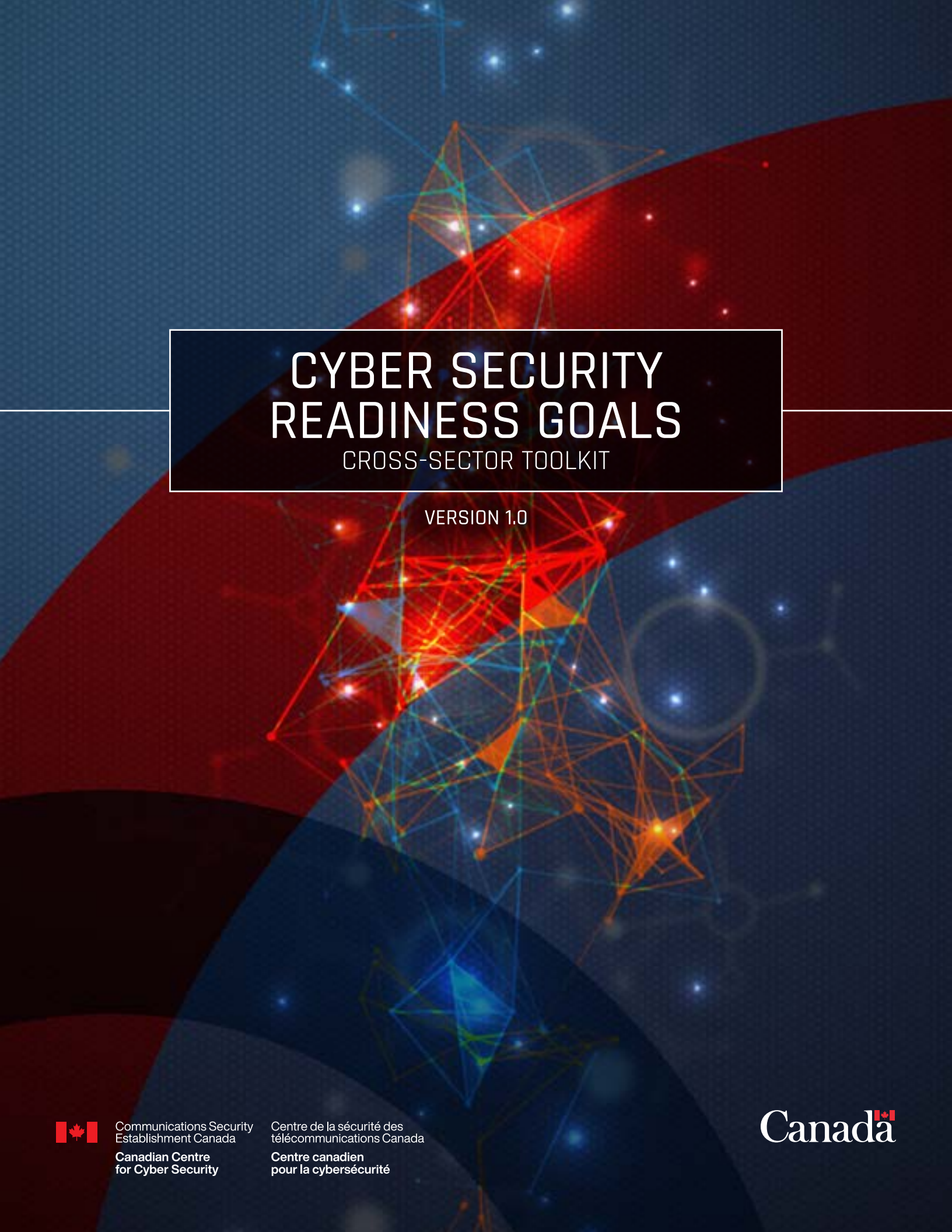

CYBER SECURITY READINESS GOALS

CROSS-SECTOR TOOLKIT

VERSION 1.0

Communications Security Establishment Canada
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications Canada
Centre canadien pour la cybersécurité

Canada

Cyber Security Readiness Goals - Cross-Sector Toolkit

D96-121/2024E-PDF
978-0-660-73262-6

The Cross-Sector Toolkit is linked to the Cyber Centre's CRGs publication. The Cross-Sector Toolkit has 36 CRGs to support Canadian CI owners and operators, from any sector, in prioritizing investments in cyber security and to elevate their cyber security posture. The table below matches each goal with the intended outcome, the recommended action, and the associated risk, such as tactics, techniques, and procedures (TTPs) from *MITRE ATT&CK* (https://attack.mitre.org), addressed by the goal. The table also includes links to relevant Cyber Centre guidance and references the *NIST Cybersecurity Framework (CSF) 2.0* (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf).

For additional context on the CRGs, see the *Cyber Security Readiness Goals* (https://www.cyber.gc.ca/en/cyber-security-readiness-goals/cyber-security-readiness-goals-securing-our-most-critical-systems) publication, available on the Cyber Centre website.

This toolkit is provided by the Cyber Centre to help organizations strengthen their cyber security posture. This PDF is a fillable form, allowing organizations to document their progress towards the CRGs. Information recorded in this form is not collected by the Cyber Centre. The form should not be returned to the Cyber Centre and any information returned to the Cyber Centre will be deleted.

