SOLUTION BRIEF

Agari App for Splunk

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 App for Splunk solves this challenge and makes it easy to surface email threats by quickly integrating valuable Agari threat intelligence into your Splunk dashboard. Your team can analyze and correlate Agari data, query logs to trigger custom alerts, and create shared views and dashboards for stakeholders in your organization.

Accelerate Incident Response and Drive SOC Efficiency

The Agari integration with Splunk empowers security teams to work more effectively to mitigate email threats. Leveraging Agari incident data and Splunk tools, security analysts can incorporate email incidents 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 Splunk and Agari Investments for Security

Agari threat data integration with Splunk Enterprise and Splunk Cloud ensures email incidents can be managed in Splunk's on-premises and cloud-native SIEM environments alike. The Agari App for Splunk supports key Agari products that protect your inbound and outbound email streams, including Agari Brand Protection and Agari Phishing Defense. Integrating email threat data across applications helps you get maximum value from your security investments and helps to safeguard your entire infrastructure against email threats.

AT A GLANCE

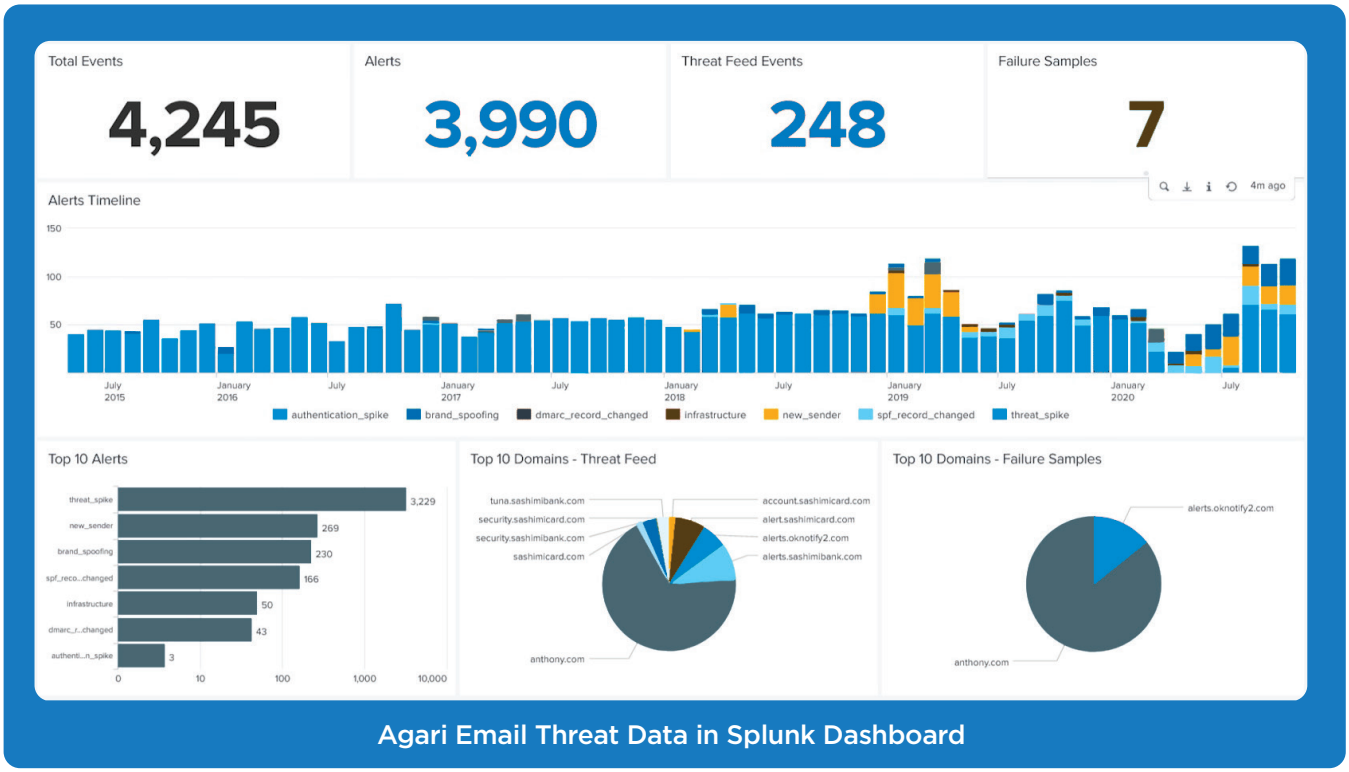
Agari App for Splunk makes it easy to connect Agari email threat data to the Splunk SIEM, improving visibility into email threats, accelerating incident response, and driving SOC efficiency.

HIGHLIGHTS

Unlock email threat intelligence
Integrate Agari email threat data across applications and improve efficiency 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 key Agari products
Connect Agari Brand Protection and Agari Phishing Defense to Splunk Enterprise and Splunk Cloud.



Agari Email Threat Data in Splunk Dashboard

Operationalize Email Threat Data to Quickly Deliver Results

The Agari App for Splunk helps your team quickly operationalize email threat data to realize value for your organization by surfacing email threats; creating standard security and compliance workflows; and simplifying incident tracking and case management.

The integration reduces complexity and includes more than ten preconfigured dashboards that enable quick visual inspection and identify policy hits including:

- Top attack types
- Top users attacked
- Threat feed spike alerts
- Authentication spikes
- Brand spoofing alerts
- DMARC record alerts
- Failure samples and more
- RUF data for monitoring for email domain abuse
- RUF data from the Agari Brand Protection Threat Feed to monitor for domain abuse

Get Started Today

The Agari App for Splunk is available to install from the Splunkbase directory 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

About Agari by HelpSystems

Agari is the Trusted Email Identity Company™, protecting brands and people from devastating phishing and socially-engineered attacks. Using applied data science and a diverse set of signals, Agari protects the workforce from inbound business email compromise, supply chain fraud, spear phishing, and account takeover-based attacks, reducing business risk and restoring trust to the inbox. Agari also prevents spoofing of outbound email from the enterprise to customers, increasing deliverability and preserving brand integrity. Agari was acquired by HelpSystems in May 2021.

Learn more at **www.agari.com**

agari by HelpSystems