Industrial Cyber Security Playbook

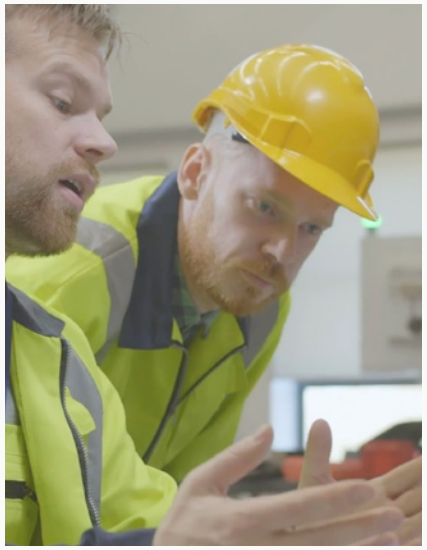
Tips for building a united defence

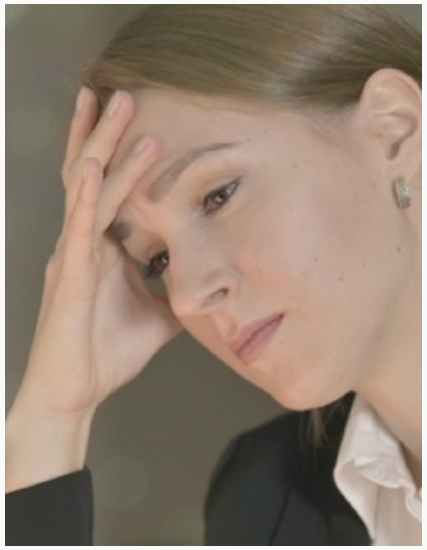
SiS Industrial Cyber Security

Contents

Section 01

Introduction





Breaches in the security of operational technology (OT) – the hardware and software used to drive industrial processes – are increasing in frequency with every given year.

And yet, breaches of this particular nature continue to be among the greatest, most overlooked threats[1] looming over global infrastructure and the safety of communities at large.

