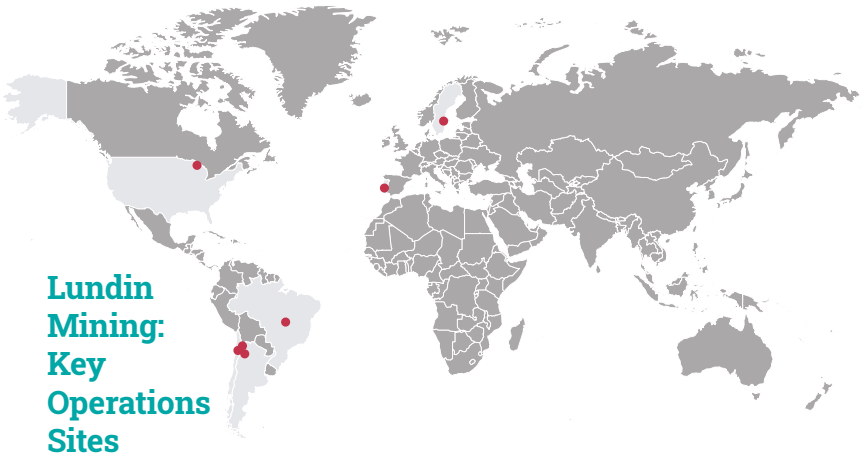
CASE STUDY

DRAGOS
SAFEGUARDING CIVILIZATION

Empowering Business Resilience

Lundin Mining's Success Story with Dragos OT Cybersecurity Platform and OT Watch

In the dynamic realm of industrial operations, safeguarding critical infrastructure against cyber threats is paramount. Global mining companies, tasked with the extraction and processing of resources, are increasingly exposed to evolving cyber risks that can disrupt operations and jeopardize safety. This case study delves into how a prominent global mining company partnered with Dragos, a leading industrial cybersecurity solutions provider, to bolster its cyber resilience. By adopting Dragos' OT cybersecurity platform and OT Watch, Lundin Mining fortified its defenses and achieved notable success in protecting its operational technology (OT) environments.



Lundin Mining: Key Operations Sites

Lundin Mining is a diversified Canadian base metals mining company with operations and projects in Argentina, Brazil, Chile, Portugal, Sweden, and the United States of America, primarily producing copper, zinc, gold, and nickel.

lundin mining

Background

In the past few years, Lundin Mining has

- With executive-level support, the company formed a cross-functional **sustainability working group** to identify areas where Lundin Mining can make a positive impact, keep pace with climate change, and meet the high metal demands of a green economy
- The sustainability working group completed an **in-depth mapping project and materiality assessment,** producing a report that included considerations from the United Nations Sustainable Development Goals (SDGs), the Global Reporting Initiative Framework (GRI), and industry best practices
- Increased **regular quarterly dividends** by 125% and paid an **inaugural performance dividend**
- Substantially completed **Neves-Corvo Zinc Expansion Project** to double zinc production capacity
- Announced the acquisition of **Josemaria Resources Ltd.** for its large copper-gold project in Argentina
- Announced majority stake acquisition in SCM Minera Lumina Copper Chile, which operates the **Caserones copper-molybdenum mine** in Chile

Lundin Mining's operational success is supported by a strong safety culture focused on operational excellence and continuous improvement. One of their core priorities is business resilience, which includes adapting to changing conditions, leveraging proven and new technologies, and forming trusted partnerships to ensure the sustained growth of their operations into the future.

Operational technology (OT) cybersecurity plays a crucial role in ensuring business resilience for Lundin Mining. The key measure of a company's resilience is its ability to withstand and recover from various disruptions, whether they are caused by natural disasters, economic downturns, or cybersecurity incidents.

