Cofense Integration Brief

COFENSE TRIAGE™ AND CISCO UMBRELLA INVESTIGATE

Cofense and Cisco Umbrella Investigate combine the power of human-reported phishing attacks with global insight into malicious domains and networks. The end result enables security analysts to make intelligent, actionable decisions using both internally-generated and global threat intelligence.

The Challenges

The Neglected Link

Attackers focus on infiltrating your defenses through your employees. What they don't realize is that humans can be your strongest defense and best source of attack intelligence.

Alert Fatigue

Phishing remains a top cyber threat, but the volume of security alerts is overwhelming. When time is of the essence, clear, actionable information is paramount.

Point Solutions

Each technology solution has a role for solving a particular problem, but must interperate with others in the security stack. Integration is necessary for organizations to achieve maximum visibility into phishing attacks.

THE PROCESS

Incident Response

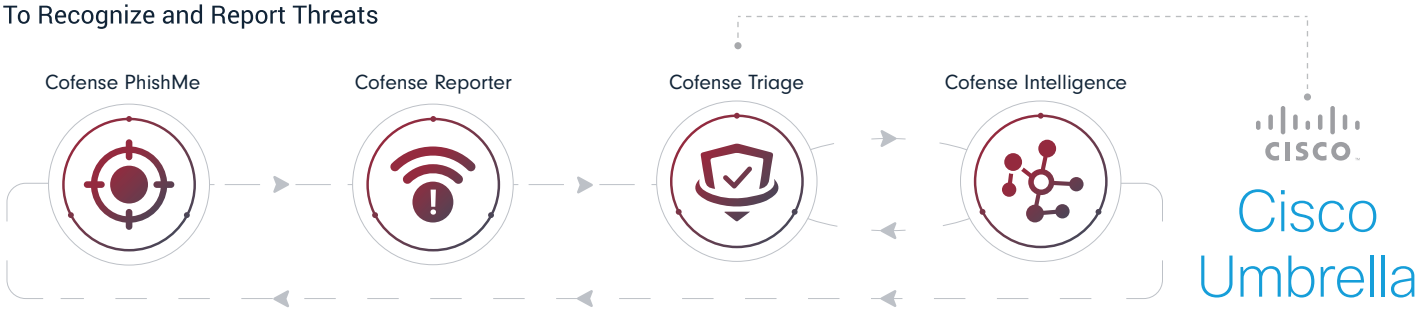
- ✓ Leverage existing intelligence investments.
- ✓ Analyze email through an anti-malware engine in tandem with global threat intelligence from Cisco Umbrella Investigate

Integration

- ✓ Collect and prioritize internally-generated phishing threats
- ✓ Analyze rich anti-malware data through an automated algorithmic engine designed to reduce excessive alerts
- ✓ Create and automate phishing incident response processes.

How It Works

CONDITION EMPLOYEES
To Recognize and Report Threats



SPEED INCIDENT RESPONSE
Collect, Analyze, and Respond to Verified Active Threats

Cofense Triage and Cisco Umbrella Investigate work together through a RESTful API to quickly prioritize security events and streamline analysts' incident response process for security risk domains, IP addresses, and associated networks contained in malicious emails.

Cofense Triage is designed to simplify phishing incident response events matching malicious content from email reported by employees that perimeter defenses missed. Triage determines contextual commonalities and indicators of phishing (IoPs) through URL and IP address analysis, anti-malware technologies, and phishing threat intelligence, as well as human intelligence reputation, volume, and severity.

Cisco Umbrella Investigate provides the most complete view of the relationships and evolution of Internet domains, IP addresses, and autonomous systems to pinpoint attackers' infrastructures and predict emergent threats. Cisco Umbrella Investigate analyzes more than 80 billion Internet requests daily from over 65 million active users across 160+ countries. Plus, 500 peering partners exchange BGP route information to show connections and relationships between different networks on the Internet.

When integrated with Triage, the analyst receives intelligence from Investigate that is contained within the appliance to rapidly highlight malicious, benign, or suspicious domains or IP addresses on the Internet. The analysis is automated at email ingestion to ease the analysts' research requirements and speed up their decision-making response time. Triage empowers the analyst to create custom procedures for similar or future events as well as escalate as part of the incident response work ow. Incident responders are armed with enriched information to prevent future events, or create specific detection criteria to glean more from the targeted attack tactics.

The ability for Triage to identify and rank threats based on its own analysis engine is complimented by Investigate to reaffirm the email contains attributes leading to credential or host compromise capabilities. The integration delivers enterprise security teams a significantly better return on security investment aimed at reducing the #1 threat facing security leaders today; spear phishing.

Cofense's Human Phishing Defense

Cofense Triage can accept input from other sources but is seamlessly integrated with Cofense Reporter and Cofense PhishMe for a comprehensive program to condition employees to recognize phishing attacks and enable them to easily report attacks to security teams.

About Cisco Umbrella Investigate

Cisco Umbrella Investigate provides threat intelligence about domains, IPs, and malware across the internet. Leveraging a diverse dataset of 80+ billion daily DNS requests and live views of the connections between different networks on the internet, we apply statistical models and human intelligence to pinpoint attackers' infrastructures and predict future threats.

cisco Cisco Umbrella

COFENSE

W: cofense.com/contact T: 703.652.0717
A: 1602 Village Market Blvd, SE #400 Leesburg, VA 20175