DQA

7 challenges when assessing security for your organisation

Threats to Australia's critical infrastructure sector are growing at an alarming rate:

50% increase

in security incidents reported to the Australian Signals Directorate between 2022 and 2023.[1]

Only 51%

of organisations feel they have the resources to properly monitor and respond to security threats.[2]

10x increase

in attempted password-based attacks globally in 2023, an average of 4,000 per second.[3]

Cyber criminals typically target critical infrastructure assets and networks to:

- Gain access to highly sensitive data.
- Affect the provision of essential services.
- Exploit links to other critical infrastructure assets or organisations.

Source: Australian Signals Directorate[4]

Most common threats for the critical infrastructure sector:

- Compromised accounts or credentials.
- Compromised assets, network or infrastructure.
- Denial-of-service (DOS attacks).
- Data breaches.
- Malware infections.

Source: Australian Signals Directorate[5]

How can technology offer a solution?

Microsoft's Extended Detection and Response (XDR) platform offers a powerful way to enhance your threat detection capabilities, streamline security operations, and safeguard your data against sophisticated cyber threats. Ideally suited to small and midsize critical infrastructure organisations, Microsoft XDR consolidates a range of sophisticated security tools into one, easy to manage solution.

Here's how a Microsoft XDR solution, implemented and managed by the experts at DQA, can address **7 common security challenges** faced by critical infrastructure organisations.

Challenges

Solutions

1. No unified view of IT environment

- Lack of a clear 'line of sight' across the entire IT environment including endpoints, servers, networks and cloud.
- Siloed data.
- Minimal compatibility between legacy systems and tools.

- Microsoft XDR can be deployed across your entire IT environment to centralise visibility and provide consolidated insights.
- DQA can ensure your critical systems are integrated and provide a 'single pane of glass' view for monitoring and threat detection.

2. Manual detection and response processes

- Minimal automated processes for effectively monitoring and filtering cyber threats.
- Security teams are overwhelmed with 'false positives', taking valuable time away from detecting real threats.

- Microsoft XDR uses AI-driven insights and machine learning to detect anomalies and identify potential threats with high accuracy.
- DQA can customise your Defender configuration, reducing false positives and ensuring timely detection of genuine threats.
- DQA can configure automated responses in Microsoft XDR to deal with common threats, reducing response times and mitigating damage.

3. Lack of resources and tools to support round-the-clock monitoring

- No in-house staff or tools to orchestrate round-the-clock detection and response workflows.
- Difficulty keeping up with rapid pace of cyberattacks: 1 in 5 critical security vulnerabilities are exploited within just 48 hours.[6]

- Microsoft XDR provides continuous monitoring to detect threats in real-time, enhancing your ability to respond to incidents quickly.
- DQA offers 24/7 monitoring and immediate incident response, ensuring threats are contained, even outside of business hours.

4. Insufficient data encryption

- Updated Security of Critical Infrastructure (SOCI) Act now requires encryption as standard.
- Only 45% of Australian organisations currently have encryption in place.[7]

- Microsoft XDR's encryption and secure communication features protect sensitive data, meeting SOCI's strict data protection requirements.
- DQA can ensure configuration is correctly applied across all critical technology systems.

5. Reliance on disparate security solutions

- Using a complex fabric of security systems can increase workloads and lengthen response times for internal security teams.
- A multi-solution approach can also result in gaps, and in potential vulnerabilities being overlooked.

- Microsoft XDR provides a single, centralised solution to manage every aspect of your security.
- DQA can customise your solution to ensure it meets your organisation's specific needs.

6. Compliance with new regulations

- Meeting new requirements under the Security of Critical Infrastructure (SOCI) Act can be complex, time-consuming and require deep security expertise.

- Microsoft XDR's reporting and logging capabilities can track incidents, vulnerabilities, and system performance – in line with Australia's legislative requirements.
- With deep expertise and experience in Australia's regulatory landscape, DQA can assist in generating reports and maintaining documentation for SOCI compliance audits, simplifying your reporting obligations.

7. Ensuring continuous improvement

- Resource constraints, reliance on outdated systems, and complexity of implementing new technologies can make it difficult to prioritise ongoing improvement.

- DQA can offer ongoing support, ensuring your organisation's security posture evolves to meet future threats and compliance requirements.
- We regularly review Microsoft XDR's performance, adapting and refining the system for maximum effect.

Why partner with DQA?

Our experienced team here specialises in highly regulated industries and high-security environments. We have a deep understanding of Australia's critical infrastructure sector, as well as of the Microsoft XDR platform and how it can deliver the security and compliance which organisations need. We can also work with your organisation at every step to ensure you are getting the most from your technology, and provide customisation, services and support to optimise your protection into the future.

Want to learn more?

Book in a scoping discussion with our team to get a deeper insight into your organisation's security status, and to determine if Microsoft XDR is suitable for you.

Please give us a call on **1800792241** or email **sales@dqa.com.au.**

1. https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/critical-infrastructure **2**. Minter Ellison, Perspectives on cyber risk, https://www.minterellison.com/articles/perspectives-on-cyber-risk-2023-the-real-cost-of-a-data-breach **3**. Microsoft, Digital Defence Report 2023, https://www.microsoft.com/en-gb/security/security-insider/microsoft-digital-defense-report-2023-state-of-cybercrime#-modal-component-oc59c6 **4**. https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/critical-infrastructure **5**. https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/critical-infrastructure **6**. https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/critical-infrastructure **7**. DigitalGuardian, 45% of organisations have encryption in place, https://www.digitalguardian.com/blog/45-percent-orgs-have-encryption-plan-place **8**. Minter Ellison, Perspectives on cyber risk, https://www.minterellison.com/articles/perspectives-on-cyber-risk-2023-the-real-cost-of-a-data-breach

DQA | Microsoft