IRONSCALES

IRONSCALES® for Manufacturing

Email Security Designed to Reinforce the Supply Chain

Inbox-level email security that keeps production schedules, supplier payments, and IP safe. Protect supplier trust, keep lines running, and reinforce a distributed workforce.

How It Works: Adaptive AI + Agentic Automation

Inbox-Level Visibility
We scan emails in real time, *after* delivery, inside your inbox. All via our API integration with M365 and GWS. No MX changes. No disruption to production or supplier communications.

Behavioral Baseline
Our Adaptive AI learns your unique communication patterns using NLP and NLU. It builds a social graph for everyone, to catch the most subtle signs of attacks.

Detect the Undetectable
Machine learning, computer vision, and intent analysis catch fraudulent pro-forma invoices, fake tooling deposits, and shipment reroute scams —even when there are no malicious links or attachments.

Agentic Automation
Themis, our agentic virtual SOC, autonomously investigates, clusters, and remediates threats across all inboxes in seconds.

Reinforced by Human Insights
Themis integrates SOC team feedback and community intelligence to sharpen detection and response.
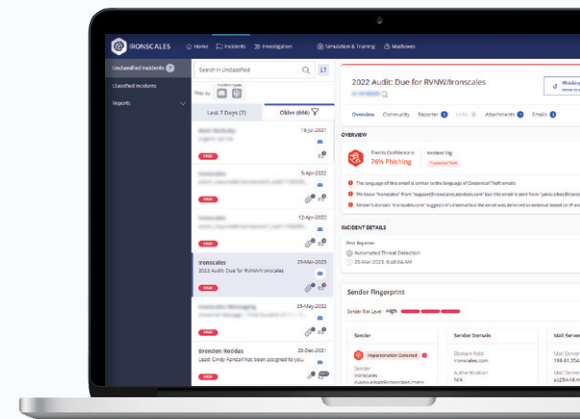
Agentic Capabilities

Adaptive AI Detection
- NLP/NLU behavioral baselining
- Social graph analysis per user
- Computer vision for visual threats

Agentic Response
- Autonomous threat clustering & remediation
- Dynamic warning banners & user alerts
- One-click incident management

Continuous Improvement
- Self-learning AI models
- SOC feedback loops
- Community-driven insights
- Audit-ready compliance

Empower Your Team

Give accounting clerks, buyers, engineers, and plant teams real-time tools to spot supplier fraud, fake invoices, and drawing review scams. Role-based training, contextual inbox banners, and a GPT-powered assistant turn your workforce into defenders without slowing operations.

Simplify Your Security

Themis, our agentic AI virtual SOC, autonomously clusters and removes malicious shipment notices, fraudulent bank requests, and other phishing threats across all inboxes. This slashes manual investigation time by 99% so your team can focus on keeping MES, ERP, and WMS running.

Get Started Fast

Deploy in just three clicks with Microsoft 365 or Google Workspace—no MX record changes, no mail reroutes, and no downtime. Adaptive AI starts protecting supplier communications, engineering exchanges, and plant workflows immediately, keeping production and payments secure.

Integrated Training That Works

Turn your buyers, engineers, accounting, and plant staff into defenders

Automated phishing simulations, integrated security awareness training (SAT), dynamic email banners, and a GPT-powered assistant sharpen employee awareness in real time—right where threats land.

- **Role-based phishing simulations** tailored for manufacturing teams using real lures like fake tooling deposits, shipment reroute requests, and review scams

- **Dynamic inbox banners** warn employees when a request involves a first-time supplier bank change, a new reply-to domain, or an unusual payment timing

- **Training records and feedback loops** provide audit-ready evidence for CMMC, SOX, and ITAR compliance
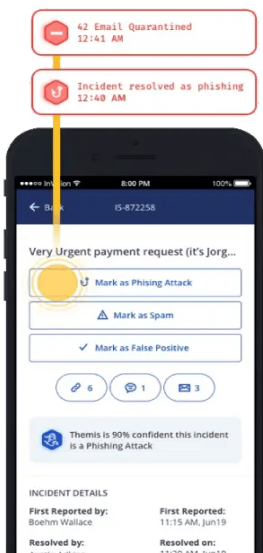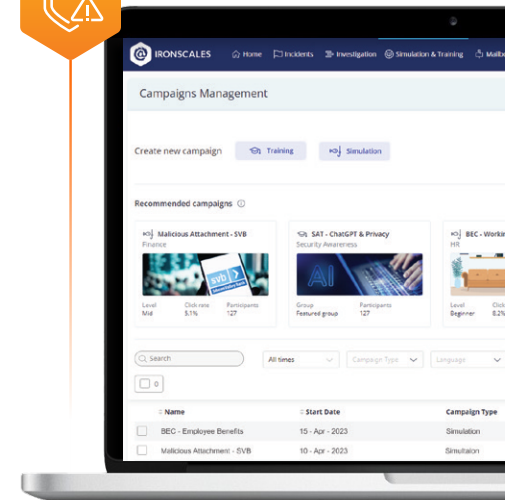
Simplify Your Security

Slash 99% of manual email security tasks with agentic automation

Themis autonomously clusters and remediates threats across inboxes—acting instantly, alerting admins only when needed. **Agentic automation** built to handle manufacturing's expansive digital footprint.

- **Remediate threats automatically** across every inbox with Themis, our agentic AI virtual SOC—clustering malicious supplier invoices, shipment notices, and impersonation attempts across all mailboxes in seconds

- **Tune to your comfort level**—adjust automation thresholds and set controls for phishing, spam, and graymail — aligning with plant and corporate policies

- **Audit-ready reporting console** provides CISOs and COOs visibility into incidents, containments, and remediation history across the manufacturing network

Quickly see what threats are lurking in your O365 mailbox with our 90-day threat scan back.

Our free 90-day scan back automatically reviews your Microsoft 365 email environment and quickly identifies malware, BEC, phishing, ATO, and other phishing threats that were missed by your SEG.

REQUEST YOUR 90-DAY SCAN BACK ↗

INCIDENT BREAKDOWN

248 INCIDENTS FOUND

- Malicious Links and Attachments
- Fake Login Page
- CEO Fraud
- Business Email Compromise
- Account Takeover

Learn how working with IRONSCALES makes us Safer Together.

Learn More ↗

Everything is just a click away, from initial installation to threat identification and removal.