6 August 2021

Operational Technology:
An intelligence-driven approach to cyber resilience

Defending the operational technology of the future

Snode

INSIGX
RISK SOLUTIONS

Table of contents

Introduction

From power grids and pipelines to water supply networks and heavy industrials such as mines and manufacturing, operational technology (OT) is central to the streamlined functioning of society.

Much of the OT systems utilised in the public and private sector today has been designed to be perimeter protected - or air gapped - from lost networks. However, these systems are becoming increasingly integrated and interconnected with IT. While digitalisation, automation and Internet of Things (IoT) devices are driving operational efficiencies, increased connectivity within OT systems has exponentially expanded the threat surface (High, 2020). Digital transformation and the advent and adoption of the Fourth Industrial Revolution (4IR) has increased the risk of ageing, legacy infrastructure being connected to the internet - both directly and indirectly. Disparities in cyber security between OT and IT systems, paired with the ever-evolving attack methods by threat actors, means that the consequences of a security breach could be far-reaching and costly.

The nature of OT attacks

While cyber defenders have traditionally concentrated on threats to organisations' IT networks, the real threat to critical infrastructure operators are their complex OT systems (Cohen, 2021). These OT attacks typically form two primary paths. The first is executed by leveraging unprotected systems with direct internet connectivity; the second entails placing an implant on the enterprise IT network through phishing or waterholing, and the attacker then pivots through credentialed access into the OT environment (Ross, 2021). Threat actors manipulate IT to compromise OT, or conversely compromise inadequately secured OT and IoT to access enterprise networks and data.

Critical infrastructure under siege

The frequency and sophistication of cyberattacks in 2021 alone has demonstrated just how insecure critical infrastructure could be to potential compromise, and what the catastrophic consequences of a sabotaged OT system could hold for civilians, corporations, and state.

Oil operations offline

In May 2021, America's Colonial Pipeline was forced to shut down more than 8 000 kilometres of pipeline after falling prey to a ransomware attack. The criminal group responsible threatened to hold data hostage until a ransom was paid. As a precautionary measure, the company halted the pipeline itself for fear that the attackers may have accessed information that would enable them to compromise susceptible parts of the pipeline (Sanger, Krauss & Perlroth, 2021). This vital pipeline transports around 45% of the East Coast's fuel supplies. The Colonial Pipeline's shutdown lasted for six days, which caused American citizens to panic-buy fuel and gas prices breached $3 per gallon for the first time in seven years (Chiwaya, 2021).

The Colonial Pipeline attack occurred because of a single compromised account that was not disabled in a timely manner. Poor password configuration controls allowed hackers to gain entry through a virtual private network account, which allowed employees to remotely access the company's systems. The account was no longer in use at the time of the attack but was still active and could still be used to access the network. The account's password was discovered inside a batch of leaked passwords on the dark web, with one employee having used that same password on a previously hacked account.

Water source sabotage

In February 2021, the town of Oldsmar in Florida fell victim to an attempted mass casualty terrorist attack. An attacker infiltrated the town's water treatment plant in an attempt to poison the water supply by increasing the amount of sodium hydroxide in the water to toxic levels (Cohen, 2021). Before any damage could be done, a plant operator noticed that a remote hacker was clicking through the water treatment plant's system controls and quickly reverted the dangerous water reading to normal. Upon investigation, it became evident that a hacker compromised the plant's TeamViewer software to gain remote access to the computer (Greenberg, 2021). While the poison would have taken up to three days to reach Oldsmar's civilians, and automated pH monitoring safeguards would have alerted the plant to the danger, the insidious intent behind the attack demonstrates the scale of threat should critical infrastructure be compromised.

It was later reported that the incident was 'very likely' caused by a disgruntled ex-employee. A supervisor working remotely had a weak password. The attacker was able to leverage this weakness, take control of the system, and increase the sodium hydroxide level beyond the safe limit.