GOVERN [0]

Privacy leadership [0.0]

Outcome A single leader or team is responsible and accountable for managing cyber-related privacy risk.

Recommended Action

Identify a named role or title as responsible and accountable for the organization's privacy risk management program. The responsible person or team establishes policies and procedures that require the organization to:

- consider the full spectrum of cyber-related privacy risks and obligations, including applicable privacy legislation
- apply that analysis to support operational decisions

The privacy risk management program could include maintaining a personal information inventory, as well as policies to limit collection and retention of personal information.

TTP/Risks

Lack of accountability, investment, or effectiveness.

References

GV.OC-03, GV.RM-06

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

Supply chain incident reporting process/policies [0.1]

Outcome Organizations more rapidly learn about and respond to known incidents or breaches across vendors and service providers.

Recommended Action

Ensure the organization's cyber security supply chain risk management program stipulates that vendors and/or service providers must notify the procuring customer of security incidents. This should be done within a risk-informed time frame, as determined by the organization, and be documented in procurement documents and contracts, such as service level agreements.

TTP/Risks

Supply Chain Compromise (Techniques (T) 1195, Industrial Control Systems (ICS) T0862).

References

GV.SC-01, GV.SC-05

Protecting your organization from software supply chain threats (ITSM.10.071) (https://www.cyber.gc.ca/en/guidance/protecting-your-organization-software-supply-chain-threats-itsm10071)

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

Vendor/supplier cyber security requirements [0.2]

Outcome Reduce risk by buying more secure products and services from more secure suppliers.

Recommended Action

Include cyber security requirements and questions in organizations' procurement documents. Ensure those responses are evaluated in vendor selection such that, given 2 offerings of roughly similar cost and function, the more secure offering and/or supplier is preferred or, when possible, the more secure option is preferred even at higher cost.

TTP/Risks

Supply Chain Compromise (T1195, ICS T0862).

References

GV.SC-05

Protecting your organization from software supply chain threats (ITSM.10.071) (https://www.cyber.gc.ca/en/guidance/protecting-your-organization-software-supply-chain-threats-itsm10071)

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

Organizational and operational technology cyber security leadership [0.3]

Outcome A single leader is responsible and accountable for cyber security within an organization. If applicable to the organization, a single leader is responsible and accountable for operational technology (OT) specific cyber security within an organization with OT assets. In some organizations, one individual may be responsible for both leaderships.

Recommended Action

Identify a named role or title as responsible and accountable for planning, resourcing, and executing cyber security activities. This role may undertake activities, such as managing cyber security operations at the senior level, requesting, and securing budget resources, or leading strategy to inform future positioning. Additionally, identify a named role or title as responsible for resourcing, and executing OT-specific cyber security activities. In some organizations, both cyber security leadership and OT leadership can be the same position.

TTP/Risks

Lack of accountability, investment, or effectiveness in cyber security or OT cyber security programs.

References

GV.RR-02, GV.PO-01, GV.PO-02

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

Improving information technology [IT] and OT cyber security relationships [0.4]

Outcome Improve OT cyber security and more rapidly and effectively respond to OT cyber incidents.

Recommended Action

At least once per year, sponsor a relationship-building activity that is focused on strengthening working relationships between IT and OT security personnel and that is not a working event (such as providing meals during an incident response (IR)). This can provide opportunities for IT and OT personnel to:

- open lines of communication
- achieve common understanding of the evolved threat surface
- establish common priorities
- create a security plan to protect both the OT and the surrounding IT

TTP/Risks

Poor working relationships and a lack of mutual understanding between IT and OT cyber security can often result in increased risk for OT cyber security.

References

GV.RR-02

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

IDENTIFY [1]

Asset inventory and network topology [1.0]

Outcome Better identify known, unknown, and unmanaged assets, including web-facing assets for the cloud and data assets. Your organization can then more rapidly detect and respond to new vulnerabilities and maintain service continuity.

Recommended Action

Maintain a regularly updated inventory of all assets within the organization's IT (including IPv6) and OT networks (if applicable). Include in the inventory accurate documentation of network topology and identified data assets, in particular sensitive or classified information. Update this inventory on a regular basis for both IT and OT, and immediately log in the existing inventory any new asset that is integrated into the organization's infrastructure.

TTP/Risks

Hardware Additions (T1200)

Exploit Public-Facing Applications (T1190, ICS T0819)

Internet Accessible Device (ICS T0883)

References

ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-04, DE.CM-01

Using information technology asset management (ITAM) to enhance cyber security (ITSM.10.004) (https://www.cyber.gc.ca/en/guidance/using-information-technology-asset-management-itam-enhance-cyber-security-itsm10004)

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

Mitigating known vulnerabilities [1.1]

Outcome Reduce the likelihood that threat actors will exploit known vulnerabilities to breach organizational networks.

Recommended Action

Patch all known exploited vulnerabilities listed in the Cybersecurity and Infrastructure Agency: Known Exploited Vulnerabilities Catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog) in Internet-facing systems within a risk-informed timespan, prioritizing more critical assets first. Identify security vulnerabilities in your systems by conducting penetration tests and using automated vulnerability scanning tools, activities which are part of a comprehensive vulnerability management strategy.

