

Case Study:
Financial Credit Union

Financial Credit Union

Credit Union gains Compliance and Protection in One Solution

This credit union is one of the largest in Australia and, for this case study, prefers not to be named. Key members of its information security team, however, are willing to discuss its Huntsman deployment one-to-one with genuinely interested parties. For this case study, we'll call it Star Credit Union (Star).

Star is one of Australia's largest customer-owned financial institutions, and provides everyday banking products and services in a highly people- and service-oriented environment. Star has won many awards for its outstanding customer service and financial loan products.

As a financial institution, Star has to demonstrate compliance with the PCI-DSS standard, which was the fundamental driver behind the need to acquire a new security solution. A related goal was compliance with the guidelines in the ISO 27000 standard and APRA's Prudential Practice Guide for managing security risk in information and information technology (PPG234) – which is similar to COBIT (USA) and ITIL (UK).

FOCUS ON THE VITAL, RISKY FEW

With membership nearing half a million, the number of security events across Star's network - from branches and ATMs to internet and mobile banking – was becoming very difficult for the security team to manage.

Star needed a security solution that could automatically triage events, so the security team could focus on the vital few that posed potential threat, and not be swamped by the trivial many.

'We needed a solution that could correlate all these alerts,' Star's CSO explains, 'from across all our channels and other security solutions like firewalls, intrusion detection systems and so on.'

"We needed a solution that could correlate all these alerts from across all our channels and other security solutions like firewalls, intrusion detection systems and so on."

Other capabilities that the new system had to demonstrate included ability to:

- Monitor alerts from across the network in real time;
- Interpret the information collected in the event logs for risks and threats;
- Fully comply with PCI-DSS; and
- Align IT security practices with APRA PPG234 and ISO 27000 guidelines.

FLEXIBLE, KNOWLEDGEABLE & GOOD VALUE

The above are issues that typically can be addressed by Security and Event Management (SIEM) systems, and Star investigated several of them.

'We chose Huntsman Enterprise SIEM because it matched the best SIEM systems for functionality,' says Star's CSO, 'but it was a lot more flexible than the others. Huntsman also offered exceptional value, which was an important consideration for us. Being a credit union, we're owned by members and it's their money.'

Another key factor in Star's decision was familiarity with APRA's PPG234, its guidelines and how to map to them. Being an Australian company with a variety of financial institutions as customers, Huntsman Security's people were well-versed in PPG234 compared to overseas competitors, who either didn't have the flexibility or the desire to adapt to local guides like PPG234. 'We saw PPG234 as a good way to ensure optimal implementation of a SIEM system,' Star's CSP explains, 'so familiarity with it was a bonus.'

Working with Huntsman Security had other advantages for Star too. Huntsman Security was established and is headquartered in Sydney and, according to the CSO for Star, that meant: 'The company's pioneering and adaptive approach to its customers was very accessible to us if we needed assistance at the start or wanted to discuss technical issues. It also meant we had direct access if we wanted to suggest new features we'd like in Huntsman down the track.'

"We chose Tier-3' Huntsman SIEM because it matches the best SIEM systems for functionality, but it was a lot more flexible than the others. Huntsman also offered exceptional value, which was an important consideration for us. Being a credit union, we're owned by members and it's their money."

EASY UPGRADE & FAST ALERTING

The initial deployment focused on compliance with financial industry standards, basic network security, and collection of event logs for forensic analysis and audit. At the time, the operational team was the main user, managing Huntsman through the central LiveView console, assisted by sets of standard queries that allowed fast on-screen retrieval of operational information from across the network.

Once Huntsman had proved itself in operational terms, its use was extended to the teams that managed Star's network, servers and applications. That meant that all teams in the IT group were using Huntsman for alerting, querying and reporting on security events, which substantially increased demand for centralised data storage and access.

This is where Huntsman's flexibility to scale proved invaluable: Star simply upgraded to a bigger configuration and increased the forensic database with zero downtime.

Huntsman's unique behavioural capability has proven itself too. Using its patented Behaviour Anomaly Detection, Huntsman alerted IT security staff about unusual, suspicious activity detected on an executive's laptop while it was connected to the Star network.

As it turned out, the laptop had been compromised and was acting as a router to exfiltrate data. This unusual activity was detected, triaged as risky, and alerted early to the IT team. As a result, the risk was mitigated before any significant data had been compromised.

At Star, Huntsman has proven its capability and value many times across all areas of compliance, network security and IT operations.

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