SUCCESS STORY

MELLIVORA TECHNOLOGY ULTRARED

STRENGTHENING SECURITY FOR A GLOBAL MINING LEADER

Continous Threat Exposure Management

Company Overview

Our customer is a prominent global mining company with operations spanning multiple sites across three continents. The organisation specialises in extracting and exporting high-value resources, including precious metals and minerals. Given the competitive and sensitive nature of their industry, the company manages a significant volume of confidential information, such as geological survey data, operational plans, and intellectual property tied to extraction processes.

Challenges

Insider Risks and Data Security

Sensitive data, including proprietary mining methodologies, export schedules, and confidential financial records, was at risk of exposure due to insider threats and unintentional data leakage. Monitoring risky user behaviour and identifying potential data exfiltration were critical to safeguarding business information and ensuring compliance with regulatory standards.

External Threat Exposure

Hosting a mix of on-premises and cloud-based services exposed the company to external cyberattacks. Threat actors targeted internet-facing services, seeking to exploit vulnerabilities to disrupt operations or steal sensitive information. As cyberattacks in the mining industry grew more sophisticated, the organisation required a robust solution to detect and neutralise these threats.

Operational Complexity Across Regions

Operating across three continents introduced significant operational complexity. Differences in regional regulations, workforce dynamics, and infrastructure maturity created challenges in maintaining a unified and robust security framework. The company needed a solution that could seamlessly integrate into its diverse environment while providing consistent security and visibility across all sites.

> **As a global mining leader, we faced immense pressure to safeguard our operations against both internal and external threats. With sensitive data spread across multiple sites and platforms, we needed a solution to provide clear visibility and control. Cyber threats in the industry have evolved, and without a robust strategy, we risked operational disruptions and potential data breaches."**
>
> ***CISO, Global Mining Company***

Deployment

To address these challenges, the company partnered with Mellivora Technology to implement two key solutions: Fortinet and ULTRA RED.

FORTINET

FortiDLP was deployed across the organisation's endpoints to monitor, detect, and prevent data leakage.

Key features and benefits included:

Advanced Analytics:
Identified risky user behaviours, such as unauthorised access to sensitive geological data or unusual file-sharing activity.

Policy-Free Visibility:
Provided instant insights into data flow throughout the business without requiring initial discovery and classification exercises.

Granular Policy Creation:
Allowed the company to classify and protect their critical data assets quickly and effectively.

The deployment, including policy creation, was completed within three months, delivering real-time alerts on potential risks and ensuring the organisation could rapidly respond to emerging threats.

ULTRARED

With a focus on External Threat Exposure Management, ULTRA RED was deployed to continuously monitor the company's internet-facing infrastructure.

Key features and benefits included:

Comprehensive Visibility:
Identified exposed services, vulnerabilities, and potential attack vectors.

Real-Time Alerts:
Provided actionable intelligence to mitigate risks before they could escalate.

Prioritised Threat Response:
Enabled the security team to address high-priority issues effectively, such as identifying an exposed API key that could allow attackers to infiltrate the cloud-hosted Active Directory. This critical issue was patched within hours thanks to ULTRA RED's alerting and prioritisation mechanisms.

The deployment required no input from the customer, allowing ULTRA RED to begin delivering results in less than a day. Within the first week, real-time alerts flagged a high-severity vulnerability, enabling the organisation to address the issue before any threat actor could exploit it.

Results

With FortiDLP and ULTRA RED in place, the organisation achieved significant improvements in their security posture:

Enhanced Data Security

The company gained detailed visibility into user behaviour, enabling rapid identification and response to insider risks. FortiDLP significantly reduced instances of data leakage, ensuring sensitive information, such as extraction plans and financial reports, remained secure.

Reduced External Threat Exposure

ULTRA RED provided actionable insights into vulnerabilities, allowing the company to patch issues proactively. For example, within days of deployment, ULTRA RED flagged an exposed API key as a critical risk. The organisation prioritised and resolved this issue within hours, averting a potential breach.

Streamlined Compliance and Risk Management

By automating data classification and threat monitoring, the company enhanced compliance with data protection regulations and mitigated the risk of financial and reputational damage. These solutions also enabled the security team to focus on strategic priorities by reducing manual effort and operational inefficiencies.

Data Leakage Incidents: Reduced by 85% within six months.
Average Response Time to Threats: Decreased from 48 hours to 4 hours.
Compliance Audit Success Rate: Achieved a 100% pass rate in the following regulatory assessments.

> **The implementation of FortiDLP and ULTRA RED transformed our security strategy. We've achieved unparalleled visibility into our data and infrastructure, allowing us to address risks proactively. The partnership provided us with the confidence to safeguard our critical assets and focus on our core operations."**
>
> ***CISO, Global Mining Company***

Conclusion

Through the deployment of FortiDLP and ULTRA RED, the mining company not only secured its critical data and infrastructure but also strengthened its overall security posture. The swift implementation and measurable outcomes underscore the value of investing in advanced cybersecurity solutions tailored to industry-specific challenges. This partnership highlights our commitment to delivering robust, scalable, and effective security strategies for global enterprises.

About ULTRA RED

ULTRA RED is a pioneer and leading provider of Continuous Threat Exposure Management (CTEM) solutions, built on a validation-first approach. Our CTEM platform helps security teams confidently reduce threat exposure by continuously identifying, validating, and prioritizing gaps across the entire attack surface. Learn more at www.ultrared.ai.