For OT assets where patching is not possible or may substantially compromise availability or safety, apply and record compensating controls (for example, segmentation, monitoring). Sufficient controls either make the asset inaccessible from the public Internet or reduce the ability of threat actors to exploit the vulnerabilities in these assets.

Carefully select automated vulnerability detection tools as they can scan systems aggressively. These tools may cause devices to behave erratically, stop working, crash, or restart, or need manual intervention to revert to an operational state.

TTP/Risks

Active Scanning: Vulnerability Scanning (T1595.002)

Exploit Public-Facing Application (T1190, ICS T0819)

Exploitation of Remote Service (T1210, ICS T0866)

Supply Chain Compromise (T1195, ICS T0862)

External Remote Services (T1133, ICS T0822)

References

ID.RA-01, ID.RA-08, ID.RA-06, PR.PS-02, PR.PS-03

Top 10 IT Security actions: No.2 patch operating systems and applications (ITSM.10.096)(https://www.cyber.gc.ca/en/guidance/top-10-it-security-action-items-no2-patch-operating-systems-and-applications-itsm10096)

Top 10 IT security actions: No. 5 Segment and separate information (ITSM.10.092)(https://www.cyber.gc.ca/en/guidance/top-10-security-actions-no-5-segment-and-separate-information-itsm10092)

How updates secure your device (ITSAP.10.096) (https://www.cyber.gc.ca/en/guidance/how-updates-secure-your-device-itsap10096)

Baseline cyber security controls for small and medium organizations (https://www.cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations)

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

Third-party validation of cyber security control effectiveness [1.2]

Outcome Identify TTPs that lack proper defences and establish confidence in organizational cyber defences.

Recommended Action

Third parties with demonstrated expertise in IT and/or OT cyber security regularly validate the effectiveness and coverage of an organization's cyber security defences. Conduct these exercises annually to include activities such as penetration tests, bug bounties, incident simulations, or table-top exercises, and include both unannounced and announced tests.

Exercises consider both the ability and impact of a potential adversary to infiltrate the network from the outside, as well as the ability of an adversary within the network (for example, assume breach) to pivot laterally to demonstrate potential impact on critical systems, including operational technology and industrial control systems.

Mitigate in a timely manner high-impact findings from previous tests so these are not re-observed in future tests.

TTP/Risks

Reduce the risk of gaps in cyber defences or a false sense of security in existing protections.

References

ID.RA-01, ID.RA-03, ID.RA-04, ID.RA-05, ID.RA-06

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

Incident response [IR] plans [1.3]

Outcome Organizations maintain, practice, and update cyber security incident response plans for relevant threat scenarios.

Recommended Action

Develop, maintain, update, and regularly drill IT and OT cyber security IR plans for both common and organization-specific (for example, by sector or locality) threat scenarios and TTPs. Consider engaging with appropriate stakeholders to conduct tabletop exercises focused on artificial intelligence-enhanced attacks.

When tests or drills are conducted, ensure they are as realistic as feasible and conform to the organization's acceptable levels of downtime. Drill IR plans at least annually and update within a risk-informed time frame following the lessons learned portion of any exercise or drill.

TTP/Risks

Inability to quickly and effectively contain, mitigate, and communicate about cyber security incidents.

References

ID.IM-04, ID.IM-02

Developing your incident response plan (ITSAP.40.003) (https://www.cyber.gc.ca/en/guidance/developing-your-incident-response-plan-itsap40003)

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

Deploy security.txt files [1.4]

Outcome Allows security researchers to submit discovered weaknesses or vulnerabilities more quickly.

Recommended Action

Ensure all public-facing web domains have a security.txt file that conforms to the recommendations in RFC 9116.

TTP/Risks

Active Scanning: Vulnerability Scanning (T1595.002)

Exploit Public-Facing Application (T1190, ICS T0819)

Exploitation of Remote Services (T1210, ICS T0866)

Supply Chain Compromise (T1195, ICS T0862)

References

ID.RA-08

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

Select a trusted cloud service provider [1.5]

Outcome If cloud is leveraged and a trusted relationship established with a mature and technically capable cloud service provider (CSP), organizations can confidently adopt cloud services, harnessing the benefits of scalability, flexibility, and cost-effectiveness while safeguarding their sensitive assets.

Recommended Action

Ensure that your selected CSP offers secure data storage, encryption, and access controls, and validate that the CSP's cyber security capability and practices are compliant with relevant security standards and regulations. This can be accomplished by confirming a CSP's adherence to existing compliance regimes, which can vary depending on the organization's business requirements.

TTP/Risks

Reduce risk of attacks and/or compromise due to immature CSP

Supply Chain Compromise (T1195, ICS T0862)

References

GV.OC-03, GV.SC-05, GV.SC-07, ID.AM-02

Top measures to enhance cyber security for small and medium organizations (ITSAP.10.035) (https://www.cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035)

Baseline cyber security controls for small and medium organizations (https://www.cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations)

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

PROTECT [2]

Changing default passwords [2.0]

Outcome Prevent threat actors from using default passwords to achieve initial access to or move laterally in a network.

