semperis

WHITE PAPER

Australian Department of Home Affairs
Critical Infrastructure Security Centre

The Security of Critical Infrastructure Act and Your Identity Infrastructure

TABLE OF Contents

Introduction

Virtually every aspect of modern life depends on the security and reliability of ***critical infrastructure assets***. These days, it's easy to take for granted the essential systems and services we depend on: energy that lights and heats our homes, businesses, and hospitals; networks that support everything from our food supply to financial services to water supplies; and the telecoms that connect all those systems—plus our phones and computers.

All these systems are interconnected, so that compromise of one system—such as energy—affects multiple essential services across society.

Recognition of this interdependence is at the heart of Australia's **Security of Critical Infrastructure Act 2018**,[1] which falls under the auspices of the Critical Infrastructure Security Centre, part of the Department of Home Affairs. Since its inception, the SOCI Act has been regularly updated.[2] It details the legal obligations of critical infrastructure organisations across 11 sectors:

- Communications
- Financial services and markets
- Data storage or processing
- Defence
- Higher education and research
- Energy
- Food and grocery
- Healthcare and medical
- Space technology
- Transport
- Water and sewerage

The SOCI Act focuses on risk management, incident response, and recovery, and imposes civil penalties in various forms (orders, injunctions, or infringement notices) in cases where responsible entities fail to appropriately protect any critical infrastructure assets in their care.

In April 2022, the SOCI Act was amended to add Enhanced Cyber Security Obligations for critical infrastructure assets that are deemed Systems of National Significance (SoNS).[3]

1 Security of Critical Infrastructure Act 2018 (SOCI)
2 Security of Critical Infrastructure Act 2018 - Federal Register of Legislation
3 Enhanced Cyber Security Obligations

Cyber threats pose a growing threat to critical infrastructure

In recent years, large public cyber security incidents have been prominent in the news. Large-scale data breaches such as those that hit Medibank,[4] Qantas,[5] and Australian Super (along with other associated superannuation funds)[6] were launched by attackers seeking financial gain.

Another category of cyberattacks aims to inflict significant destructive real-world impacts. High profile events include the Colonial Pipeline attack[7] in the United States and Russia's persistent wiper attacks on a variety of Ukraine's key national sectors such as government services, energy, education, and food production.[8,9]

The 2025 Semperis report ***The State of Critical Infrastructure Resilience***[10] reveals that cyber threats pose an ever-increasing risk to utility operators and public safety. In the study, which surveyed U.S. and UK water, water treatment, and electricity operators, respondents revealed that:

62% of utilities were targeted by **threat actors** in the previous 12 months

59% of attackers were **sponsored by a nation state**

57% of attacks **disrupted operations**

82% of attacks definitely or possibly **compromised Tier 0 identity systems**

These threat activities, together with increased geopolitical risk and resource nationalism, have led to more stringent regulations. In addition, operators and regulators have increased their focus on not just preventing cyber incidents but also ensuring operational resilience when the worst case happens.

4 How Medibank allegedly ignored the warning signs in one of Australia's worst cybersecurity breaches - ABC News
5 https://www.bleepingcomputer.com/news/security/qantas-confirms-data-breach-impacts-57-million-customers/
6 Which super funds were targeted by hackers? Here's what we know so far | SBS News
7 The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years | CISA
8 https://www.bleepingcomputer.com/news/security/google-says-former-conti-ransomware-members-now-attack-ukraine/
9 https://www.bleepingcomputer.com/news/security/sandworm-hackers-use-data-wipers-to-disrupt-ukraines-grain-sector/
10 The State of Critical Infrastructure Resilience | Semperis

The essence of the SOCI Act

The full text of the SOCI Act is a rather lengthy read, so this paper provides a high-level overview of the information that's essential for cyber security, resilience, and incident response professionals. This information should not be read as legal advice, as we're summarising a 260-page act. For cyber security and operations teams, the requirements boil down to a few core requirements:

1. Manage the risks associated with your critical infrastructure assets.
2. Identify and mitigate vulnerabilities and test your systems appropriately.
3. Establish robust business continuity measures for all critical assets and the systems they rely on for secure operations.
4. Manage any incidents that can jeopardise Australia's national security, social cohesion, and general functions.
5. Report in a timely manner to your regulator.