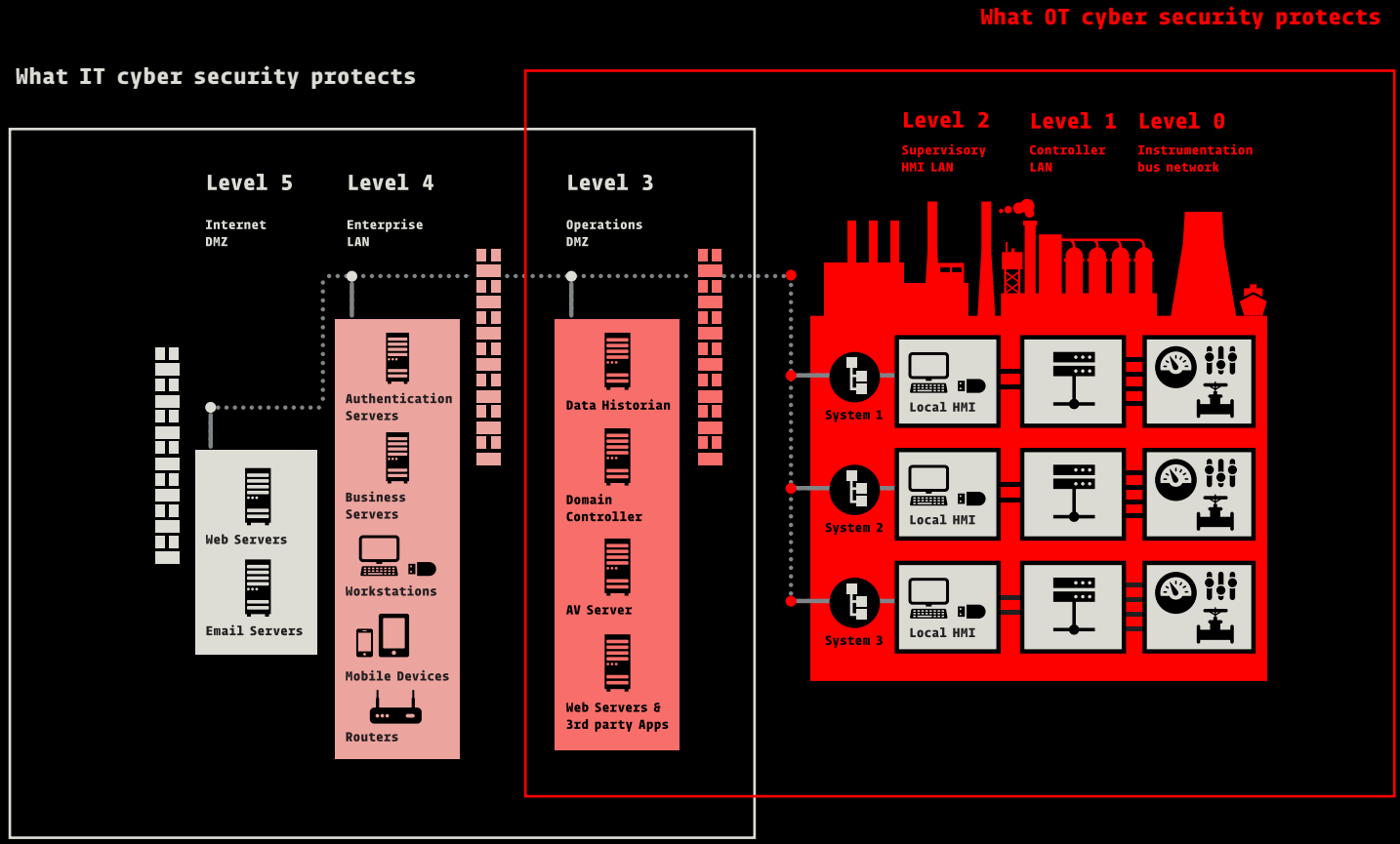
This playbook is our contribution to educating industry as much as possible concerning OT security in 2022. In the following chapters, we put forward steps for taking an effective, holistic approach to OT security using an Assess & Define, Design & Implement and Operate & Maintain model with the specialised knowledge available to us.

We also explain an element in the OT security playbook that we often feel is overlooked – people.

Here at SIS, our work is 100% focused on securing OT, so we're acutely aware of the gravity of the state of play across the world. We'd like to present a positive example moving forward for better protection of critical infrastructure.

1. The Biggest Cybersecurity Threats That More People Should Be Talking About: Industrial Hacking And Hijacking (Forbes)

IT vs OT Cyber Security



100% of our work is focused on securing OT

Section 02

2022: The OT security situation at a glance

“There are two types of companies: those that have been hacked, and those who don’t know they have been hacked” [1]

People with their eyes on the OT security landscape recently would have noticed an escalation in threats and, along with that, an increase in more successful attacks following on from those threats. Such a trend coincides with an overall reduction of budgets funnelled into OT security due to competing priorities from COVID, which SIS believes has contributed to this upsurge in industrial cyber threats and resulting incidents.

The US Federal Bureau of Investigation’s (FBI) Internet Crime Complaint Center (IC3) says it received 649 complaints of ransomware attacks targeting critical infrastructure organisations in 2021.[2] Echoing this trend worldwide, India’s critical infrastructure witnessed a 70% jump in ransomware attacks last year as well.

According to threat research lab Trellix, the final quarter of last year saw increased cyber activity targeting sectors essential to the function of society worldwide. Transportation and shipping were the target of 27% of all advanced persistent threat (APT); healthcare was the second most targeted sector, bearing 12% of total detections; and from Q3 to Q4 2021 threats to manufacturing increased 100%.[3]

In Australia, the Australian Cyber Security Centre observed ransomware continuing to target organisations of all sizes, including critical services and ‘big game’, throughout 2021.[4] This reflected the warning made in late 2020 from the then Home Affairs Minister, Peter Dutton, which highlighted a potential serious penetration of Australia’s energy sector leading to “widespread failure” of electricity networks, hospitals, transport, banking and food supplies. Furthermore, soon after his warning, the Federal Government announced updates to Australia’s Critical Infrastructure Bill, which seeks to mandate compliance of cyber security requirements for operators of critical infrastructure.