Recommended Action

Enforce an organization-wide policy and/or process that requires changing default manufacturer passwords for any/all hardware, software, and firmware before putting them on any internal or external networks. This includes IT assets for OT, such as OT administration web pages.

In instances where changing default passwords is not feasible (for example, a control system with a hard-coded password), implement and document appropriate compensating security controls. Additionally, monitor logs for network traffic and login attempts on those devices.

While changing default passwords on an organization's existing OT requires significantly more work, enforce a policy to change default credentials for all new or future devices. This is not only easier to achieve, but also reduces potential risk in the future if adversary TTPs change.

TTP/Risks

Valid Accounts: Default Accounts (T1078.001)

Valid Accounts (ICS T0859)

References

PR.AA-01, PR.AA-05

Top 10 IT security actions: No. 3 managing and controlling administrative privileges (ITSM.10.094) (https://www.cyber.gc.ca/en/guidance/top-10-it-security-actions-no3-managing-controlling-administrative-privileges-itsm10094)

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

Minimum password strength [2.1]

Outcome Organizational passwords are harder for threat actors to guess or crack.

Recommended Action

Implement a system-enforced policy that requires a minimum password length of 15* or more characters for all password-protected IT assets and for all OT assets where technically feasible.**

Consider leveraging passphrases of at least 4 words and 15 characters in length. Where suitable, use passphrases, as they are longer but easier to remember than a password of random, mixed characters.

In instances where minimum password lengths are not technically feasible, apply and record compensating controls, and log all login attempts to those assets. Prioritize for upgrade or replacement any assets that cannot support passwords of sufficient strength length.

This goal is particularly important for organizations that:

- lack widespread implementation of multi-factor authentication (MFA) and capabilities to protect against brute-force attacks (such as web application firewalls and third-party content delivery networks)
- are unable to adopt passwordless authentication methods.

Note

* Modern attacker tools can crack 8-character passwords quickly. Length is a more impactful and important factor in password strength than complexity or frequent password rotations. Long passwords are also easier for users to create and remember.

** OT assets that use a central authentication mechanism (such as Active Directory) are most important to address. Examples of low-risk OT assets that may not be technically feasible include those in remote locations, such as on offshore rigs or wind turbines.

TTP/Risks

Brute Force: Password Guessing (T1110.001)

Brute Force: Password Cracking (T1110.002)

Brute Force: Password Spraying (T1110.003)

Brute Force: Credential Stuffing (T1110.004)

References

PR.AA-01, PR.AA-05

Best Practices for Passphrases and Passwords (ITSAP.30.032) (https://www.cyber.gc.ca/en/guidance/best-practices-passphrases-and-passwords-itsap30032)

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

Unique credentials [2.2]

Outcome Attackers are unable to reuse compromised credentials to move laterally across the organization, particularly between IT and OT networks.

Recommended Action

Provision unique and separate credentials for similar services and asset access on IT and OT networks. Ensure users do not (or cannot) reuse passwords for accounts, applications, services, etc. Require that service accounts/machine accounts have unique passwords from all member user accounts.

TTP/Risks

Valid Accounts (T1078, ICS T0859)

Brute Force : Password Guessing (T1110.001)

References

PR.AA-01, PR.AA-05

Top 10 IT security actions: No. 3 managing and controlling administrative privileges (ITSM.10.094) (https://www.cyber.gc.ca/en/guidance/top-10-it-security-actions-no3-managing-controlling-administrative-privileges-itsm10094)

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

Revoking credentials for departing employees [2.3]

Outcome Prevents unauthorized access to organizational accounts or resources by former employees.

Recommended Action

Apply a defined and enforced administrative process to all departing employees by the day of their departure that:

- revokes and securely returns all physical badges, key cards, tokens, etc.
- disables all user accounts and access to organizational resources

TTP/Risks

Valid Accounts (T1078, ICS T0859)

References

PR.AA-01, PR.AA-05, PR.AA-06, GV.RR-04

Top 10 IT security actions: No. 3 managing and controlling administrative privileges (ITSM.10.094) (https://www.cyber.gc.ca/en/guidance/top-10-it-security-actions-no3-managing-controlling-administrative-privileges-itsm10094)

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

Separating user and privileged accounts [2.4]

Outcome Make it more difficult for threat actors to gain access to administrator or privileged accounts, even if common user accounts are compromised.

Recommended Action

User accounts do not always have administrator or super-user privileges. Administrators maintain separate user accounts for all actions and activities not associated with the administrator role (for example, for business email, web browsing). Reevaluate privileges on a recurring basis to validate continued need for a given set of permissions.

TTP/Risks

Valid Accounts (T1078, ICS T0859)

References

PR.AA-05

Top 10 IT security actions: No. 3 managing and controlling administrative privileges (ITSM.10.094) (https://www.cyber.gc.ca/en/guidance/top-10-it-security-actions-no3-managing-controlling-administrative-privileges-itsm10094)

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

Network segmentation [2.5]

Outcome Reduce the likelihood that threat actors will access the OT network after compromising the IT network.