Companies reporting on risk management activities must report on their maturity against one or more security controls frameworks such as The Essential Eight, ISO/IEC 27001, or similar.[11,12]

Identity security, resilience, and incident response for SOCI compliance

In 2024, the Australian superannuation fund Australian Super experienced an identity-based cyberattack. Organised attackers targeted specific high-value customers of the fund, stealing significant amounts from some customers' pensions. Meanwhile, other funds, such as Insignia Financial, saw persistent customer-focused credential stuffing attacks, in which malicious actors repeatedly attempt access using stolen passwords and username combinations from other sites until they hit a match.[13,14]

The days of protecting your critical assets as a "castle" with a moat and a wall are long gone. Attackers can quickly circumvent a traditional firewalled perimeter through phishing, exploiting vulnerabilities, or other identity-based attacks.

11 https://www.cisc.gov.au/resources-subsite/Documents/cisc-factsheet-risk-management-program.pdf
12 Guidance for the Critical Infrastructure Risk Management Program
13 https://www.news.com.au/national/aussie-superannuation-funds-hit-in-major-cyberattack/news-story/a39634e07fe0c8b9458d472888311abd
14 abc.net.au/news/superannuation-cyber-attack-rest-afsa/105137820

Effective identity and access management prevents bad actions

The "perimeter" is now defined by permissions, and extensive digitisation and automation mean that credential vulnerability and weakness exist in every level of our organisations. Interconnected systems enable a destructive event in one area to propagate and drive catastrophe across a much broader domain. The implications for organisational resilience are significant, requiring diligent application of best practices at every level and in every component.

As the cornerstone of operational access, your identity system enables you to manage permissions and access to the data and services that users trust and rely on.

Protecting identity system availability and integrity is vital

Because operational systems across critical infrastructure assets rely heavily on identity infrastructure, the availability and integrity of identity systems—in particular Microsoft Active Directory (AD) and Entra ID—are vital for all your key business areas.

Unfortunately for organisations in critical national industries and regulators seeking resilience, legacy identity systems have not always been designed and architected for security and resilience. Over its 25-year history, the AD infrastructure in most enterprise organizations has acquired significant technical debt and vulnerability to destructive events.

With the volume of change in a typical large enterprise AD, the complexities arising from hybrid on-premises and cloud identity environments, and the aging technologies in play, we must devote focused attention to identity system security as we work to establish resilient—and compliant—enterprises.

In the following sections, we discuss the identity-related areas of the SOCI Act—and how you can work toward resilience and compliance.

Identity through the lens of the SOCI Act

The following sections outline the key challenges an operator of Australian critical infrastructure assets needs to address in relation to identity infrastructure, as detailed in the ***General Guidance for Critical Infrastructure Assets*** document.[15]

The final sections add a discussion of key cyber security controls required by the Act's Enhanced Cyber Security Obligations and informed by the supporting security control frameworks that the SOCI Act integrates with.

15 https://www.cisc.gov.au/resources-subsite/Documents/cisc-factsheet-soci-obligations.pdf

Risk management

Part 2A of the SOCI Act emphasises the importance of risk management to identify and mitigate the effects of relevant hazards,[16] summarizing that the purpose of a critical infrastructure risk management program is to:

- identify each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset; and
- so far as it is reasonably practicable to do so, minimise or eliminate any material risk of such a hazard occurring; and
- so far as it is reasonably practicable to do so, mitigate the relevant impact of such a hazard on the asset.

An organisation involved with the operations of a critical asset needs to understand the asset's capability, what the asset's safe operations entail, and how to secure those operations from adverse effects.

The scope of hazards is broad, covering natural and human-caused disasters as well as cyber security and information security. Risk management requirements include personnel, supply chain, and physical security.

The Cyber and Infrastructure Security Centre provides guidance for implementing a critical infrastructure risk management program.[17]

Actions for risk management

1. Map potential hazards that relate to your identity system.
2. Understand the role of identity security in your organisation's overall risk posture.
3. Integrate identity security objectives into your strategic risk management roadmap.
4. Understand what critical services depend on the capabilities of your on-premises and cloud identity systems.
5. Define ownership of those capabilities.
6. Define activities for monitoring and managing your identity security posture.

