TEXAS RE

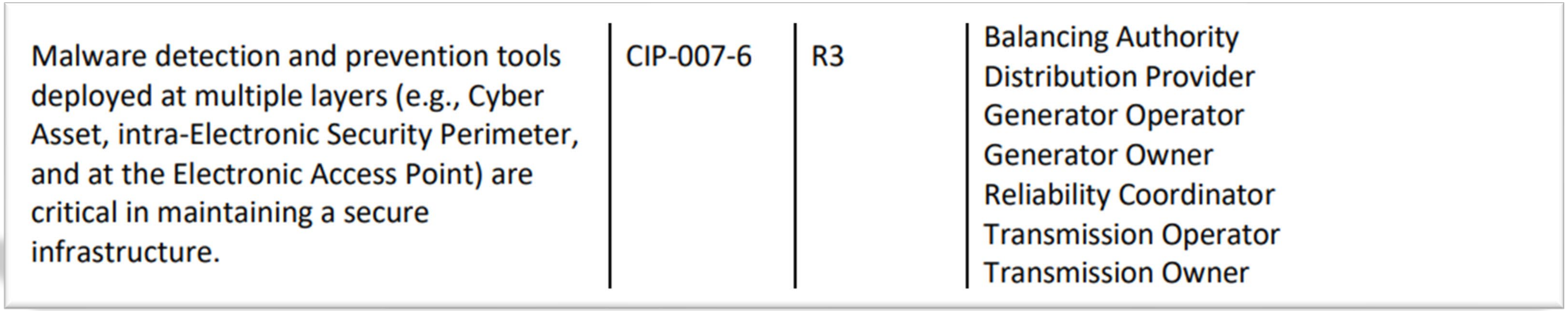
CIP-007-6 R3

Devin Ferris
Manager, CIP Compliance Monitoring

March 7, 2025

Risk Element Areas of Focus: Remote Connectivity

CIP-007-6 R3: Malicious Code Prevention



Malware detection and prevention tools deployed at multiple layers (e.g., Cyber Asset, intra-Electronic Security Perimeter, and at the Electronic Access Point) are critical in maintaining a secure infrastructure.	CIP-007-6	R3	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner

CIP-007-6 R3

Part 3.1

- Deploy method(s) to deter, detect, or prevent malicious code

Part 3.2

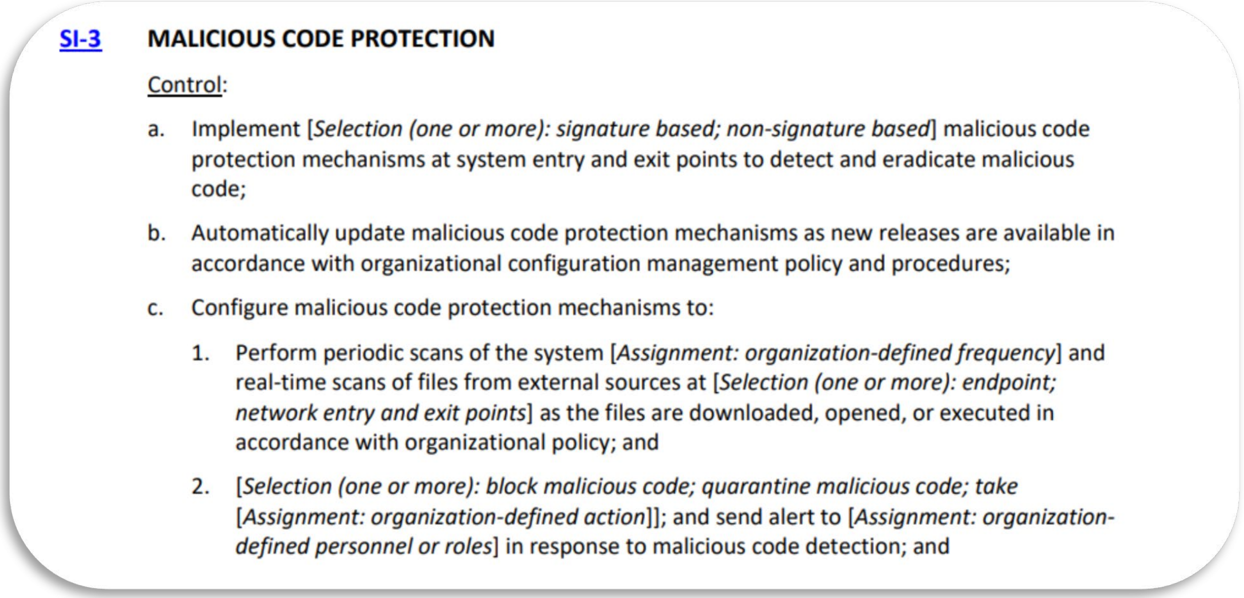
- Mitigate the threat of detected malicious code

Part 3.3

- For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.

