Communicating Cybersecurity Risk

MICHAEL D. SMITH, MSS, MS, MBA, CISSP, CSSLP

OCTOBER 24, 2023

Defining Risk

- Risk = Impact x Likelihood
- Impact is the worst-case scenario
- Likelihood is the adversary's:
  - Capability (Means)
  - Motivation (value of compromise)
  - Opportunity (existing vulnerabilities)

DoD 5 x 5 Risk Cube

- Critical - Critical risk means that a threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
- High - High risk means that a threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
- Moderate - Moderate risk means that a threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
- Low - Low risk means that a threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
- Minimal - Minimal risk means that a threat event could be expected to have a negligible adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

Risk Assessment Matrix

Probability of Occurrence/Likelihood of Use								
	Near Certainty	90%	E	Low	Moderate	High	Critical	Critical
	Highly Likely	70%	D	Low	Moderate	Moderate	High	Critical
	Likely	50%	C	Low	Low	Moderate	Moderate	High
	Low Likelihood	30%	B	Minimal	Low	Low	Moderate	Moderate
	Not Likely	10%	A	Minimal	Minimal	Low	Low	Moderate
	Risk to Utility (Operational Impact/Consequence)			1 Minimal	2 Low	3 Moderate	4 High	5 Critical

Likelihood of Risk

Level	Likelihood	Probability of Occurrence
E	Near Certain	90%
D	High Likely	70%
C	Likely	50%
B	Low Likely	30%
A	Not Likely	10%

Operational Impact / Consequence

Level	Impact	Life, Injury, Reputation, Revenue
5	Critical	$$$$$
4	High	$$$$
3	Moderate	$$$
2	Low	$$
1	Minimal	$