Mining at risk

Automation- and AI-driven operations are gaining momentum in the mining sector, from remote-operated machinery, autonomous vehicles to digital field mapping. The benefits to mining through 4IR is vast, digitised operations must be built on a foundation of comprehensive and proactive cyber security to combat the same risks faced by critical infrastructure (Burgess, 2020). In the realm of mining, mine operators must be able to proactively detect, respond to and remediate potential risks lest they disrupt business operations, damage machinery, endanger workers or harm the environment. Cyber espionage through nation-sponsored threat actors is also a critical risk. From intellectual property such as extraction and processing technology used, business strategy and pricing of commodities to restricted information on the location and value of natural deposits, unsolicited access to this information may be used as a competitive advantage or leverage in negotiations (High, 2020). The mining sector is dependent on third-party services such as equipment assembly or maintenance to streamline their processes. As these vendors engage so closely with the internal operations environment, they may present an avenue for cyberattacks if not sufficiently vetted. A third-party vendor could create an entryway for malicious software to penetrate IT systems, or create system vulnerabilities through weak credentials (High, 2020). The convergence of OT and IT and ever-evolving digitisation will continue to propel mining operations into the future; as such, cyber security should advance at the same pace to ensure mines are actively defended.

The need for proactive and holistic cyber security

Traditional approaches are no longer sufficient to secure OT infrastructure from imminent cyber threats. As a cyberattack on OT could have potentially devastating real-world repercussions, such as financial loss, threat to human lives, environmental harm, or even complete corporate shutdown, it is necessary that industrial processes and operations are defended through resilient, proactive cyber security posture to combat growing risks. A robust framework can bridge the gaps, including those of human error.

The human factor - at risk from within

Year-on-year, human error is cited as the primary factor for increasing cyber incidents. Against the backdrop of a complex and ever-evolving cyber threat landscape, employees are too often unknowingly placing the businesses they work for at risk. One human mistake can easily compromise the most well-designed, implemented and effective technical controls.

But human error can only occur where there is an opportunity for it to do so. Humans are, by our inherent nature, curious. This curiosity can lend itself to vulnerability, where attackers, through social engineering, orchestrate attacks.

Organisations need to reduce the opportunities systematically using technology, cultivating continuous employee awareness and policy enforcement. Mitigating human error begins with:

- Creating an understanding of risk where employees are aware and mindful of the impact of their activities
- Continuous training and education for employees to adopt critical thinking e.g., how to identify and respond to a suspicious email or attachment
- Creating a feedback loop which tests the effectiveness of an organisation’s training methodologies. Investing in the right solutions will allow for continuous engagement to proactively respond to human risk factors

While traditional cyber security training enables the general awareness across the organisation, this is arguably no longer enough. A more effective cyber security training and awareness programme incorporates data points to target employees based on their needs and risk. To better understand the needs and risk of employees, organisations should have greater insight into:

- HOW employees feel about cyber security. The use of sentiment analysis, through focused initiatives, will assist the organisation to identify groups of those employees that have a negative perception of cyber security
- WHAT employees will do when a breach occurs. By running periodic phishing and attack simulations, organisations will gain an understanding of how employees will respond, should an actual incident or breach take place

Snode Technologies’ and Insiox’s industry-leading OT solutions

Snode Technologies assisted a South African mining company, with a global footprint, to become the first ISO27001-certified mine. As such, Snode's defence capabilities are uniquely positioned to proactively detect, monitor, respond to and remediate threats. The Snode Guardian platform provides you with a “single source of truth” by seamlessly integrating into your key data sources and providing you with a consolidated, interactive dashboard coupled with real-time contextual alerting that enables an analyst to proactively respond to all threats in your network.

This capability leverages the following three core pillars:

- Data fusion: Regardless of the source of format of the data; Guardian handles it all by simplifying it down to one common denominator; numbers. These numbers can then be processed on a petabyte scale allowing for real-time detection and response
- Data visualisation: Visualisation is a crucial element that allows clients to easily view and manage the massive volumes of data that is created each day. It allows an analyst to have a complete and concise overview of all activity in real time, to interact with the data at any level as well as providing them with the ability to identify anomalous behaviour that would previously have been impossible to identify
- Data analytics: The use of tailored mathematical algorithms to recognise patterns of behaviour, specifically precursors to events, allows Guardian to predict potential risk exposure, activity and notable incidents. As a result, predictive analytics empowers clients to become more proactive in their decision-making process and to anticipate potential outcomes

Benefits:

Single source of truth
Providing you with a single view across complex heterogenous network architectures

Machine-assisted predictive analytics
To amplify your response capabilities through rapid and real-time responses to pre-indicators of an attack

Rapid development with zero integration risks
Customisable to bespoke cyber needs with no integration risk to current infrastructure

Real-time threat detection and response
Access to a team of trained cyber analysts actively threat hunting for new threats within your business environment on a 24/7/365 basis

Contextual alerting
Detailed remediation advice to expedite remediation efforts

In this way, you’re able to control:

- Unauthorised hardware and software detection
- Unauthorised administrative privileges
- Misconfigurations
- Known vulnerabilities
- File security
- Anomalous activities

Insiox provides their clients with a cyber security human risk management platform (cloud, SaaS) that delivers targeted phishing simulations and security awareness training, based on employees’ needs and risk. In the process, the system (ML) measures things such as employees' sentiment, psychographic profile, intention to comply, level of engagement, level of risk, etc.

