# Fraud Prevention
# & I.T. Security

Huntsman®

Defence-Grade Security Platform

# Using Huntsman® to align fraud prevention and IT security

Fraud prevention is an increasingly important issue, particularly for organisations with an online presence.

Large banks, insurance companies and retailers are obvious targets. So are government departments and critical infrastructure providers.

They are continually under attack by cyber criminals keen to exploit vulnerable online, automated or electronic transactional systems to gain bank account and credit card details, as well as personal information. Increasingly, these attacks are resulting in staggering losses and exposures, and causing reputational risk.

To counter this threat, some organisations have deployed Enterprise Fraud Detection systems, often in addition to traditional identity and access management systems and their extensive cyber security defences.

**In this paper, we discuss:**

- The scale of the cyber crime problem;
- The effect on organisations;
- How organisations can adopt intelligent SIEM systems to monitor and prevent cyber fraud, and protect their IT security investments.

## HOW BIG IS THE CYBERCRIME PROBLEM?

Cybercrime is big, and getting bigger, and can hit almost any organisation, big or small.

In 2014, US auction site, eBay, reported being hacked. The personal details of 145 million active users ended up in the hands of hackers. These included customer names, encrypted passwords, email and physical addresses, phone numbers, and dates of birth. Soon after, Brazil's Boleto payment system was found to have been breached for an extended period, resulting in an exposure running into billions of dollars. The Home Depot attacks, in Sept 2014, also affected up to 109 million customers.

The hacking of these major organisations prompted Dr Adrian Davis of (ISC)2 to comment that, when it comes to cybercrime, "no organisation is secure."[1].

Apart from hacking personal information, cybercrime can also include fraudulent credit card use, electoral fraud, and the purchase of online products between internet counterparties.

And then there's insider fraud, which is also on the rise. Worse still, it's harder to detect than external fraud, and the warning signs may only be evident through the behaviour of users, or unusual patterns of access to records or systems.

Insider fraud typically involves a trusted employee with legitimate access to company data, financial systems or employee records, who can manipulate the system to make salary payments to fictitious employees and collect their wages, pay fictitious invoices or even transfer funds for their own benefit. What's really concerning is that insiders don't need to be IT savvy to commit the crime[2].

The impact of these events on an organisation's financial and reputational profile is enormous. It's little wonder that increased fraud losses in the last 5 years have resulted in ballooning fraud teams and security budgets.

## WHY IS FRAUD PREVENTION SO DIFFICULT?

One major problem with fraud prevention is that organisations can never 'set and forget'. As soon as the IT security community adopts better solutions, or tightens controls in other ways, cyber criminals seem to find ways to circumvent them. That's why some experts refer to an 'arms race' between cyber criminals and organisations; a recent Infosecurity survey observed that "even though many organisations have raised the bar on security, their adversaries have done better"[3].

## WHAT CAN ORGANISATIONS DO TO FIGHT CYBER CRIME?

**Right now, there are three main ways organisations can protect themselves from cybercrime:**

- Dedicated fraud detection/prevention systems;
- Security information and event management (SIEM) systems; and
- Behaviour monitoring.

The benefits and drawbacks of these approaches are outlined below.

### Dedicated fraud detection/prevention systems

Enterprise fraud detection systems are great in some environments, but they can't prevent all fraudulent activity. And they commonly suffer from one or more of the following shortcomings:

- They rely on pre-defined breach rules, parameters and thresholds being set correctly;
- They rely on the patterns of fraud or the warning signs being known or anticipated;
- They are designed to monitor specific, individual transaction areas, which means that separate solutions are needed for different categories of fraud, such as data theft, spearfishing and payment card fraud;
- They are not integrated with the wider security defences or SIEM systems of organisations, and thus create divisions and silos that divide fraud and security into independent domains; or
- They are expensive to buy and deploy, and need a lot of fine-tuning.

