Night's Watch Crow

Intrusion Detection

Roadmap: 2026

Night's Watch Crow's Intrusion Detection System (IDS), a Roadmap 2026 feature, provides real-time network security monitoring through deep packet inspection and traffic analysis. Due to the intensive nature of continuous packet inspection, this service requires enhanced hardware resources to maintain performance. The system offers comprehensive threat detection through:

- Multi-layered packet inspection and protocol analysis
- Signature-based threat detection using regularly updated rulesets
- Protocol anomaly detection and behavioral analysis
- Pattern matching across packet streams
- Application layer protocol inspection
- Network flow analysis for detecting anomalous patterns
- Custom rule creation for environment-specific threats
- Alert correlation and aggregation
- Configurable alerting thresholds and severity levels
- Support for encrypted traffic analysis capabilities
- Real-time alert generation with detailed context
- Traffic logging for forensic analysis
- Performance optimization through selective inspection rules
- Hardware resource requirements scale with traffic volume and inspection depth

The system analyzes network traffic in real-time, providing threat detection capabilities while maintaining throughput performance. Alert generation includes detailed metadata about detected threats, enabling rapid incident response and investigation. The modular architecture supports rule customization and tuning to minimize false positives while maintaining comprehensive security coverage.