Risk Management Strategies

- Risk acceptance
- Risk transference
- Risk avoidance
- Risk reduction

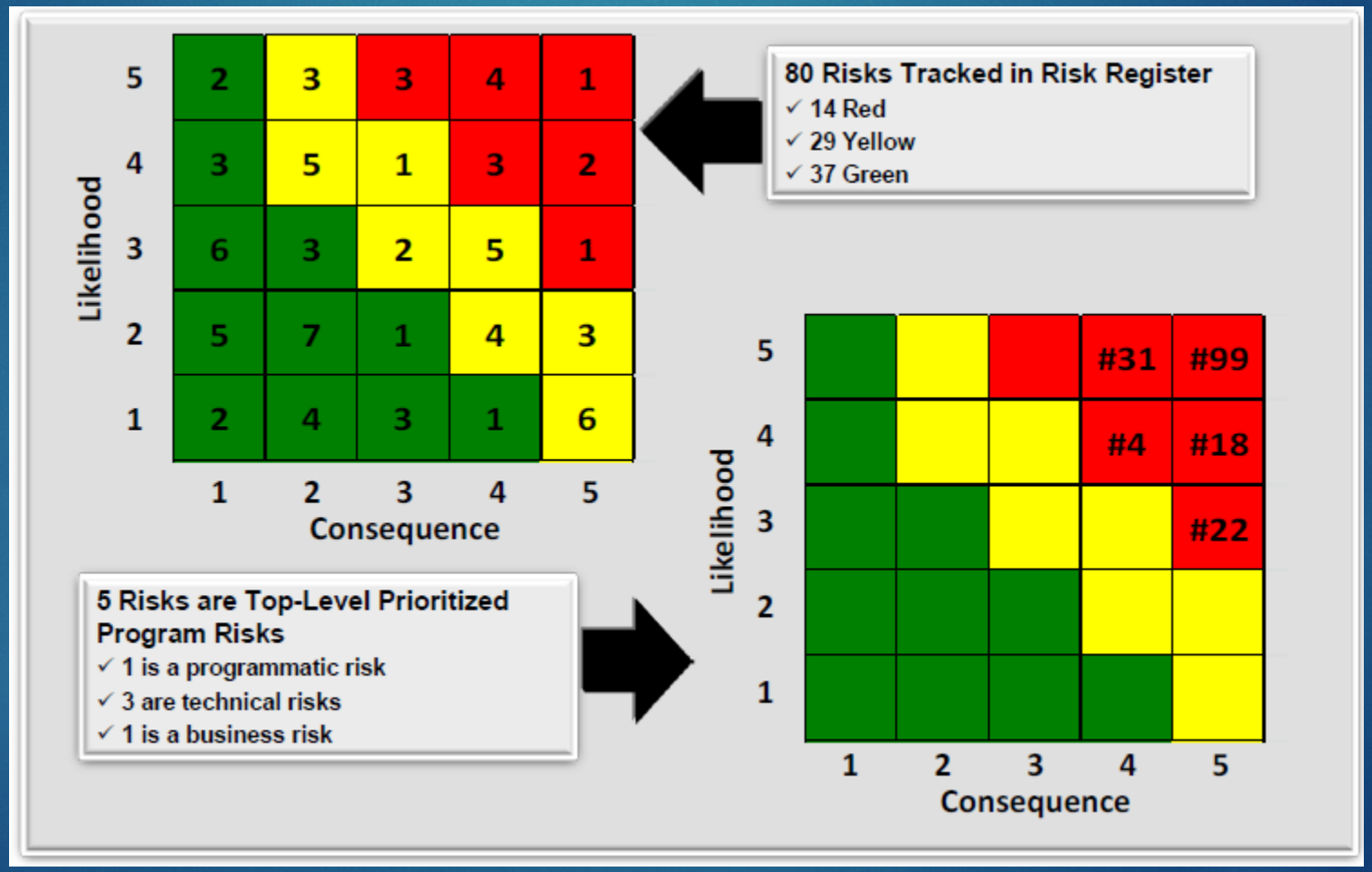
NIST NVDB & Exploit Database

- NIST National Vulnerability Database (NVD)
  - U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP).
  - This data enables automation of vulnerability management, security measurement, and compliance.
  - The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.
  - https://nvd.nist.gov/
- Exploit Database
  - The Exploit Database is a non-profit project that is provided as a public service by OffSec, an information security training company
  - The Exploit Database is a CVE compliant archive of public exploits and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers.
  - https://www.exploit-db.com/

Security Content Automation Protocol (SCAP)

