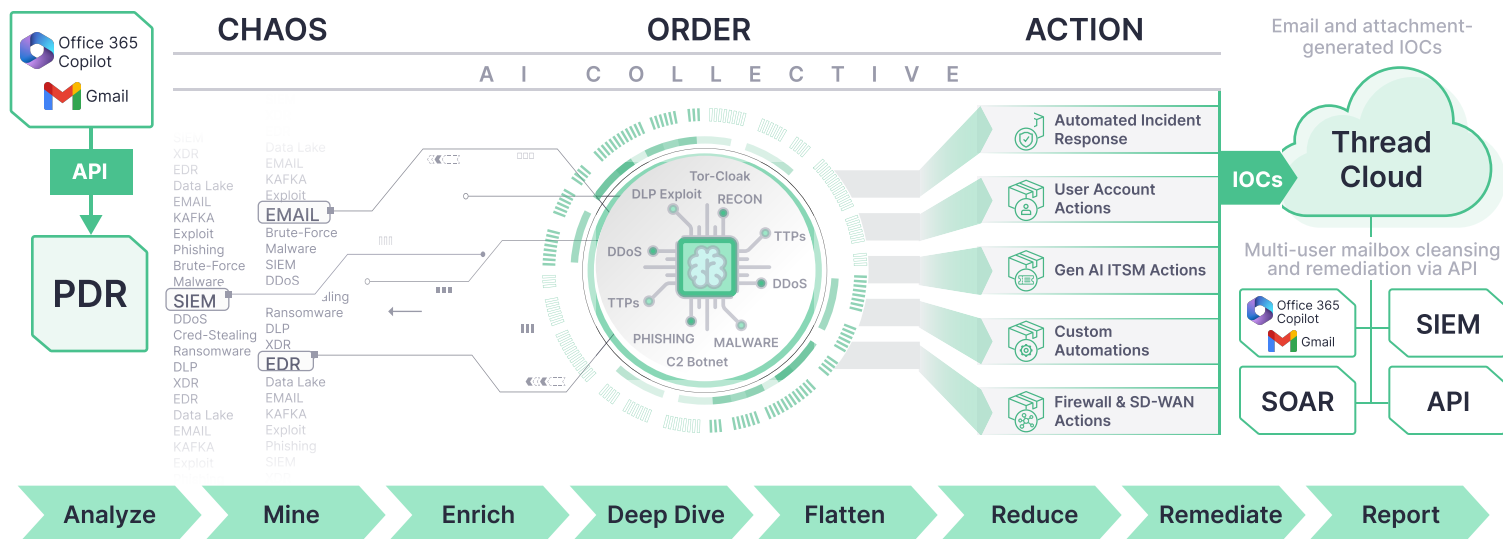# Phishing Detection & Response
Key Component Within Autonomous SOC

