Solution Overview

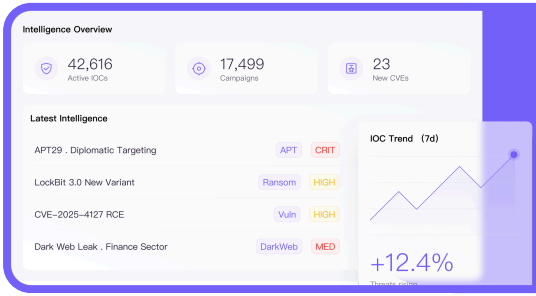
ORION

AI-Powered Threat Intelligence Platform

Make Security Decisions with Confidence

Threat intelligence only creates value when it leads to better decisions. Turn fragmented threat intelligence into confident security decisions.

Most organizations subscribe to multiple threat intelligence feeds, yet still struggle to determine which threats matter most. Effective cyber defense requires more than isolated indicators. It requires connected intelligence that correlates vulnerabilities, adversaries, malware, software supply chains, and dark web activity into a single view of risk. With that context, security teams can prioritize the threats that matter, make confident security decisions, respond faster to emerging threats, and stay ahead of an evolving threat landscape.



ORION delivers the threat intelligence generated by Digital Mind, digiDations' proprietary AI foundation, directly to security teams and their existing security tools. It provides a baseline layer of high-confidence IOC intelligence together with six specialized intelligence domains covering vulnerabilities, adversaries, malware, software supply chains, attack surfaces, and dark web activity, enabling intelligence-driven defense.

Full Lifecycle Threat Intelligence

PHASE 1 — PROACTIVE PREVENTION

Software Supply Chain Intelligence monitors more than 500,000 packages across ecosystems including NPM, PyPI, and Maven, identifying malicious or compromised dependencies before they reach production.

Vulnerability Intelligence identifies zero-day risks up to 48 hours before official disclosure, providing custom CVSS scoring and temporary mitigation guidance to reduce exposure during the remediation window.

PHASE 2 & 3 — ACTIVE DEFENSE & REAL-TIME DETECTION

Attack Surface Intelligence provides 96.8% visibility into exposed assets and shadow IT across more than 2,000 protocols, enabling continuous monitoring of external exposures for faster detection and response.

Malware Intelligence extends baseline IOC intelligence with behavioral context, delivering high-confidence indicators updated every five minutes for integration into SIEM and EDR platforms.

PHASE 4 — POST-INCIDENT RESPONSE AND ATTRIBUTION

Dark Web Intelligence monitors more than 2,500 forums and marketplaces, providing early warnings of data leaks and breach activity up to 72 hours before public reporting.

Threat Actor Profiling tracks more than 1000 threat actors delivering intelligence on tactics, techniques, and targeting patterns to support attribution and long-term defense planning.

Connected Intelligence Advantage

By correlating intelligence across multiple domains, ORION transforms fragmented indicators into a connected view of attacker behavior and intent, enabling security teams to:

- Connect vulnerabilities to active exploitation patterns and identify risks needing attention
- Identify who is being targeted, how they are being targeted, and why it matters
- Link indicators to specific threat actors, campaigns, and evolving adversary techniques
- Understand how attacker infrastructure is used in real-world campaigns to strengthen defenses

Together, these connections provide the context needed to prioritize threats, respond faster, and make more confident security decisions. ORION delivers not just more intelligence, but intelligence that is connected, contextual, and actionable.

Digital Mind AI Foundation and Platform Integration

ORION is powered by Digital Mind, digiDations' proprietary AI foundation that continuously collects, correlates, and operationalizes cyber threat intelligence. It powers every digiDations product, ensuring security teams, tools, and AI agents operate from the same continuously updated understanding of the threat landscape.

Digital Mind transforms raw threat data into structured, high-confidence intelligence for security operations, eliminating disconnected datasets and enabling a consistent approach to Autonomous Cyber Defense.

MASSIVE-SCALE GLOBAL COVERAGE

Processes more than 10TB of daily threat data across open, deep, and dark web sources, covering vulnerability disclosures, infrastructure signals, attacker activity, and software supply chain risk.

UNIFIED KNOWLEDGE GRAPH

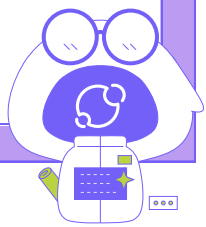
Correlates vulnerabilities, infrastructure, adversaries, and observed attack activity into a continuously updated connected model, enabling cross-domain intelligence relationships.

CONTINUOUS INTELLIGENCE

Continuously updates intelligence based on evolving adversary behavior, observations, and ecosystem signals to ensure relevance without manual curation or feed management.

HIGH-FIDELITY SIGNAL EXTRACTION

Delivers 96.5% intelligence accuracy with <0.3% false positives through AI filtering and validation, so security teams receive signal, not noise.



This shared intelligence foundation eliminates disconnected datasets, providing an always-current intelligence layer that enables a consistent approach to Autonomous Cyber Defense.

> **ORION** *transformed our threat intelligence from a 'reading list' into a 'defense list.' We now validate threats before they even hit our perimeter.*
>
> —— **Chief Information Security Officer, Global Financial Institution**

www.digidations.com
info@digidations.com

digiDations is an AI Native cybersecurity company helping organizations move from hoping their defenses will hold to knowing they will through Autonomous Cyber Defense.