SSE Project Update

Due to the recent surge in cyber-attacks against critical U.S. targets, NIST has accelerated the update to its cyber resiliency guideline, Special Publication 800-160, Volume 2, *Developing Cyber Resilient Systems*. The initial public draft has been completed and is currently undergoing an internal review. The publication is on the fast track with expected posting and release for public comment in August 2021.

This update constitutes the first revision to NIST Special Publication 800-160, Volume 2 since its original publication. There is significant new content in the updated publication that will help NIST's customers reduce their susceptibility to damaging, destructive, and costly cyber-attacks. In addition to a general update of the entire publication, there are five significant changes that either add new content or move current content to a new location. These include:

- **Updating** the controls that support cyber resiliency to be consistent with NIST Special Publication 800-53, Revision 5.
- **Standardizing** on a single threat taxonomy, the Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework.
- **Providing** a detailed mapping and analysis of the cyber resiliency implementation approaches and supporting NIST controls to the ATT&CK framework techniques, mitigations, and candidate mitigations.
- **Eliminating** Appendix F on Cyber Resiliency in the System Life Cycle. This information will be reflected in the 2021 update to NIST Special Publication 800-160, Volume 1.
- **Moving** cyber resiliency use cases and examples in Appendices I and J to the NIST Special Publication 800-160, Volume 2 website.

The focus of cyber resiliency is on mitigating cyber-attacks on systems, organizations, and critical infrastructures from the advanced persistent threat (APT). It is important to understand what effects these mitigations have on adversaries. Mapping the current or potential effects of mitigations to a threat taxonomy provides a structured way to facilitate this understanding.

Here is a sample of the types of cyber resiliency mapping tables in the draft update. The table below show mitigations or candidate mitigations for ATT&CK framework techniques, the cyber resiliency implementation approaches and supporting controls that address the threat, and the potential effects on adversaries. Similar tables are included for every technique category in the attack sequence (e.g., resource development, initial access, execution, persistence, privilege escalation, defense evasion, credential access, discovery, lateral movement, collection, command and control, exfiltration, and impact.

TABLE F-3: POTENTIAL EFFECTS OF CYBER RESILIENCY ON RECONNAISSANCE TECHNIQUES

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
Active Scanning (T1595)	Present Deceptive Information (CM1101)	Disinformation	Deceive	SC-30(4)
		Tainting	Detect	SI-20
	Passive Decoys (CM1104)	Misdirection	Deceive	SC-26
		Architectural Diversity	Exert	SC-29
	Conceal Resources from Discovery (CM1160)	Obfuscation, Functional Relocation of Cyber Resources	Degrade, Exert, Shorten	SC-7(16)
		Obfuscation	Degrade Exert	SC-28(1), SC-30, SC-30(5)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
Gather Victim Host Information (T1592)	Present Deceptive Information (CM1101)	Disinformation	Deceive	SC-30(4)
	Passive Decoys (CM1104)	Misdirection	Deceive	SC-26
		Architectural Diversity	Exert	SC-29
	Present Decoy Data (CM1113)	Disinformation	Deceive	SC-30(4)
		Tainting	Detect	SI-20
Gather Victim Identity Information (T1589)	Present Deceptive Information (CM1101)	Disinformation	Deceive	SC-30(4)
		Tainting	Detect	SI-20
	Present Decoy Data (CM1113)	Disinformation	Deceive	SC-30(4)
		Tainting	Detect	SI-20
	Enhance User Preparedness (CM1159)	Dynamic Threat Awareness	Exert	AT-2(1), AT-2(5)
		Self-Challenge	Exert	AT-2(1), AT-3(3)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
Gather Victim Network	Maintain Deception Environment (CM1102)	Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26

ATT&CK Technique	Mitigation or Candidate Mitigation	Cyber Resiliency Implementation Approaches	Potential Effects	Cyber Resiliency Controls
Information (T1590)		Misdirection	Deceive	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Present Decoy Data (CM1113)	Disinformation	Deceive	SC-30(4)
		Tainting	Detect	SI-20
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
Phishing for Information (T1598)	User Training (M1017)	Dynamic Threat Awareness	Preempt, Exert, Detect	AT-2(5)
	Adversarial Simulation (CM1107)	Dynamic Threat Awareness, Self-Challenge	Preempt	AT-2(1), AT-3(3)
	Present Deceptive Information (CM1101)	Disinformation	Deceive	SC-30(4)
	Active Decoys (CM1123)	Misdirection, Forensic and Behavioral Analysis	Detect	SC-35
	Enhance User Preparedness (CM1159)	Dynamic Threat Awareness	Detect	AT-2(1), AT-2(3), AT-2(5), AT-3(3)
	Analyze Network Traffic Content (CM2041)	Monitoring and Damage Assessment, Behavior Validation	Detect	SI-4(13)

And, here is a sample of some of the expanded candidate mitigations referenced in the table above.