Recommended Action

All connections to the OT network are denied by default unless explicitly allowed (for example, by IP address and port) for specific system functionality. Necessary communications paths between the IT and OT networks must pass through an intermediary, such as a properly configured firewall, bastion host, jump box, or a demilitarized zone, which is closely monitored, captures network logs, and only allows connections from approved assets.

TTP/Risks

Network Service Discovery (T1046)

Trusted Relationship (T1199)

Network Connection Enumeration (ICS T0840)

Network Sniffing (T1040, ICS T0842)

References

PR.IR-01, PR.AA-06

Top 10 IT security actions: No.5 segment and separate information (ITSM.10.092) (https://www.cyber.gc.ca/en/guidance/top-10-security-actions-no-5-segment-and-separate-information-itsm10092)

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

Detection of unsuccessful [automated] login attempts [2.6]

Outcome Protect organizations from automated, credential-based attacks.

Recommended Action

Log all unsuccessful logins and send to your organization's security team or relevant logging system. Ensure security teams are notified (for example, by an alert) after a specific number of consecutive, unsuccessful login attempts in a short period (for example, 5 failed attempts over 2 minutes). Log and store these alerts in the relevant security or ticketing system for retroactive analysis.

For IT assets, establish a system-enforced policy that prevents future logins for the suspicious account. For example, this could be for some minimum time or until the account is re-enabled by a privileged user. Enable this configuration when available on an asset. For example, Windows 11 can automatically lock out accounts for 10 minutes after 10 incorrect logins in a 10 minute period.

TTP/Risks

Brute Force: Password Guessing (T1110.001)

Brute Force: Password Cracking (T1110.002)

Brute Force: Password Spraying (T1110.003)

Brute Force: Credential Stuffing (T1110.004)

References

PR.AA-03, DE.CM-09

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

Phishing-resistant multi-factor authentication [2.7]

Outcome Add a critical, additional layer of security to protect asset accounts whose credentials have been compromised.

Recommended Action

Implement MFA for access to assets using the strongest available method for that asset (see below for scope).

MFA options ranked by strength, from high to low, are as follows:

1. Hardware-based, phishing-resistant MFA (for example, FIDO/WebAuthn or public key infrastructure (PKI) based).
2. If such hardware-based MFA is not available, then use mobile app-based soft tokens (preferably push notification with number matching) or emerging technology such as FIDO passkeys.
3. Only use MFA via SMS or voice when no other options are possible.

Ensure all IT accounts leverage MFA to access organizational resources. Prioritize accounts with highest risk, such as privileged administrative accounts for key IT systems.

Within OT environments, enable MFA on all accounts and systems that can be accessed remotely, including vendors/maintenance accounts, remotely accessible user and engineering workstations, and remotely accessible human-machine interfaces.

TTP/Risks

Brute Force (T1110)

Remote Services : Remote Desktop Protocol (T1021.001)

Remote Services SSH (T1021.004)

Valid Accounts (T1078, ICS T0859)

External Remote Services (ICS T0822)

References

PR.AA-01, PR.AA-03, PR.AA-05

Steps for effectively deploying multi-factor authentication (MFA) (ITSAP.00.105) (https://www.cyber.gc.ca/en/guidance/steps-effectively-deploying-multi-factor-authentication-mfa-itsap00105)

Secure your accounts and devices with multi-factor authentication (ITSAP.30.030) (https://www.cyber.gc.ca/en/guidance/secure-your-accounts-and-devices-multi-factor-authentication-itsap30030)

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

Basic and OT cyber security training [2.8]

Outcome

Organizational users learn and perform more secure behaviours. If applicable, personnel responsible for securing OT assets receive specialized OT-focused cyber security training.

Recommended Action

Provide training that covers basic security and privacy concepts, such as phishing, business email compromise, basic operational security, password security, privacy breaches, etc., and foster an internal culture of security and cyber awareness. Provide training for all employees and contractors, at a minimum annually. Require that new employees receive initial cyber security training during onboarding and recurring training at least annually, and when required by system changes or following certain events.

Ensure security and privacy programs collaborate on developing awareness and training policy and procedures.

In addition to basic cyber security training, ensure that personnel who maintain or secure OT as part of their regular duties receive OT-specific cyber security training at least annually.

TTP/Risks

User Training (M1017, ICS M0917)

References

PR.AT-01, PR.AT-02

Offer tailored cyber security training to your employees (ITSAP.10.093) (https://www.cyber.gc.ca/en/guidance/offer-tailored-cyber-security-training-your-employees-itsap10093)

Top 10 IT security actions: #6 provide tailored cyber security training (ITSM.10.093) (https://www.cyber.gc.ca/en/guidance/top-10-it-security-actions-6-provide-tailored-cyber-security-training-itsm10093)

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

Strong and agile encryption: Data in transit [2.9]

Outcome Effective encryption deployed to maintain confidentiality of sensitive data and integrity of network traffic passing through IT, OT, and cloud environments.

Recommended Action

Use a properly configured and up-to-date secure socket layer to protect data in transit, when technically feasible. Identify any use of outdated or weak encryption, update these to sufficiently strong algorithms, and consider managing implications of post-quantum cryptography. Encrypt data in transit with appropriate and approved strength of encryption in accordance with the sensitivity of the data.

