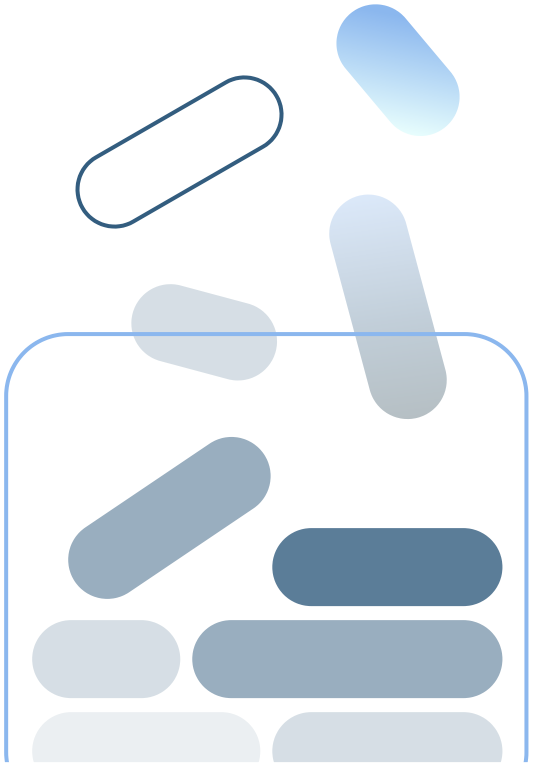
Automated Phishing Analysis | Phishing Incident Response

Archived: 2026-04-06 02:08:10 UTC

ThreatConnect for Phishing Attack Analysis and Response

Phishing is on the rise, and the best way to protect your organization is to know what you’re looking for. ThreatConnect automates phishing analysis to simplify the hunt for legitimate threats. The Platform handles suspicious emails, reducing the time to remediate active threats from days to minutes.



Save time spent on phishing email analysis with automation

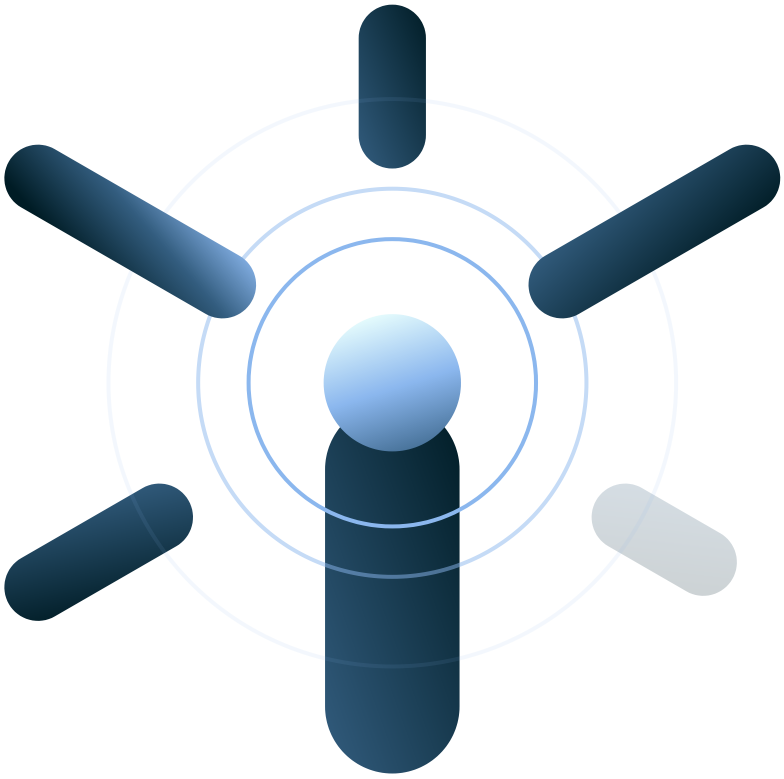
Automated phishing analysis saves you time and helps you defend against phishing attacks faster and with more precision. ThreatConnect has out-of-the-box workflow templates for phishing incident response and analysis tools that identify, enrich, and help you respond to threats.

