PROFESSIONAL SERVICES SOLUTION

Creating Correlation Dashboards in Microsoft Azure

Use Case

Being able to process malicious activity in your environment at a glance is paramount to staying ahead and being informed of the latest threats to your organization. Our correlation dashboards consolidate your threat information in a single pane of glass, allowing analysts to easily identify patterns and trends in their environment. Analysts can use these dashboards to generate reports, prioritize investigations, and gain a deeper understanding of their security environments.

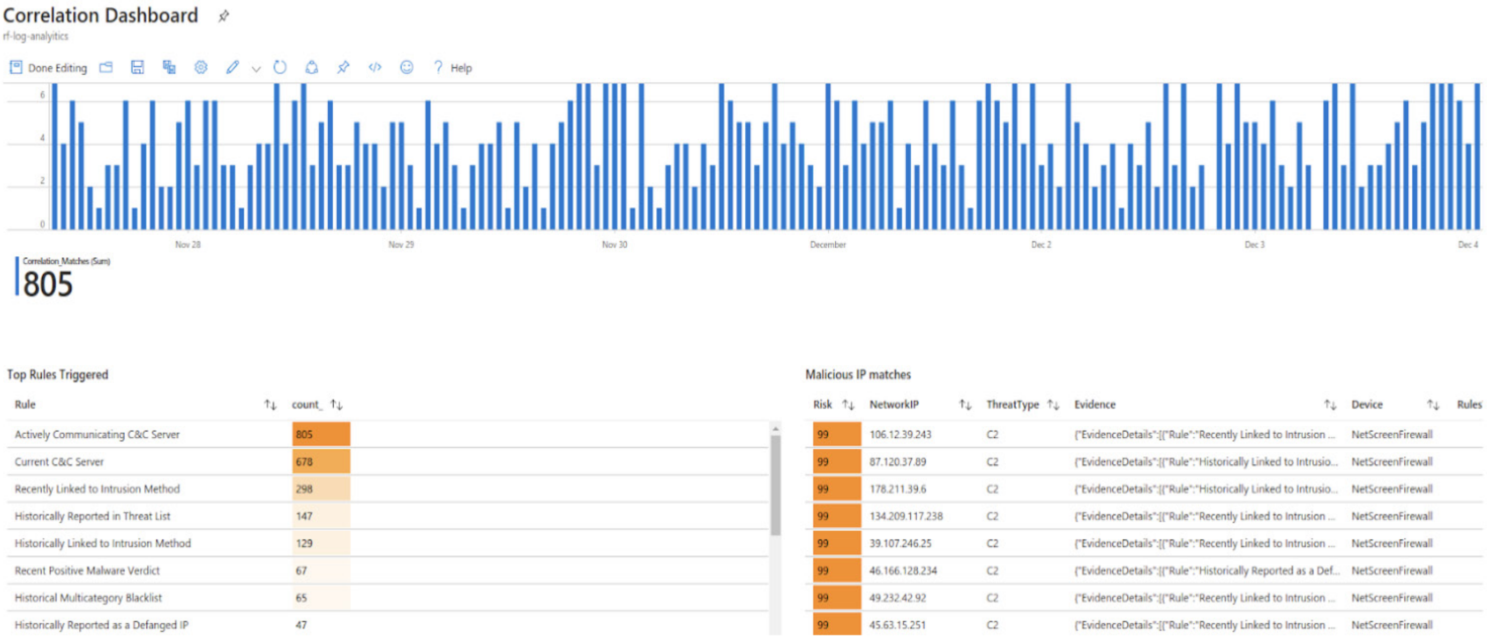
Issue

- Unable to gain a comprehensive view of Recorded Future threat data in your environment
- Unable to view the top risk rules triggered by IOCs in your environment

Solution

Recorded Future Professional Services offers an enhanced capability, allowing clients to view summary data of Risky IOCs found in their environment. Professional Services can create correlation dashboards for IP, URL, Domain, and Hash Risk Lists and/or Security Control Feeds. Correlation Dashboard panels include:

- Top Risk Rules triggered by IOCs in your environment
- Time series of correlations between client log data and Recorded Future Risk Lists
- Total number of correlation matches for a Hashes/IPs/Domains/URLs
- Table view of the most risky IOCs found in client environment, and justification for their risk



Correlation Dashboard

rf-log-analytics

Correlation_Matches (Sum)

805

Top Rules Triggered

Rule	count_
Actively Communicating C&C Server	805
Current C&C Server	678
Recently Linked to Intrusion Method	298
Historically Reported in Threat List	147
Historically Linked to Intrusion Method	129
Recent Positive Malware Verdict	67
Historical Multicategory Blacklist	65
Historically Reported as a Defanged IP	47

Malicious IP matches

Risk	NetworkIP	ThreatType	Evidence	Device	Rules
99	106.12.39.243	C2	{"EvidenceDetails":[{"Rule":"Recently Linked to Intrusion ...	NetScreenFirewall	
99	87.120.37.89	C2	{"EvidenceDetails":[{"Rule":"Historically Linked to Intrusio...	NetScreenFirewall	
99	178.211.39.6	C2	{"EvidenceDetails":[{"Rule":"Historically Linked to Intrusio...	NetScreenFirewall	
99	134.209.117.238	C2	{"EvidenceDetails":[{"Rule":"Recently Linked to Intrusion ...	NetScreenFirewall	
99	39.107.246.25	C2	{"EvidenceDetails":[{"Rule":"Recently Linked to Intrusion ...	NetScreenFirewall	
99	46.166.128.234	C2	{"EvidenceDetails":[{"Rule":"Historically Reported as a Def...	NetScreenFirewall	
99	49.232.42.92	C2	{"EvidenceDetails":[{"Rule":"Recently Linked to Intrusion ...	NetScreenFirewall	
99	45.63.15.251	C2	{"EvidenceDetails":[{"Rule":"Recently Linked to Intrusion ...	NetScreenFirewall	

Technical

From a technical perspective the integration will include and need configured:

- A new workbook being created in Microsoft Azure Sentinel
- JSON for a workbook gallery view OR JSON for an Azure Resource Manager

This service will require Threat or Brand Intelligence Modules, Splunk Integration, and Two(2) Professional Service Credits for implementation. On-going support covered by Integration or Premium Support.

ABOUT RECORDED FUTURE

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,300 businesses and government organizations across 60 countries. Learn more at recordedfuture.com.

www.recordedfuture.com @RecordedFuture