Phishing Detection & Response

Key Component Within Autonomous SOC

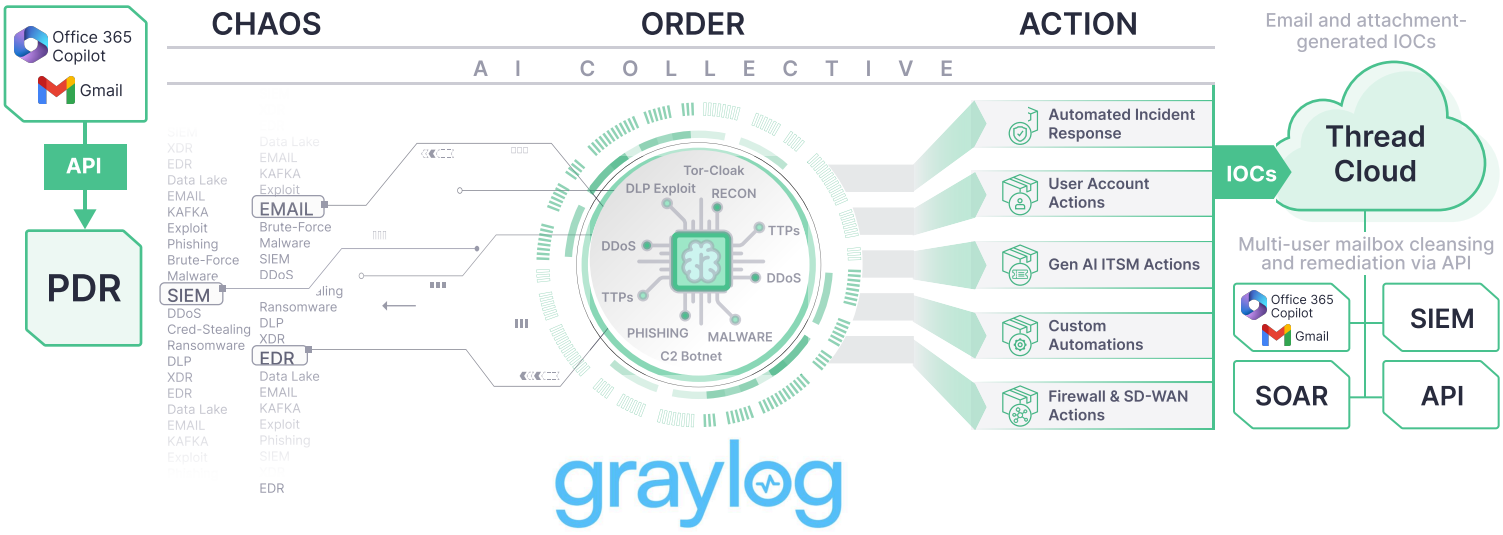
The trend in the Managed Detection and Response (MDR) marketplace is moving towards a fully automated or Autonomous Security Operations Centre (ASOC) model aimed at automating as much as possible, including ingestion, processing, and remediation. SOC Prime and its Ecosystem partners work together to deliver an autonomous SOC to MSPs, MDRs, MSSPs, and enterprises, with a focus on automating key pain points that all SOCs encounter.

Phishing incidents still account for over **80%** of security events in a modern-day SOC. Despite customers and MDRs being equipped with email content filtering and phishing solutions, attacks continue to slip through. Yet, automation helps to tackle these risks by detecting, protecting, and preventing future attacks. Threat intelligence gathered from automated detection and threat hunting is then shared to strengthen other SOC areas like SIEM, EDR, and CASB, further enhancing overall protection.

