Cisco Umbrella with Enforcement API App for IBM Resilient

Boost network visibility and gain actionable insight

Benefits

- **Single console simplicity** combines threat visibility, detection, and quick response
- **Power and flexibility** to integrate containment response activities into your workflow
- **Reduced security risk** from accelerating incident response

Overview

IBM Security and Cisco Security have joined forces to deliver advanced integrations to improve network visibility and speed threat detection and response.

The Cisco Umbrella and IBM Resilient solution enhances customer security efficiency by providing data enrichment, threat analysis and suspicious domain containment in a single dashboard. Cisco Umbrella Enforcement API, included with Umbrella Platform, integrates directly with the IBM Resilient incident response platform.

Example: when tracking a suspicious domain in a security incident, analysts can add a DNS entry that will trigger an Umbrella evaluation, querying a list of domains. From the resulting table, analysts can drill down on a domain for investigation, remove good domains from the blacklist, and add malicious domains to the blacklist.

Key Capabilities

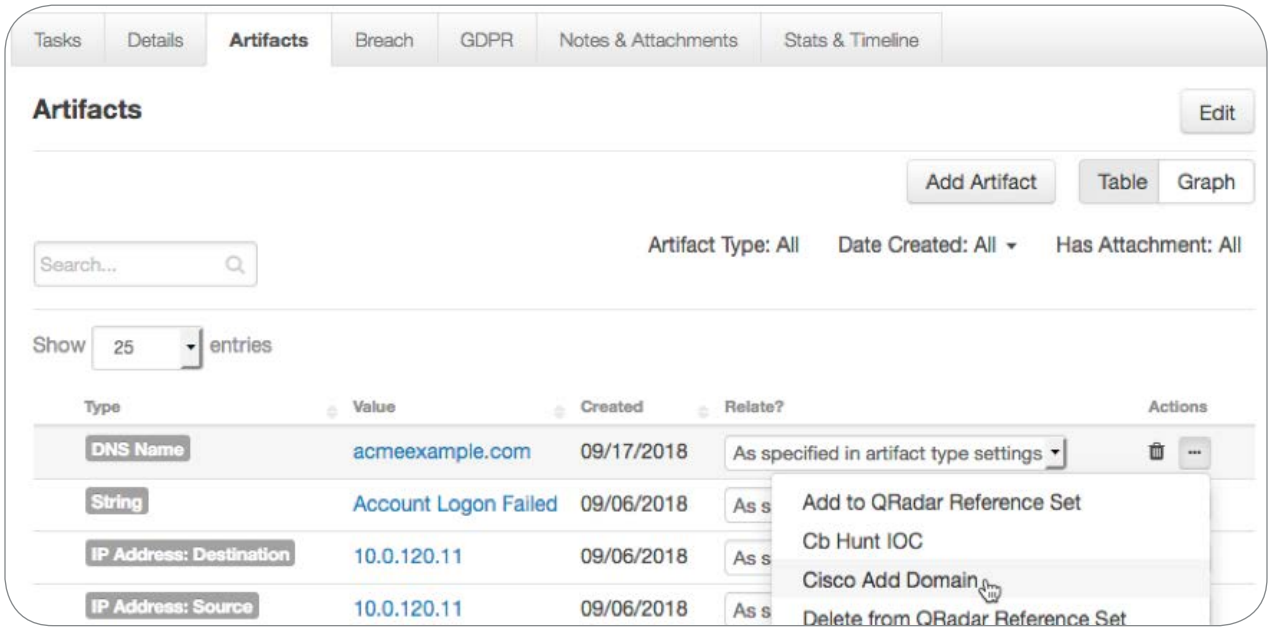
- **Threat analysis**
  Enriched data from Cisco Umbrella and IBM Resilient provides the intelligence to perform advanced threat analysis
- **Suspicious domain containment**
  Cisco Umbrella's enforcement API can take action and block suspicious domains
- **Simple integration**
  Resilient administrators can easily add Umbrella Enforcement API functions to a Resilient activity from menu-item actions to complex automatic workflows

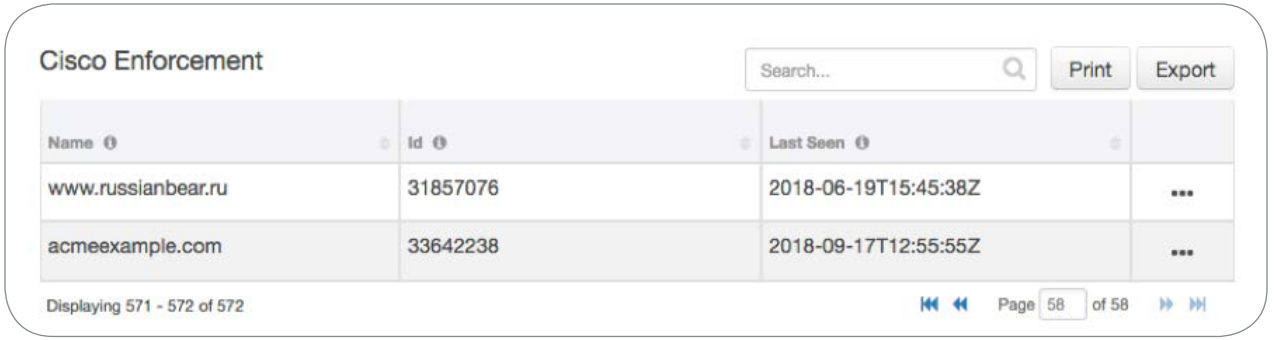
Fast Threat Response

Security analysts are faced with the daunting task of detecting advanced threats, analyzing them to determine the severity, and conducting rapid incident responses. Many of these tasks are manual and labor intensive, causing missed threat indicators and delayed responses to the most severe events. The integration of Cisco Umbrella and IBM Resilient can accelerate incident response, helping the customer reduce risk and increase efficiency in their security operations.

The Cisco Security and IBM Security Advantage

The ongoing collaboration between Cisco Security and IBM Security helps organizations strengthen their security posture against increasingly sophisticated cyberattacks. Rather than working in silos, these two leading security providers are collaborating to build solutions and share threat information that will empower clients to act at extreme speed and scale to see a threat once – and protect everywhere.





Next Steps

The Cisco Umbrella and IBM Resilient solution provides customers with more efficient solutions to rapidly detect and analyze threats. This application enables customers to protect their environments through orchestrating incident responses. These capabilities eliminate redundant and tedious tasks typically performed by security analysts which translates to more effective security operations. This app is now available on the IBM Security App Exchange. For more information visit http://cs.co/ibmsec.