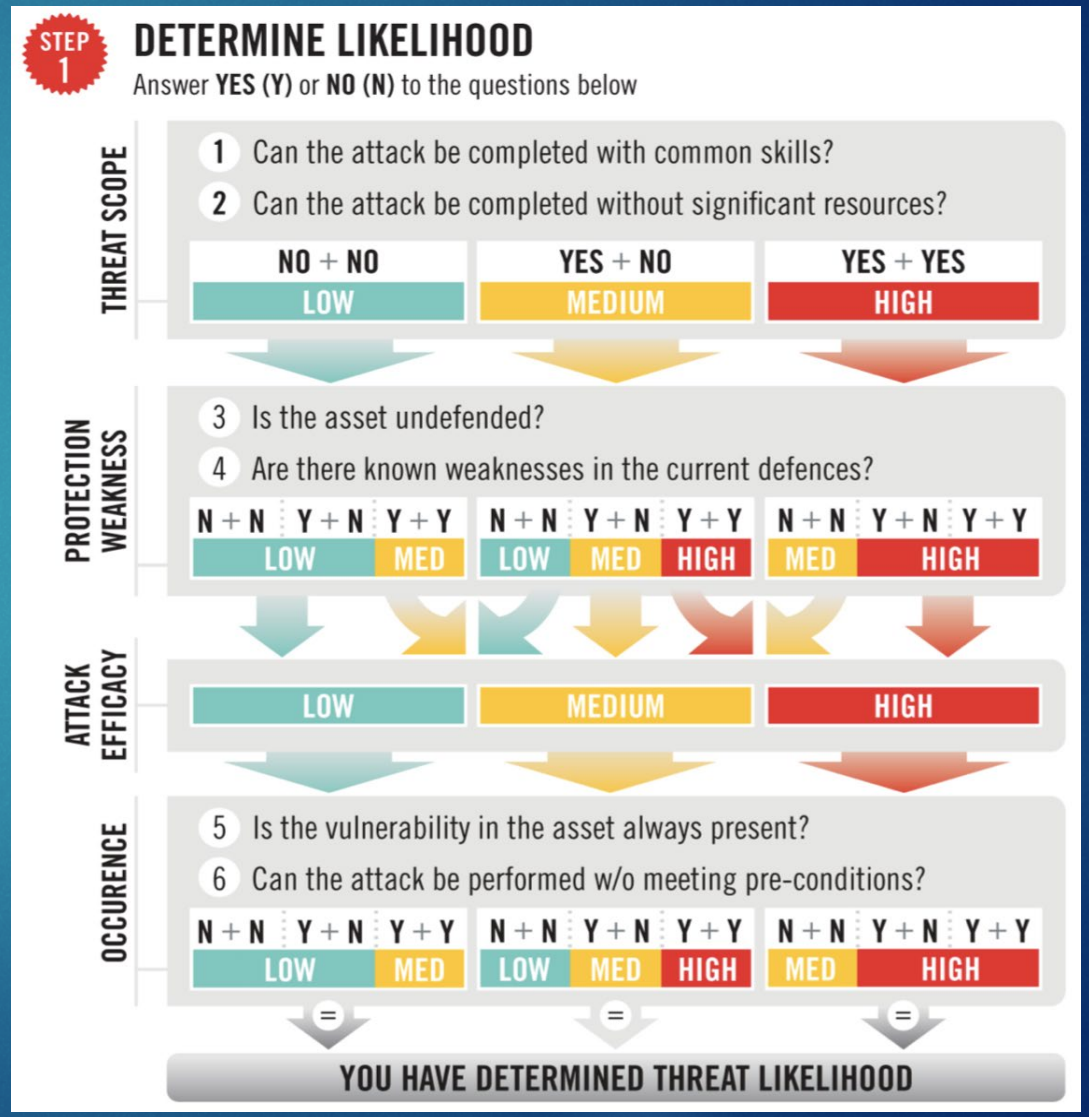
- The Security Content Automation Protocol (SCAP) utilizes the following standards
  - Open Vulnerability and Assessment Language (OVAL)
  - Open Checklist Interactive Language (OCIL)
  - Common Platform Enumeration (CPE)
    - Structured naming scheme for information technology systems, software, and packages
  - Software Identification (SWID) Tags
  - Common Configuration Enumeration (CCE)
  - Common Vulnerabilities and Exposures (CVE)
    - List of records—each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities
  - Common Vulnerability Scoring System (CVSS)
  - Common Configuration Scoring System (CCSS)

