DXC TECHNOLOGY

Early detection the best defence with cyber security

CUSTOMER
Large Australian transportation company

LOCATION
Sydney, Australia

INDUSTRY
Transportation

Challenge

- The need for a more proactive approach to cyber security
- Limited visibility of the security environment
- Education for senior executives and the board around the importance of cyber security

Solution

- A Security Operations Centre (SOC) with 24/7 monitoring
- Proactive security monitoring, vulnerability scanning, digital threat management and intelligence
- Robust processes to triage incidents and escalate as required

Results

- Improved executive understanding of the importance of cyber security
- Proactive prevention of unauthorised access and reduced risk of adverse impacts on operations
- Clear cyber security strategy

Early detection the best defence with cyber security

This large Australian corporation (customer) recently signed a multi-million-dollar deal with DXC to improve security posture and maturity. The organisation contributes significantly to the local and national economy and offers world-class services to its customers.

"We introduced Mark Hughes, DXC's senior vice president, security to the customer's CIO and head of cyber and they continue to have regular candid conversations which add significant value in terms of strategic insight and guidance on current cyber security trends."

— Peter Dowley
Senior security principal at DXC

The lack of visibility into cyber threats caused concern, with senior management requesting improved reporting and transparency. The Board drove this high priority project with DXC providing substantial contributions in shaping the security strategy and direction and supporting changes to the internal cyber team.

Business challenges

Given the ever-increasing frequency and sophistication of cyber threats, the customer's biggest challenge was limited visibility and reporting of threats, which left them susceptible to significant financial and reputation damage. Early detection of potentially malicious activity is vital to avoid attacks while also supporting aggressive response and remediation to minimise impact. This customer lacked high-level awareness of and commitment to cyber security. They needed a more proactive approach to cyber security management, and executive education around what could occur if they continued on the same path.

Reliance on outdated and obsolete infrastructure also left significant gaps in the customer's security program and high vulnerability levels. When a routine scan caused a major outage due to old storage failure, the current infrastructure's fragility was highlighted. Many of the customer's systems are high priority for service delivery, so if attacked, could cause major disruption to the business.

DXC's SOC operatives may also handle more in-depth investigations and forensic analysis of security breaches, as well as coordinating security incident responses.

Why DXC?

Following a public RFP process with invited participants, DXC was selected to implement a Security Operations Centre (SOC). DXC had a small existing IT managed services contract with the customer, but were engaged based on our security expertise and ability to educate and support the customer to ensure a deeper appreciation of the importance of a robust cyber security approach.

Peter Dowley, senior security principal at DXC, commented, "We introduced Mark Hughes, DXC's senior vice president, security to the customer's CIO and head of cyber and they continue to have regular candid conversations which add significant value in terms of strategic insight and guidance on current cyber security trends."

DXC had the expertise to establish an outsourced SOC for the customer while also building other services to improve security visibility and uplift cyber maturity. This included industry-specific advice such as a six-monthly threat report and security tabletop exercises.

The customer recognised DXC as having strong local capabilities with additional access to global expertise.

DXC's 24x7 SOC uses technologies and security controls such as logging, threat management and vulnerability management to minimise the likelihood and impact of cyber attacks.

The solution

The overall objective was to implement a SOC to provide a robust cyber defence capability to protect the customer from cyber threats and provide management (up to and including the Board) with clear security reporting.

DXC's Managed Security Services (MSS) team operates the Sydney-based SOC 24/7 to monitor alerts. The SOC identifies scenarios that can relate to suspicious activity, configures detection technologies, monitors security alerts, searches for active threats, and validates them.

Once a potential threat is identified, further analysis is triggered and the core security team conduct triage before deciding on the next step. This will often involve escalation to relevant Level 2 parties (either a DXC or customer contact).

DXC Technology's Security Platform helps the customer deliver an efficient security response, streamline remediation, and visualise security posture.

DXC has become the customer's trusted advisor and partner for cyber security.

