ORNA™

Extended Managed Detection & Response (X-MDR).

A true 24/7/365 extension of your team, empowered by the industry's only collaborative incident response platform.

Managed Detection and Response vendors are a dime a dozen. **But the promise is flawed.**

At ORNA, we believe that true MDR should go all the way. Lightning-fast alert triage and incident containment every minute of every year, yes. But also, regulatory compliance, communications, executive risk management, legal, HR, and even 3rd party guidance at every step of the incident 24/7/365. And around-the-clock transparency through the world's first vendor-customer collaborative X-MDR platform.

24/7/365 Response
Our threat response team will investigate and contain attacks on your business every minute of every day of the year

Full-Service
Unlike typical MDR vendors, we drive response across the entire incident, not just initial triage and containment

Total Visibility
Through ORNA, you see everything: alerts, investigations, evidence, reports, even asset risks and compliance KPIs

Risk Mitigation
ORNA automatically correlates with the NIST CSF framework and guides your risk mitigation journey proactively

Quick Win
ORNA has over 200 integrations with your existing tools, and is rolled out in less than a week by our own team

Your Stakeholders

You see everything in an unprecedented level of detail in one single correlated MDR hub.

Your entire tech stack feeds into ORNA through 200+ integrations.

- Full visibility into alerts, investigations, and more.
- Automated external and internal comms, escalations.
- NIST CSF risk scoring, asset risk analytics, compliance.
- Instant detailed custom incident reports.
- Automated cross-functional IR, DR, BCP playbooks.

Our SOC Team

We monitor your entire infrastructure 24/7/365 using ORNA and respond to threats.

The team is responsive through built-in conversation features.

- On-premises, cloud, ICS/OT - we monitor your entire stack.
- 24/7 threat hunting and response by experts.
- Heuristics and complex multi-factor threat analysis.
- 1200+ detection rules enhanced with ML and AI.
- Responding to the entire attack, not just triage.

Join over 175 companies across 8 industry verticals in 11 countries that already love ORNA and are happy to put their name to it.

"Orna Incident Management gives me and my directors confidence that if we were to sustain a cyber attack, we can react confidently with the added comfort of knowing an ORNA specialist is available 24/7.
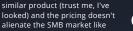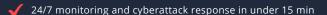
"ORNA allows the ability to have high-end capability with the added advantage of being simple to use when responding to phishing incidents. It gives my team the confidence in containing a more significant cyber security incident if we ever fell victim to an attack.

★★★★★
ORNA's guidance and support, and response to any issues we have or spotting an issue before it hits us is critical to the way we operate today and in the future.

Elliott Steele
IT Director, Powell Group

★★★★★
In the first month of operating with the ORNA platform, Indeloy has been able to identify our most targeted assets.

Jamie Sleigh
Director, Indeloy

Technical Highlights

Startup Business of the Year — Canadian SME Awards
Canada's Top 15 Cyber Startups 2023 — Canada Venture News
Top 50 InsurTech Companies — Plug & Play Ventures
Cyber Platform of the Year — Wealth & Finance
Collision 2022 Startup Awards Finalist — Collision Conference
Top 100 Cyber Startups for FinTech — FinTech Global

- 24/7 monitoring and cyberattack response in under 15 min
- 24/7 live insights into alerts, investigations, assets, & more
- 24/7 threat hunting and early-warning attack disruption
- Cyberattack response support for all business functions
- Detailed, automated cross-functional IR, DR, BCP playbooks
- Advanced heuristics and instant complex threat correlation
- Resilient monitoring agents with anti-tampering protection

- File integrity monitoring, including detecting changes in permissions
- Insider threat and complex behavioral anomaly detection capabilities
- Advanced log and alert correlation and deduplication dashboard
- NIST CSF dashboard with proactive risk mitigation guidance and KPIs
- Malware, rootkits and anomaly detection for on-prem, cloud, and more
- Asset risk analytics and register, dynamically correlated with alert data
- Detailed, instant reporting for all incidents with customizable depth