and R on their own are critical, but the link between them is even more critical! If your SOC and CIRT (at the higher end of the organizational security maturity) work really well – but not together – the chance that the attacker will WIN and you will LOSE is still very high, despite all the technology investments." (On Space Between Detection and Response, Gartner, August 31, 2015)

INTRODUCING A NEW STAGE BETWEEN DETECTION AND RESPONSE

All roads lead to the need for a new way of looking at cybersecurity. Until now, the security process has been seen to have two key components: detection and response/remediation. But there is a stage in between – **verification** – that is importantly distinct from either detection or remediation and often overlooked. It is in this intervening stage that the major breakthroughs can occur in reducing the time at risk and in turn business exposure.

So, really, it is not so much a 'transition from D to R' (to quote Anton Chuvakin), but the creation of a completely new stage – 'V' for 'Verification'. This is the process of gathering and analysing data to determine if machine generated alerts are actual threats or false positives. Th analysis element of this manual process is taking hours and days at best, never mind the Alert Triage waiting room itself.

This Verification stage will only grow in significance as more threat detection technologies are integrated into the security solution sets of organisations in the quest to broaden their radar / threat context.

COULD AUTOMATION BE THE ANSWER?

Automation is a step change in the incident management process, and promises to level the playing field in the war with cyber criminals by pitting machine against machine and slashing the time an organisation is at risk.

An automated threat verification capability can more quickly sift through mountains of threat information and context to verify whether reported threats are real and whether they pose an unacceptable risk to the organisation.

In short, a machine-based threat verification capability allows 'real' threats to be more rapidly investigated and resolved by analysts, thereby reducing the organisation's risk exposure.

This is a major breakthrough that addresses a critical issue that, until now, has frustrated the cyber security industry. Some have likened it to the way computers were used in the 1940s by British code breakers to churn through millions of data points – replacing manual processing using paper and pencils – to crack the German army's famed Enigma code.

And the case for automation is gaining momentum. In another blog, Chuvakin states the case for 'good automation': "Overall, this category of 'good automation' covers ways to acquire more useful data to make a decision, to help humans make a decision, [and] streamline routine, and other boring repetitive tasks." (Security: Automate And/Or Die, Gartner, September 11, 2015)

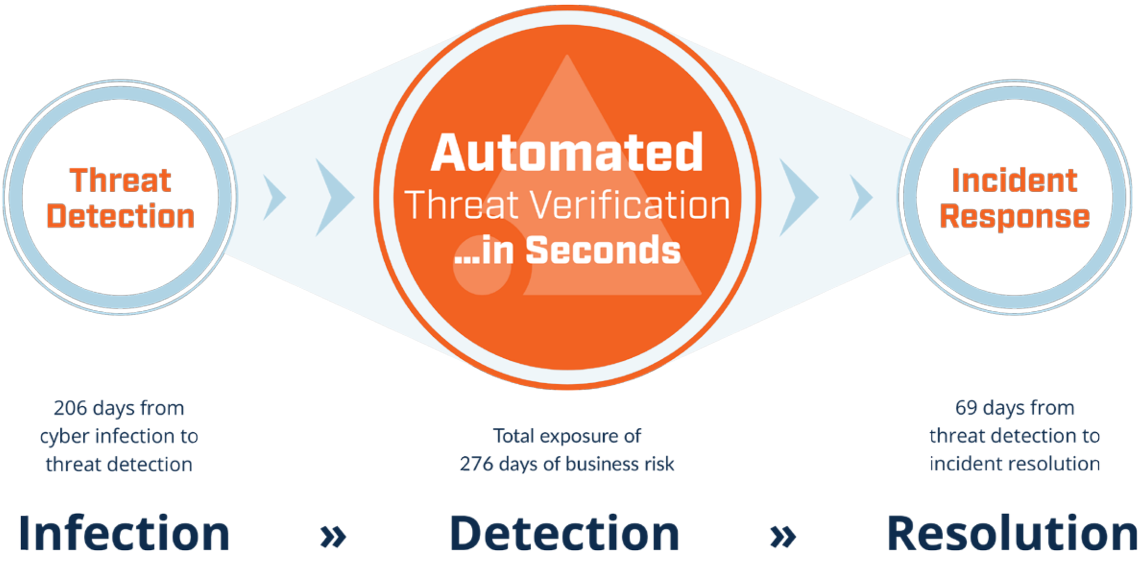
THE BENEFITS OF AUTOMATION

In summary, here is what Automated Threat Verification can deliver to your business:

- **Reduced operational cost** Eliminates the need for analysts to manually unpack, aggregate, investigate and interpret massive amounts of information from multiple technology silos.
- **Reduced time at risk** Eliminates false alarms – and prioritises real threats – to bridge the gap between insight and action.
- **Consistency of process** Significantly improves the efficiency of security operations functions by allowing security specialists time to focus their skills on resolving the threats that matter.
- **Reduced time at risk** Dramatically reduces the critical triage delay between threat detection and resolution.
- **Opportunity cost of scarce highly skilled resources** Releases time and expertise to conduct activities that actually help defend networks and systems (such as improving patching).

MORE ON AUTOMATING THREAT VERIFICATION

Huntsman Security has uniquely built Automated Threat Verification into its cyber security solutions. Find out more about automating threat verification at **www.huntsmansecurity.com**.


Threat Detection
Automated Threat Verification ...in Seconds
Incident Response
206 days from cyber infection to threat detection
Total exposure of 276 days of business risk
69 days from threat detection to incident resolution
Infection
»
Detection
»
Resolution

Author: Peter Woollacott
Co-Founder and CEO, Tier-3

Peter Woollacott is the co founder and CEO of Tier 3 Pty Ltd, the software company that holds the patent for Behavioural Anomaly Detection and developed Huntsman® Intelligent Security.

He has 25 years' experience in operational and risk management with companies like Lend Lease, CBA, AXA, EDS, PWC and Bain International. Peter holds Masters Degrees in Applied Finance and in Business Administration, and lectures in executive post graduate education at Macquarie and Sydney Universities.

Peter may be contacted at
pwoollacott@huntsmansecurity.com

Please visit the Huntsman Resources page at
www.huntsmansecurity.com/resources
for White Papers, Compliance Guides, Solution Briefs and more resources by this author.

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