DXC's Security Platform combines DXC's security operational processes and advanced workflows to automate manual processes and prioritise threats, incidents and vulnerabilities based on their potential impact on the business. This ensures continuous monitoring and management of incidents and vulnerabilities to improve efficiency and lower costs. Indicators of compromise are automatically linked with security incidents and vulnerabilities, streamlining and automating the manual process of threat investigation and incident triage.

DXC's SOC operatives may also handle more in-depth investigations and forensic analysis of security breaches, as well as coordinating security incident responses. In this customer's case, when a security issue or potential risk is identified, they are usually handed over to service owners at the customer for further response and remediation. DXC provides recommendations for action where appropriate.

To keep up with continuously changing threats, security operations must become intelligent, constantly adapting to counter adversaries. The key services provided as part of the customer's capability include:

- Security monitoring: core to the customer's solution and offering 24/7 monitoring of security events with accelerated threat detection and automated reporting. DXC security experts prioritise incidents requiring immediate attention and resolution. The customer can access event details, incident status, and reports through the DXC MSS portal.
- Managed endpoint protection: helps the customer prevent intruders from derailing operations by defending devices throughout the organisation against a new generation of security threats.
- Firewall management: administration of network firewalls and firewall rules.

- Digital threat management: a structured approach to monitor the internet and dark web services for suspicious activities directly related to the customer, executives and other personnel. This covers a vast range of areas, including fake sites, scamming or phishing schemes, and helps analysts identify potential threats early, conduct triage, and make necessary decisions on action.
- Vulnerability scanning: a broad set of capabilities that help uncover system and network flaws and prioritise remediation planning. This helps the customer with proactive prevention, ensuring a better understanding of exposures and the ability to manage potential impact through timely, cost-effective actions that mitigate risk.
- Distributed denial of service (DDoS) protection: this form of network-based attack on a customer's internet services has the potential to cripple a business. DXC's DDoS protection helps the customer defend against high volume malicious attacks to their network, which would affect a range of business systems. DXC works directly with the customer to identify best practices and harden defences.
- Threat intelligence: in collaboration with the customer, DXC ensures more effective detection with real-time visibility into other global attacks. DXC and the customer receive regular notifications from security partners, government and transport-sector organisations on known attacks and attack methods. DXC works closely with the customer to apply this intelligence effectively.
- Security governance & risk management: a coordinated approach to managing risk in the most cost-effective way. DXC provides intelligence on threats and visibility into priorities. It looks at trends – both within the customer and with other organisations globally to identify potential issues and vulnerabilities to help direct spending.

"That ongoing contact with senior DXC security staff in Australia has been particularly valuable for this customer. The customer's Head of IT maintains regular contact with DXC's regional Head of Security, and is reliant on the advice and guidance provided around what's happening with other customers and on best practice approaches in dealing with certain issues."

— Peter Dowley
Senior security principal at DXC

Business benefits and outcomes

DXC Technology's Security Platform helps the customer deliver an efficient security response, streamline remediation, and visualise security posture. Core benefits include clear visibility on cyber posture via reporting, improved executive-level awareness and appreciation of potential impact, and progress to ensure appropriate controls are in place to manage risk. Previously the customer could have been targeted by a security attack, with no one realising until it was too late. With regular scanning and monitoring for suspicious activity, early detection can prevent a potential large-scale incident.

DXC has become the customer's trusted advisor and partner for cyber security. Another primary benefit is the close engagement between DXC security experts and the customer's senior security and technology staff. Mr Dowley commented, "That ongoing contact with senior DXC security staff in Australia has been particularly valuable for this customer. The customer's head of IT maintains regular contact with DXC's regional head of security, and is reliant on the advice and guidance provided around what's happening with other customers and on best practice approaches in dealing with certain issues."

The organisation now understands the importance of cyber security, and will continue to maintain protection. Executives (including the Board) understand how risks and threats have progressed, are aware of cyber gaps and priorities, and recognise the need to address them.

Learn more at
dxc.com/us/en/services/security