Threat-Based Controls Scoring - Data Primer

Developed by: GSA FedRAMP PMO

Version 1.0

1/18/2022

info@fedramp.gov

fedramp.gov

Overview

FedRAMP, in collaboration with the DHS CISA .govCAR team, developed a methodology for scoring each National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 security control against threat frameworks to determine which security controls and capabilities are most effective to protect, detect, and respond to current prevalent threats. In February of 2021, the govCAR team worked with GSA to score the NIST 800-53 Rev 5 control baseline against the MITRE ATT&CK Framework. The goal of this initiative is to enable agencies, Cloud Service Providers (CSPs), and other industry partners to prioritize security controls that are relevant and effective against the current threat environment.

The results of the scoring effort were leveraged to inform the updates to the FedRAMP NIST 800-53 Rev 5 baselines. In addition, FedRAMP published a white paper outlining the methodology behind the threat-based scoring approach. As a companion to this whitepaper, the data from the 800-53 controls scoring effort was released. This data primer provides additional detail describing the components of that data set.

The threat-based controls scoring data set consists of the following four worksheets:

1. **Control Protection Values** - provides a listing of all security controls scored along with each control's protection value.
2. **Control Rationale** - provides the rationale, conditions, dependendencies, and assumptions leveraged in the scoring of each control.
3. **Raw Scores** - provides the protect, detect, and respond scores for each security control across all techniques of the MITRE ATT&CK Framework.
4. **Heat Map** - provides the heatmap value for each technique in the MITRE ATT&CK Framework.

Disclaimer: Use of Information

The information provided on this dataset does not, and is not intended to, constitute cloud security advice; instead, all information, content, and materials available within this data set are for general informational purposes only. Information from FedRAMP may not constitute the most up-to-date threat landscape or other information. This methodology contains references to other third-party partners. Such partners are only disclosed for the convenience of the reader, user or browser.

Worksheet - Control Protection Values

The “Control Protection Values: worksheet contains the following fields:

- **Control Number** - provides the numerical ID for each control.
- **Control Name** - provides the name of each control scored.
- **Protection Value** - provides the numerical values indicating the scores ability to protect, detect, and respond to the techniques in the MITRE ATT&CK framework.
- **Cut Line** - represents the numerical value below which scores fall in the bottom 20th percentile of all controls scored.

Worksheet - Control Rationale

The “Control Rationale” worksheet contains the following fields:

- **Control** - provides the numerical ID for each control.
- **Name** - provides the name of each control scored.
- **Baselines** - provides the applicable baselines for each security control.
- **Eng** - provides the number of Mitre ATT&CK techniques related to the control.
- **Rationale/Condition** - describes the rationale, conditions, and assumptions leveraged in the scoring of each control.
- **Dep.** - describes the related security controls and/or Mitre ATT&Ck techniques considered when evaluating the control.

Worksheet - Raw Scores

The “Raw Scores” worksheet contains the following fields:

- **Attack ID** - provides the unique ID for each ATT&CK technique.
- **Tactic** - provides the name of Tactic associated with each ATT&CK technique.
- **Name** - provides the name of each ATT&CK technique.
- **NO’s** - provides the number of controls that do not provide a protection, detection, or response action for the Mitre ATT&CK technique.
- **Coverage** - the percent of controls that have some score (i.e. P,D,R) to this technique.
- **Control Scores (i.e. columns F - RK)** - provides the protect, detect, and respond scores for each control.

Worksheet - Heat Map

The “Heat Map” worksheet contains the following fields:

- **Tactic** - provides the name of Tactic associated with each ATT&CK technique.
- **Tech Name** - provides the name of each ATT&CK technique.
- **PrevCount** - indicates the number of times the technique was utilized by the adversary (i.e. based upon cyber threat intelligence)
- **TechID** - provides the unique ID for each ATT&CK technique.

- **HMV** - provides the overall heat map value for each technique. High values indicate more prevalent techniques.