**A Crowdsourcing Exchange for mapping various sources of Information security vulnerabilities, exposures, threats, and controls data**

**What are you asking?**

The Columbus Collaboratory is asking the community to help us create mappings from CWE (common weakness enumeration) to NIST 800-53r4 moderate controls using our initial mapping formula.

**Why are you asking?**

The Collaboratory team is trying to surface correlations and semantic relationships between available sources of information security vulnerabilities and exposures to attack types so we can better understand how attackers think about exploiting them. By also relating controls sets like NIST 800-53 we hope to give cybersecurity teams comprehensive, threat-informed information that can help them manage and mitigate risk in various parts of their program.

**How?**

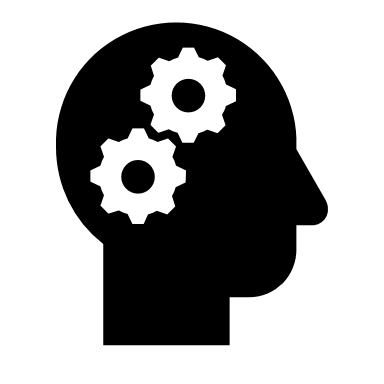
The Collaboratory team in their analytical approach has focused on the relationships between the following data sets:

* NVD
* CWE
* CVE
* CAPEC
* ATT&CK Technique
* NIST SP 800-53r4 moderate

Below is our data model and a sample of the “mashup”. We have found that relating CVE, CWE, CAPEC, and ATT&CK technique to be fairly repeatable and programmatic whereas relating the controls set to be more challenging and manual. We have chosen to crowdsource this aspect of the analysis and below is the initial mapping formula to guide your analysis.

|  |  |  |
| --- | --- | --- |
| **CAPEC** |  | **CVE** |
| ID, Name |  | ID |
| Description |  | Description |
| Likelihood |  | CVSS: |
| Severity |  | * Attack Vector |
| Related Attack Patterns (CAPEC) |  | * Complexity |
| Execution Flow |  | * Privileges Required |
| Prerequisites (Attack |  | * User Interaction |
| Path/Affected Assets) |  | * Impact Score |
| Skill Required (To Exploit) |  |  |
| Indicators |  |  |
| Consequences |  |  |
| Mitigations |  |  |
| Examples (CVE) |  |  |
| Related Weaknesses (CVE) |  |  |
| Taxonomy Mapping (ATT&CK) |  |  |

|  |  |  |
| --- | --- | --- |
| **ATT&CK** |  | **CWE** |
| ID, Tactic/Technique |  | ID, Name |
| Description |  | Description/Extended Description |
| Permissions Required |  | Platform |
| Platform |  | Mode of Introduction |
| Attack Phase |  | Consequences |
| Detection |  | Detection |
| Mitigation |  | Mitigation |
| References |  | Examples (CVE) |
| Data Sources |  | Affected Resources |
| APT Name |  | Taxonomy Mappings |
| APT Description |  | Related Patterns |
| APT Targets |  |  |

****

|  |
| --- |
| **NIST SP 800-53** |
| Controls |
|  |
|  |
|  |
|  |