So it's not surprising to read in a recent Forrester Research report that large financial institutions are 'striving for predictive models that self-calibrate to match ever-changing online fraud schemes, rather than manually refreshing models based on out-dated rules[4].'

The Forrester report's main focus is the use of big data analysis techniques to process more data more quickly and thus improve fraud prevention outcomes. There are several ways to deal with this issue. One is that an organisation hires an even bigger team of data scientists to supplement their fraud analysts. These specialists are extremely hard to find and very expensive to hire.

The better alternative is to leverage more capable technology to create a more integrated security and fraud detection process.

## Intelligent SIEM systems

If you've deployed a SIEM system for IT security monitoring and compliance with industry or government regulations, then you're probably collecting some of the data you need for fraud detection. The event logs of systems, application, network and platform activity that are being monitored to detect fraud are likely to be similar to those your IT security team checks for security issues.

What is typically missing is the actual transaction logs from within the applications or the business processes.

The good news is that organisations can get greater value and risk reduction by better leveraging their SIEM system to monitor infrastructure and operations functions. A flexible SIEM solution can be configured to accept almost any log data (including applications) and interpret the context or situation surrounding the incident. Depending on the capability of your particular SIEM, value can be derived from its use in both security and a wider fraud prevention agenda. This multiple use adds significantly to the business case and ROI for a SIEM with advanced analytics capabilities.

For rapid response online and internal fraud prevention, your system must:

- Function in real time with the ability to process events in-stream;
- Be capable of high-speed event correlation and analysis;
- Be able to collect and parse a wide variety of logs including those from application/transactional data sources;
- Allow the definition of look-up based rules and alerting to allow fraud indicators to be used as reference data; and
- Have behavioural capabilities that allow machine-based learning of normal operational profiles, not just pre-defined user invoked thresholds or limits to pinpoint suspicious events.

A warning here; SIEM systems that focus largely on compliance reporting and analytics may not bridge the security and fraud divide. But an intelligent SIEM system, like Huntsman®, certainly will.

Intelligent SIEM systems can aggregate information from system and transaction logs, web server logs and more, and have analysis capabilities that range from definitive data rules through to Behaviour Anomaly Detection (BAD) ones. By 'standing in the shoes' of a fraudster, threat scenarios can be anticipated and preventative actions triggered by certain combinations of events, patterns or usage profiles. Some of these common signs of fraudulent online activities include:

- Numerous withdrawals of small amounts, often just under a specific limit;
- Simultaneous transactions originating from different IP addresses or geographies;
- Repeat purchases from the same device, card, email or IP address; and
- Use of a card or login from multiple different devices in a 24-hour period.

Huntsman® is one example of an Intelligent SIEM system that can bridge the security and fraud divide by correlating across the wide range of activities necessary to help keep your organisation one step ahead of cyber criminals.

## Behaviour Anomaly Detection (BAD)

Rule-based systems have limitations, no matter how refined or simple the rules are. Independently, you need to know exactly what you are looking for to establish a 'rule'.

BAD, however, is less limited and deterministic in its ability to analyse events. It operates in a different dimension and works on a different set of parameters, namely: activity that deviates from established (or preferably 'learned') baselines.

Using machine learning, BAD can add critical context from the correlation of data from other sensors to validate indicators of compromise and so risk adjust outcomes to eliminate false positives – across both the security and fraud domains. This is important because the rapid growth of network traffic and attack sophistication means that false positives are a growing problem for IT security teams as they waste effort and resources on false alarms. In fact, the Information Security Forum advises its Members (amongst other things) to use behaviour patterns to flag fraud events earlier and to harvest data (for context) from multiple sources[5].

### CASE STUDY: DEBIT CARD FRAUD

One financial sector customer traditionally used a manual process to detect fraud by utilising a series of simple thresholds and visual checks.

