FORTRA

SOLUTION BRIEF

# Agari Integration for Palo Alto Networks Cortex XSOAR

## Integrate Email Threat Data to Improve Threat Visibility and Accelerate Incident Response

Email is a primary vector for attacks on your business today—and email threats are evolving faster than ever. But actionable data about email attacks is often inaccessible to time-strapped security operations and incident response teams. That disconnect leaves your business vulnerable and unable to mitigate hidden email threats.

### Improve Visibility with Integrated Email Threat Data

The Agari integration with Palo Alto Networks Cortex XSOAR solves this challenge and makes it easy to surface email threats by quickly integrating valuable Agari threat intelligence into the Cortex XSOAR dashboard. Your team can analyze and correlate Agari data in playbooks, query logs to trigger custom alerts, enrich incidents with Agari threat data, and create shared views and dashboards for stakeholders in your organization.

### Accelerate Incident Response and Drive SOC Efficiency

The Agari integration with Cortex XSOAR empowers security teams to work more effectively to mitigate email threats. Leveraging Agari incident data and Cortex XSOAR's orchestration tools, security analysts can incorporate email incidents in custom workflows to improve investigations and accelerate resolution—without needing to jump through hoops to transform log data or manually import feeds. With the ability to track and resolve security incidents through a single pane of glass, your team can focus on remediation of email threats, not repetitive labor and administrative overhead.

### Leverage Your Strategic Palo Alto Networks and Agari Investments for Security

The Agari integration with Cortex XSOAR supports Agari Phishing Defense to stop phishing, BEC, and other identity deception attacks that target employees. Integrating email threat data across applications helps you get maximum value from your security investments and and helps to safeguard your entire infrastructure against email threats.

### AT A GLANCE

Agari integration with Palo Alto Networks Cortex XSOAR makes it easy to connect Agari email threat data to Cortex XSOAR, improving visibility into email threats, accelerating incident response, and driving SOC efficiency.

#### HIGHLIGHTS

**Unlock email threat intelligence**

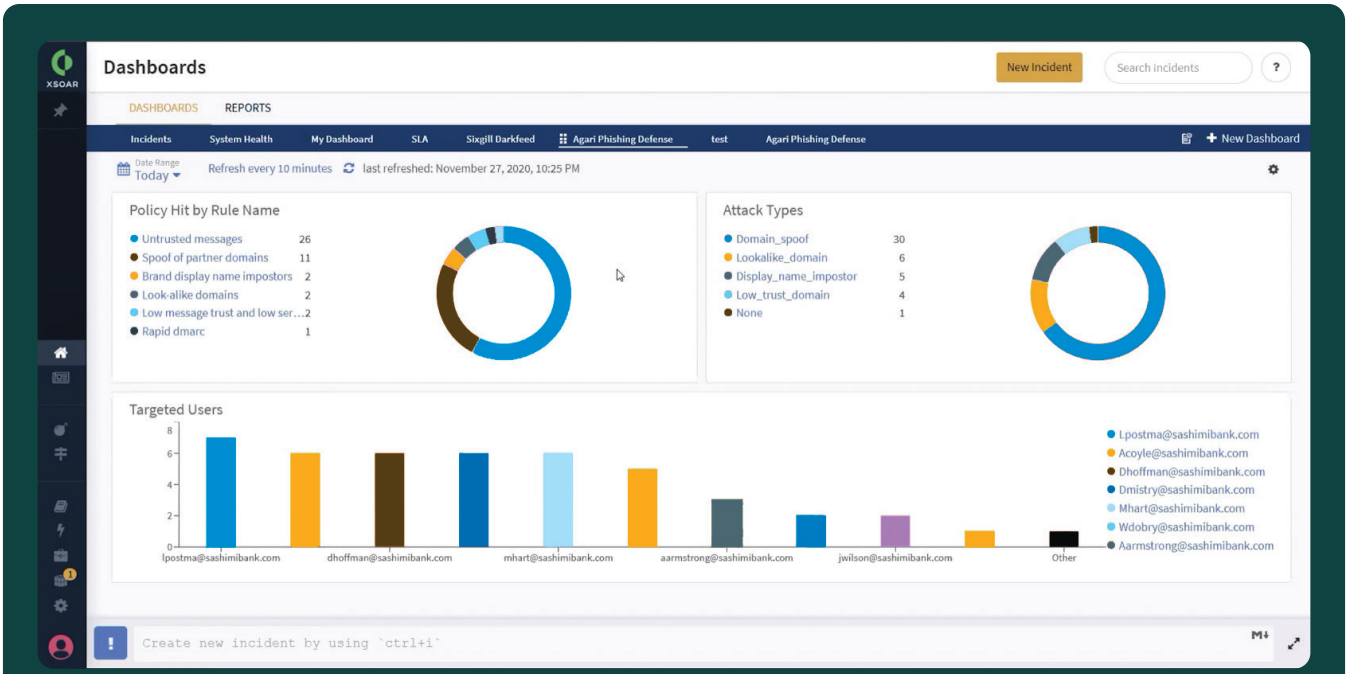
Integrate Agari email threat data across applications and orchestrate workflows to manage security incidents through a single pane of glass.