In the words of the Australian Federal Government: [5]
“Critical infrastructure is increasingly interconnected and interdependent. Connectivity without proper safeguards creates significant vulnerabilities. Interconnectedness means that compromise of one critical infrastructure asset can have a domino effect that degrades or disrupts others and results in cascading consequences across Australia’s economy and national security.”

With remote workplaces and remote access becoming our ‘new normal’, attacks on our infrastructure are sure to intensify, which is why implementing a playbook for vastly improved OT security is imperative for anyone responsible for infrastructure.

1. John T. Chambers, former executive chairman and CEO, Cisco Systems
2. FBI: 649 Ransomware Attacks Reported on Critical Infrastructure Organizations in 2021 (Security Week)
3. ‘Attacks on critical infrastructure continue - Trellix report (Security Brief Asia)
4. 2021 Trends Show Increased Globalized Threat of Ransomware (Australian Cyber Security Centre)
5 Australian Government, Department of Home Affairs

Case Study

The Florida fiasco

A high-profile case in point occurred at the beginning of 2021 when a Florida water treatment plant in the USA fell victim to a cyber attacker who sought to poison the city's water supply.

The attacker gained remote access to the computer that controlled the plant's infrastructure, increasing the amount of sodium hydroxide (lye) in the water supply by a factor of 100-fold. If the tampering had gone unnoticed, such an attack would have resulted in widespread severe illnesses and deaths.

Investigations into the breach revealed not so much the attacker's shrewdness but the shortcomings of the security systems (or lack thereof) protecting the water treatment plant's critical infrastructure. An official investigating the breach stated: [1]

"The cyber actors likely accessed the system by exploiting cyber security weaknesses including poor password security, and an outdated Windows 7 operating system to compromise software used to remotely manage water treatment. The actor also likely used the desktop sharing software TeamViewer to gain unauthorized access to the system."

The Florida example demonstrates that lax processes around operational security can have serious consequences. It also underscores how IT and OT security need to be approached differently while complementing each other, without being unreasonably lumped in the same category of responsibility (which is more often than not the case).

1 GOT SECURITY? Breached water plant employees used the same TeamViewer password and no firewall (ARS Technica)

Section 03

The obstacles to better OT security

“Cybercrime is big business. Attackers only need to be successful once. Defenders need to be successful all the time.” [1]

Considering the current situation, the practical question to ask is: why aren’t industrial organisations concentrating more on securing operational technology?

With threats constantly evolving and hackers learning more sophisticated methods for infiltrating OT, it can be difficult for organisations to keep pace of processes required to stem attacks. This is one of the reasons why external experts in OT security – those people, like SIS, who specialise in keeping abreast of such threats – are in high demand.

But, undoubtedly, one of the greatest obstacles to vastly improved OT security is that organisations just don’t know what they don’t know. Not understanding the threat to operational technology from cyber adversaries (based internationally or otherwise), how this threat can be curbed and the potential damage it can do to any given organisation and, by extension, to the broader community is preventing better OT security globally.

Generally, we see this presenting itself in the following ways:

- Company budgets channelled incorrectly [2] (e.g. into IT, with OT considered only as a passing gesture) or almost non-existent. Without the funds to support OT security, systems are subjected to a set-and-forget approach, which fails to acknowledge the sophistication of threat adversary skills and the evolution of their tactics. The paradox here is that operational technology is where the profits lie, and yet OT continues to receive the smaller slice of the funding pie when it comes to cyber security.
- Insufficient application of OT security standards – the number of compliance standards available internationally to help guide companies with practices for thwarting cyber threats is well-intentioned but unfortunately contributes to industry confusion. Application of these standards needs to be deciphered by OT security experts to get it right.
- Legacy systems being layered with new technology – this creates a technology stack that is outdated and likely to topple under pressure. Obsolete or unpatched software configurations can become hidden within this stack, making OT vulnerable to hackers who are looking for these ‘weak links’. Additionally, relying on proprietary devices and protocols from multiple vendors can produce a similar scenario.

