Choose a controlling authority.

Communications Security Establishment | Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

Defending against data exfiltration threats

MANAGEMENT

Canada

Foreword

Defending Against Data Exfiltration Threats (ITSM.40.110) is an UNCLASSIFIED publication issued under the authority of the Head of the Canadian Centre for Cyber Security (Cyber Centre). For more information, email or phone our Contact Centre:

Contact Centre

contact@cyber.gc.ca

(613) 949-7048 or 1-833-CYBER-88

Effective Date

This publication takes effect on April 12, 2023.

Revision History

Revision	Amendments	Date
1	First release.	April 12, 2023

D97-4/40-110-2023E-PDF
978-0-660-48080-0

Overview

According to National Institute of Standards and Technology (NIST), exfiltration is the unauthorized transfer of data from a network, system, or device [1]. Data exfiltration is a tactic used by threat actors to accomplish their objectives, such as data theft, financial extortion and gain (e.g. ransomware or cultivating insider threats), and service disruption. Data exfiltration attacks occur in various forms, including data espionage, user or system credentials theft, financial data theft, digital identity compromise, and data de-anonymization. To protect against these attacks, your organizations should secure your data lifecycle processes (e.g. creation, operation, and destruction) from end to end. In this document, we discuss some known data exfiltration techniques and propose protection strategies that can be deployed to mitigate the impact from such threats.

Data exfiltration can be an indication of a network compromise and confirmation of threat actor activity within your network. Detecting a data exfiltration event could be the last line of defense to safeguard your organization's data from full compromise. A data exfiltration event should be treated as a data breach incident and should trigger your organization's incident management process. Depending on the scale and the industry sector, a data exfiltration event with productivity, reputational, or financial consequences may trigger regulatory and legal reporting requirements. Thwarting the ability of adversaries to execute the data exfiltration phase can help contain and disrupt a network compromise attack in progress. This involves a multi-layer data protection strategy which relies on secure data governance practices, technical security controls to harden data systems, strengthening identity and authentication mechanisms, and user awareness training. Phishing, malware, ransomware, and insider threats can lead to a data exfiltration event. For example, a sophisticated threat actor can use spear phishing and malware attacks to infiltrate an organization's network to exfiltrate trade or national secrets. Financially motivated threat actors will use malware tools to steal electronic payment card information from payment processing systems, a technique described as payment card skimming (when threat actors inject custom code into an organization's website to scale-up and extract payment card information).

Table of contents

1 Introduction 5
1.1 Data exfiltration and security frameworks 5
1.1.1 Information technology security risk management process (ITSG-33) 5
1.1.2 MITRE ATT&CK 6
1.1.3 Center for internet security (CIS) controls 6
2 Data exfiltration attacks 7
2.1 Phases of data exfiltration attacks 7
2.2 Exfiltration methods 8
3 Mitigation strategies 10
4 Conclusion 15
5 Supporting content 16
5.1 List of abbreviations 16
5.2 Glossary 16
5.3 References 17

List of figures

Figure 1: Phases of data exfiltration attacks 7

List of annexes

Annex A Exfiltration: CIS control v8 vs ATT&CK techniques mapping 18

1 Introduction

Data is crucial to the operation of any organization. Unaddressed cyber security risks to its confidentiality, integrity and availability can severely impact the business goals. Reported cases of data breach incidents continue to rise as threat actors and cybercriminal groups increasingly take advantage of gaps in many organizations' data security management strategies. Many organizations struggle with identifying and implementing effective technical controls to secure their data lifecycle processes. Business units and users introduce security risks through siloed data creation and management approaches to their organization's data. Threat actors typically target sensitive information, such as:

- corporate proprietary information
- trade secrets
- intellectual property
- customer or employee personal identifiable information (PII)
- sensitive business information
- system configuration settings
- environment variables
- authentication credentials

Threat actors often launch a variety of attacks against organizations, with their main objective often being the unauthorized access to your organization's sensitive data. To safeguard sensitive corporate data against exfiltration threats, your organization should be aware of attack techniques that could impact your data. Your organization should adopt a threat-centric defensive approach that proactively identifies these threats and implements security controls to protect them.