To minimize the impact to latency and availability, use encryption where feasible, usually for OT communications connecting with remote/external assets.

TTP/Risks

Adversary-in-the-middle (T1557)

Automated Collection (T1119)

Network Sniffing (T1040, ICS T0842)

Wireless Compromise (ICS T0860)

Wireless Sniffing (ICS T0887)

References

PR.DS-02

Using encryption to keep your sensitive data secure (ITSAP.40.016) (https://www.cyber.gc.ca/en/guidance/using-encryption-keep-your-sensitive-data-secure-itsap40016)

Guidance on becoming cryptographically agile (ITSAP.40.018) (https://www.cyber.gc.ca/en/guidance/guidance-becoming-cryptographically-agile-itsap40018)

Preparing your organization for the quantum threat to cryptography (ITSAP.00.017) (https://www.cyber.gc.ca/en/guidance/preparing-your-organization-quantum-threat-cryptography-itsap00017)

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

Secure sensitive data: Data at rest [2.10]

Outcome Protect sensitive information from unauthorized access.

Recommended Action

Ensure sensitive data, including credentials, is not stored in plain text anywhere in the organization and that it can only be accessed by authenticated and authorized users. Store credentials in a secure manner, such as with a credential/password manager or vault or other privileged account management solution. Encrypt sensitive data at rest with appropriate and approved strength of encryption in accordance with the sensitivity of the data.

TTP/Risks

Unsecured Credentials (T1552)

Steal or Forge Kerberos Tickets (T1558)

Operating System (OS) Credential Dumping (T1003)

Data from Information Repositories (T1213, ICS T0811)

Theft of Operational Information (T0882)

References

PR.DS-01

Password managers-security (ITSAP.30.025) (https://www.cyber.gc.ca/en/guidance/password-managers-security-itsap30025)

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

Email security [2.11]

Outcome Reduce risk from common email-based threats, such as spoofing, phishing, and interception.

Recommended Action

On all corporate email infrastructure:

- enable STARTTLS
- enable Sender Policy Framework and DomainKeys Identified Mail
- ensure Domain-based Message Authentication, Reporting, and Conformance (DMARC) is enabled and set to “reject”

Additionally, set encryption for email to an appropriate and approved level in accordance with the sensitivity of the email contents.

TTP/Risks

Phishing (T1566)

Business Email Compromise

References

PR.DS-01, PR.DS-02, PR.DS-10, PR.AA-03

Implementation guidance: email domain protection (ITSP.40.065) (https://www.cyber.gc.ca/en/guidance/implementation-guidance-email-domain-protection)

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

Disable macros by default [2.12]

Outcome Reduce the risk from embedded macros and similar executive code, a common and highly effective threat actor TTP.

Recommended Action

Establish a system-enforced policy that disables Microsoft Office macros or similar embedded code by default on all devices. If macros must be enabled in specific circumstances, set a policy for authorized users to request that macros are enabled on specific assets.

TTP/Risks

Phishing: Spearphishing Attachment (T1566.001)

User Execution: Malicious File (T1204.002)

References

PR.PS-01, ID.RA-07

How to protect your organization from malicious macros (ITSAP.00.200) (https://www.cyber.gc.ca/en/guidance/how-protect-your-organization-malicious-macros-itsap00200)

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

Hardware and software approval process [2.13]

Outcome Increase visibility into deployed technology assets and reduce the likelihood of breach by users installing unapproved hardware, firmware, or software.

Recommended Action

Implement an administrative policy or automated process that requires approval before new hardware, firmware, or software/software version is installed or deployed. Maintain a risk-informed allow list of approved hardware, firmware, and software that includes specification of approved versions, when technically feasible. For OT assets specifically, align these actions with defined change control and testing activities.

TTP/Risks

Supply Chain Compromise (T1195, ICS T0862)

Hardware Additions (T1200)

Browser Extensions (T1176)

Transient Cyber Asset (ICS T0864)

References

PR.PS-01, ID.RA-07

Application allow list (ITSAP.10.095) (https://www.cyber.gc.ca/en/guidance/application-allow-list-itsap10095)

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

System backups and redundancy [2.14]

Outcome Organizations reduce the likelihood and duration of data loss of service delivery or operations.

Recommended Action

Regularly back up all systems that are necessary for operations. Determine on a case-by-case basis what systems to back up and the exact frequency since every system will have different backup and recovery requirements. Store backups separately from the source systems and test on a recurring basis, no less than once per year. Ensure stored information for OT assets includes at a minimum:

- configurations
- roles
- programmable controller (PLC) logic
- engineering drawings
- tools

Implement adequate redundancies (as determined by the organization) such as network components and data storage. Ensure that the redundant secondary system is not collocated with the primary system and can be activated without loss of information or disruption to operations.