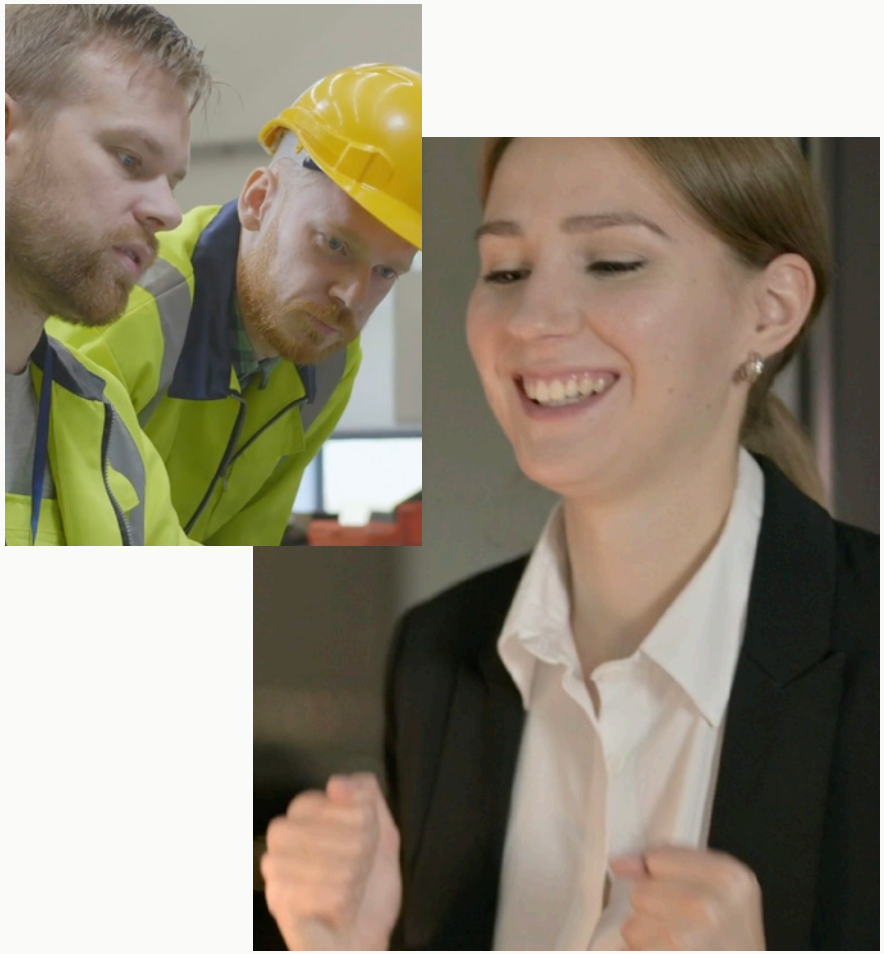
1. Tania Fryer, Director, City West Water
2. How to spend wisely when it comes to OT security (SIS Insight)

- Failure to accordingly monitor OT assets on an ongoing basis – if you're not monitoring properly, you're running blind when it comes to rating performance and detecting unexpected or unauthorised activity in your plant. Such monitoring demands a specialised approach because, unlike IT, OT assets cannot be easily turned off for important system checks and upgrades.
- Unintentional incidents due to human error – not all cyber security incidents are nefarious; in fact, many can be attributed to basic human error from employees who may have experienced a lapse in judgement or been lumped with responsibility outside their capabilities. The Colonial Pipeline incident [1] is one example of where poor cyber hygiene in the form of leaked passwords and dormant accounts took down the largest fuel pipeline in the US. Errors can be circumvented if there are checks and balances put in place, as well as the facilitation of cross-organisational skills and communications.
- A breakdown in the relationship between IT and OT [2] – those working in each of these corresponding departments need to communicate properly and understand their (sometimes) competing priorities to foster a collective approach to the cyber security of the organisation at large. When IT and OT work in silos, or one imposes a process on the other, cyber vulnerabilities emerge. Employees may wear 'different uniforms' (corporate versus plant/operational) but everyone in any given organisation is playing for the same team.
- Only by organisations understanding and acknowledging gaps in operational technology security will they be capable of building fortitude against cyber threats. Accepting that you don't know what you don't know – and getting help from those who really do – is a powerful position for your organisation to adopt.
- Similarly, understanding how people power can elevate your OT security is an important detail in your playbook. It is the missing ingredient for turning your cyber security team into a formidable opponent.