**Quickly connect and deploy**

The preconfigured integration is easy to connect and get started, but is highly flexible to meet your organization's unique needs.

**Integrate email threat data from Agari Phishing Defense**

Connect Agari Phishing Defense to Cortex XSOAR.



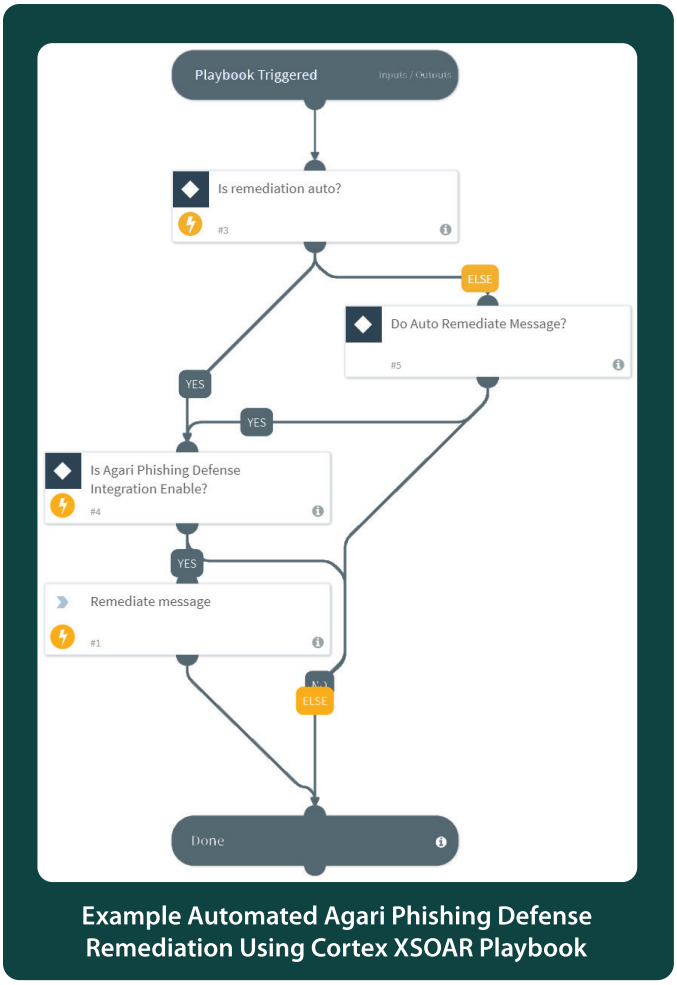

Agari Email Threat Data in Cortex XSOAR Dashboard

## Build and Orchestrate Workflows to Quickly Deliver Results

The Agari integration with Cortex XSOAR helps your team quickly operationalize email threat data to realize value for your organization by leveraging automated, orchestrated collaborative workflows; creating standard security and compliance playbooks; and simplifying incident tracking and case management.

Preconfigured playbooks help address common use cases, including remediating incidents flagged by Agari Phishing Defense policy events. This example of playbook automation retrieves email data and attachments from EWS Office 365, Microsoft Graph integration, Gmail, and other mail systems and initiates remediation in Agari Phishing Defense. Integration with Cortex XSOAR helps reduces complexity to help you solve other common needs such as:

- Simplifying ingest without the need to transform syslog or STIX TAXXI feeds
- Operationalizing indicators of compromise (IOC) and other threat data directly from Agari
- Enabling fast, active sharing of IOCs and threat intelligence into XSOAR to find other events that match
- Creating rules and triggers to reduce remediation and response time
- Customizing dashboards to enable quick visual inspection and identity policy hits on:
  - Top attacks
  - Attack recipients
  - Top users attacked
  - Partner domains spoofed
  - Untrusted messages
  - Presence of attachment
  - Attack IP address
  - Authenticity Score
  - Attack sender's email and domain
  - Attack message subject line
  - Sender domain reputation
  - Risk score
  - Mail from domain
  - Reply-to address
  - And more




**Example Automated Agari Phishing Defense Remediation Using Cortex XSOAR Playbook**

## Get Started Today

The Agari integration with Cortex XSOAR is available to install from the Cortex XSOAR Marketplace today. Contact your Agari representative to learn more.

## The Company We Keep

Top 3 Social Networks | 6 of the Top 10 Banks | Top Cloud Providers

Microsoft HSBC aetna citi CHASE Google

**Learn More:** www.agari.com/products

FORTRA

Fortra.com

**About Fortra**

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.