Incident response and reporting

Threat actors have been advancing their capabilities at a significant pace. For defenders, this means that prevention alone isn't enough. You must be prepared with a plan for containing the initial breach, recovering essential systems, and fully restoring operations.

16 https://www.legislation.gov.au/C2018A00029/2023-10-20/2023-10-20/text/original/epub/OEBPS/document_1/document_1.html#_Toc149392335

17 Guidance for the Critical Infrastructure Risk Management Program

SOCI Part 2C covers the Act's Enhanced Cyber Security Obligations. **Sections 30CD-CJ** require that an organisation adopts, maintains, and regularly reviews an incident response plan, which is described as a written plan that:

- applies to the entity responsible for a system of national significance; and
- relates to the system; and
- is purposely intended for responding to cyber security incidents that could impact the system; and
- complies with specified rules.

Those rules may:

- require general incident response planning
- relate to one or more specified SoNS
- relate to one or more specified types of cyber security incidents

Your plan should also include specific considerations for your identity systems. Legacy identity systems such as AD can be notoriously difficult to restore to a ***known secure*** state. Attackers can elevate privileges in ways that enable them to partially or totally overwrite identity system logs.

You need to know:

- Your logs are intact and have not been tampered with
- What changes have been made by a potential attacker (as well as your own teams)

In addition to incident response planning, Sections 30BC-BD describe requirements for notification of cyber security incidents. The SOCI Act specifies reporting within tight timelines, which requires the ability to quickly identify root causes of outages and breaches.

Timeline	Section	Description
12 hours	30BC	An entity must report where an incident is occurring or has occurred and where there is direct or indirect and significant impact on the availability of the asset.
72 hours	30BD	An entity must report incidents, whether occurring or past and having or likely to have an impact on the critical assets, within 72 hours to the relevant authority.

Actions for incident response readiness

1. Conduct a thorough security risk assessment, reviewing and mapping attack pathways leading to Tier 0 assets, to ensure a deep understanding of your identity infrastructure including shadow administrators, nested groups, and local administrative rights.
2. Devise an incident response plan that includes clearly defined roles and responsibilities for each member of your team—and test the plan regularly.
3. Ensure the integrity of your identity infrastructure logs and establish the ability to monitor changes to AD in real time.
4. Establish the ability to collect forensically sound data on your identity infrastructure and to perform forensic investigations that determine the origin and methods of an attack.
5. Ensure your identity forensics capabilities are integrated and tested as part of your broader incident response readiness.

Cyber security exercises

SOCI Part 2C, Sections 30CM-CT, lay out the requirements for cyber security exercises that demonstrate your preparedness and ability to respond to and recover from any and all cyber security incidents that might impact your ability to deliver critical infrastructure operations and services.

The Secretary of the Department of Home Affairs can require an entity operating a critical asset to perform a cyber security exercise—and can specify individuals to monitor those exercises.

The Act summarises the scope of cyber security exercises by explaining that the test needs to cover the entity's ability and preparedness to:

- Respond to *all types of cyber security incidents* that could impact the system—and mitigate the impact
- Respond to and mitigate the impact of *specified types of cyber security incidents*

Cyber security testing can take many forms. Typically, organisations in critical sectors opt for "red-and-blue team" tabletop exercises—advanced simulations of cyberattack and defence. If the red team (or an actual attacker) targets your AD, you need a good level of confidence that you will detect the attack and be able to respond and contain the threat.

Post breach, you need to be able to quickly and confidently restore the identity system to a safe and trusted operational state.

To deter and stop an attacker, it is important to apply learnings from the simulation to harden the identity system and patch vulnerabilities. If you are caught out by the cyber security exercise, you must be able to identify root causes and rapidly report to the regulator your plan for remediation.

Actions for conducting regular cyber security exercises

1. Establish a strong baseline understanding of your identity security posture from which to launch identity system hardening and vulnerability management programs.
2. Establish your own schedule of cyber security exercises to proactively build maturity and reduce exposures in the systems supporting your critical infrastructure asset.
3. Align your cyber security exercise schedule with your programs for prevention, detection, and defence of cyber incidents.
4. After every cyber security exercise—whether your own test or mandated by SOCI—ensure you appropriately address gaps in your incident response preparedness.

Vulnerability assessments

SOCI Part 2C, Sections 30CU-DA cover requirements for vulnerability assessments. The Act allows the Secretary to request a vulnerability assessment of a critical system using one or more cyber security vulnerability testing activities.

