INFOSYS AND FERROGLOBE: JOURNEY TOWARDS A ROBUST AND SECURE CYBER LANDSCAPE

Abstract

In today's digital age, the metallurgical industry is radically exposed to grave cyber risks! This is mainly due to the adoption of advanced technologies in the OT systems, that are adopted to render smart production. The possibility of being targeted by a malicious code or ransomware infesting on the internet is real, and can cripple production for days, thereby damaging the reputation of the company.

Keeping in mind such rising threats in the cyber landscape, Ferroglobe, a global leader in advanced metallurgical products is determined to strengthen its cybersecurity posture and hence partnered with Infosys. The engagement underpinned containing immediate threats and building medium to long term strategies for managing cybersecurity risks in the IT and OT environments. Infosys developed a secure by design approach by strengthening network security, building capability to monitor, contain and respond to security threats, implementing ISMS, and providing IT/OT security roadmap for the future.

Infosys®

Navigate your next

Commencement of the Cybersecurity Journey

In today's age, cyber risks have become a major concern for organizations in every industry and our client, Ferroglobe, is no exception.

Ferroglobe is a worldwide leading producer of Silicon Metal and ferroalloys, headquartered in London and listed in the U.S. Nasdaq.

Considering the evolving threat landscape and associated risks, Ferroglobe wanted to elevate its security posture as a proactive cybersecurity measure.

Further, it also wanted to migrate its applications to cloud in alignment with digital adoption.

Following are a few challenges it deciphered in its technology landscape:

Existence of legacy IT and OT infrastructure leading to high risk of cyber attacks

Limited capability to monitor, detect and respond to cyber threats and vulnerabilities

CHALLENGES

Manual management of perimeter firewalls and use of legacy technologies leading to non-standardized security policies

Lack of proper documentation for Information Security Governance structure, ISMS and Risk Management framework

To overcome these challenges, Ferroglobe strategically partnered with Infosys to build a systematic and holistic approach for cybersecurity. Infosys recommended and implemented various remedial actions to effectively mitigate Ferroglobe's medium to long term cybersecurity risks, thereby enhancing their cybersecurity maturity.

Strengthened the perimeter defense by upgrading perimeter legacy firewalls to next generation firewalls

Infosys diagnosed that Ferroglobe had legacy firewalls of multiple makes and models which were being managed in silos and were approaching end of life. This posed a significant risk to Ferroglobe's security posture, making it vulnerable to cyberattacks.

Infosys upgraded the legacy firewalls to next generation firewalls with AI/ML threat intel for advanced security and threat protection capabilities. Infosys also implemented centralized security policies for management of firewalls, and secure remote access VPN capabilities using multifactor authentication (MFA).

Embracing next-generation firewall solution helped Ferroglobe to proactively address firewall vulnerabilities and significantly strengthen the overall security posture. This preemptive approach helped in protecting critical data, mitigating security risks, and ensuring secure remote access, thereby safeguarding Ferroglobe's operations.
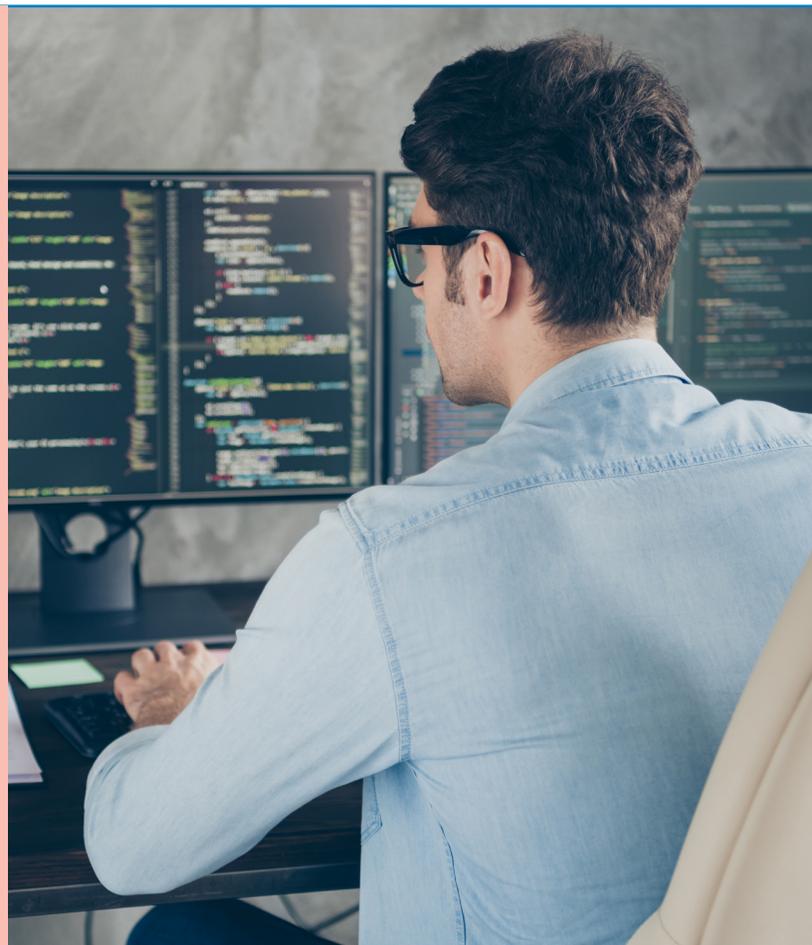
Bolstered threat detection and prevention capabilities with Infosys Cyber Watch Platform

Ferroglobe had limited threat detection capabilities to respond to security alerts in their IT environment, leading to high risk of cyberattacks, zero-day attacks and sophisticated advanced persistent threats (APTs).