Ten Ways a Strong OT Cybersecurity Program Helps Lundin Mining Achieve Business Resilience Goals

1. **Protecting Critical Infrastructure:** Mining operations heavily rely on complex OT systems and industrial control systems (ICS) to extract, process, and transport valuable resources. Dragos OT cybersecurity technology safeguards Lundin Mining's critical systems from cyber threats, ensuring that the core infrastructure remains operational during disruptive events.
2. **Minimizing Downtime:** Cybersecurity incidents, such as ransomware attacks or data breaches, can disrupt mining operations and lead to costly downtime. Effective OT cybersecurity measures help prevent and mitigate these incidents, minimizing operational disruptions and financial losses.
3. **Ensuring Safety:** Safety is paramount in the mining industry. OT systems control various safety-critical processes, including equipment monitoring, ventilation, and emergency response systems. A cyberattack on these systems could jeopardize the safety of employees and the environment. OT cybersecurity helps maintain safety protocols and prevent potential disasters, an important pillar within Lundin Mining's safety program.
4. **Protecting Reputation:** A cybersecurity breach can damage a mining company's reputation and erode trust among stakeholders, including investors, customers, and regulatory bodies. Maintaining a robust OT cybersecurity posture demonstrates Lundin Mining's commitment to responsible and secure operations.
5. **Regulatory Compliance:** Many countries and regions have stringent regulations governing cybersecurity in critical infrastructure sectors like mining. Adhering to these regulations is essential for avoiding legal penalties and ensuring business continuity. A long-term commitment to OT cybersecurity helps mining companies stay compliant with evolving cybersecurity standards.
6. **Supply Chain Resilience:** Mining operations depend on a global supply chain for equipment, software, and services. Ensuring that suppliers adhere to cybersecurity best practices is crucial to preventing supply chain disruptions caused by cyberattacks or compromised components.
7. **Data Protection**: In an increasingly digital world, mining companies accumulate vast amounts of sensitive data, including geological data, operational data, and financial information. OT cybersecurity safeguards this data from theft or unauthorized access, protecting the company's intellectual property and competitive advantage.
8. **Efficient Incident Response:** Even with robust prevention measures, cybersecurity incidents can still occur. Effective OT cybersecurity includes incident response plans and procedures to minimize the impact of an incident, recover operations swiftly, and maintain business continuity.
9. **Long-Term Viability:** Cyber threats are evolving, and attacks on critical infrastructure are becoming more sophisticated. A mining company's ability to adapt and enhance its OT cybersecurity over time is crucial for its long-term viability and resilience in an ever-changing threat landscape.
10. **Business Continuity Planning:** OT cybersecurity is an integral part of business continuity planning. By identifying potential cyber risks and implementing mitigation strategies, mining companies can better prepare for unexpected events and disruptions, ensuring that critical operations continue without significant interruptions.

Lundin Mining understands that OT cybersecurity is not just a technical requirement; it is a strategic component of business resilience. By protecting critical infrastructure, ensuring safety, maintaining compliance, and preserving the company's reputation, OT cybersecurity contributes to the overall resilience of the organization, enabling it to withstand disruptions and thrive in a challenging environment.

Challenges and Solutions: Protecting Lundin Mining's Complex Mining Operations Around the World

With mining operations spanning multiple continents, Lundin Mining faced complex challenges in securing its diverse OT systems. These systems, ranging from legacy to state-of-the-art, formed an intricate web of interconnected industrial control systems (ICS) and OT assets. Ensuring the availability, integrity, and confidentiality of these systems was pivotal for maintaining production levels, complying with stringent regulations, and mitigating financial risks.

Lundin Mining's primary challenges included:

Diverse OT Environments

- **CHALLENGE:** Each mining site may have a different mix of OT systems, ranging from legacy to modern equipment. Managing the cybersecurity of this diverse OT environment can be challenging.
- **IMPACT:** Inconsistent security measures across sites can make it easier for attackers to exploit weaknesses.

Remote Locations

- **CHALLENGE:** Mining operations are often situated in remote and isolated areas with limited network connectivity and physical security.
- **IMPACT:** Remote locations can hinder the deployment of cybersecurity measures, making it difficult to monitor and respond to threats in real-time.

Supply Chain Risks

- **CHALLENGE:** Mining companies rely on a global supply chain for equipment and software, which can introduce cybersecurity risks if suppliers have inadequate security practices.
- **IMPACT:** Vulnerabilities in the supply chain can lead to compromised OT systems and data breaches.

