CLAROTY & KUDELSKI SECURITY

Complete Operational Technology Protection for the Mining Sector

Mining organizations are facing complex challenges when it comes to securing their operations. Most companies operate in complicated environments, involving multiple units and control systems distributed across broad and remote geographical areas. These organizations rely on legacy systems and traditional, IT-centric security tools that often do not document or represent the system or network resources accurately. Additionally, disruptions to operations that incur downtime can be difficult to recover from, interrupting optimal performance.

Protecting the Operational Environment

The Claroty Platform bridges the gap between information technology (IT) and operational technology (OT) environments and has been deployed across enterprises and geographical regions successfully. These enterprises and critical infrastructure operators can leverage their existing IT security processes and technologies to improve the availability, safety, and reliability of their OT assets and networks seamlessly and without requiring downtime or dedicated teams.

Together with Claroty, Kudelski Security provides comprehensive, centralized security visibility and management for blended IT/OT environments. Our Operational Technology Monitoring service is built upon an advanced monitoring platform that identifies OT network incidents and vulnerabilities and leverages the expertise of our Cyber Fusion Center (CFC) for 24x7x365 triage and response. Kudelski Security helps enterprises monitoring and secure their OT environments effectively without introducing additional business risk or operational drag. Combining the visibility platform of Claroty with our own suite of advisory and managed security services, we provide a comprehensive approach to OT monitoring and controls.

Comprehensive OT Protection and Monitoring

- Complete Network Monitoring and Protection
- Solutions Tailored to Client Needs
- Solutions Backed by Managed Security Services
- 24x7x365 Monitoring and Protection

Claroty bridges the industrial cybersecurity gap between information technology (IT) and operational technology (OT) environments. Organizations with highly automated production sites and factories that face significant security and financial risk especially need to bridge this gap. Armed with Claroty's converged IT/OT solutions, these enterprises and critical infrastructure operators can leverage their existing IT security processes and technologies to improve the availability, safety, and reliability of their OT assets and networks seamlessly and without requiring downtime or dedicated teams. The result is more uptime and greater efficiency across business and production operations.

No matter where your organizations is in the IT/OT journey, our team of experts and analysts are available to assist with access management policies, plans to identify and protect internal assets, and proactive management of vulnerabilities and threats.

Kudelski Security

Next-Generation Managed Security Services

Kudelski Security amplifies the power of the Claroty solution through its advanced Managed Security Services, providing security teams a range of benefits.

- Improve resilience to attack

  We reduce threat detection time through fusion of security data and contextual intelligence, gathered from a vast range of sources

  We deliver fast, effective threat analysis and thorough investigation of relevant alerts

  Daily threat hunting detects hidden activity of an advanced attack, which would otherwise be missed
- Adopt a streamlined response to incidents with our clear, actionable recommendations
- Gain broad visibility into the state of your security, through our MSS Client Portal
- Easy-to-understand dashboards and monthly service reporting

Claroty

Next-Generation Operational Technology Protection

The Claroty Platform is deployed to protect a company's Industrial Control Systems (ICS) networks from cyberattacks through platform components such as Continuous Threat Detection (CTD) and the Enterprise Management Console (EMC). Continuous Threat Detection offers deep packet inspection technology to present details on assets on the OT network, regardless of the device's underlying technology. Enterprise Management Console provides a unified view of assets and activities across the enterprises sites.

- Reduction of OT complexity through technology-agnostic solutions and the leveraging of existing IT infrastructure
- Protects the bottom line by ensuring uptime and efficiency across operations
- Improve reliability and safety of OT assets within critical infrastructure

info@kudelskisecurity.com | www.kudelskisecurity.com

KUDELSKI SECURITY