During these activities, it is crucial that the responsible entity consider identity security.

Vulnerabilities and misconfigurations of AD and Entra ID are a significant source of exposure for lateral movement and privilege escalations. In its 2024 threat report, Splunk[18] noted that **47%** of reported cyber security incidents were attributed to identity management attacks. Microsoft sees **600 million attacks a day** against the Entra ID identity infrastructure, and they suspended nearly 64 million abusive administrative accounts in 2023.[19] And in the Semperis 2025 Ransomware Risk Report,[20] 83% of organisations in Australia and New Zealand reported being targeted by ransomware in the previous 12 months; of those **93% said the attack compromised their identity infrastructure**.

When a vulnerability assessment is required, the entity responsible for the SoNS must arrange for the assessment to:

- Specifically relate to the SoNS
- Address vulnerabilities for all types of cyber security incidents
- Be completed within a specified timeframe

Proactively performing regular vulnerability assessments—rather than only on demand—enables you to perform ongoing mitigation activities and reduce potential exposure and risk.

18 Splunk | State of Security 2024
19 Microsoft Digital Defense Report 2024
20 Ransomware Risk Report | Semperis

Actions for vulnerability assessment

1. Map the core services that support your critical systems.
2. Where identity systems are a part of these services, establish a mechanism to automatically identify and prioritise vulnerabilities.
3. Establish an operational procedure to systematically remediate vulnerabilities.

Identity systems and internal controls

The following discussion provides an overview of the controls to consider from the frameworks referenced in the Guidance for the Critical Infrastructure Risk Management Program.[21] The guidance document encourages responsible entities to develop their critical infrastructure risk management program by referring to internationally recognised standards and frameworks, including:

- Australian Standard AS ISO.IEC 27001:2015
- Essential Eight Maturity Model published by the Australian Signals Directorate
- Framework for Improving Critical Infrastructure Cybersecurity published by the National Institute of Standards and Technology of the United States
- Cybersecurity Capability Maturity Model published by the U.S. Department of Energy
- The 2020-21 AESCSF Framework Core published by Australian Energy Market
- Operator Limited (ACN 072 010 327)

Each of these standards incorporates some focus on identity and access management because identity remains a primary threat vector for organised crime and nation-state sponsored cyber attackers.

For your cyber security program to be effective, you should harden your identity systems, ensure optimal threat and vulnerability detection, and optimise your ability to perform forensic analysis after an incident.

21 Guidance for the Critical Infrastructure Risk Management Program

Actions to establish a robust program of identity and access management

1. Implement a least-privilege access model.
2. Implement just-in-time and privileged access management principles to safeguard your most sensitive accesses (aka **Tier 0 for Active Directory**).
3. Review the Entra ID Connect synchronisation rules to be sure proper segregation of access exists between AD and Entra ID and only the necessary principals are synchronised.
4. Execute active red teaming or incident response tabletop exercises and ensure the identity infrastructure is in scope.
5. Invest in automated monitoring, detection, and remediation for the identity infrastructure.

Identity system recovery is critical

To achieve meaningful operational resilience against cyber incidents, you will need to make sure you can recover to a secure state and in a timely manner in case of an outage or breach.

In 2020 and 2024, ASX had issues with its settlement system, causing outages for brokers. The 2020 issue pertained to incorrect order identification numbers causing market closures for a whole day.[22] In December 2024, an outage shut down trading on a Friday and took an entire weekend to resolve. The resulting extended investigation revealed a vulnerability that had been lurking in the identity system for a decade.[23]

The threat of destructive events has linked information security and operational resilience. In 2024 the NCC Group tracked 94 criminal groups leveraging destructive capabilities to hold organisations to ransom. Organizations that aren't prepared for such threats at best face a costly and time-consuming recovery; at worst, a total rebuild from scratch of essential services.[24]

Overcoming blocks to timely identity recovery

Your identity infrastructure is key for the availability of most, if not all, digitally enabled services. Without a disaster recovery plan for AD and Entra ID, you are unlikely to be able to restore your overall services from a major destructive event.