Limited IT-OT Integration

- **CHALLENGE:** The separation between IT (Information Technology) and OT networks is common in industrial settings. Bridging the gap between these two domains can be challenging.
- **IMPACT:** Insufficient integration can hinder visibility into potential threats and slow down incident response efforts.

Complex Vulnerability Management:

- **CHALLENGE:** Mining operations often involve a diverse technology landscape, with a mix of modern and legacy equipment and software. These technologies may have varying levels of compatibility with vulnerability scanning and patching tools.
- **IMPACT:** Managing vulnerabilities across multiple sites with many different technologies is complicated, as each type of equipment may require unique approaches to assessment and remediation.

Staff Training and Awareness:

- **CHALLENGE:** Ensuring that staff at all sites have the necessary cybersecurity training and situational awareness is crucial but can be logistically challenging.
- **IMPACT:** Untrained or unaware employees can inadvertently introduce vulnerabilities through their actions or decisions.

Scalability:

- **CHALLENGE:** As mining operations expand or contract, maintaining consistent OT cybersecurity practices across all sites can be difficult.
- **IMPACT:** Inconsistent security practices can lead to gaps in cybersecurity coverage, leaving some sites more vulnerable than others.

Emerging Threat Landscape

- **CHALLENGE:** The threat landscape for OT environments is constantly evolving, with new attack techniques and malware targeting critical infrastructure.
- **IMPACT:** Staying ahead of emerging threats requires continuous monitoring and proactive security measures, which can be resource-intensive.

Limited Budget and Resources:

- **CHALLENGE:** Allocating sufficient budget and resources to OT cybersecurity across multiple sites can be a financial constraint.
- **IMPACT:** Insufficient investment in cybersecurity can lead to inadequate protection against cyber threats.

Addressing these challenges requires a comprehensive and tailored cybersecurity strategy that considers the unique aspects of each mining site while providing centralized monitoring and response capabilities. The **Dragos OT Cybersecurity Platform** is the centerpiece of this program, and the team uses the Platform in the following ways:

- Finding the root cause analysis of operational issues
- Conducting automated asset inventory
- Verifying and prioritizing vulnerabilities or supply chain compromise risks
- Responding to regulatory audits
- Detecting changes in configuration or communications to/from critical equipment [crown jewels]
- Hunting for threats based on threat intelligence

In addition to the Dragos Platform, the Lundin Mining team also leverages **OT Watch**, an elite group of ICS intrusion detection analysts and investigators dedicated to proactively hunting for adversary activity. Here's how the team uses OT Watch:

- Managed threat hunting using the latest intelligence-based IOCs and adversary TTPs
- Notification triage and response support, escalating high severity alerts
- Alert and asset configuration tuning, enriching asset characteristics and alert severities
- Mapping and zone configuration with ongoing improvement of asset, zone, and network communication visualizations
- System health and status monitoring
- Dragos Platform optimization with regular updates to detections, characterizations, and playbooks
- Executive reporting on overall status of the ICS environment, findings, and recommendations for continuous improvement