Read Customer Story on Phishing Automation

Prioritize phishing emails to reduce time to respond

ThreatConnect’s phishing response playbook includes in-platform scoring that prioritizes emails and automates enrichment. You no longer need to manually identify malicious indicators, cutting down on your response time.

Join a Monthly Live Demo



Maximize insights on phishing trends

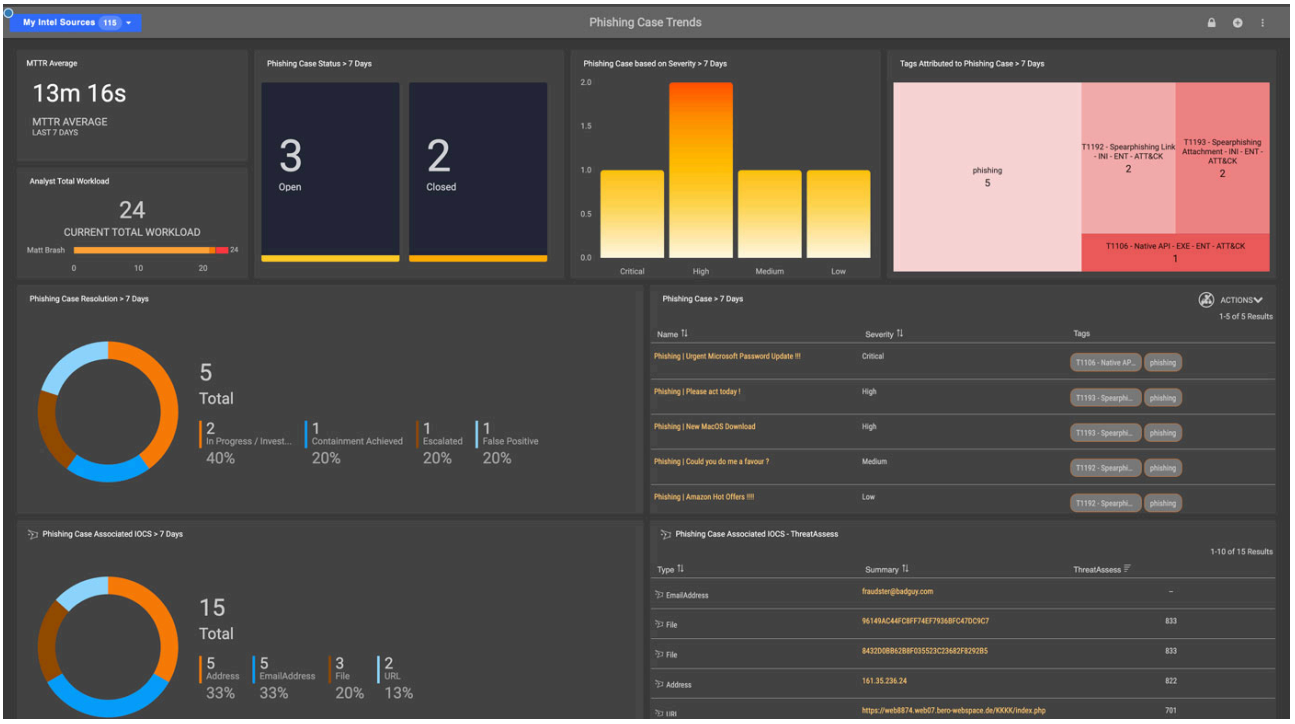
Phishing attacks evolve as attackers learn what works and what doesn’t. Your organization needs phishing analysis tools to keep up with the latest trends. ThreatConnect provides accurate, current information about messages based on collective threat intelligence.

