Solution brief

# Cisco Umbrella Investigate App for IBM Resilient

## Enhance network visibility and take action with increased insight

## Benefits

- **Single console simplicity** combines threat visibility, detection, and quick response
- **Simple to use "Investigate" menu-item actions and custom automatic rule** in Resilient give access to powerful analysis tools in Umbrella Investigate
- **Out-of-the-box data enrichment workflows** provide threat analysis in a single workbench
- **Vast security intelligence** through Cisco Umbrella Investigate global intelligence and research team

## Overview

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

One key solution is the integration of Cisco Umbrella Investigate and IBM Resilient. With this solution, Cisco Umbrella Investigate integrates directly with the IBM Resilient incident response platform and provides quick analysis of security incidents.

When investigating and responding to security threats, a new incident is created to track a suspicious domain. Integration with Cisco Umbrella Investigate aids in the analysis by providing access to security intelligence and analysis tools.

## Key Capabilities

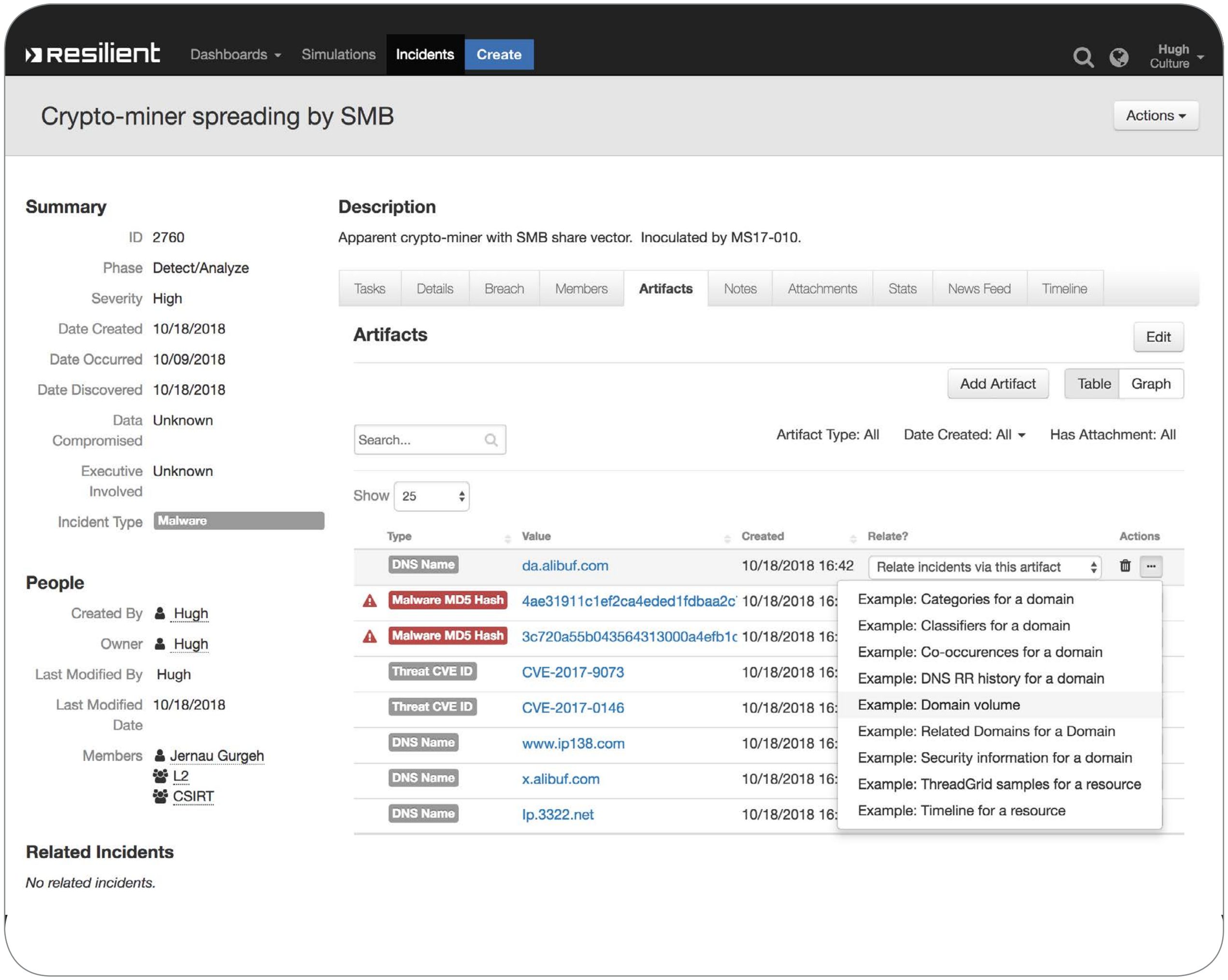
- **Discrete functions and out-of-the-box actions**
  Easy to use functions and turn-key actions are integrated in the Resilient and Umbrella Investigate apps
- **Actions menu**
  Simple menu enables analysts using Resilient to query the list of malicious domains, IPs, and malware based on the context
- **Simple integration**
  Resilient administrators can easily add Umbrella Investigate functions to a Resilient activity from menu-item actions to complex automatic workflows
- **Umbrella Investigate identification**
  Umbrella Investigate integration enables security teams to quickly identify incidents, access detailed data, and take action to mitigate the issue

## 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.



Crypto-miner spreading by SMB

**Summary**

| | |
|---|---|
| ID | 2760 |
| Phase | Detect/Analyze |
| Severity | High |
| Date Created | 10/18/2018 |
| Date Occurred | 10/09/2018 |
| Date Discovered | 10/18/2018 |
| Data Compromised | Unknown |
| Executive Involved | Unknown |
| Incident Type | Malware |

**People**

| | |
|---|---|
| Created By | Hugh |
| Owner | Hugh |
| Last Modified By | Hugh |
| Last Modified Date | 10/18/2018 |
| Members | Jernau Gurgeh<br>L2<br>CSIRT |

**Related Incidents**

*No related incidents.*

**Description**

Apparent crypto-miner with SMB share vector. Inoculated by MS17-010.

**Artifacts**

Artifact Type: All  Date Created: All  Has Attachment: All

Show 25

| | Type | Value | Created | Relate? | Actions |
|---|---|---|---|---|---|
| | DNS Name | da.alibuf.com | 10/18/2018 16:42 | Relate incidents via this artifact | |
| ⚠ | Malware MD5 Hash | 4ae31911c1ef2ca4eded1fdbaa2c | 10/18/2018 16: | | |
| ⚠ | Malware MD5 Hash | 3c720a55b043564313000a4efb1c | 10/18/2018 16: | | |
| | Threat CVE ID | CVE-2017-9073 | 10/18/2018 16: | | |
| | Threat CVE ID | CVE-2017-0146 | 10/18/2018 16: | | |
| | DNS Name | www.ip138.com | 10/18/2018 16: | | |
| | DNS Name | x.alibuf.com | 10/18/2018 16: | | |
| | DNS Name | Ip.3322.net | 10/18/2018 16: | | |

Example: Categories for a domain
Example: Classifiers for a domain
Example: Co-occurences for a domain
Example: DNS RR history for a domain
Example: Domain volume
Example: Related Domains for a Domain
Example: Security information for a domain
Example: ThreadGrid samples for a resource
Example: Timeline for a resource

## Next Steps

The Cisco Umbrella Investigate 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.