Risk Matrix Showing Prioritized Results



Binary risk method

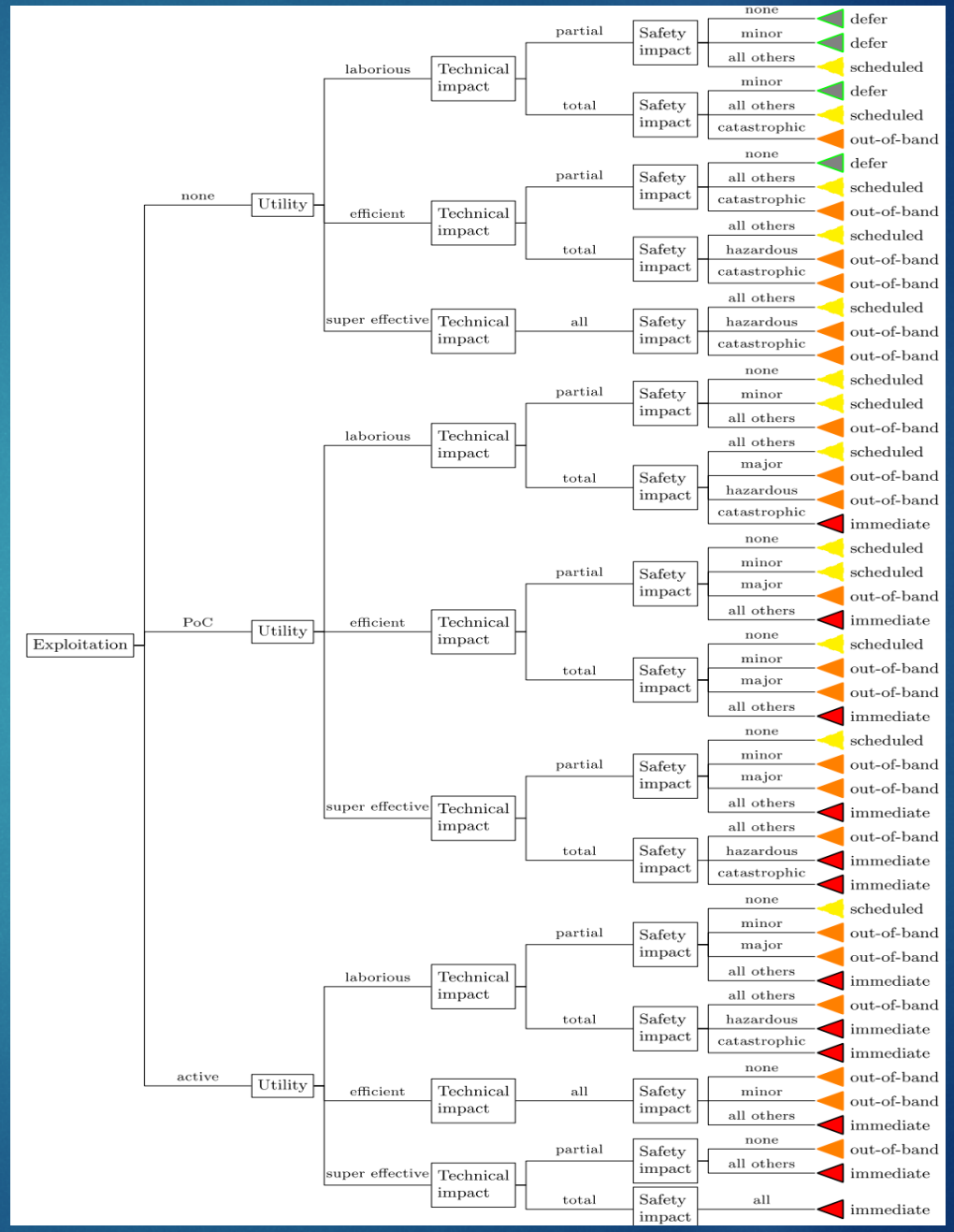
- The risk category of Low/Medium/High is determined through a series of ten binary questions, e.g., threat scope, protection weaknesses, the efficacy of attacks, and impact of attack.
- The standard provides some definition for each question and how to determine a YES or NO answer.



Stakeholder Specific Vulnerability Classification (SSVC)

- Developed by Carnegie Mellon University Software Engineering Institute (SEI)
  - Funding by the US Department of Homeland Security (DHS) / Cybersecurity and Infrastructure Security Agency (CISA)
- Prioritization of weaknesses and vulnerabilities in systems based on their risk.
- Four questions that determine categories of risk-based actions.
  - Is there an exploit?
  - How hard/costly to fix?
  - How much impact does the vulnerability have on the system (criticality of part)?
  - Are there safety/mission impacts that matter?