This platform presents live dashboards with the overall human risk picture at user, department, or organisation level, providing a solid foundation for risk decision-making and treatment prioritisation.

OT security controls defined:

- Define roles and responsibilities related to security for all employees, managers and third-party vendors
- Ensure employers have insight into employees’ perceptions around cyber security
- Implement and maintain an OT-specific security incident management process
- Ensure proper backup, restore and data recovery procedures are in place
- Create a policy to manage all portable media
- Maintain and update an inventory of all OT equipment and software
- Establish a proper network segregation internally and externally
- Automate logging and reviewing of actual security events
- Implement a secure configuration process
- Implement a formal patching process

Through the merging of people, processes and technology; Snode Technologies and Insiox work cohesively to provide organisations with a holistic, intelligence-driven approach to manage their IT and OT security posture.

About Snode Technologies

Snode Technologies, a cyber defence firm based in Centurion, South Africa, has been a finalist and winner of some of Africa's most prestigious innovation awards, most recently, an overall winner at the SA Innovation Summit 2020 and the MEST Africa Challenge 2019. Snode was also listed, by Slingshot (Singapore), as one of the (2020) Top 100 Deep Tech innovations globally.

About Insiox

Insiox is a company based in Cape Town, South Africa, offering digital risk solutions to that enable organisation to manage risks holistically. From forensic to IT, legal to cyber, their diverse skills assist organisations to solve complex problems, using innovation, insights, intelligence, technology, and experience.

Authors

Nithen Naidoo

CEO and Founder of Snode Technologies

Nithen Naidoo is the CEO and founder of Snode Technologies. As a cyber security evangelist, with over 20 years of experience, Nithen provides cyber defence solutions globally, and most recently was recognised by the prestigious AfricArena tech accelerator as an Emerging Entrepreneur of 2021. Nithen is also a sought-after public speaker.

Nick Osborne

Director and Co-Founder of Insiox Digital Risk

Nick Osborne heads the Insiox cyber offering which provides a comprehensive set of cyber and information security services, solutions, and products to the market. Nick has 18 years of big 4 audit firm experience, of which 7 years were spent in London, UK. He has led, managed, and delivered IT risk and forensic offerings at multinational clients across South Africa, UK, Kenya, Tanzania, and Malawi.

References

Burgess, M. 2020. OT cyber security – it's all about the money. Mining Review Africa. Retrieved from: https://www.miningreview.com/gold/its-all-about-the-money-making-the-case-for-ot-cyber-securit y/

Chiwaya, N. 2021. Gas prices are spiking in the South. Here's where the jumps are highest. NBC News. Retrieved from: https://www.nbcnews.com/news/us-news/gas-prices-are-spiking-south-here-s-where-jumps-aren1267 175

Cohen, J. 2021. Water After Oldsmar: How to Prevent the Next Attack on Our Water Infrastructure. Cyberdefense Magazine. March 2021.

Greenberg, A. 2021. A Hacker Tried to Poison a Florida City's Water Supply, Officials Say. Wired. Retrieved from: https://www.wired.com/story/oldsmar-florida-water-utility-hack/