1.1 Data exfiltration and security frameworks

Data exfiltration is a common tactic highlighted in threat actor intrusion frameworks such as the MITRE ATT&CK, CIS controls and the cyber kill chain. In the section below, we review a few security frameworks and discuss how data exfiltration is analyzed.

1.1.1 Information technology security risk management process (ITSG-33)

The Government of Canada (GC) and its departments are required to identify and maintain security controls to protect their business activities from IT-related threats as part of the IT security risk management process. IT Security Risk Management: A Lifecycle Approach (ITSG-33) [2] defines a set of processes and control profiles for GC departments to perform their business activities. Departments are also required to conduct a threat and risk assessment (TRA) for their IT projects. The threat assessment should identify threat actors and commensurate controls required to secure their business processes against data exfiltration threats.

1.1.2 MITRE ATT&CK

The MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework is a knowledge base of threat actor tactics and techniques observed from publicly reported intrusion events. The framework describes exfiltration as an adversarial tactic used to steal data from a target network and often involves threat actors using additional methods to ensure such data transfer activities are not detected. MITRE breaks down the exfiltration tactic into several detailed techniques including exfiltration over command and control (C2) infrastructure, exfiltration through software code repositories and cloud services, and exfiltration through covert channels. For more information on other exfiltration techniques, refer to exfiltration on MITRE's website [3].

1.1.3 Center for Internet Security (CIS) controls

CIS recommends a set of critical security controls that organizations should prioritize to protect their assets against known attacks. CIS published Control Version 8, which highlights 18 priority control actions and 153 safeguards divided into three implementation groups (IGs). Using the CIS Security Controls Navigator [4] and mapping them to ATT&CK exfiltration techniques, 11 priority control actions and 25 safeguards were identified as protections to mitigate data exfiltration attacks. For more information on this mapping, please refer to Appendix A for the full mappings.

2 Data exfiltration attacks

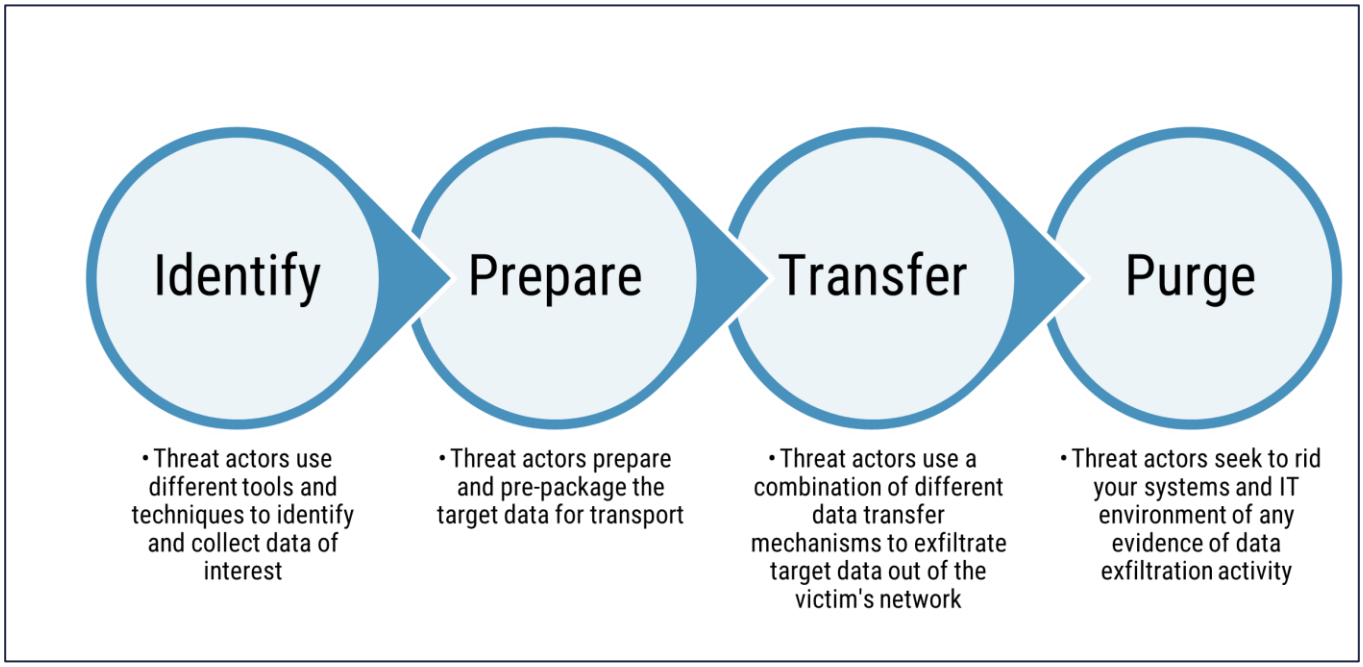
Understanding how threat actors launch data exfiltration attacks and their methods is important to propose the appropriate detection and prevention controls. In this section, we review the phases of data exfiltration attacks and exfiltration methods.

