valkyrie™ AUTOMATED SECURITY

Go Beyond Network Monitoring.

Securing OT environments shouldn't require digging for data manually, or relying on generic tools and pricey retainers. Valkyrie collects and correlates host and network data–through both batch and streaming sources–giving your team a faster, more complete picture of potential threats. The result: quicker detection, faster response, and reduced operational risk.

Designed with flexibility in mind, Valkyrie easily adapts to your infrastructure–whether it's deployed via virtual machine, on-premise, or the Cygnet Flyaway Kit. It's scalable without being cost-prohibitive, delivering full coverage without overextending your budget. By tailoring detection rules to your specific environment and threat landscape, you gain meaningful insights that drive action rather than noise. Valkyrie Automated Security offers effective protection while minimizing downtime and streamlining incident response.

Save Time

Detect and respond to threats in near real-time by automating data collection and correlation.

See More

Stay ahead of threats by expanding visibility with host and network data monitoring, while focusing on proactive security.

Flexible Deployment

With virtual and physical deployment options, you can choose what fits your environment best without complexity.

Tailored Detection

Customize detection logic to track specific threat groups based on the most relevant risks.

Threats are becoming more sophisticated each day. Valkyrie Automated Security is the dynamic cybersecurity solution designed to withstand the risks of tomorrow.

Insane Cyber™

Schedule a Demo

Get a personal tour and see Valkyrie in action today.

valkyrie AUTOMATED SECURITY

Comprehensive Asset Visibility

- Continuous discovery of assets and their communication patterns through a combined process of active and passive scanning and correlating datasets
- Identification of unauthorized or rogue devices

Near Real-Time Threat Detection

- Behavioral anomaly detection tailored to OT environments
- Signature and heuristic-based detection of known threats
- Detection of unauthorized protocol usage and lateral movement

Deep Packet Inspection

- Granular analysis of industrial protocols
- Identification of misconfigurations, unauthorized commands, and vulnerabilities

Host-Based Security Monitoring

- System integrity scanning for industrial endpoints
- Detection of unauthorized software installations and file changes

Network Traffic Analysis

- Passive monitoring of control system communications
- Identification of anomalous traffic patterns and policy violations
- Baseline creation for normal OT network behavior

Incident Response & Forensics

- Historical data retention and organization from different sources into a single, normalized view to correlate different points of evidence
- Running signature, heuristic, and statistical behavior detections
- Detecting unauthorized protocols and lateral movement

Seamless Integration & Deployment

- Lightweight deployment with minimal impact on OT operations
- Compatibility with existing security tools
- Flexible and scalable deployment options through cloud, virtual machine, hardware or hybrid approach

Regulatory & Compliance Support

- Aligns with NIST, IEC 62443, NERC CIP, and other OT security frameworks
- Reporting to support compliance audits and security assessments