Network Security Monitoring and Detection Standard for Canadian Telecommunications Service Providers (CTSPs)

V1.1 January 20, 2020

Authored by: Canadian Telecommunications Cyber Protection (CTCP) working group for
Presentation by: Canadian Security Telecommunications Advisory Committee (CSTAC)

Contents

Revision History 3
1. Network Security Monitoring and Detection Standards 4
1.1 Monitoring Network Infrastructure 4
1.2 Types of Traffic to Monitor 5
1.2.1 Malware Controls 5
1.2.3 Message Abuse Controls 5

Revision History

The following table highlights edit changes to the document.

Editor	Date	Notes
CTCP Architecture committee	June 1, 2019	Content created
Kevin Miller, SaskTel	Sept 12, 2019	Draft started
Marc Kneppers, TELUS	Jan 20, 2020	Minor update based on stakeholder feedback

The following table highlights major content or policy changes to the document.

Section	Contribution	Date

1. Network Security Monitoring and Detection Standards

1.1 Monitoring Network Infrastructure

Canadian Telecommunications Service Providers (CTSPs) should have the capability to:

1. Monitor critical assets from both external and internal threats.
2. Define the criteria for the classification of systems based on their criticality to service delivery or business operations (e.g. network elements, DHCP, DNS, provisioning systems, OSS, CRM, etc.) and on their exposure (e.g. Internet, Customers, Internal), and define the logging, monitoring and audit requirements for each category (syslog/snmp, netflow, monitoring level, audit frequency, etc.).
3. Operate a security information and event management system that collects and correlates information from a variety of systems and devices, which is actively monitored by the CTSP.
4. Monitor all network connections (including cloud, co-located or remote connections).
5. Monitor flows within their networks to detect anomalies relevant to cybersecurity. This would include, among other things, volumetric monitoring of traffic, as well as network protocols, anomalies and whitelisted/blacklisted IPs..
6. Subscribe, receive and process threat indicators from public, private, and third party sources in a timely manner.
7. Define their response plans for traffic identified as suspicious by their monitoring activities. Automated response techniques should be leveraged where possible to lessen the time to mitigation.
8. Define the monitoring and audit requirements for all network planes (Management, Control and Data planes), considering their exposure to the Internet and customers. Please see BGP, SS7 and DNS sections in CSTAC Security Best Practices Policy for further details on monitoring these protocols.
9. Regularly audit systems for compliance to corporate security policies and applicable standards (including cloud, co-located or remote systems).
10. Offload logs (cloud, co-located or remote systems) to a secure location (secure data in transit).

11. Define the security requirement for log collection and storage based on their sensitivity (e.g. retention period, encryption/authentication/authorization requirements).
12. Protect and discard cached customer traffic or collected traffic descriptors (e.g. netflow). (e.g secure data in transit, at rest, while processed).

1.2 Types of Traffic to Monitor

1.2.1 Malware Controls

CTSPs should have the capability to:

1. Identify the source of malicious traffic when originating on their network, when possible.
2. Respond to reports (that can be reasonably validated) of malicious activity on their networks.
3. Monitor for different types of malicious traffic (e.g. open resolvers, SMTP relay).
4. Detect malware by signature and volume characteristics.

1.2.2 Network Service Abuse Controls

CTSPs should have the capability to:

1. Monitor traffic flows from internal customers to the provider's critical infrastructure-related network services. These network services may include OSPF, BGP, DNS, DHCP, NTP, etc.
2. Where required and/or feasible, monitor customers for basic network vulnerabilities, such as open resolvers and insecure config that exposes services that could be actively exploited.
3. Refer detected anomalies to Incident Response procedures to address the issue.

1.2.3 Message Abuse Controls

CTSPs should have the capability to:

1. Monitor for misuse, including specific monitoring of outbound message volumes and high numbers of intended message recipients, if they are providing email services.
2. Ensure that customers that exceed message volume and high-number thresholds are identified and follow-up action is taken.

3. Ensure that third party service agreements for outsourced message services include controls and processes for monitoring and responding to message abuse.
4. Monitor for high volumes of spam-related traffic coming from individual customer IP addresses in order to notify those customers of a potential infection or take other actions to stop such traffic.