2.1 Phases of data exfiltration attacks

As depicted in Figure 1, threat actors typically execute data exfiltration in the following four general phases:

1. **Identify:** This step involves adversaries identifying and collecting data sets or information of interest. This may involve the adversary moving laterally across the environment and searching through data streams or repositories to identify and collect target data. In some data extortion attacks, this phase is executed after exfiltrated data is transported to an attacker-controlled infrastructure.
2. **Prepare:** This involves a set of activities or mechanisms performed to prepare data identified before exfiltration. This may involve the adversary performing data compression, data encryption, encoding or other pre-packaging techniques to conceal the data before it is transferred out of the environment.
3. **Transfer:** This phase involves an adversary using data transport mechanisms to transmit the target data from within the environment to an attacker-controlled system or network. This may involve the use of common networking protocols, covert tools, or physical media capabilities to complete this step.
4. **Purge:** This phase is optional and depending on the sophistication of the threat actor, may not be completed. Threat actors may take additional steps to remove all indications of their activities. This may occur shortly after the initial breach and may be repeated as necessary, especially when system logging capabilities cannot be disabled. Examples of such activities include deleting original copies, deleting event logs, or triggering a diversion attack to mislead system owners.

Figure 1: Phases of data exfiltration attacks



2.2 Exfiltration methods

Threat actors can use an organization's network infrastructure and system applications to facilitate the illicit transfer of data. Legitimate corporate systems and tools can be used to transfer data into a threat actor-controlled environment. In this section, we discuss some of the techniques used by threat actors to perform these activities.

- **Cryptographic mechanisms:** Encryption and other cryptographic mechanisms can be used to conceal target data and defeat data monitoring and detection controls. Threat actors leverage available cryptographic algorithms in the target environment or deploy custom cryptographic solutions designed to bypass detection controls. Data security monitoring controls relying on string matching may be easily defeated with this technique.
- **Data transformation:** Threat actors can use data transformation methods such as text-pattern substitution, data encoding, data obfuscation, or custom compression methods to reduce their target data size before any additional processing and data exfiltration. Data transformation technologies such as text-to-speech or text-to-image processing tools can be used to evade text-only detection tools. Data compression tools may not offer capabilities to evade detection controls, but they can be used during the data preparation phase to reduce payload sizes before data encryption and transfer.
- **Networking protocols:** Given how relatively easy it is to setup; threat actors often use custom-developed networking protocols to exfiltrate and transfer stolen data. Commonly known networking protocols, as well as unused network protocols, may also be abused to setup covert channels and used to transport stolen data. Threat actors can also use network traffic mirroring and protocol tunneling techniques to forward legitimate network traffic from a compromised network gateway device to a threat-actor controlled-environment. For example, the Domain Name System (DNS) protocol can be exploited to exfiltrate data through DNS queries, a technique called DNS tunneling.
- **Steganography:** This concept involves embedding data within another file format to conceal it from detection. Steganography is used for legitimate purposes such as in digital watermarks. However, threat actors have incorporated this technique to hide stolen data within images or file metadata before exfiltration out of a victim's network environment.
- **Command and control (C2):** Command and control channels can be created to remotely execute commands or retrieve information from within the compromised network. Threat actors can embed data within C2 network communications with an attacker-controlled or publicly accessible infrastructure.
- **Physical drives or peripheral devices:** Threat actors with physical access to the internal network may use physical media or removable drives such as USBs, media drives, portable and mobile devices to move data out of the network. Improper decommissioning processes for devices and media drives may also introduce unintended data exit points if proper device sanitization techniques are not followed. The rise in the use of individual or corporate connected smart devices, internet of things (IoT), and bring your own devices (BYOD) in corporate environments could also increase the exit points threat actors can leverage.
- **Cloud or web storage platforms:** Threat actors may exploit the growing use of cloud storage and application services for business operations to hide and blend with existing business traffic patterns. A threat actor may funnel

its data transfer through an organization's approved cloud or web service provider. Often, organizations may already have legitimate traffic flowing to such platforms, thus making it difficult to detect malicious data transfers.