1. Colonial Pipeline attack: Everything you need to know (ZDnet)
2. Why people could be the secret ingredient in your industrial cyber security recipe (SIS Insight)

Section 04

Creating a Winning OT Security Team



The model for better operational technology security may sound highly technical but there is a secret tactic that underpins every aspect in this approach: people.[1]

We've all heard the old adage that 'a computer is only as good as the person operating it', so to say that people could be the secret to protecting your OT is anything but a revolutionary concept. Yet, despite the acceptance of this wisdom in our modern parlance, many of us frequently forget to apply it in our daily business operations.

When it comes to OT security, organisations are just as guilty of this folly, if not more so. The very nature of OT security – especially given 'technology' is one of two words in this acronym – is the application of technology to mitigate risk and secure your industrial assets. Despite technology being the lynchpin in the equation, in our experience, we've found that getting OT security to work properly tends not to fall with the technology itself, but with a schism between expectation, expertise and the people in any given organisation.

1. Why people could be the secret ingredient in your industrial cyber security recipe (SIS Insight)

To forge ahead, IT teams need to work alongside OT engineers to ensure a deep understanding and appreciation of what they are protecting, and how to protect these assets without disrupting production. This IT/OT collaboration will only be successful if both sides have something to gain in terms of their job roles, and if they have visibility and understanding of where the other team members are positioned.

Building a united team requires addressing the requirements of everyone and fostering true collaboration, which can be as simple as equipping both IT and OT with insight into their differing responsibilities and creating a KPI matrix that identifies them as working towards the same goal (or, the very least, understanding what each other does and where their motivations in their daily responsibilities lie).

By recognising that IT and OT personnel function differently in their roles and attitudes, you're taking the first positive step in correcting a potential flaw in your IT/OT playbook. Regardless of other differences, your IT and OT talents will be motivated by a common objective: to protect the company. This common outcome is where you can bring the two together through appropriate training and team reprogramming.

You don't know what you don't know

Make it that you do know by investing in the right training for giving you the know-how to protect your operational technology. Stakeholders in charge of critical infrastructure, engineers, developers/project managers and ICT professionals can all play a monumental role in minimising risk at any given organisation by:

- Learning a proven methodology that can be applied across your plant environment
- Getting hands-on experience attacking and defending
- Understanding elements of the Threat Neutralisation Cycle (see page 17)

You can only be trained effectively if you are instructed by specialists in OT security; those who make it their business to be across innovative practices and developments in cyber security in the critical infrastructure space.

Never underestimate the importance of getting the people formula and people skills aligned properly. Because, in the end, people are the ones invested in operational technology and the ones who ultimately suffer when things go wrong.

Section 05

The Playbook for Vastly Improved OT Security

“End users often think they know what they’re doing but their security methodology isn’t refined enough. When you’re trying to do things in-house, you often don’t have the necessary resources for success.” [1]

There are multiple standards or methodologies that can be applied to companies for protecting their operational technology, and a mix of all of them provides the greatest value.

Organisations often look for that elusive ‘silver bullet’ but the truth is no one-size-fits-all method exists. Once you fully appreciate this, and the specialities required to protect your plant’s most precious assets, you’re in a strong position to ensure your OT is as secured as it can possibly be.

