Solution brief
Public

Cisco Threat Grid and IBM Resilient

Orchestrate incident response

Benefits

- **Maintain audit trail** and logging to preserve a courtroom-admissible audit trail of an incident response
- **Track the incident** and create detailed notes and tasks throughout the incident lifecycle
- **Identify threats in real time**, analyze threat severity, and rapidly orchestrate incident response

Overview

The IBM Resilient and Cisco Threat Grid solution provides security teams with the actionable insights needed to accelerate and sharpen incident response. This enterprise-grade integration is built directly into the Resilient Incident Response Platform. Analysts can rapidly drill down from Resilient into the Threat Grid unified malware analysis and threat intelligence platform.

Analysts in Resilient can look up indicators of compromise within Threat Grid and submit suspected malware for detonation within the sandbox technology. These findings are automatically pulled into an incident report.

Security teams gain valuable incident data such as Indicators of Compromise (IoC), forensic evidence, and threat intelligence. They can then populate it into Resilient's powerful and dynamic response playbooks.

The consolidated view enables organizations to orchestrate the people, processes, and technology involved in the entire threat investigation and incident response process.

Key Capabilities

Advanced threat analysis

- Malware file detonation and sandbox analysis (see graphic)
- Threat scoring and prioritization
- Process mapping
- Attack correlation

Orchestration

- Case management
- User tasks, roles, and responsibilities
- Process assessment and improvement
- Dynamic playbooks that guide responses

Automation

- Integration with existing security and IT tools
- Automated incident escalation, enrichment, and remediation
- Scripted actions that enable analysts to fulfill tasks automatically

© 2018 Cisco and/or its affiliates. All rights reserved. | © Copyright IBM Corporation 2018 IBM Security Solutions

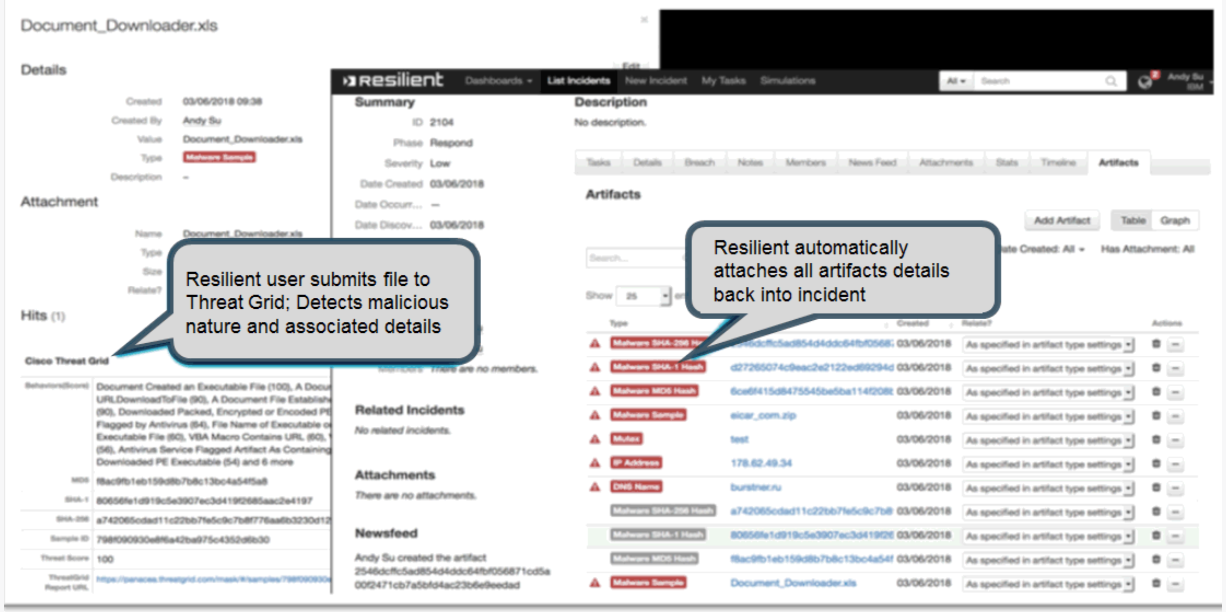
Respond to threats faster

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 intelligent orchestration capabilities of Threat Grid and Resilient help expedite these functions, reducing operational overhead and increasing efficiency in security operations.