- **Misconfigurations and vulnerabilities:** Misconfigured on-premise or off-premise application services may expose an organization's data and allow threat actors to gain access. Zero-day or unpatched known system vulnerabilities may allow threat actors to exploit the information system and bypass protections to hide and exfiltrate data from the network.
- **Backdoors:** Threat actors may compromise the device or service before or during procurement processes to install backdoors within systems. These backdoors can then be used to gain and maintain unauthorized access to the network and transfer data out of the network.
- **Phishing or social engineering:** A successful phishing email or social engineering attack can lead to your users volunteering confidential data or being part a threat actor's exfiltration infrastructure.
- **Third-party customer services:** Threat actors can take advantage of trust relationships that may exist between third-party or customer networks to your infrastructure to exfiltrate data. Threat actors may funnel stolen data through a trusted third party's network.
- **Wireless and Wi-Fi services:** Insecurely designed or implemented guest and corporate wireless services could provide eavesdropping opportunities for threat actors to collect and exfiltrate data. Actors with physical access to an organization's facilities may be able to implant wireless surveillance devices to collect and exfiltrate data.
- **Covert channels:** Threat actors can use covert channels for low bandwidth data theft by exploiting emanations from sounds, vibrations, or electromagnetic signals. These techniques can be very difficult to detect. Covert timing channels and TEMPEST[1] attacks are some techniques used by sophisticated nation-state actors.

[1] A TEMPEST attack is a method of remotely capturing unintended electro-magnetic signals from devices to obtain information about the data or system being observed.

3 Mitigation strategies

Data exfiltration protection strategies require multiple layers of aligned security controls to provide defence-in-depth protection and a resilient solution. The security controls you deploy should complement other layers of existing safeguards to limit damage. Mitigation controls should be selected by balancing your business risks against your business goals and service delivery requirements. Note that protection controls will not prevent all data exfiltration cases; however, securely architecting your systems and processes to frustrate exfiltration attempts against your organization's sensitive data is desirable.

Your organization's architecture plays a significant role in your overall security strategy. Legacy corporate networks were setup with the traditional assumption that traffic flows originating from internal systems are secure and that external flows inbound are not. However, the shift towards the hybrid (on-premise and cloud) architecture model challenges these assumptions. Threat actors' ability to exfiltrate data with little or no restrictions from your network may be aided by your enterprise architecture and the choice of system tools implemented within your corporate environment. Below are some recommended practices:

- **Establish a governance model for data in your organization.** Data management is a shared responsibility and, organizations can unintentionally introduce additional security risks by encouraging siloed data management practices. A central governance model will guide activities for creating and managing data across your organization. Elements of that model will include data policies and procedures guiding how data is created, stored, transmitted, and destroyed. Encourage the use of data security champions to promote accountability. Ensure data security is prioritized during development and deployment of projects. Consider the following topics: data collection, data ownership, handling different forms of data (structured or unstructured), access management, data classification, compliance, and regulatory requirements.
- **Architect your organization's network and IT assets to be resilient**. Design your enterprise network architecture to be inherently resilient against data leakage attacks. Design security controls for your systems and processes from an assumed breach standpoint. The assumed breach principle is based on the notion that your corporate systems and assets may already be compromised. Design systems and controls based on zero-trust architecture (ZTA) principles and eliminate the notion of implied trust in your systems. Architect services and systems with capabilities to provide continuous monitoring, continuous authentication, and re-validation of rights and privileges. Implement security controls using principles that re-validate and verify trust relationships. Implement additional levels of controls around sensitive and higher value systems and data. For more information on ZTA, see Zero Trust Security Model (ITSAP.10.008) [5].
- **Conduct a threat assessment.** Evaluate the threats and risks faced by your organization's data in relation to your business environment. Determine your organization's most sensitive assets and identify attack surface exposures. Conduct regular threat and risk assessments (TRA) of your environment to identify your network gaps and exposures that could be exploited to exfiltrate data from your network. Using threat modeling techniques, map out potential threats to your organization's data. Threat modeling should identify threats from data flows, use of weak technology, and third-party relationships. Utilize up-to-date threat intelligence to identify and defend against potential threat actors likely to target your organization. Use threat assessment as a guide for deliberate selection