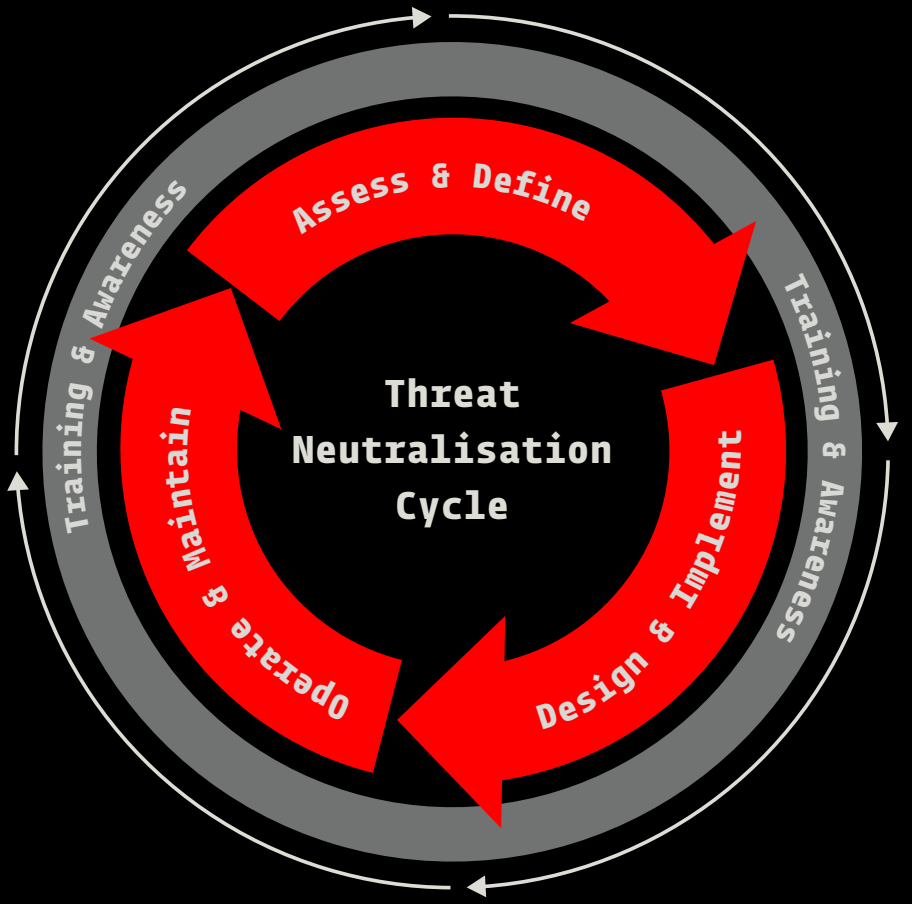
1. Dr Christopher Beggs, Founder & Principal, SIS Industrial Cyber Security

As specialists in the OT security field, SIS applies bespoke methodologies to our clients' operations. However, we do so with a Threat Neutralisation Cycle in mind:

- Assess & Define
- Design & Implement
- Operate & Maintain

Before we proceed: It's extremely important to note that a winning team is the common denominator that underpins every point in the Threat Neutralisation Cycle. The human component is the glue that binds, creating the understanding of both IT and OT business requirements at every point in the cycle.

Let's explain some more...



1.

Assess & define

Critical systems, processes and procedures already in place at any given organisation need to be assessed first as part of an asset inventory, before anything else. Only after this step can vulnerabilities and gaps be identified and benchmarked against industry standards for risk mitigation.

To apply systems, processes and procedures without this initial assessment can be compared to building a house without laying the proper foundations – it will eventually fall over, if not straight away.

Consider the overlapping and competing business demands of the IT and OT functions of your organisation by applying holistic approach across all levels of OT system functions for identifying cross-over and conflict. Via this process, you will identify the corporate interfaces that feed into your OT systems.

Steps for Assess & Define include:

- Site survey and asset inventory
- Technical vulnerability assessment and security testing including red/blue teaming and purple teams.
- Health check, gap analysis and maturity assessments, benchmarked to leading industrial cyber security standards

The People Part:

Cross-disciplinary subject matter experts to provide transparency into corporate and OT priorities and requirements.

