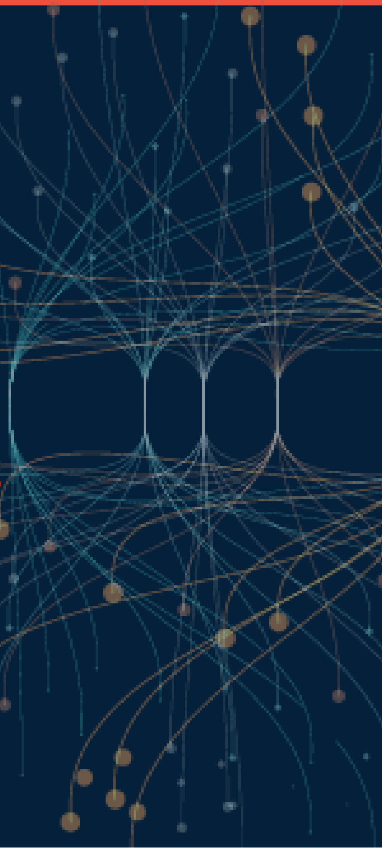
IronTraps



Automated Email Phishing Investigation, Orchestration & Response

Organizations of all sizes are failing to detect and respond to malicious emails delivered to employee inboxes in a timely manner. Phishing awareness training is only partially effective for email phishing protection, and when employees do spot a suspicious message they quite often lack the tools to report it. But even when such messages are reported, SOC and security teams have to deal with the incident analysis and response manually - a process which is too slow and too labor intensive.

In today's phishing threat landscape, security and risk management leaders need automated email phishing protection and incident response capabilities.

Key Business Benefits

1.

Allow users to be part of the email phishing protection solution, report suspicious emails missed by technical controls such as SEG.

2.

Leverage user training by providing the tools for employees to be able to report suspicious emails.

3.

Reduce manual email analysis and response with automation, improving efficiency for SOC/security

4.

Minimize potential for business disruption or financial fraud due to phishing attacks.

Post Email Phishing - Delivery Incident Response

IronTraps is the first and only automated email phishing protection, detection and incident response module, combining human intelligence with machine learning to streamline phishing incident analysis, threat intelligence gathering (forensics), orchestration and response automatically or at the click of a button.

Acting as a virtual force multiplier for IT operations, security operations and managed security service providers (MSSPs), IronTraps eliminates the need for highly trained SOC or security analysts to manually deal with every email phishing threat, while reducing the time from phishing detection to remediation from weeks or months to just seconds.

Even if end-users don't report on every phishing email, IronTraps' patented machine learning algorithms automatically clusters and find similarities in phishing emails in real time, preventing email permutations such as polymorphic attacks/campaigns from going undetected.

SC Lab Reviews

FEATURES:
★★★★★

PERFORMANCE:
★★★★★

DOCUMENTATION:
★★★★★

SUPPORT:
★★★★★

VALUE FOR MONEY:
★★★★★

EASE OF USE:
★★★★★

5/5

How Does IronTraps Facilitate Rapid Response?

IronTraps collects email threat data and alerts from different sources, where incident analysis and triage can be performed automatically leveraging a combination of human and machine power to help define, prioritize and drive standardized incident response activities according to a standard workflow, making it quick and easy for security analysts to classify reported email incidents.

Why IronTraps?

- Detect and prevent advanced phishing threats
- Reduce the time phishing emails lay idle in employee mailboxes
- Decrease email admin resources (no more scripts and tools)
- Use technical and end-user control to detect phishing emails

Features

- Automated phishing forensics, orchestration and remediation
- Intuitive dashboard built for rapid response
- Multi-client phishing report button
- Integration and orchestration with other 3rd party tools
- Resolve incidents on the go on mobile

Deployment

IronTraps is available as a quick and easy two-click deployment for Office365 and G Suite in the cloud, on premise, or hybrid, with no MX records changes required.

Other Products

- IronShield
- IronTraps
- Themis
- IronSights
- Federation
- IronSchool

IRONSCALES

For more information
visit our website at www.ironscales.com
and follow @ironscales on Twitter
Contact us at contact@ironscales.com

Headquartered in Tel Aviv, Israel, IRONSCALES was incubated in the 8200 EISP, the top program for cyber security ventures, founded by Alumni, the Israel Defense Forces' elite intelligence technology unit.