and implementation of security controls. Use results from your risk assessment to prioritize controls around devices or systems of higher risk. Periodically test the effectiveness of controls implemented and identify gaps that need to be addressed. For more information on threat assessments, see the Harmonized Threat and Risk Assessment (HTRA) Methodology [6].

- **Establish and maintain a data classification scheme for the organization.** The classification scheme should apply to both structured and unstructured data. The classification scheme should be backed up by policy and guardrails on how your users may access or use data. Implement a coherent data strategy that tracks and maps the location of your organization's data. Data sensitivity should be a consideration when defining minimum set of controls. For example, security and storage of user or system credentials or authenticators may require additional controls.
- **Design and implement a data leakage protection (DLP) program.** The DLP program should address technical, process and user behavioral risks to your data. As part of the overall program, deploy technical controls to safeguard your data across all egress and ingress point. Apply the DLP solution to safeguard your sensitive applications and their associated data flows. Before selecting a DLP solution, it is advisable to conduct extensive testing to ensure it fits your needs and future architecture projections. Conduct a user education and awareness campaign to train your users ahead of full deployment. Periodically assess the reliability of your DLP solution by reviewing its effectiveness and performance.
- **Implement endpoint data security solutions.** Often, a data leakage incident occurs via the endpoint device. Technical controls such as antimalware, antivirus solutions, endpoint firewalls, and endpoint detection and response (EDR/XDR) solutions can be considered to detect and block data exfiltration attempts. The Cyber Centre recommends enabling events monitoring on endpoint devices to log activity events.
- **Harden systems and deploy network security protections.** Threat actors will target exposed systems and use that access to propagate within your network. Prevent network intrusions from taking hold in your environment. Implement network segmentation to limit the impact of threat actor activity on your network. Deploy network intrusion protections such as signature or behaviour-based solutions and implement safeguards against code injection or web service exploitation attacks. Deploy malware prevention, secure email gateway, and web application firewalls (WAFs) solutions. Isolate and clean infected systems as quickly as possible. Restrict network communications to and from sensitive data network environments. Identify and block access to malicious websites. Secure your data backups. Disable use of insecure protocols. Remove default system passwords and disable unnecessary accounts, applications, and services.
- **Inspect network communications to identify suspicious encrypted traffic.** Threat actors are using the widespread support for Hypertext Transfer Protocol Secure (HTTPS) and Transport Layer Security (TLS) services to evade detection controls on the network. We recommend implementing an enterprise network traffic inspection solution to inspect and monitor encrypted tunnels between internal and external hosts. Inspecting encrypted traffic will improve the effectiveness of your DLP solution. Use artificial intelligence to identify suspicious traffic or protocols within your environment. Monitor for DNS tunneling, unauthorized use of VPN software, or similar techniques that can be abused to create a covert channel for outbound traffic.
- **Protect all remote access connections.** Many organizations rely on remote technologies to enable remote employees and to deliver and access services. These services also exacerbate the threat environment, potentially

increasing your attack surface. Secure all remote connections including third-party and employee remote working connections. Ensure all remote connections are authenticated via at least two-factor authentication credentials. Apply DLP controls to also secure remote access connections.