Because AD is a core foundation of myriad technology-enabled services, restoring it after an incident is time consuming and high risk for complex and large organisations. And because AD infrastructure is highly complex and includes many interdependencies, legacy identity systems can be notoriously difficult to restore to a *known* secure state.[25] The official Microsoft guidance details the process to restore a single AD forest—requiring 28 steps covered in a 150-page document—during which even a slight deviation will curtail a successful recovery.

---

22 Nasdaq has 'full attention and resources' on ASX outage
23 ASX faces ASIC, Reserve Bank blowtorch over December settlement outage
24 NCC Group releases Annual Cyber Threat Monitor Report 2024 | NCC Group
25 Top Manual AD Forest Recovery Pitfalls | Semperis Guides

For many organisations, recovery is further complicated because of other services (such as DHCP and DNS) running on AD, hybrid cloud and on-premises integrations, and the sheer number of changes that occur daily in a large AD forest.

Depending on backup frequency, *AD backups may also be compromised*. Thus, once an AD forest is recovered, it still cannot be trusted for use without extensive forensic analysis to remove persistence mechanisms that enable the attacker to retain a footprint.

A well-developed disaster recovery plan includes mechanisms for avoiding these onerous and devastating recovery delays, including:

- Frequent, immutable identity system backups
- Automated and timely AD forest recovery
- Thorough and rapid post-incident forensics

Actions to ensure robust recovery capabilities for your critical identity systems

1. Define a plan for identity infrastructure recovery, including defining the roles and tasks of specific team members.
2. Confirm measures to ensure clean-state AD recovery, including immutable backups.
3. Establish a live-like test environment and perform frequent testing of your restore process.
4. Ensure disaster recovery activities are implemented and integrated with broader business continuity and crisis management plans and exercises.

Tool specialisation

The SOCI Act provides high-level guidance for resilient operation of critical infrastructure assets. Our assertion is that for any such asset, automation is essential for security assessments, vulnerability and threat management, incident response, and recovery of key identity systems.

Internal IT and security teams rarely have the skills or capacity to manage the risk of compromise and destructive events, nor are they typically able to ensure recovery if the worst should happen. Specialised toolsets purposely designed to secure identity systems will allow you and your organisation to shift focus from day-to-day security operations to a strategic focus.

In addition, unifying your people, technology, and processes with a centralised, out-of-band crisis management platform can empower you to quickly and efficiently implement policies and procedures to keep your identity systems—and operations—resilient, even when the worst happens.

How can Semperis help?

Consider evaluating solutions purpose-built for identity security, such as those from Semperis. Semperis offers both community and commercial enterprise solutions that directly address the challenges of complying with the SOCI Act.

Semperis' products are enhanced by deep research from the experts in their identity security and AD-focused security research team.

Challenge	How Semperis can help	Solution
Risk management Knowing your assets and their risks, vulnerabilities, and possible exposures is key to achieving a truly resilient enterprise.	• Map threat and vulnerability indicators in AD and Entra ID. • Provide visibility into identity security posture. • Deliver semi-automated, research-led view of software vulnerabilities and misconfigurations. • Provide ongoing risk identification and management.	• Security Assessment services provide a clear view of identity and operational security posture and guidance for addressing security exposures at the strategic, operational, and tactical levels. • Purple Knight (no-cost community tool) provides point-in-time security assessment of AD that empowers you to understand vulnerabilities and delivers remediation guidance to help you reduce risks in your identity system. • Directory Services Protector (DSP) provides continuous threat and vulnerability detection and automated rollback of risky and malicious changes. • DSP provides comprehensive logging and highly specialised AD and Entra ID threat analysis, enabling up-to-date and industry leading insights and enrichment of security operations centre visibility through SIEM integration.

