Snode

Operational Technology

Defending the operational technology of the future

8 June 2021

www.snode.com
info@snode.com
+27 12 880 0989

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 unsecure networks. However, these systems are becoming increasingly integrated and interconnected with IT. While digitalisation, automation and 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 operational technology attacks

While cyber defenders traditionally have concentrated on threats to organisations' IT networks, the real threat to critical infrastructure operators are their complex industrial control 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.

The need for proactive cyber security

As such, traditional approaches are no longer sufficient to secure OT infrastructure from imminent cyber threats. As a cyberattack on operational technology 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.

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).

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.

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 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 operational technology 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.

Snode’s industry-leading operational technology 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 detect, monitor, respond to and remediate threats that may appear in the OT/IT interface.

Snode’s interactive dashboard of comprehensive features creates complete and concise visibility of all activity across data sources in real time. The Snode platform’s ability to rapidly respond in a highly automated way means that in the event of a threat vector, the vulnerability can be quickly detected in real time, response capabilities can be increased, and the threat can be remediated without blocking critical business communications or operations.

Snode can be deployed into any operational system without any architecture or system changes in order to seamlessly integrate into the environment, securing both managed and unmanaged devices and infrastructure. Through-the-line protection enforces a robust security posture that minimises the risks presented by ever-evolving technology and its impact on both operational and information technology.

About Snode Technologies

Snode is a cyber defence company focused on making the unknown known. Snode is driven by excellence and the desire to tackle client challenges with bleeding-edge cyber technology.

Snode has over 80 global points of presence, protecting large industrial, agricultural, telecommunications and financial infrastructures.

Author

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.

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.

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-security/

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-aren1267175

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.html