Case Study: **Managed Security Services Provider**

Huntsman®

Defence-Grade Security Platform

Managed Security Services Provider

This MSSP prefers not to be named but is willing to discuss its Huntsman deployment with Huntsman Security prospects. For this case study, we'll call the company Tri-Gate. It is part of a global group that offers Managed Services in IT and IT security, to both corporate and government organisations.

BACKGROUND

Tri-Gate helps these organisations to assess their risk profiles, and formulates security plans to address exposures according to agreed priorities and needs. Security design and deployment takes in critical data, applications and networks. Governance, risk and compliance management services are also offered as part of the managed services. Tri-Gate prides itself on matching the expertise of its people with a best-of- breed approach to the security solutions it selects for customers.

CHALLENGE

Tri-Gate handles mission-critical data for a number of government organisations, making strong and reliable security an absolute requirement, especially event correlation and fault finding. A SIEM system it had implemented some time before had proved unreliable and could no longer handle Tri-Gate's growing transaction volumes in terms of event logging and reporting. 'On one hand, we had outgrown the system,' Tri-Gate's Chief Security Architect (CSA) explains, 'on the other, the vendor had no local support resources'.

As a result, Tri-Gate looked for a solution that

- could log all current transaction volumes with ease;
- could scale up to process volumes that were growing at 130% a year per device;
- could collect data from a wide variety of systems;
- could perform event correlation across a multi-tiered gateway and multi-layered network;
- ensured data sovereignty (chain of custody);
- was well-supported by local resources.

'The huge volumes of transactions and events we deal with daily are merely the prerequisites,' Tri-Gate's CSA stresses. 'Our real priorities are threat and risk management, which are vital given the critical nature of some of the client data we handle. We have to report in detail on privileged access to data and applications, as well as on system level access. We constantly check that our controls are working, so we can be sure we can pass any forensic audit we might have to.'

Tri-Gate defined a set of criteria and reviewed these against major SIEM vendors. Detailed evaluation and testing began with seven vendors, a number of whom were eliminated in the initial few weeks because they fell short of expectations. The major areas for which Tri-Gate tested all vendors were:

- Event logging, log management and reporting;
- Volume and storage capacity;
- Flexibility to collect a broad variety of data types;
- Scalability;
- Data integrity;
- Simultaneous visualisation of multiple customers data sets;
- Ability to integrate with external Ticket Manager systems
- Pricing.

SOLUTION

Some vendors ran into capacity constraints, others proved unable to collect certain data types - the Argus billing system was a pertinent example. Others fell down on log management, a crucial element for ensuring the data integrity, security and compliance that are so important to Tri-Gate's government customers.

Pricing was also a significant issue since some SIEM vendors based their pricing on events processed per second. With Tri-Gate operating in the highly competitive Managed Services market, pricing had to be competitive and costs easy to calculate and budget.

In the end, Tri-Gate chose Huntsman for these reasons:

- Outstanding log management with no volume or capacity constraints;
- Best scalability of all solutions tested; additional modules build on those already installed;
- Ability to collect the most data types from the greatest variety of sources;
- Capacity to correlate events and find faults across Tri-Gate's multi-layered network;
- LiveView console providing single, holistic view of a complex threat environment.

Huntsman's grid architecture also held a lot of appeal for Tri-Gate, as it allows linear upgrades using non-proprietary hardware and provides clearly predictable capacity increases. Another deciding factor was Huntsman's LiveView console, which allows the entire network to be monitored through a single screen.

According to Tri-Gate's CSA, 'LiveView is simply one of the best tools for finding the "needle in the haystack". A related advantage is that Huntsman collects data once and allows us to run any number of queries against it to drill down into the details surrounding a particular event.'

RESULTS

Huntsman was deployed 12 months ago, and Tri-Gate's CSA says it has delivered everything Huntsman Security promised. An unexpected spin-off was that Huntsman gave Tri-Gate's IT staff new insights into their IT environment, such as more visibility of network configuration and traffic flow. 'Huntsman is one of the best tools we've come across for finding faults in server or network configuration,' Tri-Gate's CSA makes clear. 'That's a welcome side benefit.'

Having access to local support resources is another plus for Tri-Gate. 'Huntsman Security's people are very responsive,' Tri-Gate's CSA confirms. 'Most issues we raise are solved over the phone but, if we need an engineer to come to our site, they usually arrive the next day. Dealing with an accessible company has other benefits too: we are in the feedback loop, which means we can give Huntsman Security direct input on product performance and suggest desirable enhancements for the future. We're very happy with our decision.'

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