Explore ThreatConnect Platform in Interactive Tour

ThreatConnect Advantages

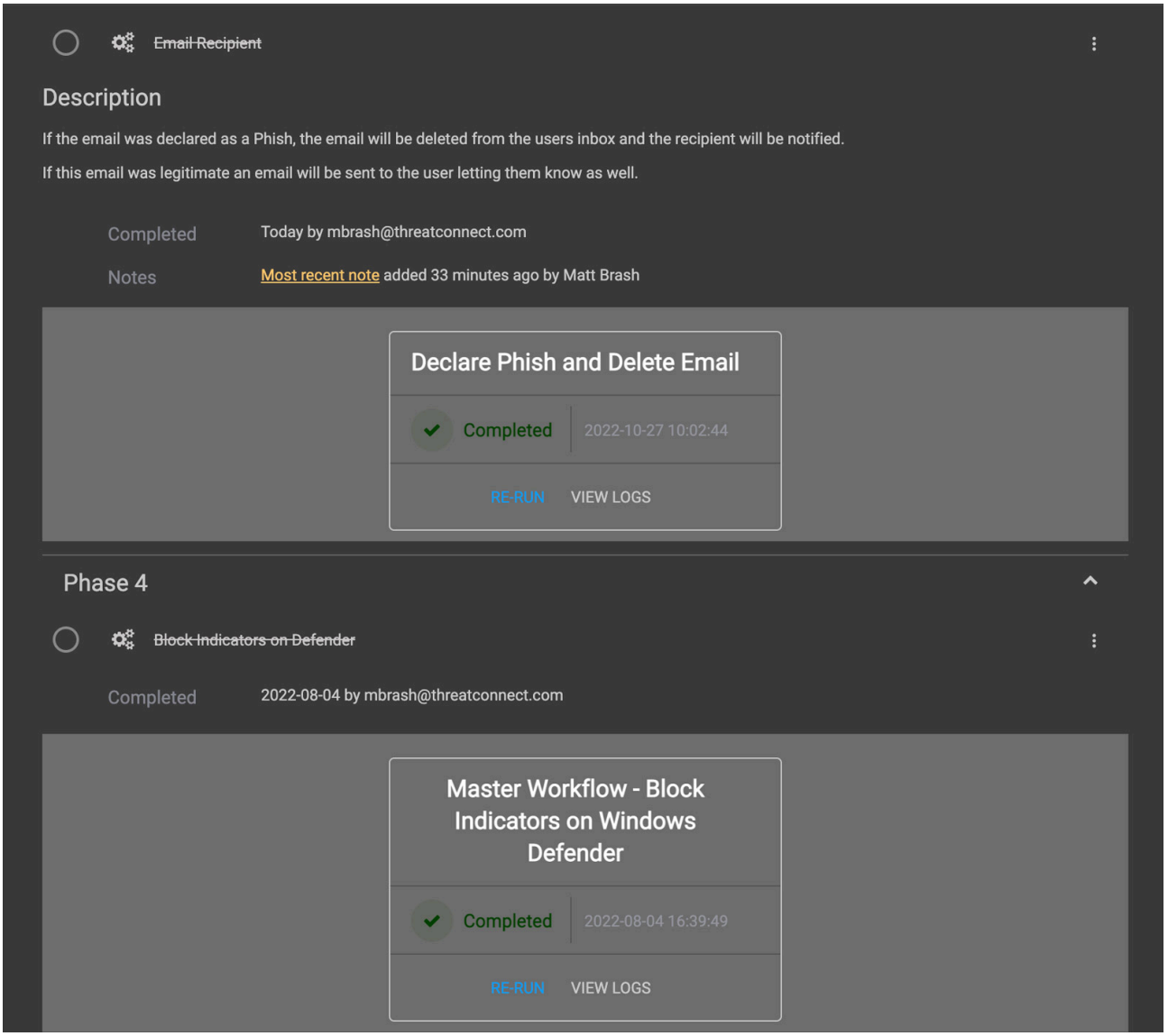
Automated email analysis

ThreatConnect lets you automatically analyze reported emails to look for indicators across file attachments, embedded links, and other information. Enrich indicators with threat intelligence from third-party feeds and CAL™ to identify known malicious indicators and automatically send the indicators to your security tools, like secure email gateway and firewalls, to respond.