Challenge	How Semperis can help	Solution
Incident response and reporting SOCI imposes strict incident response and reporting requirements on operators of critical infrastructure.	• Secure your logs for forensic analysis. • Enhance ability to detect actions of a malicious actor and rapidly report incidents and attacks impacting AD and Entra ID.	• DSP provides continuous threat and vulnerability detection and automated rollback of risky and malicious changes. • Identity Runtime Protection uses machine learning to perform attack pattern detection by capturing, analysing, and correlating AD user activities with Semperis' identity threat intelligence to signal malicious behaviour. • Active Directory Forest Recovery (ADFR) can map and automate forest recovery, including relevant dependencies. • ADFR also allows for post-breach forensics to identify persistence, recover AD to a trusted state, and enable timely reporting. • Ready1 centralises and unifies all aspects of cyber crisis planning and incident response, ensuring seamless crisis response through preparation, collaboration, and enterprise-wide communications.
Cyber security exercises Compliance with SOCI requires a strong capability to avoid adverse findings in testing and rapidly address existing vulnerabilities and misconfigurations.	• Before the exercise, remediate critical vulnerabilities in your identity infrastructure. • Provision a realistic test environment. • Operationalize proven crisis and incident response frameworks, enhanced with expert playbooks—from preparation to after-action review. • Address test findings after the exercise.	• DSP enables continuous monitoring of AD and Entra ID security posture, ensuring the underlying identity systems are secure and trustworthy. • Ready1 centralises crisis response in a unified, out-of-band platform, enabling teams to develop, test, remediate, and continuously improve incident response planning. • ADFR allows for post-breach forensics to identify persistence and recover AD to a trusted state.

Challenge	How Semperis can help	Solution
Vulnerability assessment Your identity infrastructure is a rich source of vulnerabilities and misconfiguration, requiring skill and dedication for meaningful detection.	• Provide AD and Entra ID monitoring to identify and eradicate misconfigurations and vulnerabilities. • Comprehensively control the constantly changing AD environment with its rich attack surface. • Provide visibility into AD-focused attacks and changing vulnerabilities.	• Purple Knight provides point-in-time security assessment of AD. • Forest Druid (no-cost community tool) discovers and automatically maps attack paths to Tier 0 assets and helps identify excessive privileges that attackers can exploit. • DSP provides continuous threat and vulnerability detection, capturing every change made in AD, helping identify malicious changes, and automatically rolling back risky changes. • DSP provides comprehensive logging and highly specialised AD and Entra ID threat analysis, enabling up-to-date and industry leading insights and enrichment of security operations centre visibility through SIEM integration.
Identity & Access Management Establishing strong controls helps you ensure robust identity and technology resilience.	• Enable rapid restore in case of an outage to enable teams to continue working securely. • Map dependencies to understand attack paths leading to administrative access and enable AD restore. • Provide privileged access management and identity and access management for all users. • Enhance protections for identity security capabilities, including attack prevention and post attack recovery.	• ADFR reduces the time for a full AD forest restore by 90% compared to manual recovery. • ADFR can map and automate forest recovery, including relevant dependencies. • DSP enables continuous monitoring of AD and Entra ID security posture, ensuring the underlying identity systems are secure and trustworthy. • Forest Druid supports identity teams in mapping attack paths automatically.

Challenge	How Semperis can help	Solution
Identity system restore For risk reduction under your SOCI program, you need to be able to restore your identity system capabilities rapidly, to a known clean state—and have testing that proves you can.	• Enable early detection or avoidance of a security breach of your identity system and dependent technology-enabled services. • Provide proven, clean-state restore with validated recovery objectives. • Operationalize proven crisis and incident response frameworks, enhanced with expert playbooks—from preparation to after-action review.	• ADFR automates forest recovery, restoring AD quickly and safely without reintroducing malware. • ADFR also allows for post-breach forensics to identify persistence and recover AD to a trusted state. • Disaster Recovery for Entra Tenant (DRET) recovers Entra ID objects. • Ready1 centralises crisis response, enabling teams to develop, test, remediate, and continuously improve incident response planning.

Conclusion

The SOCI Act applies to various critical industries in Australia, focusing on strong risk management, the ability to respond to cyber security incidents, and resilience of critical infrastructure.

To comply with the regulation, we recommend you establish six major capabilities for the resilience of your identity infrastructure, including:

1. Establish governance and ownership for your identity system.
2. Build visibility to risks and dependencies.
3. Establish comprehensive and automated exposure, threat, and vulnerability monitoring and integrate these capabilities into your security operations centre.
4. Reduce identity system vulnerabilities to reduce the attack surface for penetration testers and attackers alike.
5. Build robust incident response capabilities that enable rapid identity and operational recovery, incident reporting, and forensic capabilities.
6. Have an automated and tested recovery process to enable rapid restoration of the identity infrastructure in case of a destructive incident.

In our experience, achieving these capabilities is challenging. Sustaining them over time is not possible without significant automation. Semperis market-leading products and services can provide you with this threat-led, automated capability.