- **Deploy access control mechanisms to manage access to sensitive data.** Use data access control lists (ACLs) to limit and manage access to your organization's sensitive data. Use the least privilege principle to assign user rights to your data. Users should only have the minimum rights to perform required tasks. Excessive rights will make user accounts an attractive target for threat actors. Separate administrative functions and protect administrative interfaces. Limit the use of administrative accounts to only administrative tasks and restricted only to the approved use window. Do not use administrative accounts for day-to-day activities. Implement role-based access control (RBAC). Where possible, implement multi-factor authentication (MFA) for all user or administrative accounts and services.
- **Restrict the use of system tools and websites that could facilitate data exfiltration.** Use domain filtering controls to restrict access to web applications, tools, and websites that could be used to exfiltrate data from your network. Limit or block the installation and use of software applications and external storage applications that could facilitate unauthorized data transfer. Access to video conference or online meeting applications, messaging platforms, web and internal email, secure messaging platforms, and social media platforms should be restricted.
- **Use cryptographic protections to enforce data confidentiality controls.** Use encryption as a layer of defense to mitigate unauthorized and inadvertent disclosure of your data. However, weigh the impact of data encryption to your legitimate business processes. Ensure safe proper encryption key management measures are implemented. Consider implementing encryption throughout your data value chain - at rest, in processing, and in transit. For data transport to cloud environments, consider client-side encryption to ensure your data is protected. Use transport TLS protocols for securing network communications and use only up-to-date and approved cryptographic libraries.
- **Protect sensitive data using secure data enclaves.** Setup secure data enclaves by standing up dedicated environments to provide controlled access and secure storage to your sensitive data. These environments will house sensitive confidential data and access to them should be restricted to specific operations. All interactions in such environments are logged and audited. Implement strict controls on how data enters and leaves the enclave environment. Data enclaves should be setup as a closed environment with no access to the internet. Ensure data backups, replication activities and other system management operations within this environment are secured.
- **Ensure monitoring controls captures various data types.** Advances in digital data transformation technologies through artificial intelligence, advanced image and video processing, natural language processing (NLP), and other similar technologies presents new capabilities. By leveraging these technologies, threat actors can transform data types such as text into video, audio, images, or other digital media types. Expand your monitoring controls to identify different forms of data streams and implement capabilities to detect and prevent data exfiltration attempts from your systems. Test and validate those controls to ensure they remain effective if your sensitive data format changes.
- **Implement audit logging and network monitoring measures.** Actively monitor data flows across your network by implementing activity logging and suspicious data flow detection mechanisms. Consider measures to detect suspicious data flows and unexpected bumps in data across egress points. Also, consider time-based and

geographical monitoring to detect and thwart potential data exfiltration attempts. Techniques such as triggering, re-authentication, data masking, and behavioral monitoring are some examples. Implement controls to monitor the occurrence of new services and new protocols on your network. Periodically review network protocols in your environment and ensure suspicious services are investigated. Implement a logging architecture designed to be resilient against threat actor attacks. Ensure logs on critical systems are collected in real-time and stored off-device to a highly secured location. Leverage security information and event management (SIEM) solutions to correlate activities with events and improve your detection capabilities.

- **Implement proper data destruction measures.** Media with data storage capabilities should be wiped using certified data deletion techniques or physically destroyed. Use secure data destruction practices such as cryptographic rewrites using approved cipher suites and protocols, media sanitization, and physical destruction of devices. This will help avoid inadvertent data exfiltration or data theft through decommissioned devices. Ensure devices no longer fit for operation are securely decommissioned and disposed.
- **Develop data exfiltration incident management runbooks**. Data exfiltration incident response runbooks will help provide a vetted and actionable set of instructions on how to manage a data exfiltration incident. Develop processes, procedures, and technical action plans on how to investigate, contain, and recover from a data exfiltration event. Vetted response procedures will ensure containment actions do not inadvertently impact on investigations while also providing a path to safely removing the actors from your system.
- **Leverage automation to accelerate incident response processes.** Implement automation to aid detection and response actions to network intrusion or threat actor activity within your environment. Deploy network intrusion prevention tools. The speed of your incident response activities can help thwart the progression of attacks on your network. Hence, use security orchestration, automation, and response (SOAR) tools to provide automation support to security teams. Leverage anomaly-based detection systems and machine learning techniques to analyze and identify suspicious deviations in communications on your network.
- **Deploy cloud security controls to secure data in the cloud.** Do not blindly trust cloud service traffic traversing your network. Assume your cloud provider or instance can be compromised. Implement controls to validate data inbound and outbound to your cloud infrastructure. Use cloud access security broker (CASB) tools to enforce your data security policies in the cloud. Use CASB to restrict cloud applications interacting with your data and inspect data flows to ensure compliance with security policies. You should also ensure your data is encrypted when at rest in the cloud.
- **Patch systems and ensure basic security hygiene is implemented**. Update and patch your systems and applications to reduce the chances of exploitation of known vulnerabilities. Consider a centralized patch management deployment model to automate and expedite deployment of patches. Ensure device firmware are protected against unauthorized changes. Consider implementing a testing regime for validating software updates before they are applied. Use secure versions of common Internet protocols such as Domain Name System Security Extensions (DNSSEC).
- **Restrict and monitor the use of administrative tools within your environment.** Restrict the deployment and use of administrative tools to approved use-cases only. Exceptions to this rule should be monitored and investigated. When these tools are used, do not leave copies unattended on target devices. Separate administrative systems and