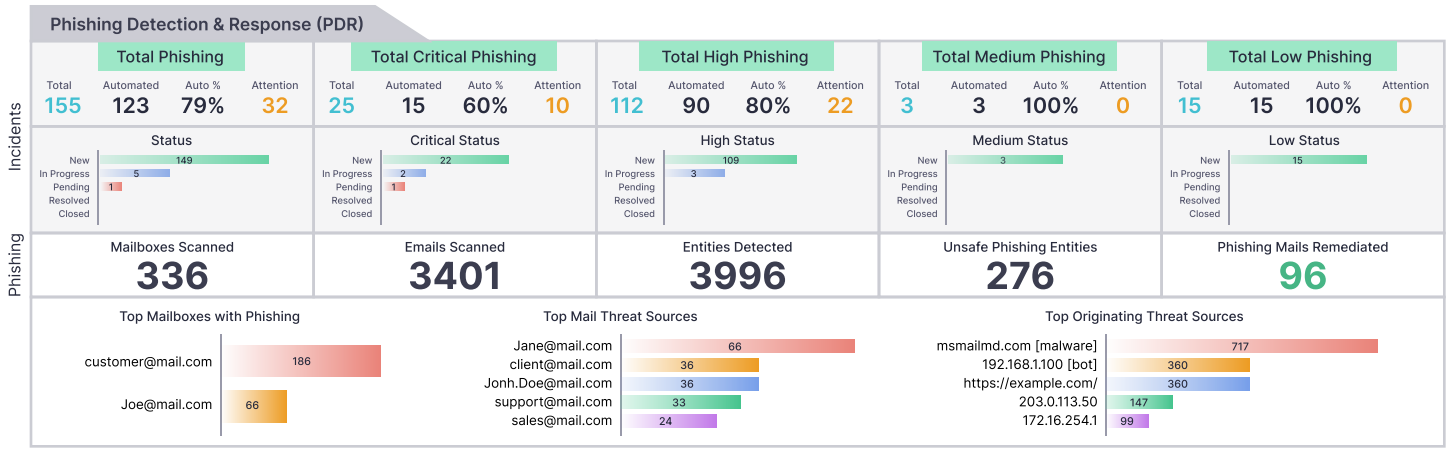
Email Threat and Phishing Detection App

DataHelix AI's Phishing Detection & Response (PDR) seamlessly integrates via API with popular email platforms such as Office 365 and Gmail. It applies DataHelix AI's threat detection and hunting algorithms to all email content, including attachments and, more importantly, embedded web links within emails, to detect all phishing attacks targeting the organization.

Graylog Phishing Detection and Response (PDR)



Phishing SOC Analyst Dashboard



PDR threat hunts all emails and attachments and then automates Incident Response to them:

- Search Microsoft 365 Copilot or Gmail for all users' mailboxes similarly infected
- Delete and clean up mailboxes
- IOC Search across SIEM, EDR, and other security tooling to ensure the eradication of phishing attacks
- Automatically blocks attacks via Firewalls and SOARs
- Creates and maintains an Enterprise Threat Cloud to be used for Threat Hunting and defending against longer-term “Living off the Land” attacks

The Benefits

- Delivers an automated phishing detection service with minimal resources required
- Performs advanced security content & behavioral analysis of emails and attachments
- Enriches and compliments Microsoft 365 Copilot, Gmail, and existing email security
- Threat hunts every email based on the company-specific criteria
- Sends only surfaced detections and alerts to SIEMs and ticketing systems
- Performs to scale and can be SaaS, on-premises, or hybrid-based

Why DataHelix PDR?

- Phishing forensics inspection at scale
- Phishing response automation & orchestration
- Linkage with other platforms for cross-platform detection
- Email checking against the latest threat vectors

DataHelix AI: Next-Gen Autonomous SOC Solution

DataHelix AI represents a next-gen autonomous SOC solution that leverages automation at multiple layers within the SOCs. A key feature of the platform is that it is completely data-agnostic, meaning it can support any data plane, including logs, API calls, databases, network packets/traffic, email, web proxies, SIEMs, and SD-WANs.

Start applying AI and Automation to your SOC now, with expert guidance from us! For more details on the Autonomous SOC approach powered by DataHelix AI, reach out to your local sales representative at sales@socprime.com or kick off your journey with SOC Prime at https://socprime.com/.