Threat Detection and Prevention

`2021.1`

In order to preserve the integrity of data that MiCT stores, processes, or transmits for Customers, MiCT implements strong intrusion detection tools and policies to proactively track and retroactively investigate unauthorized access. This include threat detection and prevention at both the network and host level, as well as threat intelligence monitoring.

Policy Statements

MiCT policy requires that:

(a) All critical systems, assets and environments must implement realtime threat detection or prevention.

Controls and Procedures

System Malware Protection

1. All end-user workstations and production systems must have antivirus running. The default anti-malware solution used is Carbon Black PSC. The anti-malware solution will include protection against malicious mobile code.
    - Next generation endpoint protection agent may be used as an equivalent solution.
    - Hosts are scanned continuously for malicious binaries in critical system paths. Additionally, if supported, the agent is set to to scan system every 2 hours and at reboot to assure no malware is present.
    - The malware signature database is kept up to date, changes are pushed continuously.
    - Logs of virus scans and alerts are maintained according to the requirements outlined in System Auditing.
2. Detected malware is evaluated and removed following the established incident response process.
3. All systems are to only be used for MiCT business needs.

Firewall Protection

Firewall protection is implemented at the following layers

- **Network** - including Network ACL and Security Groups in AWS as well as on- premise firewalls between the office networks and the Internet.
- **Host** - local firewalls are enabled on the user endpoints as well as servers (compute and database instances in AWS are protected by security groups)

- **Application -** web application firewall (WAF) and content distribution are configured at the application layer to protect against common web application attacks such as cross site scripting, injection and denial-of-service attacks.

Network Intrusion Detection

Intrusion Detection for On-Premise Internal Networks

- MiCT leverages AWS GuardDuty and Cisco Meraki for network security of its on-premise environments.
- AWS GuardDuty and Cisco Meraki features stateful firewall inspection and intrusion detection/prevention (IDS/IPS) of applicable incoming and outgoing network traffic. Attacks and suspicious network activities are blocked automatically.
- MiCT IT manager is responsible for configuring the firewall and IDS/IPS rules and review the configuration as least quarterly.

Intrusion Detection in AWS Cloud Environments MiCT implemented a real-time threat detection solution by monitoring AWS Cloudtrail events and/or VPC flow logs.

- Cloudtrail events are monitored by **AWS GuardDuty and Cisco Meraki**
- VPC flow logs are sent to and analyzed by **AWS GuardDuty and Cisco Meraki**.

Additional monitoring is provided by our infrastructure service provider AWS.

Host Intrusion Detection

Host based intrusion detection is supported via one of the following:

- On Windows and macOS systems: **AWS Inspector and Carbon Black PSC** agents for malware detection and behavior-based endpoint threat detection.

- On Linux servers: **AWS Inspector and Carbon Black PSC** agents for activity monitoring, vulnerability scanning, and threat detection. This includes all virtual instances running in the cloud environment.

Web Application Protection

leverages AWS Services to protect web applications against common attacks such as SQL injection, cross-site scripting, and denial-of-service (DoS/DDoS) attacks. The services used include AWS Shield, WAF, Cloudfront, and/or API Gateway.

Centralized Security Information and Event Management

Security events and alerts are aggregated to and correlated by one or both of the following solutions:

- JupiterOne
- Internally developed security automation tooling

Threat Intelligence Monitoring

NH-ISAC

MiCT is an active member of the National Health Information Sharing and Analysis Center (NH-ISAC).

MiCT Security team is subscribed to receive threat alerts from NH-ISAC.

Intelligence Feeds

Additional intelligence feeds are received automatically through some of the 3rd party security solutions that have been implemented on the networks and/or endpoints. The data gathered through these external intel feeds is automatically used by the security solutions to analyze events and generate alerts.

Regulatory Requirements Updates

The Security and Privacy Officer actively monitors the regulatory compliance landscape for updates to regulations such as HIPAA, PCI and GDPR.