applications from user environment and implement execution restrictions to limit how these tools can be executed within your environment.

- **Educate your users and leverage threat intelligence**. Restrict malicious emails as an attack vector through education and the use of technology. Educate your users on recent threats associated with phishing emails. Implement advanced anti-phishing solutions to scan incoming emails including deploying DomainKeys Identified Mail (DKIM) or Domain-based Message Authentication, Reporting & Conformance (DMARC) solutions. Implement controls to monitor email channels for attempts of data exfiltration. Additionally, leverage threat intelligence indicators to hunt for known malicious activity that may be occurring on your network. For more information on DKIM and DMARC, see Implementation Guidance: Email Domain Protection (ITSP.40.065) [7].

4 Conclusion

Safeguarding your organization's sensitive data should be at the core of your security strategy. Although it may be difficult to protect all data against exfiltration or leakage, proactively assessing your environment and implementing active security controls will reduce business impact should an incident occur. You should consider a holistic approach that improves the visibility around your data flows, enhances your cyber security hygiene for data assets, and implements monitoring and logging of activities on your network. These are key measures you can take to reduce impacts to your organization and improve your overall cyber security posture.

5 Supporting content

5.1 List of abbreviations

Term	Definition
CASB	Cloud Access Security Broker
CSE	Communications Security Establishment
DKIM	DomainKeys Identified Mail
DMARC	Domain-based Message Authentication, Reporting & Conformance
DNSSEC	Domain Name System Security Extensions
GC	Government of Canada
HTTPS	Hypertext Transfer Protocol Secure
IT	Information Technology
ITS	Information Technology Security
MFA	Multi-factor Authentication
RBAC	Role-Based Access Control
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation, and Response
TLS	Transport Layer Security

5.2 Glossary

Term	Definition
Backdoor	An undocumented, private, or less-detectable way of gaining remote access to a computer, bypassing authentication measures, and obtaining access to plaintext.
Covert timing channels	A system feature that enables one system entity to signal information to another by modulating its own use of a system resource in such a way as to affect system response time observed by the second entity. (Source: NIST)
Defence-in-depth	An IT security concept (also known as the castle approach) in which multiple layers of security are used to protect the integrity of information. These layers can include anti-virus and anti-spyware software, firewalls, hierarchical passwords, intrusion detection, and biometric identification.
Multi-factor authentication	A tactic that can add an additional layer of security to your devices and account. Multi-factor authentication requires additional verification (like a PIN or fingerprint) to access your devices or accounts. Two-factor authentication is a type of multi-factor authentication.
Role-based access control	A model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities.

Term	Definition
TEMPEST	The name for specifications and standards for limiting the strength of electromagnetic emanations from electrical and electronic equipment which lead to reduced vulnerability to eavesdropping. This term originated in the U.S. Department of Defense.
Zero-day	A zero-day vulnerability is a software vulnerability that is not yet known by the vendor, and therefore has not been mitigated. A zero-day exploit is an attack directed at a zero-day vulnerability.

5.3 References

Number	Reference
1	National Institute of Standards and Technology. *SP.800-53 Security and Privacy Controls for Information Systems and Organizations*. September 2020.
2	Canadian Centre for Cyber Security. *IT Security Risk Management: A Lifecycle Approach (ITSG-33)*. November 2012.
3	Att&ck.MITRE.org. *Exfiltration*. July 2019.
4	Centre for Internet Security. *Critical Security Controls Navigator*.
5	Canadian Centre for Cyber Security. *Zero Trust Security Model (ITSAP.10.008)*. November 2022.
6	Canadian Centre for Cyber Security. *Harmonized Threat and Risk Assessment (HTRA) Methodology*. October 2007.
7	Canadian Centre for Cyber Security. *Implementation Guidance: Email Domain Protection (ITSP.40.065)*. August 2021.