2.

Design & Implement

An OT secure architecture needs to be designed specifically for any given plant by specialists who know how to capture requirements for secure by design, and to install and configure security products and technologies. These specialists can act as the link between your corporate and operational teams, laying the groundwork for cross-organisational collaboration now and into the future.

Cookie-cutter approaches to architecture fail to consider the eccentricities of an organisation, which leaves cracks in both the architectural framework itself and the relationships in the company that infiltrators can then exploit.

You design the architecture so IT can interweave with OT and assist with the delivery of systems into your OT services.

Steps for Design & Implement include:

- Establishment of cyber security requirement specifications
- Design of security architecture
- Security zone and conduit modelling constructs
- Design of infrastructure layouts and security platforms
- Design of implementation plans and transition-state architectures
- Test plan (FAT and SAT) development and execution
- Installation and configuration of OT security products and technologies

The People Part:

Creating the architecture can be a common goal that both IT and OT can understand, working together towards a mutually attainable and satisfying outcome. Centralising and removing silos assists in bringing people together, and the viability of the undertaking (i.e., project of great value) builds unison and morale of the team.

3.

Operate & Maintain

Defining the operational requirements to maintain key security services – such as security monitoring, patch management, change management and backup and recovery procedures – is key to the ongoing protection of assets. Such operational activities form the key pillar of any Cyber Security Management Systems (CSMS).

A fully dedicated OT SOC (Security Operations Centre) is the best means for protecting complex industrial networks from the growing threat of cyber attack, with 24/7 monitoring to detect and response to potential attacks. This can only be truly achieved by engaging the skills of a specialised partner in enhanced OT SOC services.

Steps for Operate & Maintain include:

- Development of Cyber Security Management Systems (CSMS)
- OT-SOC-security monitoring managed services
- Incident response managed services
- Vulnerability/patch management managed services
- Cyber forensics
- Audit and compliance assessments
- Device robustness testing and assurance

The People Part:

Resources from both IT and OT are supporting architecture controls, which means your people get to work together to ensure security systems are functioning correctly and effectively. As part of the process, there's an opportunity to up-skill across the organisation – monitoring OT threats requires OT experience (note: respect your engineers).

By engaging in training, you can create a level playing field – everyone knows the same terminologies, the same acronyms; everyone is speaking the same language.

Case Study

A SIS success story

Precious Partnership

SIS had been working with a base and precious metals mining company when they identified an opportunity to help them benefit from better cyber visibility into their production capabilities. Given this company's round-the-clock operations, any halt to production – no matter how minimal – could potentially cost them millions of dollars, so protecting their infrastructure should be top of mind.

An important player in the resources sector, the company had lacked the necessary in-house skills to fully protect and monitor their OT effectively. Management recognised that outsourcing these highly specialist skills could prove a far more efficient, cost-effective and timely alternative to solely skilling up internally or rolling the dice and leaving their assets vulnerable to external threats and even human error.

By agreeing to engage SIS for their managed security services, they have been delivered a refined methodology for securing the monitoring of their OT assets, presented to them in a language that has spoken to both their IT and OT teams. This cross-departmental approach by SIS has captured stakeholder buy-in, united the company as a team and consolidated their position of cyber strength.

From security monitoring design through to implementation of OT-Security Operations Centre (SOC) wholly managed by SIS, this mining company is now actively protected through monitoring, vulnerability management, file integrity monitoring, detection, and alerting and analysis of threats and events targeting their OT systems and devices.

SIS continues to protect their operation technology on an ongoing basis and provide greater visibility into OT cyber threats.

We help OT and IT come together as a united cyber security team.

About SIS

Founded by Dr Christopher Beggs, SIS comprises an elite team of industrial cyber security specialists. 100% of our work is on Operational Technology (ICS/SCADA). This laser-like focus keeps us in front of current and developing cyber threats.

Our services are delivered through a combination of consulting, managed services and training.

Please contact us to discuss your specific OT cyber security requirements.

Phone: +61 1300 071 261
Email: info@sis-ics.com