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
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.