YourIT!
Your Logo Goes Here

NIST CSF Assessment

NIST CSF Detect Worksheet

Prepared for:
Your Client's Company
Prepared by:
YourIT Company

NIST CSF Detect Worksheet

Anomalies and Events (DE.AE)

1.1 - Baseline

List all tools used to establish a baseline of network operations and expected data flows for users and systems. Enter one per line.

Visio

1.2 - Event Analysis

Are detected events analyzed to understand attack targets and methods? Please provide any additional notes or support documentation.

No

1.3 - Event Correlation

Are event data collected and correlated from multiple sources and sensors. Please provide any additional notes or support documentation.

No

1.4 - Event Impact

Is the impact of events determined? Please provide any additional notes or support documentation.

No

1.5 - Incident Alert Thresholds

Are incident alert thresholds are established? Please provide any additional notes or support documentation.

No

Security Continuous Monitoring (DE.CM)

2.1 - Network Monitoring

List all tools used to monitor the network and detect potential cybersecurity events. Enter one per line. Leave blank if no tools are used.

Cyber Hawk

2.2 - Physical Environment

Describe how the physical environment is monitored to detect potential cybersecurity events (i.e., cameras, badge entry systems, etc.). Attach photo evidence. Leave blank if no monitoring is performed.

CCTV implemented and monitored throughout the organization's physical office location.

2.3 - Personnel Activity

Describe how personnel activity is monitored to detect potential cybersecurity events? Leave blank if no monitoring is performed.

Network user access logs are reviewed on a weekly basis to identify network access anomalies. When such anomalies are identified, the internal security team investigates the anomaly and identifies the anomaly's root cause. Then corrective action is taken.

2.4 - Unauthorized Mobile Code

Describe how unauthorized mobile code is monitored to detect potential cybersecurity events? Leave blank if no monitoring is performed.

Mobile device usage to access network resources is not authorized or enabled.

2.5 - External Service Provider Activity

Describe how external service provider activity is monitored to detect potential cybersecurity events? Leave blank if no monitoring is performed.

External service providers are contractually required to report all cyber security events to the organization.

2.6 - Unauthorized Personnel, Connections, Devices, and Software

Describe how your organization monitors for unauthorized personnel, connections, devices, and software? Leave blank if no monitoring is performed.

Network user access logs are reviewed on a weekly basis to identify network access anomalies. When such anomalies are identified, the internal security team investigates the anomaly and identifies the anomaly's root cause. Then corrective action is taken.

Detection Processes (DE.DP)

3.1 - Roles and Responsibilities

Are roles and responsibilities for detection well defined to ensure accountability? Attach supporting documentation describing the roles and responsibilities for detection.

No

3.2 - Detection Activity Requirements

Do detection activities comply with all applicable requirements?

No

3.3 - Detection Process Testing

Are part of this assessment process, you should perform a test of the detection process. Describe below how the process was tested and findings.

Cyber Hawk alerts are reviewed for accuracy and consistency on a monthly basis.

3.4 - Communication of Event Detection Information

Is event detection information communicated?

No

3.5 - Continuous Improvement

Are detection processes continuously improved?

No