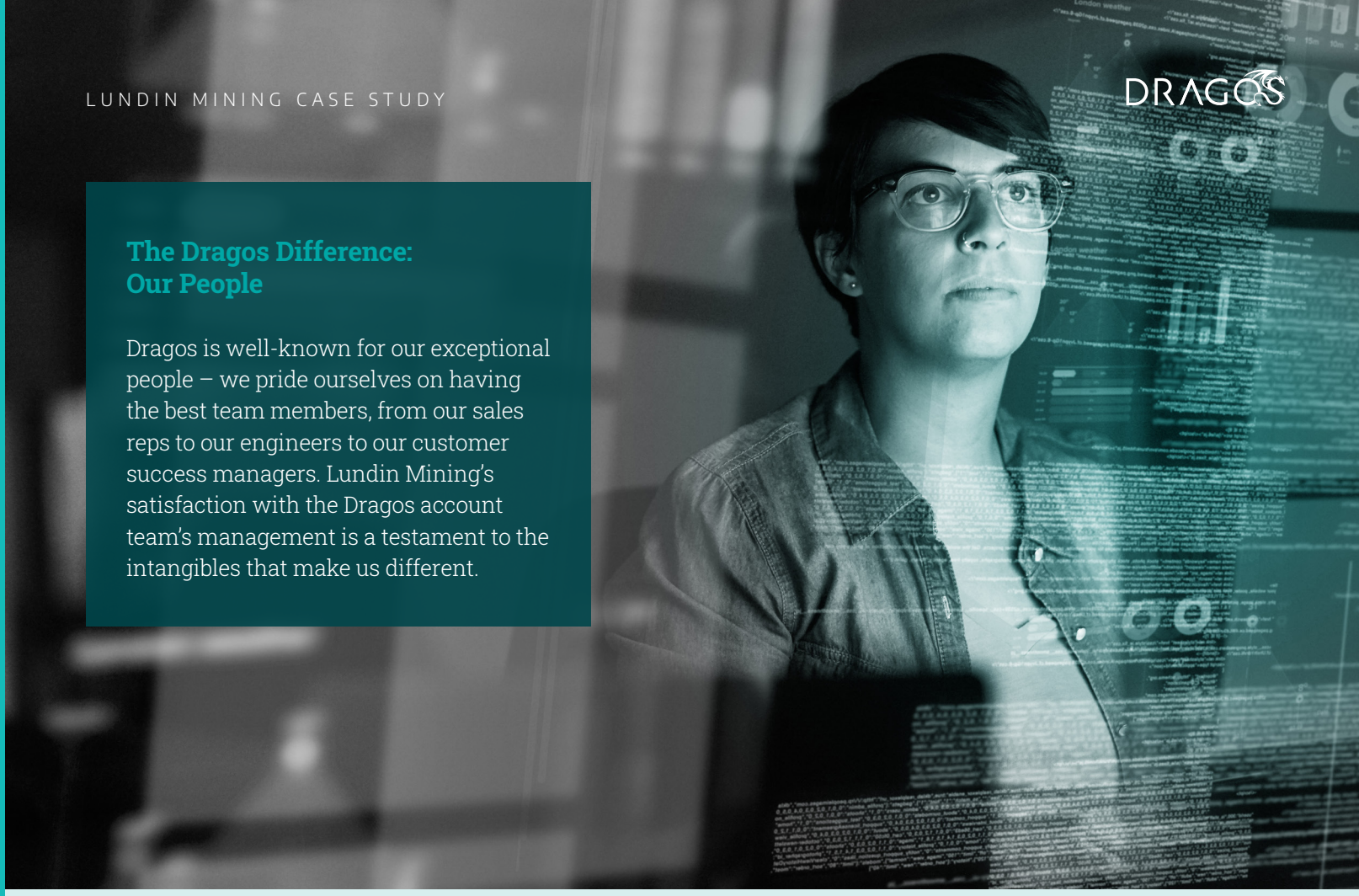
Lundin Mining's resolute commitment to OT cybersecurity, coupled with its partnership with Dragos, has fortified the security of its OT environments. The implementation of Dragos' OT cybersecurity Platform and OT Watch facilitates the detection, mitigation, and response to cybersecurity threats across their networks, increasing trust and collaboration with internal and external stakeholders.

The implementation of the Dragos Platform, complemented by Dragos' OT Watch threat detection and response service, enabled the following critical improvements:

- **Enhanced Visibility and Asset Management:** Dragos' platform offers real-time visibility into the OT assets and network, allowing Lundin Mining to identify all devices and associated vulnerabilities accurately. This asset management capability streamlines maintenance efforts and enhances operational efficiency.
- **Proactive Threat Detection:** OT Watch provides continuous monitoring of the company's OT environment for anomalous activities and known threat indicators. The mining industry-specific threat detection capabilities ensure high precision in identifying potential threats, thus enabling proactive mitigation without the false alarms.
- **Incident Response Excellence:** In case of a cybersecurity incident, Lundin Mining will be able to leverage Dragos' incident response expertise quickly and easily. Expert-authored playbooks guide their security team through investigations, reducing response times and improving efficiency.
- **Simplified Compliance:** The Dragos Platform features in-depth reporting tools, simplifying adherence to industry regulations. These features reduce compliance-related risks and facilitate audit processes.