Annex A Exfiltration: CIS control v8 vs ATT&CK techniques mapping

S/N	CIS controls v8	CIS safeguards	Asset type	Title	Description
1	**CIS Control 2** - Inventory and Control of Software Assets	2.3	Applications	Address Unauthorized Software	Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.
2	**CIS Control 2** - Inventory and Control of Software Assets	2.5	Applications	Allowlist Authorized Software	Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.
3	**CIS Control 3** - Data Protection	3.3	Data	Configure Data Access Control Lists	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.
4	**CIS Control 3** - Data Protection	3.1	Data	Encrypt Sensitive Data in Transit	Encrypt sensitive data in transit. Example implementations can include Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).
5	**CIS Control 4** - Secure Configuration of Enterprise Assets and Software	4.1	Applications	Establish and Maintain a Secure Configuration Process	Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile; non-computing/IoT devices; and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
6	**CIS Control 4** - Secure Configuration of Enterprise Assets and Software	4.2	Network	Establish and Maintain a Secure Configuration Process for Network Infrastructure	Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
7	**CIS Control 4** - Secure Configuration of Enterprise Assets and Software	4.4	Devices	Implement and Manage a Firewall on Servers	Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.
8	**CIS Control 4** - Secure Configuration of Enterprise Assets and Software	4.6	Network	Securely Manage Enterprise Assets and Software	Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.
9	**CIS Control 4** - Secure Configuration of Enterprise Assets and Software	4.7	Users	Manage Default Accounts on Enterprise Assets and Software	Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include disabling default accounts or making them unusable.
10	**CIS Control 4** - Secure Configuration of Enterprise Assets and Software	4.8	Devices	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.
11	**CIS Control 5** - Account Management	5.3	Users	Disable Dormant Accounts	Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.
12	**CIS Control 6** - Access Control Management	6.1	Users	Establish an Access Granting Process	Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.
13	**CIS Control 6** - Access Control Management	6.2	Users	Establish an Access Revoking Process	Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.
14	**CIS Control 6** - Access Control Management	6.8	Data	Define and Maintain Role-Based Access Control	Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to

S/N	CIS controls v8	CIS safeguards	Asset type	Title	Description
					successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.
15	**CIS Control 7** - Continuous Vulnerability Management	7.6	Applications	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets	Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.
16	**CIS Control 7** - Continuous Vulnerability Management	7.7	Applications	Remediate Detected Vulnerabilities	Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
17	**CIS Control 9** - Email and Web Browser Protections	9.2	Network	Use DNS Filtering Services	Use DNS filtering services on all enterprise assets to block access to known malicious domains.
18	**CIS Control 10** - Malware Defenses	10.3	Devices	Disable Autorun and Autoplay for Removable Media	Disable autorun and autoplay auto-execute functionality for removable media.
19	**CIS Control 12** - Network Infrastructure Management	12.2	Network	Establish and Maintain a Secure Network Architecture	Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.
20	**CIS Control 12** - Network Infrastructure Management	12.8	Devices	Establish and Maintain Dedicated Computing Resources For all Administrative Work	Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed Internet access.
21	**CIS Control 13** - Network Monitoring and Defense	13.3	Network	Deploy a Network Intrusion Detection Solution	Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service.
22	**CIS Control 13** - Network Monitoring and Defense	13.4	Network	Perform Traffic Filtering Between Network Segments	Perform traffic filtering between network segments, where appropriate.
23	**CIS Control 13** - Network Monitoring and Defense	13.8	Network	Deploy a Network Intrusion Prevention Solution	Deploy a network intrusion prevention solution, where appropriate. Example implementations include the use of a Network Intrusion Prevention System (NIPS) or equivalent CSP service.
24	**CIS Control 18** - Penetration Testing	18.3	Network	Remediate Penetration Test Findings	Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.
25	**CIS Control 18** - Penetration Testing	18.5	N/A	Perform Periodic Internal Penetration Tests	Perform periodic internal penetration tests based on program requirements, no less than annually. The testing may be clear box or opaque box.