TTP/Risks

Data Destruction (T1485, ICS T0809)

Data Encrypted for Impact (T1486)

Disk Wipe (T1561)

Inhibit System Recovery (T11490)

Denial of Control (ICS T0813)

Denial/Loss of View (ICS T0815, T0829)

Loss of Availability (T0826)

Loss/Manipulation of Control (T0828, T0831)

References

PR.DS-11

Tips for backing up your information (ITSAP.40.002) (https://www.cyber.gc.ca/en/guidance/tips-backing-your-information-itsap40002)

Baseline Cyber security Controls for SMOs (https://www.cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations)

Top measures to enhance cyber security for small and medium organizations (ITSAP.10.035) (https://www.cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035)

Top 10 IT security actions – No. 7 protect information at the enterprise level (ITSM.10.097) (https://www.cyber.gc.ca/en/guidance/top-10-security-actions-no-7-protect-information-enterprise-level-itsm10097)

Security considerations for your website (ITSM.60.005) (https://www.cyber.gc.ca/en/guidance/security-considerations-your-website-itsm60005)

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

Log collection [2.15]

Outcome Achieve better visibility to detect and effectively respond to cyberattacks.

Recommended Action

Collect and store logs for use in both detection and IR activities (for example, forensics), including the following logs:

- Access- and security-focused (for example, intrusion detection systems/ intrusion prevention systems
- firewalls
- data loss prevention
- virtual private networks (VPN)

Notify security teams when a critical log source is disabled, such as Windows Event Logging.

For OT assets where logs are non-standard or not available, collect network traffic and communications between those assets and other assets.

TTP/Risks

Delayed, insufficient, or incomplete ability to detect and respond to potential cyber incidents

Impair Defences (T1562)

References

PR.PS-04

Network security logging and monitoring (ITSAP.80.085) (https://www.cyber.gc.ca/en/guidance/network-security-logging-monitoring-itsap80085)

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

Secure and central log storage [2.16]

Outcome Organizations' security logs are protected from unauthorized access and tampering.

Recommended Action

Ensure logs are stored in a central system, such as a security information and event management (SIEM) tool or central database, and can only be accessed or modified by authorized and authenticated users. Store logs for a duration informed by risk or pertinent regulatory guideline.

TTP/Risks

Indicator Removal on Host: Clear Windows Events Logs (T1070.001)

Indicator Removal on Host: Clear Linux or Mac System Logs (T1070.002)

Indicator Removal on Host: File Detection (T1070.004)

Indicator Removal on Host (ICS T0872)

References

PR.PS-04

Network security logging and monitoring (ITSAP.80.085) (https://www.cyber.gc.ca/en/guidance/network-security-logging-monitoring-itsap80085)

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

Prohibit connection of unauthorized devices [2.17]

Outcome Prevent malicious actors from achieving initial access or data exfiltration via unauthorized portable media devices.

Recommended Action

Maintain policies and processes to ensure that unauthorized media and hardware are not connected to IT and OT assets, such as by limiting use of USB devices and removable media or disabling AutoRun.

Establish procedures to remove, disable, or otherwise secure physical ports in OT environments to prevent the connection of unauthorized devices, or establish procedures for granting access through approved exceptions.

TTP/Risks

Hardware Additions (T1200)

Replication Through Removable Media (T1091, ICS T0847)

References

PR.AA-05, PR.PS-01, PR.DS-01

Defending against data exfiltration threats (ITSM.40.110) (https://www.cyber.gc.ca/en/guidance/defending-against-data-exfiltration-threats-itsm40110)

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

Limit OT connections to public Internet [2.18]

Outcome Reduce the risk of threat actors exploiting or interrupting OT assets connected to the public Internet.

Recommended Action

Ensure no OT assets are on the public Internet, unless explicitly required for operation. Require that exceptions be justified and documented and that excepted assets have additional protections in place to prevent and detect exploitation attempts (for example, logging, MFA, mandatory access via proxy or other intermediary).

TTP/Risks

Active Scanning: Vulnerability Scanning (T1595.002)

Exploit Public-Facing Application (T1190, ICS T0819)

Exploitation of Remote Service (T1210, ICS T0866)

External Remote Services (T1133, ICS T0822)

References

PR.IR-01

Protect your operational technology (ITSAP.00.051) (https://www.cyber.gc.ca/en/guidance/protect-your-operational-technology-itsap00051)

Security considerations for industrial control systems (ITSAP.00.050) (https://www.cyber.gc.ca/en/guidance/security-considerations-industrial-control-systems-itsap00050)

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

Document device configurations [2.19]

Outcome More efficiently and effectively manage, respond to, and recover from cyber attacks against the organization and maintain service continuity.

Recommended Action

Maintain accurate documentation describing the baseline and current configuration details of all critical IT and OT assets to facilitate more effective vulnerability management and response and recovery activities. Perform and track periodic reviews and updates.

TTP/Risks

Delayed, insufficient, or incomplete ability to maintain or restore functionality of critical devices and service operations.

References

PR.PS-01

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

No exploitable services on the Internet [2.20]

Outcome Unauthorized users cannot gain an initial system foothold by exploiting known weaknesses in public-facing assets.

Recommended Action

Ensure assets on the public Internet do not expose any exploitable services, such as remote desktop protocol. Where these services must be exposed, implement appropriate compensating controls to prevent common forms of abuse and exploitation. Disable all unnecessary OS applications and network protocols on Internet-facing assets.

