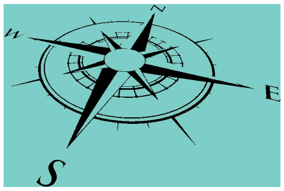
Trusted Internet Connections 3.0 -- Vol. 3: Security Capabilities Handbook

The Security Capabilities Handbook provides a list of deployable security controls, security capabilities, and best practices. The handbook is intended to guide secure implementation and satisfy program requirements within discrete networking environments. The Security Capabilities Handbook offers actionable guidance for employing the principles articulated in the TIC 3.0 Program Guidebook, as well as the secure architecture and components outlined in the TIC 3.0 Reference Architecture. Additionally, the capabilities included in this document can be aligned with service provider overlays to enable deployment of existing and future TIC Use Cases.

Universal Security Capabilities — Universal capabilities are enterprise-level capabilities that outline guiding principles for TIC Use Cases and apply across use cases. Agencies have the discretion to determine the level of rigor necessary for applying universal capabilities based on federal guidelines and risk tolerance. The table below provides: (1) a list of the universal security capabilities, (2) a description of each capability, and (3) a mapping of each capability to relevant NIST Cybersecurity Framework (CSF) categories. While universal capabilities are broadly applicable, certain use cases may provide unique guidance on specific capabilities where necessary. [In this StratML rendition, the universal capabilities are documented as objectives under the broader goals.]

Contents



Cybersecurity and Infrastructure Security Agency (CISA)

Description:

Cybersecurity Division

Mission

To provide a list of deployable security controls, security capabilities, and best practices.

Values

Connection

Security

Agility: The Security Capabilities Handbook is intended to keep pace with the evolution of policy and technology.

Responsiveness: Consequently, this document will be updated periodically to assess existing TIC capabilities against changes in business mission needs, market trends, and the threat landscape.

1. Traffic

Manage Traffic

Observe, validate, and filter data connections to align with authorized activities; least privilege and default deny

1.1. Configuration

Implement a formal plan for documenting, and managing changes to the environment, and monitoring for deviations.

Configuration Management

1.2. Inventory

Develop, document, and maintain a current inventory of all systems, networks, and components so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

1.3. Privilege

Design the security architecture such that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

Least Privilege

1.4. Synchronization

Coordinate clocks on all systems (e.g. servers, workstations, network devices) to enable accurate comparison of timestamps between systems.

Time Synchronization

1.5. Parity

Consistently apply security protections and other policies, independent of the conveyance mechanism used.

Policy Enforcement Parity

1.6. Integration

Defining polices such that they apply to a given agency entity no matter its location.

Integrated Desktop, Mobile, and Remote Policies

2. Confidentiality

Protect Traffic Confidentiality

Ensure only authorized parties can discern the contents of data in transit; sender and receiver identification and enforcement

2.1. Authentication

Verify the identity of users, devices or other entities through rigorous means (e.g. multi-factor authentication) before granting access.

Strong Authentication

3. Integrity

Protect Traffic Integrity

Prevent alteration of data in transit; detect altered data in transit

3.1. Administration

Perform administrative tasks in a secure manner, using secure protocols.

Secure Administration

3.2. Vulnerability

Proactively work to discover vulnerabilities, including the use of both active and passive means of discovery, and taking action to mitigate discovered vulnerabilities.

Vulnerability Assessment

3.3. Auditing & Accounting

Capture business records, including logs and other telemetry, and making them available for auditing and accounting as required.

3.4. Situational Awareness

Maintain effective awareness, both current and historical, across all components.

4. Resiliency

Ensure Service Resiliency

Promote resilient application and security services for continuous operation as the technology and threat landscape evolve

4.1. Performance

Ensure that systems, services, and protections maintain acceptable performance under adverse conditions

Resilience

4.2. Threats

Obtain threat intelligence from private and government sources, and implementing mitigations for the identified risks.

Enterprise Threat Intelligence

Stakeholder(s):

Private Sources **Government Sources**

4.3. Shared Services

Employ shared services, where applicable, that can be individually tailored, measured to independently validate service conformance, and offer effective protections for tenants against malicious actors, both external as well as internal to the service provider.

Effective Use of Shared Services

5. Response

Ensure Effective Response

Promote timely reaction and adapt future response to discovered threats; policies defined and implemented; simplified adoption of new countermeasures

5.1. Backup & Recovery

Keep copies of configuration and data, as needed, to allow for the quick restoration of service in the event of malicious incidents, system failures or corruption.

5.2. Logs

Store telemetry needed to discover and respond to malicious activity in a manner that facilitates security analysis and data fusion.

Central Log Management with Analysis

5.3. Incidents

Document and implement a set of instructions or procedures to detect, respond to, limit consequences of malicious cyberattacks, and restore the integrity of the network and systems.

Incident Response Plan and Incident Handling

5.4. Discovery

Use dynamic approaches (e.g. heuristics, baselining, etc.) to discover new malicious activity.

Dynamic Threat Discovery

Administrative Information

Start Date: 2019-12-31
End Date: 2020-01-31

Publication Date: **2020-05-20**
Source: https://www.cisa.gov/sites/default/files/publications/Draft%20TIC%203.0%20Vol.%203%20Security%20Capabilities%20Handbook.pdf

Submitter:

Given Name: Owen
Surname: Ambur
Email: Owen.Ambur@verizon.net
Phone: