

Intrusion Detection System

1.0 Purpose

The purpose of this policy is to ensure the detection, reporting, and effective response to any security incidents or events that threaten the confidentiality, integrity, and availability of Cyber Tree Systems (CTS) information assets, information systems, and the networks that deliver the information. This policy aims to provide guidance for the deployment of Intrusion Detection Systems (IDS) and the necessary procedures for incident response and to specify the monitoring of VPN traffic for unusual activity and the formal integration between Firewalls and IDS.

2.0 Scope

This policy applies to all CTS employees, all information systems, and all network resources managed by the Information Security (InfoSec) team. This document outlines procedures for detecting, reporting, and responding to intrusions and other security-related incidents, ensuring appropriate actions are taken in a timely manner.

3.0 Policy

3.1 Guidelines

There must be a minimum of two network-based Intrusion Detection Systems always running on CTS's network. Both should be located at the perimeter of the network, at the firewall bordering the DMZ.

The IDS should be configured to monitor VPN traffic for unusual activity, ensuring that any abnormal behavior within encrypted tunnels is detected and flagged for further investigation.

The IDS should be fully integrated with the firewall, providing automated responses and correlation of events. The firewall and IDS should communicate regularly to exchange data regarding blocked traffic, intrusion attempts, and other security events. This integration ensures a rapid response to potential threats.

IDS signatures must be updated every 2 weeks from the vendor to keep the IDS(s) at the current signature level. Any suspected intrusions, suspicious activity, or unexplained erratic system behavior discovered by administrators, users, or computer security personnel must be reported to the organizational IT computer security office within 1 hour, and the Incident Response Plan should be initiated.

All intrusions with financial or customer data loss must be reported to CEO, CFO, CIO within 7 days of the loss.

Refer to the CTS Incident Response Policy Manual for further details regarding events.

3.2 Detection and Reporting

Any detected security incidents must be reported by the SOC personnel or Threat Intelligence Unit. The SOC is responsible for event detection and ensuring the escalation procedures are followed to minimize the time to respond to security threats. Event notification and escalation should be explicitly defined as a responsibility of these teams, not general employees.

3.3 IDS Coverage

IDS systems will be implemented to monitor all critical network segments, servers, endpoints, and other assets deemed crucial to CTS's operations. The IDS should be configured to detect common attack signatures, anomalous behavior, and any signs of compromise.

3.4 Incident Reporting and Categorization

3.4.1 Reporting

When an intrusion or security incident is detected by SOC personnel or Threat Intelligence Unit, they are responsible for reporting the incident to the InfoSec team immediately. This report should include the type of incident, severity level, and any immediate action taken.

3.4.2 Automated Response Handling

Once an event is confirmed, automated response handling through a SIEM system will be used to trigger containment and remediation procedures, eliminating the need for opening a ticket through the help desk.

3.4.3 Incident Categorization

Security-related incidents will be immediately reported to the InfoSec team. Incident categories should be clearly defined and prioritized, ensuring that the most urgent events receive immediate action by the SOC team. The categorization should include a clear distinction between incidents, such as denial-of-service attacks, which require urgent responses due to their potential for significant disruption.

3.5 Ownership

Responsibility for maintenance, including signature updates, firmware updates, and system testing, as well as any future iterations of IDS implementations, will fall to the InfoSec team with ultimate approval from the CISO and InfoSec manager.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	Definition
Intrusion Detection System (IDS)	Used to detect several types of malicious behaviors that can compromise the security and trust of a computer system.

VPN Traffic Monitoring	Monitoring VPN connections for unusual or malicious activity to ensure that encrypted communications are not being exploited by attackers.
------------------------	--

6.0 Revision History

Revision Number	Date	Editor	Reason
2.0	1/16/2025	Aidan Schmeckpeper	Separated into library and prepared for future edits.
2.1	2/19/2025	Aidan Schmeckpeper	Better conform to new organizational chart and firewall/VPN policy