CID SOC Review
District Name

Report date: Date
Meeting date: Date

Section: Assets review

Status: Follow up

License usage

- Crowdstrike area(s) reviewed
  - Exposure management > Assets > Managed assets
  - Exposure management > Assets > Unmanaged assets
  - Support and resources > General settings > CID details
- Original request:
- Last seen
  - Last day:
  - Last 30 days:
  - Last 45 days:
- Device type
  - Servers:
  - Workstations:
  - Domain controllers:
- Additional Crowdstrike modules? No

MiSecure feedback

-
- Are there more planned Crowdstrike Agent sensor installations? Yes
- Are there any physical servers w/out the sensor? Yes
  - e.g. HVAC, Security camera

Sensor review

- Crowdstrike area(s) reviewed
  - Dashboards and reports > Reports > Sensor report
  - Host setup and management > Manage endpoints > Sensor health
  - Exposure management > Assets > Managed assets

    - Exposure management > Assets > Unmanaged assets
    - Support and resources > General settings | Channel file update controls
- Sensors
    - Sensor release: 7.16.18613
    - Latest release: 7.17.18721
    - Sensor update policy: N-1 ✅
    - At correct release? Yes
    - Agents in Reduced Functionality Mode (RFM): 0
    - Agents in End of Service (EOS): 0
    - Inactive sensors: 0
    - Duplicate sensors: 0
- Rapid response content: General Availability ✅
- Sensor operations channel files: General Availability ✅

MiSecure feedback

-

Policy review

- Crowdstrike area(s) reviewed
    - Endpoint Security > Configure > (all)
- Prevention policies
    - Windows
        -
    - Linux
        -
    - Mac
        -
- Exclusions
    - Machine Learning Exclusions:
    - Indicator of Attack (IOA) Exclusions:
    - Sensor Visibility Exclusions:
    - Custom IOA Rule Groups:
    - IOC management: 1 Allow
        - PurpleKnight.exe
            - Allowed by juan.vielma@crowdstrike.com on 9/10/24 at 11:51 AM EST
            - sha256: e23f159511b7293f0719a78c1318b2d0418ee7dbca2bd7823d0525b8069ed1bc
            - Added by CrowdStrike to all MiSecure CIDs

MiSecure feedback

-

- IOC exclusion inserted statewide to address false-positive alerts. Can be removed, recommended to leave it as-is.

Internet exposure

- Crowdstrike area(s) reviewed
  - Exposure management > Assets > Managed assets
- XX machines
  -

MiSecure feedback

-

Section: Vulnerabilities

Status: Clear

Vulnerabilities

- Crowdstrike area(s) reviewed
  - Exposure management > Vulnerability management > Vulnerabilities
- Assets in ExPRT (critical) / CVSS (critical) / Exploited (critical) :
  -
- Assets in ExPRT (critical) / CVSS (critical) / Exploited (high) :
  -

MiSecure feedback:

-

Section: Participation

Status: Follow up

-

MiSecure feedback:

-

Section: Applications

Status: Follow up

Applications

- Crowdstrike area(s) reviewed
    - Exposure Management > Applications > Applications > Applications
    - Exposure Management > Applications > Applications > Browser Extensions
    - Exposure Management > Applications > Applications > All > Category: Remote Management and Monitoring
- Application review
    -
- Browser extensions review
    -

MiSecure feedback

-

Section: Detections / Incidents

Status: Attention

New Detections/Incidents

- Crowdstrike area(s) reviewed
    - Endpoint Security > Endpoint Detections
    - Endpoint Security > CrowdScore Incidents
    - Next-Gen SIEM > Advanced event search
    - Falcon Complete > Message center
- Detections: 0
- Overwatch generated alert, sent to Complete team: 0

MiSecure feedback:

-

Quarantined files

- Crowdstrike area(s) reviewed
    - Endpoint security > Quarantined files
- Quarantined files: 0
    -

MiSecure feedback:

-

Review

- Previous detections or incidents to review: none

Section: Communications / Alerts

Status: Follow up

Communications

- Crowdstrike area(s) reviewed
  - Falcon Complete > Falcon Complete > Contact Management
  - Next-Gen SIEM > Fusion SOAR > Workflows
  - Support and resources > Support > Support portal
- CSCommunications: ✅
  -
- MiSecure contacts: ✅
  -
- Crowdstrike alerts: ✅
  -
- Notification review:
  - Last test of contact notifications: Date
- Crowdstrike Support: ✅
  - Access the Support portal to sign up for alerts

MiSecure feedback

-
- Confirm all users added **+1-737-212-9729** to their phones for caller ID and whitelisted in DND

Section: Accounts

Status: Follow up

Failed Logins

- Crowdstrike area(s) reviewed
  - Dashboards and Reports > Dashboards > All Dashboards > Assets - Login Activity > Most failed logins by username
  - Exposure management > Accounts > Failed logins
- Failed logins
  -

Most logins by username

- Crowdstrike area(s) reviewed
  - Dashboards and Reports > Dashboards > All Dashboards > Assets - Login Activity > Most failed logins by username
  - Exposure management > Accounts > Dashboards
- Most successful logins
  -

- Most failed logins
    -

File

Successful domain admin logins

- Crowdstrike area(s) reviewed
    - Exposure management> Accounts > Successful logins
-

Busiest Machine

- Crowdstrike area(s) reviewed
    - Exposure management> Accounts > Dashboard
-

Falcon Users

- Crowdstrike area(s) reviewed:
    - Host Setup and Management > Falcon Users > User Management
-

MiSecure feedback:

-

Section: Other recommendations

Status: Attention

- Set up firewall alerts if possible
    - Remote management software
    - DCSync
    - Unexpected outgoing data surge
- Set up firewall rule (disabled) to:
    - Allow sensor communication
    - Block all traffic
- VPN alerts (failed logins and/or successful logins)
- Set up MFA on VPN/RDP
- Audit authorized remote user accounts
    - Disable any not currently needed

MiSecure feedback:

-

MiSecure Notes
•