To overcome this challenge, Infosys onboarded Ferroglobe log sources to the Infosys Cyber Watch platform for security operations. This included monitoring of security alerts from endpoints and carrying out daily/weekly/monthly vulnerability assessments.

This enhanced the detection and prevention capabilities of Ferroglobe helping them proactively contain immediate risks.

Strengthened the cloud security infrastructure with Azure security services

Ferroglobe sought to migrate some of their applications to the cloud for improving reliability and scalability.

Infosys successfully implemented Azure security services with built-in native controls to protect Ferroglobe's cloud environment on Azure. In addition, Infosys established multiple layers of security controls to safeguard the cloud infrastructure, including firewalls, Azure multifactor authentication, Azure information protection, vulnerability detection, continuous threat monitoring, and incident response.

These measures immensely elevated the overall security of Azure cloud infrastructure.

Enhanced the OT security maturity as a result of OT gap assessment

Ferroglobe wanted to increase the visibility of their OT network across their global plants to improve both efficiency and cybersecurity posture. Getting real-time insights of OT assets, network performance and potential threats, would help Ferroglobe optimize operations, minimize downtime, and protect critical infrastructure from cyberattacks.

Infosys used the OT security diagnostic framework and industry best practices to assess and analyze the cyber risks in Ferroglobe's OT assets and network. Based on the evaluation, Infosys recommended a remediation approach prioritizing critical infrastructure as per the risk score.

Infosys also suggested implementing an automated system to discover assets, map vulnerabilities, calculate risk scores, and establish a monitoring mechanism for detecting unusual behavior on the OT network.

Elevated governance with Information Security Management System (ISMS)

Ferroglobe wanted to build an enterprise level ISMS policies, procedures, and framework for harmonization of security objectives and policies across the organization, also leading to improved security of their information assets.

Infosys helped in building the Information Security Management System (ISMS) based on ISO27001 to elevate the information security governance. As part of this, Infosys also carried out gap assessment as per ISO27001 and shared the findings and recommendations to be implemented. Based on this, Infosys built the required ISMS policies, processes and RARTP (Risk assessment and Risk treatment) framework.

This enhanced the overall security governance with defined information security policies, processes, risk management framework and ensured continual improvement of the ISMS.

Secured identities with centralized identity management

Ferroglobe had multiple Active Directories (AD) spread across the globe, being managed by the teams locally, exposing them to higher risk of identity theft, increased attack surface, inconsistency in security configurations, complex user management and compliance efforts.

Infosys recommended AD consolidation in a phased approach to ensure smooth migration using identity management solution (IDAM/IGA). This proactive measure helped Ferroglobe bolster their IT environment by elevating security, efficiency, and manageability of user access, and strengthening the security of identities on the principal of least privilege access.

About Ferroglobe

Ferroglobe is a leading global producer of silicon metal, silicon-based and manganese-based ferroalloys serving a customer base across the globe in dynamic and fast-growing end markets, such as solar, automotive, consumer products, construction and energy.

About Infosys Cyber Security Practice

Infosys combines technological expertise with more than a decade of experience in digital security to provide a complete suite of services including security consulting, transformation, and managed services. We help enterprises navigate towards a secure future by fulfilling the promise of "Digital-trust. Assured" to our clients. Guided by our three principles of Secure by Design, Secure by Scale and Secure the Future, we are committed towards building a holistic Cybersecurity program with our portfolio of service offerings, that follows a four-dimensional approach of Diagnose-Design-Deliver-Defend.

> Infosys has proven to be a valuable partner in our cybersecurity journey. They have demonstrated their ability to not only help us contain immediate critical and high risks in a short term but also take informed decisions in the medium to long term risk mitigation strategies, thereby improving our overall cybersecurity posture. Infosys has transformed our security landscape by implementing and managing 24x7 SOC monitoring and response, next-gen firewall technology, vulnerability management, EDR technologies, and providing a secure cloud infrastructure. They have helped us assess our OT and IT environment, potential risks to identity and access management, and provided visibility to the associated security risks and recommended best practices for implementation.
>
> Infosys is also partnering with Ferroglobe to implement many other cybersecurity initiatives. They have been a flexible partner, open to adopt and change their approach to cater to our specific needs, and solving new challenges identified during the execution phase.
>
> **BEATRIZ GARCÍA-COS MUNTAÑOLA**
> Chief Finance Officer & IT, Ferroglobe

For more information, contact askus@infosys.com

Infosys®
Navigate your next

Infosys.com | NYSE: INFY

Stay Connected