SSVC Illustrated



Conducting Risk Assessments

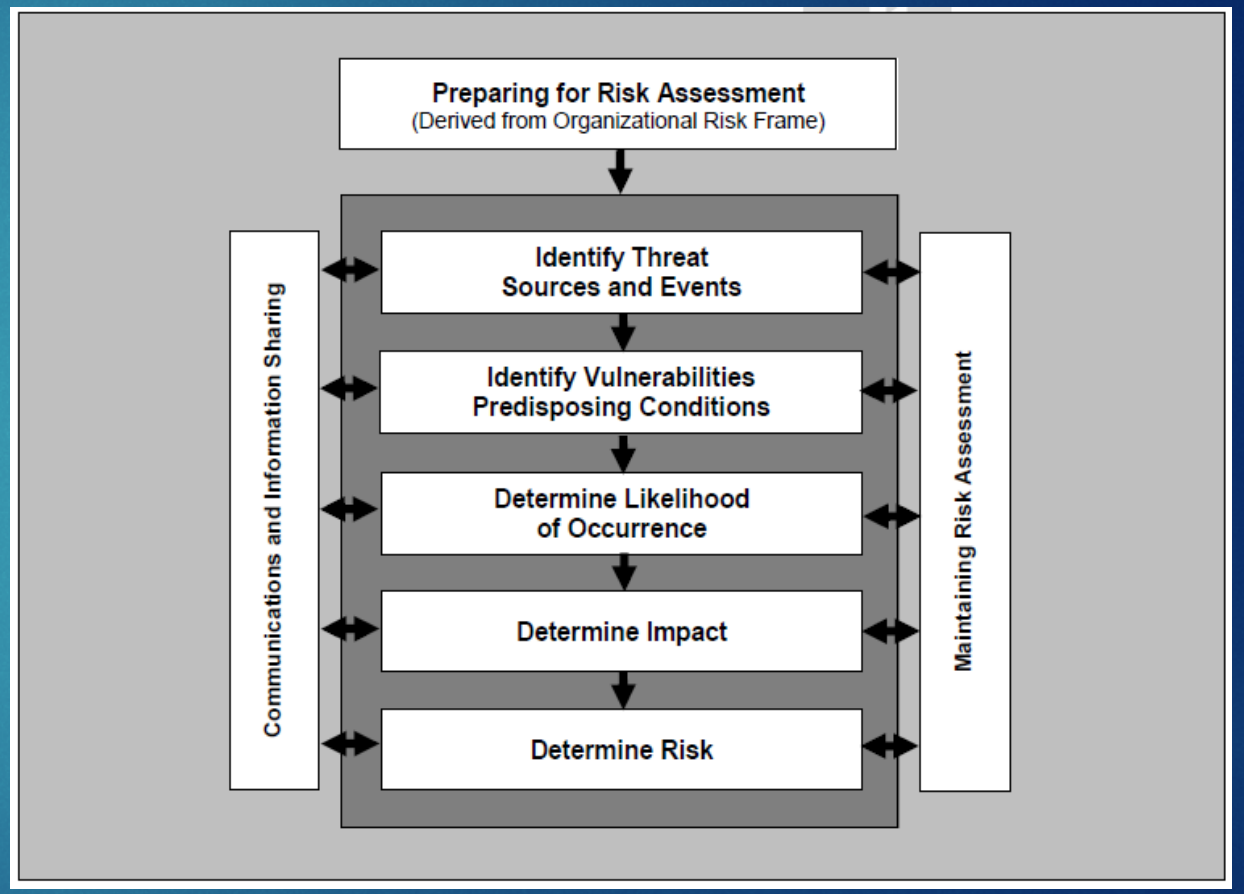
Per NIST Special Publication (SP) 800-30 Revision 1, Guide for Conducting Risk Assessments, Risk assessments can help organizations:

- Determine the most appropriate risk responses to ongoing cyber attacks or threats from man-made or natural disasters;
- Guide investment strategies and decisions for the most effective cyber defenses to help protect organizational operations (including missions, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; and
- Maintain ongoing situational awareness with regard to the security state of organizational information systems and the environments in which the systems operate.