They deployed Huntsman® to leverage the profiling capability within the BAD technology. It was configured to track the unique profiles of each account holder. Using the normal activity profile, and such information as ATM locations, times, transaction amounts, it was able to detect and report anomalous, potentially fraudulent activity to the fraud and loss prevention functions.

By utilising the real time processing, correlation and anomaly detection capabilities provided by the BAD engine within Huntsman® the organisation can now identify the behaviours associated with a range of debit card fraud and reduce its losses significantly.

It is important here to draw a distinction between two variations of BAD – network-based (often called NBAD) and full (i.e. comprehensive, multi-layer). NBAD works at the network layer while full BAD works across all 7 layers of the stack (including application activity streams). The former can only flag unusual traffic patterns across a network or between hosts; while the latter can identify system accesses, user activity and application behaviour patterns.

BAD is especially useful for preventing insider fraud, because it will compare the situation where an employee or customer is using an application or system in a way that is either different to their own normal usage pattern or deviates from the typical profile of activity of their peers.

Extending this to wider data types, organisations can gain insights into people using a different printer from the one they routinely use, running queries that return high volumes of results, or identifying people moving through different entry and exit points in the building, all of which can be signs of suspicious activity.

An intelligent BAD system, like Huntsman®'s BAD technology, enables organisations to set rules and triggers for highly specific events and profiles to flag anomalies where their statistical significance is an indicator that further investigation is needed in applications, transaction logs and at the platform level, as well as within the network traffic.

For any detected breach of security controls that sparks interest and leads to an investigation, the resulting workflow requires data and tools to register an incident for investigation. Here, Huntsman®'s role as a data collection engine with advanced drilldown and query tools, supports real time investigation, diagnosis and reporting of risky incidents.

## USING HUNTSMAN® AS YOUR WEAPON TO FIGHT CYBERCRIME

Fraud monitoring and IT security monitoring are both focussed on looking for known and unknown patterns of activity and indicators of compromise that are consistent with cybercrime.

Huntsman®'s integrated approach to fraud prevention and IT security is the ideal solution for organisations that need a fraud detection and threat management system but that can't justify the expense of buying and deploying separate systems.

Huntsman® provides intelligent security controls with advanced features like BAD, threat intelligence and application-aware log collection to benefit an organisation's security and fraud specialists.

Huntsman® also has benefits for organisations that have already invested in fraud management systems, and want to align fraud prevention and IT security to gain a unified risk view. Huntsman®'s integrated approach to fraud prevention and IT security can provide:

- A more complete understanding of the cyber risk profile across your organisation, particularly where the exposure of a cyber-incident is fraud related;
- Better understanding of fraud and security patterns originating inside and outside the business;
- Faster identification of common occurrences of fraud and security incidents; and
- More rapid and informed response to incidents resulting from better information and context to reduce the time at risk for your organisation.

### CASE STUDY: CREDIT CARD FRAUD

A list of stolen credit card numbers will span several banking institutions and issuers.

One card scheme wanted to investigate ways to act against fraud when the activity is spread across a number of organisations.

The challenge was to achieve this within  seconds and determine the common point of purchase CPP where all these credit card credentials were stolen from.

Historical analysis confirms that a fraud occurred, but it doesn't provide a real time ability to determine the scope of the fraud.

The customer deployed Huntsman® Intelligent SIEM and using its real time correlation and analysis engine, Huntsman® was able to help the organisation in automatically detecting any common point of purchase and prevent other fraudulent activity from occurring from credit cards that has been stolen from the same CPP.

## REFERENCES

1 The eBay security breach - more lessons to learn, Computerworld UK, May 23, 2014

2 Insider Fraud in the Financial Services Industry, Software Engineering Institute, Carnegie Mellon, 2012

3 PWC, CIO & CSO Global State of Information Security Survey, July 2014

4 Bid Data in Fraud Management: Variety leads to Value and Improved Customer experience, Forrester, October 16, 2014

5 The Future of Aligning Information Security and Fraud Prevention, Information Security Forum (ISF)

**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