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.
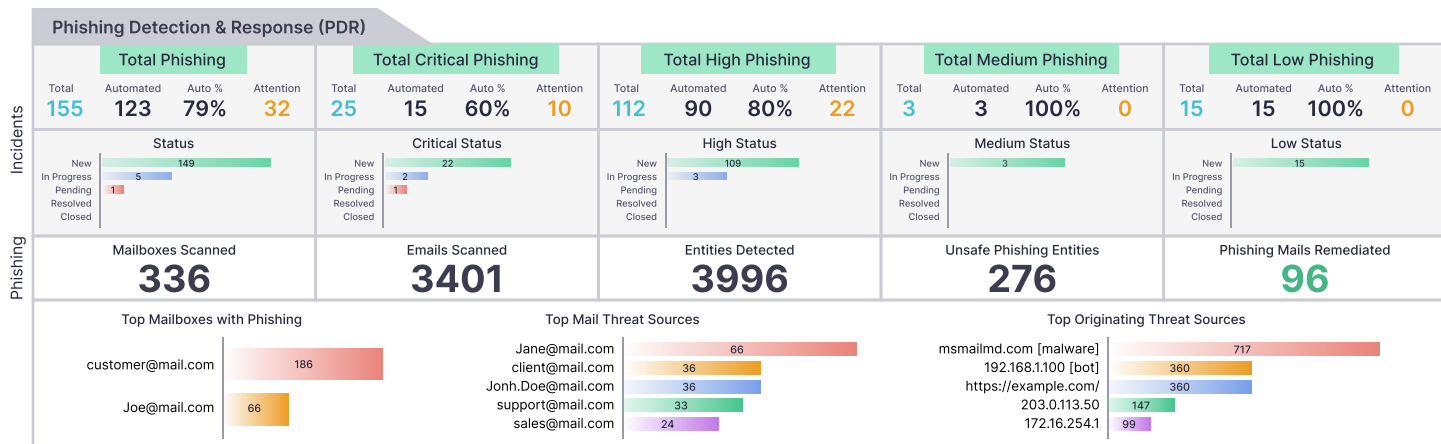
Phishing incidents still account for over **80%** of security events in a modern-day SOC. Despite customers and MDRs being equipped with email content filtering and phishing solutions, attacks continue to slip through. Yet, automation helps to tackle these risks by detecting, protecting, and preventing 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.

SOC PRIME

Office 365 Copilot
Gmail

CHAOS | **ORDER** | **ACTION**

Email and attachment-generated IOCs

A I   C O L L E C T I V E

API

PDR

XDR
EDR
Data Lake
EMAIL
KAFKA
Exploit
Phishing
Brute-Force
Malware
SIEM
DDoS
Cred-Stealing
Ransomware
DLP
XDR
EDR
Data Lake
EMAIL
KAFKA
Exploit

Data Lake
EMAIL
KAFKA
Exploit
EMAIL
Brute-Force
Malware
SIEM
DDoS

Ransomware
DLP
XDR
EDR
Data Lake
EMAIL
KAFKA
Exploit
Phishing
SIEM

SIEM
EDR

Tor-Cloak
DLP Exploit   RECON
TTPs
DDoS
DDoS
TTPs
PHISHING   MALWARE
C2 Botnet

Automated Incident Response
User Account Actions
Gen AI ITSM Actions
Custom Automations
Firewall & SD-WAN Actions

IOCs

Thread Cloud

Multi-user mailbox cleansing and remediation via API

Office 365 Copilot
Gmail
SIEM
SOAR
API

| Analyze | Mine | Enrich | Deep Dive | Flatten | Reduce | Remediate | Report |

Phishing SOC Analyst Dashboard

Phishing Detection & Response (PDR)

Incidents

	Total Phishing				Total Critical Phishing				Total High Phishing				Total Medium Phishing				Total Low Phishing			
	Total	Automated	Auto %	Attention	Total	Automated	Auto %	Attention	Total	Automated	Auto %	Attention	Total	Automated	Auto %	Attention	Total	Automated	Auto %	Attention
	155	123	79%	32	25	15	60%	10	112	90	80%	22	3	3	100%	0	15	15	100%	0

Status	Critical Status	High Status	Medium Status	Low Status
New 149	New 22	New 109	New 3	New 15
In Progress 5	In Progress 2	In Progress 3	In Progress	In Progress
Pending 1	Pending 1	Pending	Pending	Pending
Resolved	Resolved	Resolved	Resolved	Resolved
Closed	Closed	Closed	Closed	Closed

Phishing

Mailboxes Scanned	Emails Scanned	Entities Detected	Unsafe Phishing Entities	Phishing Mails Remediated
336	3401	3996	276	96

Top Mailboxes with Phishing

customer@mail.com	186
Joe@mail.com	66

Top Mail Threat Sources

Jane@mail.com	66
client@mail.com	36
Jonh.Doe@mail.com	36
support@mail.com	33
sales@mail.com	24

Top Originating Threat Sources

msmailmd.com [malware]	717
192.168.1.100 [bot]	360
https://example.com/	360
203.0.113.50	147
172.16.254.1	99

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

- 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/.