RISK ASSESSMENT PROCESS

Summary of Key Activities – Maintaining Risk Assessments

- Identify key risk factors that have been identified for ongoing monitoring.
- Determine frequency of risk factor monitoring activities and the circumstances under which the risk assessment needs to be updated.
- Reconfirm the purpose, scope, and assumptions of the risk assessment.
- Conduct the appropriate risk assessment tasks, as needed.
- Communicate the updated risk assessment results to appropriate organizational stakeholders.



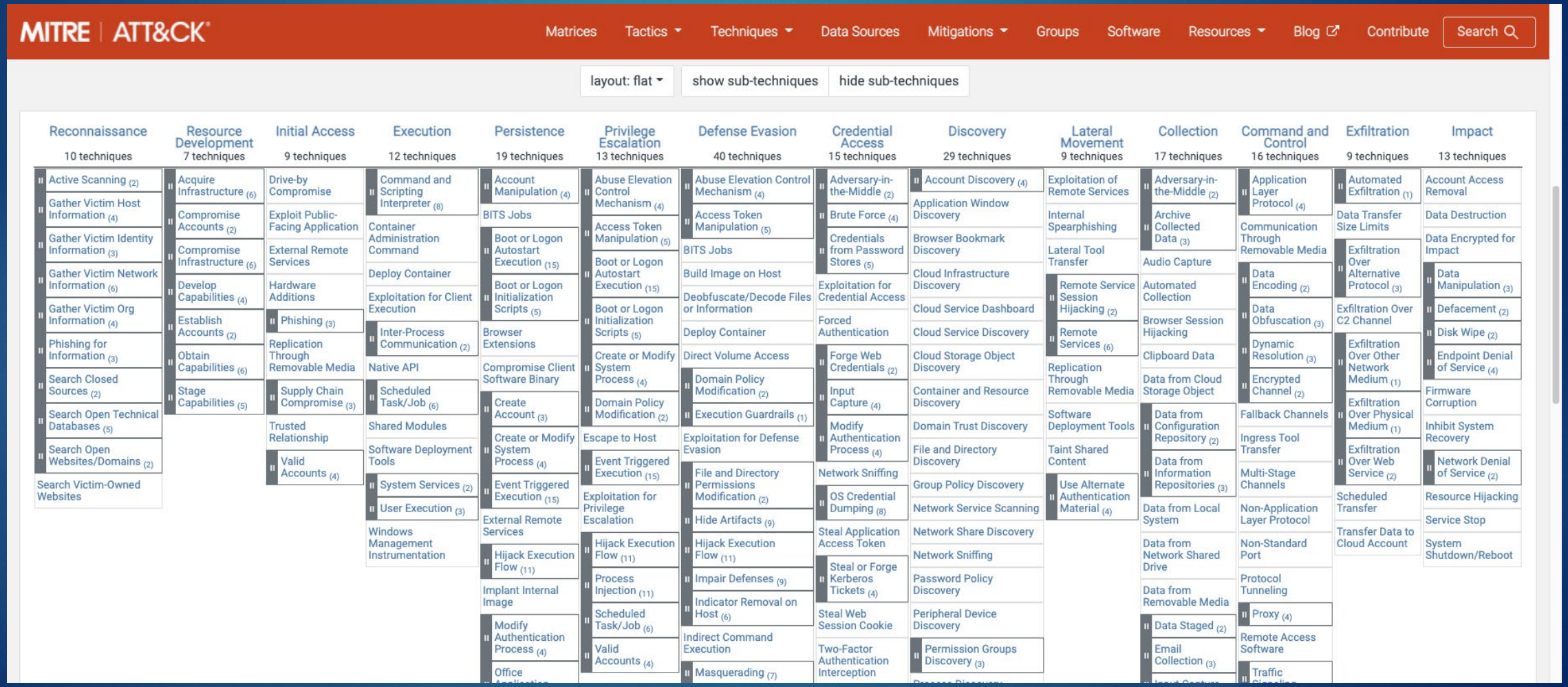
Communicate Risk

- MITRE ATT&CK®
  - Globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.
  - The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.
- MITRE D3FND
  - MITRE D3FEND™ is a knowledge base—defined as a "knowledge-graph"
  - Library of defensive cybersecurity countermeasures, technical components, and their associations and capabilities.
  - Complementary to the MITRE ATT&CK® framework of cyber adversaries' Tactics, Techniques, and Procedures (TTP).