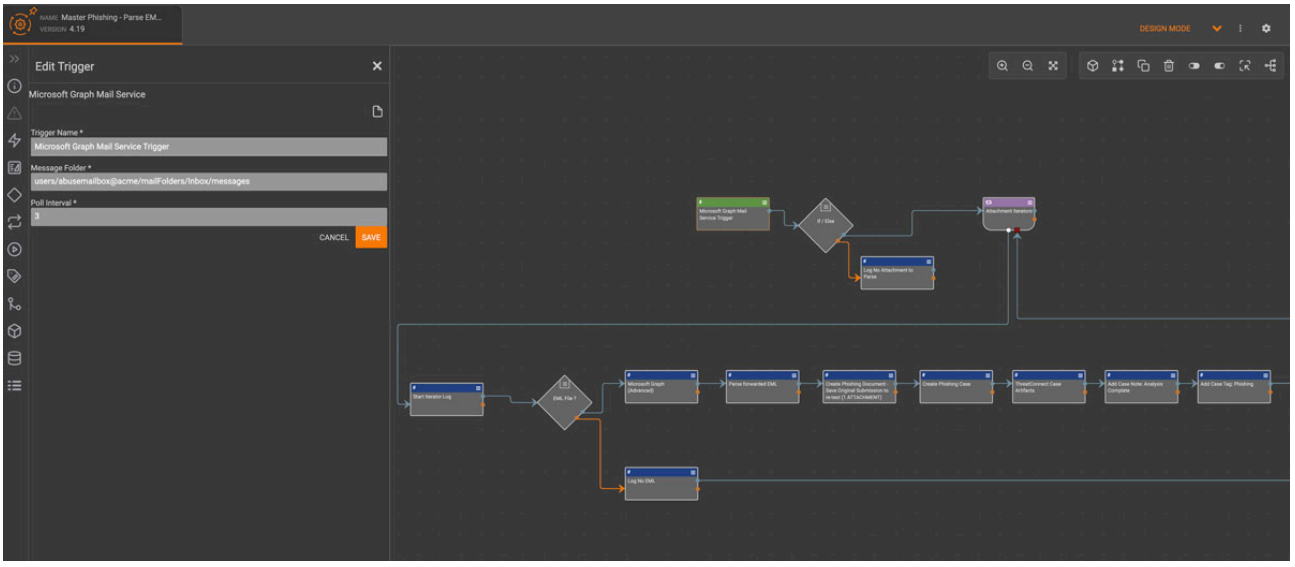
Quicker response times

Get automated notifications when an email contains malicious indicators, triggering response efforts like blocking the indicator in phishing defense tools like firewalls and secure web gateways. If an email is marked safe you can mark the indicator as a false positive in your threat library and add it to your exclusion list for future investigations.



Easy user reporting

Make it easy for your team members to report suspicious emails. Set up a mailbox for centralized reporting of potential phishing emails from all sources, including both humans and technologies. When the mailbox receives a message, the rest of the Playbook is triggered to automate the analysis and corresponding response efforts.



> With ThreatConnect, we automated our phishing triage, analysis, and response, and reduced the time it took to analyze thousands of phishing emails from 3+ hours per campaign to minutes. Mean time to remediate decreased by 92% vs the original 15% target over baseline.

SOC Team Lead

Global Forbes 2000 Hospital & Healthcare System

Trusted by leading companies

- **Reduce false positives**
- **Reduce time to analyze a phishing email**
- **Reduce mean time to remediate**

Take time back in your day by automating phishing analysis and response.
