Case Study:
The Retail Bank

Huntsman®

Defence-Grade Security Platform

The Retail Bank

This bank prefers not to be named but is happy to discuss its Huntsman deployment one-to-one. For this case study, we'll call it Icon Bank – a national retail bank which is part of a global financial institution.

Icon focuses on innovative saving and loan products for consumers and savings packages for business customers, and several of Icon's products have received awards for their convenience, transparency, flexibility and low fees.

CHALLENGE

Icon Bank operates as an autonomous division of its parent company. It faces the same security challenges as the parent yet is responsible for its own IT operations. That means that Icon must adhere to the same corporate IT security, risk and compliance standards yet achieve this goal with more limited resources.

As Icon Bank grew, so did the IT infrastructure needed to support the business, resulting in a mixture of disparate IT and security systems. This disparity made it difficult for IT staff to track all the events that impacted on operation and security, let alone to coordinate effective responses.

'We found ourselves with a number of information silos,' Icon's Manager of Network Security (MNS) explains, 'which made it difficult to see events in context. Some of our systems don't generate alerts, which meant IT staff had to check their logs constantly. We needed a system that gave us a single view of our operations and our security environment, and one that alerted us to all potentially serious events.'

With multiple systems and information silos, it became impossible for Icon's IT staff to identify all security issues in real-time. Even after-the-event remediation was difficult, since it was not possible to monitor all the event logs generated by different systems. Prior to using Huntsman, the standard of log collection and management was inadequate to achieve compliance with financial industry regulations such as PCI-DSS.

SOLUTION

Icon set a number of selection criteria for its prospective solution, foremost among them

- Ability to provide a single view of events across the network;
- Log Management that ensures complete data sets for forensic audits and ensuring data sovereignty;
- Flexible reporting to meet compliance requirements;
- Ease of use, deployment, configuration and implementation;
- Low impact on performance of existing IT and security systems;
- Responsive technical support.

Globally, Icon had standardised on a North American SIEM vendor, but that company did not have global technical support. This was one reason Icon evaluated other solutions including Huntsman. ‘We have limited IT and security resources,’ Icon’s MNS says, ‘so the presence of local technical support was a key criterion in our selection, but we found the product had a lot to offer as well.’

One key Huntsman feature was its flexible reporting. Competing solutions provided a host of pre-defined templates, but these needed a lot of work to customise to individual reporting needs. By comparison, reporting templates for Huntsman were easy to create. However, Icon needed some assistance to set up and implement the rules and filters for event monitoring.

‘This was one area where access to local expertise was a real help,’ Icon’s MNS makes clear, ‘but we didn’t select Huntsman for that reason alone. We chose Huntsman because it had a rich feature set, it monitored the systems we had in place without impacting performance, and because it was easier to deploy, maintain and use than other solutions. In short, it was system we could manage with our limited resources without losing any functionality.’

RESULTS

Using Huntsman, Icon's security posture is vastly improved, with IT staff able to identify security issues and respond as soon as they arise. Huntsman's LiveView console has proved a genuine advantage for Icon, given its ability to pull information together from diverse systems and sources into a single view. 'Using Huntsman, our security analysts can investigate and make informed decisions based on real time, factual information presented in a visual and evidential manner.'

Huntsman's Behavioural Anomaly Detection (BAD) module has also played a role in reducing Icon's exposure to risk. BAD alerts IT security staff to events or behaviour that deviates from an established baseline. 'In part it builds from a statistical basis,' Icon's MNS makes clear, 'and, using different tools at several levels, helps to reduce overall exposure so BAD plays an important role. There's no doubt in my mind that we've averted a number of threats we simply wouldn't have seen before.'

Icon has been in full compliance with industry regulations since Huntsman was implemented a few years ago, passing a recent audit without problems. 'We didn't buy Huntsman to solve a compliance problem,' Icon's MNS makes clear, 'yet it was a must-have for us and, I'm happy to say, it's no longer an issue. Huntsman is a great product, and we've had consistently responsive support from Huntsman Security. If need be, a technician will come on site to look at a problem the same day we log it. We can't ask for more than that.'

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