MITRE ATT&CK®

- ATT&CK Matrix for Enterprise
  - Reconnaissance (10 techniques)
  - Resource Development (8 techniques)
  - Initial Access (9 techniques)
  - Execution (14 techniques)
  - Persistence (19 techniques)
  - Privilege Escalation (13 techniques)
  - Defense Evasion (42 techniques)
  - Credential Access (17 techniques)
  - Discovery (31 techniques)
  - Lateral Movement (9 techniques)
  - Collection (17 techniques)
  - Command and Control (16 techniques)
  - Exfiltration (9 techniques)
  - Impact (13 techniques)

MITRE ATT&CK®


MITRE | ATT&CK
Matrices
Tactics
Techniques
Data Sources
Mitigations
Groups
Software
Resources
Blog
Contribute
Search
layout: flat
show sub-techniques
hide sub-techniques
Reconnaissance
10 techniques
Active Scanning (2)
Gather Victim Host Information (4)
Gather Victim Identity Information (3)
Gather Victim Network Information (6)
Gather Victim Org Information (4)
Phishing for Information (3)
Search Closed Sources (2)
Search Open Technical Databases (5)
Search Open Websites/Domains (2)
Search Victim-Owned Websites
Resource Development
7 techniques
Acquire Infrastructure (6)
Compromise Accounts (2)
Compromise Infrastructure (6)
Develop Capabilities (4)
Establish Accounts (2)
Obtain Capabilities (6)
Stage Capabilities (5)
Initial Access
9 techniques
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (3)
Replication Through Removable Media
Supply Chain Compromise (3)
Trusted Relationship
Valid Accounts (4)
Execution
12 techniques
Command and Scripting Interpreter (8)
Container Administration Command
Deploy Container
Exploitation for Client Execution
Inter-Process Communication (2)
Native API
Scheduled Task/Job (6)
Shared Modules
Software Deployment Tools
System Services (2)
User Execution (3)
Windows Management Instrumentation
Persistence
19 techniques
Account Manipulation (4)
BITS Jobs
Boot or Logon Autostart Execution (15)
Boot or Logon Initialization Scripts (5)
Browser Extensions
Compromise Client Software Binary
Create Account (3)
Create or Modify System Process (4)
Event Triggered Execution (15)
External Remote Services
Hijack Execution Flow (11)
Implant Internal Image
Modify Authentication Process (4)
Office
Privilege Escalation
13 techniques
Abuse Elevation Control Mechanism (4)
Access Token Manipulation (5)
Boot or Logon Autostart Execution (15)
Boot or Logon Initialization Scripts (5)
Create or Modify System Process (4)
Domain Policy Modification (2)
Escape to Host
Event Triggered Execution (15)
Exploitation for Privilege Escalation
Hijack Execution Flow (11)
Process Injection (11)
Scheduled Task/Job (6)
Valid Accounts (4)
Defense Evasion
40 techniques
Abuse Elevation Control Mechanism (4)
Access Token Manipulation (5)
BITS Jobs
Build Image on Host
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain Policy Modification (2)
Execution Guardrails (1)
Exploitation for Defense Evasion
File and Directory Permissions Modification (2)
Hide Artifacts (9)
Hijack Execution Flow (11)
Impair Defenses (9)
Indicator Removal on Host (6)
Indirect Command Execution
Masquerading (7)
Credential Access
15 techniques
Adversary-in-the-Middle (2)
Brute Force (4)
Credentials from Password Stores (5)
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials (2)
Input Capture (4)
Modify Authentication Process (4)
Network Sniffing
OS Credential Dumping (8)
Steal Application Access Token
Steal or Forge Kerberos Tickets (4)
Steal Web Session Cookie
Two-Factor Authentication Interception
Discovery
29 techniques
Account Discovery (4)
Application Window Discovery
Browser Bookmark Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Cloud Storage Object Discovery
Container and Resource Discovery
Domain Trust Discovery
File and Directory Discovery
Group Policy Discovery
Network Service Scanning
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery (3)
Lateral Movement
9 techniques
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking (2)
Remote Services (6)
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material (4)
Collection
17 techniques
Adversary-in-the-Middle (2)
Archive Collected Data (3)
Audio Capture
Automated Collection
Browser Session Hijacking
Clipboard Data
Data from Cloud Storage Object
Data from Configuration Repository (2)
Data from Information Repositories (3)
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged (2)
Email Collection (3)
Command and Control
16 techniques
Application Layer Protocol (4)
Communication Through Removable Media
Data Encoding (2)
Data Obfuscation (3)
Dynamic Resolution (3)
Encrypted Channel (2)
Fallback Channels
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy (4)
Remote Access Software
Traffic
Exfiltration
9 techniques
Automated Exfiltration (1)
Data Transfer Size Limits
Exfiltration Over Alternative Protocol (3)
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium (1)
Exfiltration Over Physical Medium (1)
Exfiltration Over Web Service (2)
Scheduled Transfer
Transfer Data to Cloud Account
Impact
13 techniques
Account Access Removal
Data Destruction
Data Encrypted for Impact
Data Manipulation (3)
Defacement (2)
Disk Wipe (2)
Endpoint Denial of Service (4)
Firmware Corruption
Inhibit System Recovery
Network Denial of Service (2)
Resource Hijacking
Service Stop
System Shutdown/Reboot

