

Seceon OTM Platform - Dark Web Scan



Product Overview

Seceon's OTM Platform Dark Web Scan is an advanced threat intelligence capability that continuously monitors the dark web for compromised organizational data, leaked credentials, and emerging threats. As part of the comprehensive Open Threat Management platform, this feature provides real-time visibility into underground cybercriminal activities targeting your organization. The Dark Web Scan integrates seamlessly with Seceon's AI-driven threat detection and response capabilities, enabling proactive security measures before threats materialize into active attacks against your infrastructure.



What We Scan For

Compromised Credentials

Username/password combinations, email addresses, and authentication tokens associated with your organization.

Corporate Data Leaks

Sensitive company information, proprietary documents, and intellectual property being traded or sold.

Personal Information

Employee PII, customer data, social security numbers, and other sensitive personal information.

Financial Data

Credit card numbers, banking information, payment processing details, and financial records.



Highlights



GAIN TRUST WITH UNIFIED VISIBILITY AND THREAT INTELLIGENCE CAPABILITIES

Uncover a myriad of threat vectors lurking inside your existing logs, auto-discovered hosts, network, cloud, OT and IoT infrastructure. Seceon aiSIEM combines this telemetry with 360° inference drawn from events, network traffic, packets, identities and behavioral patterns.



REDUCE MEAN TIME TO DETECT AND RESPOND

Considerably shorten Mean-Time-To Detect (MTTD) and Mean-Time-To Response (MTTR) with automated threat detection and remediation in real-time and score them by confidence level and criticality.



EFFORTLESS DEPLOYMENT AND INTEGRATIONS

With just one collector, you can start sending flows and logs and deploy Seceon aiSIEM. Then you can connect your existing technology stack with hundreds of integrations.



CONTINUOUS COMPLIANCE

Ensure compliance 24x7 with Seceon's audit and reporting capabilities for PCI-DSS, HIPAA, NIST, GDPR and more. Additionally monitor security postures, operations and investigations reporting.

Threat Intelligence

Discussions about planned attacks, vulnerability exploits, and cybercriminal activities targeting your sector.

Brand Monitoring

Unauthorized use of company branding, domain spoofing, and impersonation attempts.



Scanning Frequency & Coverage

Continuous 24/7 Monitoring

Parameter	Specification
Scan Frequency	Real-time continuous monitoring with regular updates
Data Sources	1000+ dark web forums, marketplaces, and underground sites
Detection	Continuous threat monitoring and detection
Data Retention	Historical threat data maintained for 12 months
Coverage Areas	Global dark web monitoring across all major regions



Actionable Alerts & Response

Intelligent Alert Prioritization

AI-powered risk scoring automatically prioritizes alerts based on threat severity, organizational impact, and exploitability. Critical threats trigger immediate notifications while lower-risk items are queued for review.

Multi-Channel Notifications

Real-time alerts are delivered via email, SMS, SIEM integration, and the OTM platform dashboard. Customize notification preferences by threat type and severity level.

Automated Response Actions

Trigger automated security responses, including credential resets, account lockouts, and security policy updates based on detected threats.

Contextual Threat Intelligence

Each alert includes detailed context about the threat source, affected assets, recommended actions, and integration with existing security tools.

Alert Categories

- **Critical** - Immediate Action Required
- **High** - Response Within 4 Hours
- **Medium** - Response Within 24 Hours
- **Low** - Informational/Monitoring

Key Benefits

Proactive Threat Detection

Identify threats before they become active attacks

Rapid Response Time

15-minute detection and immediate alerting

Reduced False Positives

AI-driven filtering ensures relevant, actionable alerts

Seamless Integration

Native integration with OTM platform and third-party tools

Dark Web Scan

Continuous Threat Intelligence & Monitoring



What We Monitor

Compromised Credentials Passwords, emails, tokens	Corporate Data Sensitive company info
Personal Information Employee & customer PII	Financial Data Credit cards, banking info
Threat Intelligence Planned attacks & exploits	Brand Monitoring Unauthorized use & spoofing



Coverage & Performance

24/7 Continuous Monitoring	1000+ DARK WEB SOURCES
15 min DETECTION TIME	12 mo DATA RETENTION

Alert & Response Workflow



Threat Detection



AI Risk Scoring



Multi-Channel Alerts



Automated Response



Proactive Detection

Identify threats before they become attacks



Rapid Response

15-minute detection with instant alerts



Reduced False Positives

AI-driven filtering for actionable alerts



Seamless Integration

Native OTM platform & API integration



Integration & Implementation

OTM Platform Integration

Fully integrated with Seceon's aiSIEM, aiXDR, and other OTM components for comprehensive threat management and automated response orchestration.

API-First Architecture

RESTful APIs enable custom integrations with existing security tools, ticketing systems, and workflow automation platforms.

Rapid Deployment

Cloud-based deployment with configuration completed in under 24 hours. No additional hardware or software installation required.



Support

Professional Services

- **Rapid Deployment:** 30-day implementation timeline
- **Custom Configuration:** Tailored to specific environments and requirements
- **Training and Certification:** Comprehensive education programs
- **Ongoing Optimization:** Regular health checks and tuning

Support Options

- **24/7/365 Support:** Global support coverage
- **Dedicated Customer Success:** Assigned technical account managers
- **Regular Updates:** Quarterly feature releases and monthly security updates

Learn more about Seceon



Schedule a Demo

www.seceon.com/contact-us/