TTP/Risks

Active Scanning: Vulnerability Scanning (T1595.002)

Exploitable Public-Facing Application (T1190, ICS T0819)

Exploitation of Remote Services (T1210, ICS T0866)

External Remote Services (T1113, ICS T0822)

Remote Services: Remote Desktop Protocol (T1021.001)

References

PR.AA-03, PR.AA-05, PR.IR-01

Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089) (https://www.cyber.gc.ca/en/guidance/top-10-it-security-actions-protect-internet-connected-networks-and-information-itsm10089)

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

Secure Administrator Workstation [2.21]

Outcome

Limited-use dedicated Secure Administrator Workstations (SAWs) reduce cyber security risks from malware, phishing, and pass-the-hash attacks. This allows administrators (for example, users with privileged access) to securely connect to the organization's network.

Recommended Action

Organizations provide administrators with SAWs to perform their administrative tasks. Create secure and hardened SAWs by:

- isolating SAWs from the public IT network, and when present, from the data plane
- deactivating capability to install other software
- restricting access to the Internet or email services

For cloud administration from this dedicated workstation, ensure it requires a VPN or allow lists to access the cloud tenancy.

TTP/Risks

Credential Dumping (T1003)

Use Alternate Authentication Method (T1550)

Exploitation for Privilege Escalation (T1068)

(ICS) Exploitation for Privilege Escalation (T0890)

Valid Accounts (T1078)

Remote Services (T1021)

Command and Scripting Interpreter (T1059)

Data from Local System (T1005)

Exploitation for Defense Evasion (T1211)

Account Discovery (T1087)

Network Sniffing (T1040)

References

PR.AA-05, PR.PS-01, PR.PS-02, PR.PS-03, PR.PS-04, PR.PS-05

Top 10 IT security actions: No. 3 managing and controlling administrative privileges (ITSM.10.094) (https://www.cyber.gc.ca/en/guidance/top-10-it-security-actions-no3-managing-controlling-administrative-privileges-itsm10094)

Foundational cyber security actions for small organizations (ITSAP.10.300) (https://www.cyber.gc.ca/en/guidance/foundational-cyber-security-actions-small-organizations-itsap10300)

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

DETECT [3]

Detect relevant threat and TTPs [3.0]

Outcome Organizations are aware of and able to detect relevant threats and TTPs in a timely manner.

Recommended Action

Document a list of threats and cyber threat actor TTPs relevant to the organization (for example, based on industry, sectors, etc.), and ensure the ability to detect instances of those key threats (for example, through rules, alerting, or commercial prevention and detection systems).

TTP/Risks

Without knowledge of relevant threats and the ability to detect them, organizations risk that threat actors may exist undetected in their networks for long periods.

References

ID.RA-02, ID.RA-03, DE.CM-01, DE.CM-03, DE.CM-06

Best practices for setting up a security operations centre (SOC) (ITSAP.00.500) (https://www.cyber.gc.ca/en/guidance/best-practices-setting-security-operations-centre-soc-itsap00500)

Network security logging and monitoring (ITSAP.80.085) (https://www.cyber.gc.ca/en/guidance/network-security-logging-monitoring-itsap80085)

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

RESPOND [4]

Incident reporting [4.0]

Outcome Assist the Cyber Centre and other organizations to understand the broader scope of a cyber attack and be better able to help.

Recommended Action

Maintain codified policy and procedures on to whom and how to report all confirmed cyber security incidents to appropriate external entities.

Report known incidents to the Cyber Centre and other parties within time frames directed by applicable regulatory guidance or, in the absence of guidance, as soon as capable of doing so safely.

TTP/Risks

Without timely incident reporting, the Cyber Centre and other groups are less able to assist affected organizations and lack critical insight into the broader threat landscape (such as whether a broader attack is occurring against a specific sector).

References

RS.CO-02, RS.CO-03, RS.MA-01, RS.MA-02, RS.MA-04

Report a cyber incident (https://www.cyber.gc.ca/en/incident-management)

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

RECOVER [5]

Incident planning and preparedness [5.0]

Outcome Organizations are capable of safely and effectively recovering from a cyber security incident.

Recommended Action

Develop, maintain, and execute plans to recover and restore to service business or mission-critical assets or systems that might be impacted by a cyber security incident.

If a cyber incident does occur, perform a hotwash post-recovery to determine lessons learned and prevent future incidents. Integrate any lessons learned into improvements in governance processes and/or the IR plan.

TTP/Risks

Disruption to availability of an asset, service, or system.

References

RC.RP-01, ID.IM-02, ID.IM-03, ID.IM-04

Developing your incident response plan (ITSAP 40.003) (https://www.cyber.gc.ca/en/guidance/developing-your-incident-response-plan-itsap40003)

Developing your IT recovery plan (ITSAP.40.004) (https://www.cyber.gc.ca/en/guidance/developing-your-it-recovery-plan-itsap40004)

Assessment

- ◯ Not Started Date: _____
- ◯ Scoped Date: _____
- ◯ In Progress Date: _____
- ◯ Implemented Date: _____

Notes

NOTES