The partnership with Dragos delivered substantial enhancements to Lundin Mining's cybersecurity posture, yielding the following outcomes:

- **Minimized Downtime:** Proactive threat detection and mitigation limits downtime due to cyber incidents, ensuring uninterrupted operations.
- **Streamlined Asset Management:** Precise asset inventory facilitates efficient maintenance and operational optimization.
- **Increased Efficiency and Productivity:** More effective vulnerability management results in less alert fatigue, more situational awareness among team members, and higher levels of productivity (for both equipment and human resources.) Fewer man-hours are needed to do asset inventory, verification, and changeover.
- **Effortless Compliance:** Advanced reporting ensures that Lundin Mining meets or exceeds compliance requirements, enhancing readiness for audits and averting potential penalties.
- **Cyber Threat Resilience:** Lundin Mining is better prepared to counter evolving cyber threats, and the company continues operations with confidence, knowing their OT environment is secure.
- **Operational Continuity:** With cyber resilience in place, the company's leadership and stakeholders have greater assurance in the continuity of their operations



The Dragos Difference: Our People

Dragos is well-known for our exceptional people – we pride ourselves on having the best team members, from our sales reps to our engineers to our customer success managers. Lundin Mining's satisfaction with the Dragos account team's management is a testament to the intangibles that make us different.

Here's a breakdown of Lundin Mining's key areas of satisfaction and their significance:

Trust and Accountability

- **SIGNIFICANCE:** Trust is the foundation of any successful business relationship. Lundin Mining's trust in the Dragos team members, from sales to solution architects to customer success managers, reflects the team's dedication to acting in the best interest of their customers. Accountability and reliability ensure that commitments are met consistently, enhancing the company's confidence in Dragos' services.

Technical Expertise

- **SIGNIFICANCE:** Understanding the unique OT environment and threat landscape is essential for effective cybersecurity. Lundin Mining's satisfaction with the Dragos team's technical resources highlights our deep knowledge and proficiency in securing industrial control systems. This expertise is critical in providing tailored solutions that address a mining company's specific needs and challenges.

Seamless Onboarding and Planning

- **SIGNIFICANCE:** The ability to efficiently onboard and implement cybersecurity solutions across five global sites in less than six months with zero downtime is a remarkable achievement. This proves that the Dragos team not only possesses technical competence but also excels in project management and execution. Impeccable onboarding and planning set a solid foundation for a successful partnership.

Operational Understanding

- **SIGNIFICANCE:** The Dragos team's extensive knowledge of the mining company's operations and sites is invaluable. This understanding enables the team to provide tailored recommendations, such as ideal sensor placement, which can significantly enhance the effectiveness of cybersecurity measures. It showcases a commitment to delivering solutions that align with the company's unique operational requirements.

Continuous Improvement

- **SIGNIFICANCE:** By actively seeking ways to enhance our solutions and services, the Dragos team helps Lundin Mining stay ahead of evolving cyber threats

Conclusion

Dragos' advanced technology and deep expertise in OT cybersecurity position have helped to ensure Lundin Mining's successful and resilient future. By providing comprehensive solutions tailored to the mining industry's unique challenges, Dragos empowers Lundin Mining to safeguard its critical infrastructure, maintain operational continuity, and protect against evolving cyber threats. With seamless onboarding and extensive operational knowledge, Dragos not only fortifies the mining company's cybersecurity posture but also lays the foundation for efficient and secure growth. This partnership sets the stage for a future where Lundin Mining can thrive amidst challenges, adapt to emerging threats, and maintain a resilient and secure operational landscape.

About Dragos, Inc.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

Learn more about our technology, services, and threat intelligence offerings:

Request a Demo | Contact Us

info@dragos.com @DragosInc @Dragos, Inc.