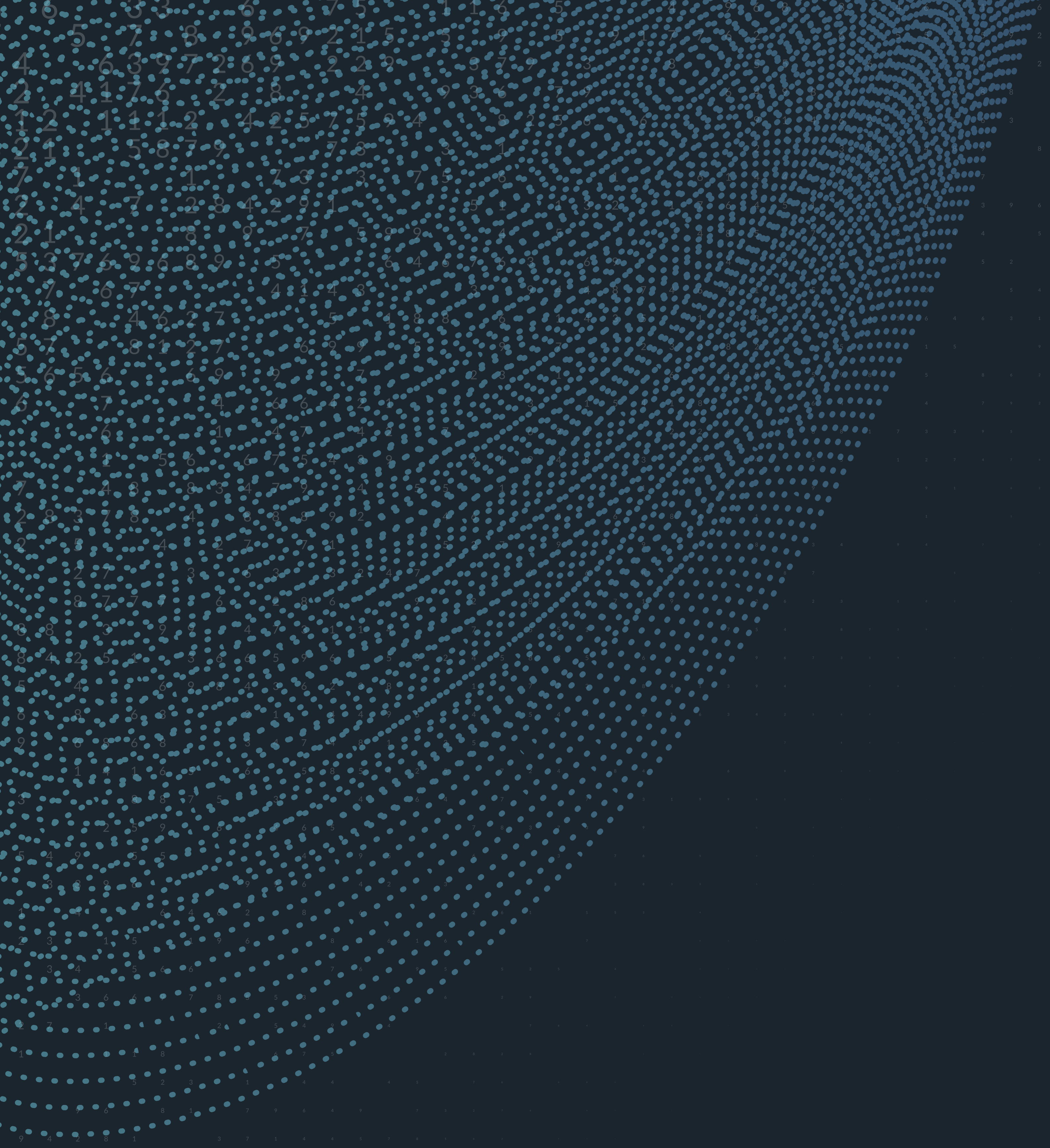
High, M. 2020. How digital transformation impacts mining cybersecurity. Mining Global. Retrieved from: https://miningglobal.com/automation-and-ai/how-digital-transformation-impacts-mining-cybersecurity

Ross, A. 2021. It's an Operational Technology World, and Attackers Are Living in It. Security Intelligence. Retrieved from: https://securityintelligence.com/posts/interview-critical-infrasttructure-operational-technology/

Sanger, D.E., Krauss, C. & Perlroth, N. 2021. Cyberattack Forces a Shutdown of a Top U.S. Pipeline. The New York Times. Retrieved from: https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.htm

Stamford, Conn. 2021. Gartner Predicts By 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully Harm or Kill Humans. Retrieved from: https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we

Verizon 2021 Data Breach Investigations Report. Retrieved from: https://www.verizon.com/business/en-gb/resources/reports/dbir/



INSIOX

RISK SOLUTIONS

🌐 www.insiox.co.za

✉ info@insiox.co.za

Snode

🌐 www.snode.com

✉ info@snode.com

☎ +27 12 880 0989