TABLE F-17: CANDIDATE MITIGATIONS TO REDIRECT, PRECLUDE, IMPEDE, OR LIMIT THREAT EVENTS

Identifier	Name	Description	Cyber Resiliency Approaches	Controls
CM1101	Present Deceptive Information	Present deceptive information about systems, data, processes, and users. Monitor uses or search for presence of that information.	Disinformation, Tainting	SC-30(4), SI-20
CM1102	Maintain Deception Environment	Maintain a distinct subsystem or a set of components specifically designed to be the target of malicious attacks for detecting, deflecting, and analyzing such attacks.	Monitoring and Damage Assessment, Forensic and Behavioral Analysis, Misdirection, Disinformation, Predefined Segmentation	SC-7(21), SC-26, SC-30(4)

Identifier	Name	Description	Cyber Resiliency Approaches	Controls
CM1103	Detonation Chamber	Use a dynamic execution environment to handle potentially harmful incoming data.	Forensic and Behavioral Analysis, Misdirection, Predefined Segmentation	SC-44
CM1104	Passive Decoys	Use a factitious systems or resources to decoy adversary attacks away from operational resources.	Misdirection, Architectural Diversity	SC-26, SC-29
CM1105	Component Provenance Validation	Validate the provenance of system components.	Provenance Tracking	SR-4, SR-4(1), SR-4(2), SR-4(3)
CM1106	Supply Chain Diversity	Provide multiple distinct supply chains for system components.	Supply Chain Diversity	PL-8(2), SR-3(1), SR-3(2)
CM1107	Adversarial Simulation	Simulate adversary activities to test the effectiveness of system protections and detection mechanisms.	Self-Challenge	AT-2(1), AT-3(3), CA-8, CA-8(2), SC-7(10)
CM1108	Dynamically Restrict Traffic or Isolate Resources	Dynamically reconfigure networking to restrict network traffic or isolate resources.	Dynamic Resource Allocation, Adaptive Management, Dynamic Reconfiguration, Dynamic Segmentation and Isolation	AU-5(3), IR-4(2), SC-7(20)
CM1109	Virtual Sandbox	Use virtualization to create a controlled execution environment, which is expunged after execution terminates.	Non-Persistent Services, Dynamic Segmentation and Isolation	SC-7(20), SI-14
CM1120	Trusted Path	Provide an isolated communications path between the user and security functions.	Predefined Segmentation	SC-11
CM1145	Defend Failover and Recovery	Increase sensor activity and restrict privileges to defend against an adversary taking advantage of failover or recovery activities.	Adaptive Management, Dynamic Reconfiguration, Orchestration, Functional Relocation of Sensors, Dynamic Segmentation and Isolation, Mission Dependency and Status Visualization, Dynamic Privileges	AC-2(6), IR-4(2), IR-4(3), SC-7(20), SC-48, SC-48(1), SI-4(1)

NIST will be seeking inputs, feedback, and comments on this work as soon as it is published—in particular, in the new areas described above. Stayed tuned for further updates as we continue to move forward in this project.

Cyber-attacks are inevitable. Successful cyber-attacks are not.

> *"If a full on 'turn the lights off' cyber war were to happen today, we would lose. Think about that. We would lose a cyber war. With a few clicks of the mouse, and in just a few seconds, hackers … could turn off our electricity, millions would lose heat, groceries would spoil, banking machines would not work, and people could not get gasoline. It would be what we have seen down in Texas, but on national scale and with no end in sight. That we have escaped a digital catastrophe thus far is not due to skill. It is due to blind luck and restraint from our adversaries."*
>
> **Mike Rogers, February 2021**
> **Former Member of Congress, House Intelligence Committee**