Solution overview
Public

IBM Security

Cisco Threat Grid App and IBM QRadar SIEM

Expedite Threat Investigation

Benefits

Today's businesses require the tools to gain better visibility to capture and analyze malicious files and take immediate action to remediate and protect the business. Through the Cisco Threat Grid app and IBM QRadar, organizations can:

- Gain visibility across their network, endpoints, users, and cloud
- Detect and analyze threats in real time and then escalate to prioritize for further action
- Reduce the time to detect, remediate, and respond to advanced threats
- Detect long and slow attacks
- Avoid alert fatigue with the potential for missing alerts in the noise of event data

Overview

The Cisco Threat Grid app integrates with IBM QRadar Security Information and Event Management (SIEM), enabling analysts to quickly identify, understand, and respond to system threats rapidly through the QRadar dashboard. Downloadable via the IBM Security App Exchange, this powerful app combines advanced sandboxing, malware analysis, and threat intelligence in a single unified solution.

Threat Grid and QRadar integration enables analysts to quickly determine possible malicious files that have been submitted to Threat Grid within their environment and rapidly drill down from QRadar into the Threat Grid unified malware analysis and threat intelligence platform for deeper analysis. This integration expedites the threat investigation process via a dashboard view into the highest priority threats, delivered directly through QRadar versus having to pivot on disparate tools and interfaces.

Results from the sandbox analysis of Threat Grid can be analyzed by QRadar to determine whether the potential threats within the organization are malicious or benign. Potential threats are identified and assigned a threat score, which depicts their severity and risk.

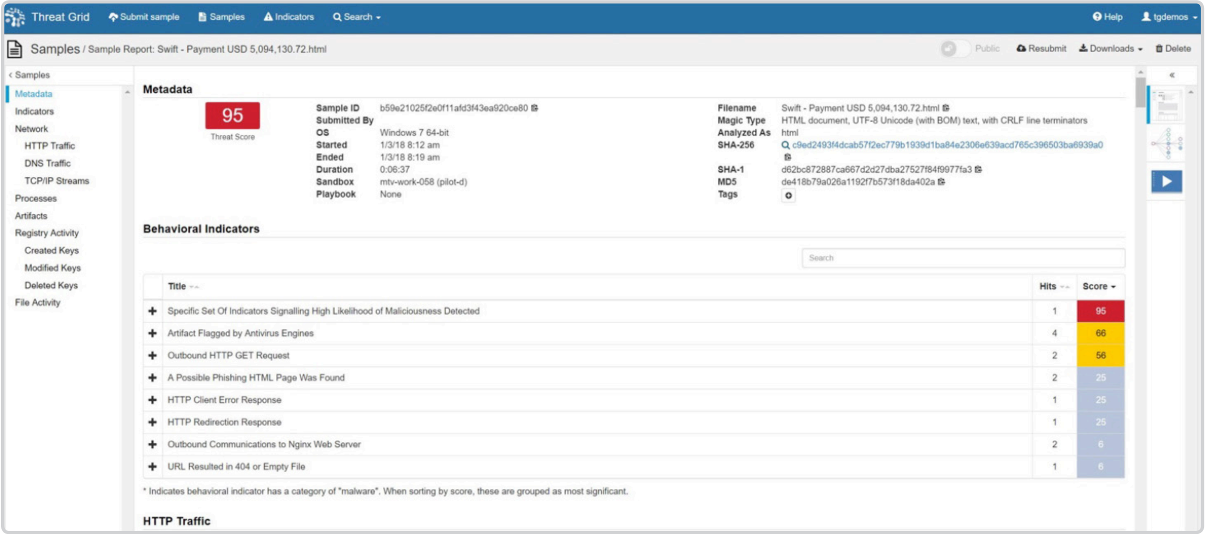
Customer Challenges

Cyber threats are more complex as cyber criminals are developing more creative methods to compromise and exploit sensitive business data. Customers, as a consequence, are challenged to keep pace and protect their business interests. They are faced with:

- Complex multivendor environments
- A lack of visibility into threats to users, devices, processes, and applications
- Ineffective sharing of threat information across the network
- The inability to detect and analyze malware threats and assign a severity level for taking appropriate action

Customers require tools that facilitate easier security operations to simplify protection and mitigate risks.

Threat Scoring Dashboard View



Samples / Sample Report: Swift - Payment USD 5,094,130.72.html

Metadata

95
Threat Score

Sample ID	b59e21025f2e0f11afd3f43ea920ce80
Submitted By	
OS	Windows 7 64-bit
Started	1/3/18 8:12 am
Ended	1/3/18 8:19 am
Duration	0:06:37
Sandbox	mtv-work-058 (pilot-d)
Playbook	None
Filename	Swift - Payment USD 5,094,130.72.html
Magic Type	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Analyzed As	html
SHA-256	c9ed2493f4dcab57f2ec779b1939d1ba84e2306e639acd765c396503ba6939a0
SHA-1	d62bc872887ca667d2d27dba27527f84f9977fa3
MD5	de418b79a026a1192f7b573f18da402a
Tags	

Behavioral Indicators

	Title	Hits	Score
+	Specific Set Of Indicators Signalling High Likelihood of Maliciousness Detected	1	95
+	Artifact Flagged by Antivirus Engines	4	66
+	Outbound HTTP GET Request	2	56
+	A Possible Phishing HTML Page Was Found	2	25
+	HTTP Client Error Response	1	25
+	HTTP Redirection Response	1	25
+	Outbound Communications to Nginx Web Server	2	6
+	URL Resulted in 404 or Empty File	1	6

* Indicates behavioral indicator has a category of "malware". When sorting by score, these are grouped as most significant.

HTTP Traffic

How it Works

The Cisco Threat Grid app and IBM QRadar offer a complimentary solution that combines advanced sandboxing, malware analysis, and threat intelligence in one unified solution. This delivers faster threat analysis to expedite threat investigations, with a dashboard view into the highest priority threats. The combined solution accelerates alert triage and threat discovery with behavioral analysis. Together, this integration enables customers to:

- **Capture unknown threats**–An unknown file is seen by best-of-breed security products
- **Submit the sample to Threat Grid**–The file sample is submitted to Threat Grid for dynamic and static malware analysis
- **Automate malware analysis**–Threat Grid analyzes the behavior of the sample and determines a threat score, which is displayed in the Threat Grid app for QRadar
- **Alert and pivot to report**–An analyst is alerted to samples with a high threat to the network and right-clicks to view the analysis report in Threat Grid
- **Gain intelligence and respond faster**–Threat Grid provides integrated behavior and threat intelligence to take incident response action with Resilient or other remediation

The Cisco Security and IBM Security Advantage

The ongoing collaboration between IBM Security and Cisco is helping 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 see a threat once, act at extreme speed and scale, and protect everywhere.

Next Steps

The Cisco Threat Grid and IBM QRadar integration provides customers with more efficient tools to rapidly capture and analyze malware threats to today's enterprises. These capabilities enable customers to understand their exposure cyber threats and reduce their risk of data loss, thus delivering more peace of mind.

For additional information, visit: https://cs.co/ibmsec.

For additional questions or for opportunities and connections, email us:

cisco-ibm-security@cisco.com

cisco-ibm-security@us.ibm.com

Download the app for free at https://www.ibm.com/security/community/app-exchange.