Malicious Code Protection Controls

NIST Control Example



SI-3 **MALICIOUS CODE PROTECTION**

Control:

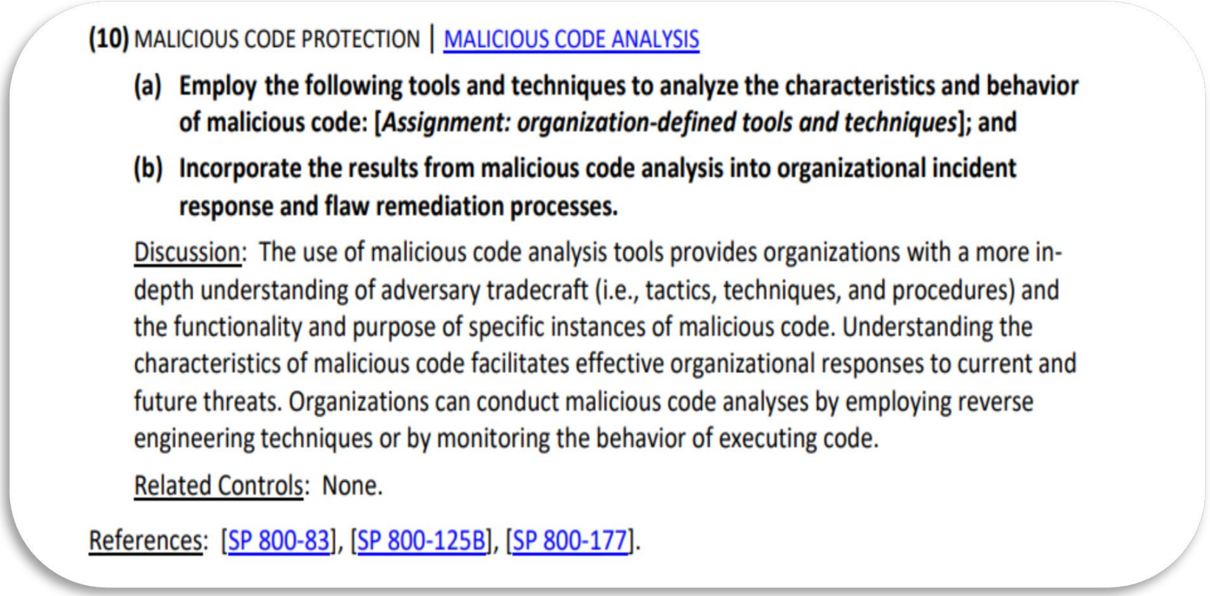
a. Implement [*Selection (one or more): signature based; non-signature based*] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;

b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;

c. Configure malicious code protection mechanisms to:

1. Perform periodic scans of the system [*Assignment: organization-defined frequency*] and real-time scans of files from external sources at [*Selection (one or more): endpoint; network entry and exit points*] as the files are downloaded, opened, or executed in accordance with organizational policy; and

2. [*Selection (one or more): block malicious code; quarantine malicious code; take* [*Assignment: organization-defined action*]]; and send alert to [*Assignment: organization-defined personnel or roles*] in response to malicious code detection; and



(10) MALICIOUS CODE PROTECTION | MALICIOUS CODE ANALYSIS

(a) Employ the following tools and techniques to analyze the characteristics and behavior of malicious code: [*Assignment: organization-defined tools and techniques*]; and

(b) Incorporate the results from malicious code analysis into organizational incident response and flaw remediation processes.

Discussion: The use of malicious code analysis tools provides organizations with a more in-depth understanding of adversary tradecraft (i.e., tactics, techniques, and procedures) and the functionality and purpose of specific instances of malicious code. Understanding the characteristics of malicious code facilitates effective organizational responses to current and future threats. Organizations can conduct malicious code analyses by employing reverse engineering techniques or by monitoring the behavior of executing code.

Related Controls: None.

References: [SP 800-83], [SP 800-125B], [SP 800-177].

Questions?

TEXAS RE
Ensuring electric reliability for Texans