The Cisco Security and IBM Security advantage

The ongoing collaboration between Cisco Security and IBM Security helps organizations strengthen their posture against increasingly sophisticated cyberattacks. Rather than working in silos, as is the industry norm, 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.



[redacted]

Document_Downloader.xls

Details

Created	03/06/2018 09:38
Created By	Andy Su
Value	Document_Downloader.xls
Type	Malware Sample
Description	–

Attachment

Name	Document_Downloader.xls
Type	
Size	
Relate?	

Hits (1)

Cisco Threat Grid

Behaviors(Score)	Document Created an Executable File (100), A Docu URLDownloadToFile (90), A Document File Establish (90), Downloaded Packed, Encrypted or Encoded PE Flagged by Antivirus (64), File Name of Executable o Executable File (60), VBA Macro Contains URL (60), (56), Antivirus Service Flagged Artifact As Containing Downloaded PE Executable (54) and 6 more
MD5	f8ac9fb1eb159d8b7b8c13bc4a54f5a8
SHA-1	80656fe1d919c5e3907ec3d419f2685aac2e4197
SHA-256	a742065cdad11c22bb7fe5c9c7b8f776aa6b3230d12
Sample ID	798f090930e8f6a42ba975c4352d6b30
Threat Score	100
ThreatGrid Report URL	https://panacea.threatgrid.com/mask/#/samples/798f090930

Summary

ID	2104
Phase	Respond
Severity	Low
Date Created	03/06/2018
Date Occurr...	—
Date Discov...	03/06/2018
Members	There are no members.

Related Incidents

No related incidents.

Attachments

There are no attachments.

Newsfeed

Andy Su created the artifact 2546dcffc5ad854d4ddc64fbf056871cd5a 00f2471cb7a5bfd4ac23b6e9eedad

Description

No description.

Artifacts

Type		Created	Relate?	Actions
Malware SHA-256 Hash	2546dcffc5ad854d4ddc64fbf0568	03/06/2018	As specified in artifact type settings	
Malware SHA-1 Hash	d27265074c9eac2e2122ed69294d	03/06/2018	As specified in artifact type settings	
Malware MD5 Hash	6ce6f415d8475545be5ba114f208	03/06/2018	As specified in artifact type settings	
Malware Sample	eicar_com.zip	03/06/2018	As specified in artifact type settings	
Mutex	test	03/06/2018	As specified in artifact type settings	
IP Address	178.62.49.34	03/06/2018	As specified in artifact type settings	
DNS Name	burstner.ru	03/06/2018	As specified in artifact type settings	
Malware SHA-256 Hash	a742065cdad11c22bb7fe5c9c7b8	03/06/2018	As specified in artifact type settings	
Malware SHA-1 Hash	80656fe1d919c5e3907ec3d419f26	03/06/2018	As specified in artifact type settings	
Malware MD5 Hash	f8ac9fb1eb159d8b7b8c13bc4a54f	03/06/2018	As specified in artifact type settings	
Malware Sample	Document_Downloader.xls	03/06/2018	As specified in artifact type settings	

Resilient user submits file to Threat Grid; Detects malicious nature and associated details

Resilient automatically attaches all artifacts details back into incident

Next Steps

The Cisco Threat Grid and Resilient solution provides customers with more efficient solutions to rapidly detect and analyze threats, and subsequently orchestrate the incident responses to protect their environments. These capabilities eliminate redundant and tedious tasks typically performed by security analysts, creating more effective security operations. For additional information, visit: http://cs.co/ibmsec.

For additional questions or for opportunities and connections:

Cisco: cisco-ibm-security@cisco.com or IBM: cisco-ibm-security@us.ibm.com.

© Copyright IBM Corporation 2018 IBM Security Solutions

© 2018 Cisco and/or its affiliates. All rights reserved. This document is Cisco Confidential. For Channel Partner use only. Not for distribution. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)