Course of Action (COA) Evaluation Criteria

CRITERIA	WEIGHT
Operational Overhead	4
Ease of Use	2
Central Management	2
Initial Cost	1
Sustainment Cost	1

Criteria of higher importance have higher weight.

Course of Action (COA) Comparison

COA	Operational Overhead	Ease of Use	Central Mgmt	Initial Cost	Sustainment Cost	Total
	4	2	2	1	1	
Product 1	3 (12)	3 (6)	3 (6)	1 (1)	2 (2)	27
Product 2	2 (8)	2 (4)	2 (4)	2 (2)	3 (3)	21
Product 3	1 (4)	1 (2)	1 (2)	3 (3)	1 (1)	12

- Largest value for each evaluation criteria indicates highest rank (from 3 to 1).
- Rank is multiplied by Weight to obtain score in parentheses.
- Largest Total is the Recommended Product.

Product 1 is Recommended

Incident Response

- NIST SP 800-61 Computer Security Incident Handling Guide
- Hold mock interviews and press conferences during incident handling exercises. Example Media Questions:
  - Who attacked you? Why?
  - When did it happen?
  - How did it happen?
  - Did this happen because you have poor security practices?
  - How widespread is this incident?
  - What steps are you taking to determine what happened and to prevent future occurrences?
  - What is the impact of this incident?
  - Was any personally identifiable information (PII) exposed?
  - What is the estimated cost of this incident?

References

- Guide for Conducting Risk Assessments
  - https://csrc.nist.gov/files/pubs/sp/800/30/r1/final/docs/sp800-30-rev1-ipd.pdf
- DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle
  - https://permanent.fdlp.gov/gpo62894/Cybersecurity%20Guidebook%20v1%2008_signed.pdf
  - https://acqnotes.com/acqnote/tasks/risk-reporting-matrix
- MITRE ATT&CK®
  - MITRE ATT&CK®
- MITRE D3FEND™
  - D3FEND Matrix | MITRE D3FEND™
- Computer Security Incident Handling Guide
  - https://csrc.nist.gov/pubs/sp/800/61/r2/final
- CMU Stakeholder Specific Vulnerability Classification (SSVC)
  - https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=636379

Thank You!

MDSMITH.HOME@VERIZON.NET