MiSecure CrowdStrike Onboarding Process

Crowdstrike provides in-depth visibility into your technology infrastructure and operations. Because it is focused on improving your overall cybersecurity, the tool provides visibility into nearly every aspect of your operations - it can be overwhelming upon first glance. We encourage you to use this document to help you get acquainted with the tool.

Initial account setup

When the initial CID is set up for a district, an account for the primary contact will be created and they will receive an email from CrowdStrike for initial access. A response to this email needs to happen **within 48 hours**. Be prepared to...

a. Set a strong password
b. Set up MFA
c. Fill out schedule B with contact names, emails and numbers

☐	Completed

Watch onboarding video

This 40 minute video will help you to get started with the Crowdstrike interface:

CrowdStrike Kickoff Call.mp4

☐	Completed

Add users

- Gather all email addresses of users that will be accessing CrowdStrike (in addition to those listed on the Schedule B). Note that domains need to be school domains and not email providers (e.g. gmail.com)
- Create a Support ticket to have their domains added to the CID for any additional email domains. MiSecure Wiki Adding email domain to CID

Add users

- Once the Support ticket is complete, create accounts for users based on least privilege access. There are extensive roles within CrowdStrike, so it may take some research to determine what roles they require.
    - https://falcon.us-2.crowdstrike.com/users-v2/roles-and-permissions and https://falcon.us-2.crowdstrike.com/documentation/page/f20650df/default-roles-reference
    - We suggest that districts group their users into those that need to manage and take actions and those users that just need read-only/view access.
    - Crowdstrike offers many options for user roles. Roles can be changed at any time.
    - Remember to maintain least-privileged permissions
- Review the contacts using the menu: “Falcon complete” > “Contact management”

☐	Completed

Sensor deployment

Crowdstrike uses a single sensor for each server. Sensors will be upgraded automatically and are unique for each operating system. They can be accessed through the Crowdstrike dashboard. Go to Host setup and management > Deploy > Sensor downloads
Items you may want to consider prior to Sensor deployment:

- Host Groups (or Fine Grained Access) or purchasing a child CID to contain users to only those servers they need access to, if that is something you want to do.
    - Further reading below with more details.
- Many districts will tag devices with the district domain. You can use multiple tags (e.g. “sunnyvaleschools.org”, “powerschool”)
- CrowdStrike Sensor installation instructions
    - MiSecure Wiki - https://wiki.michit.org/public/misecure/agent-deployment-and-tagging
    - CrowdStrike Documentation on Sensor deployment - https://falcon.us-2.crowdstrike.com/documentation/category/ea9b123c/sensor-deployment-and-maintenance

☐	Completed

Stay informed

- Test your alerts: https://wiki.michit.org/public/misecure/testing-crowdstrike-notifications
- Set your CrowdStrike Tech Alerts: https://wiki.michit.org/public/misecure/setting-crowdstrike-tech-alert-notification-settings

☐	Completed

Begin using the tool

Watch the Vulnerability Management video

- CrowdStrike Enablement Asset_Vulnerability Management.mp4

☐	Completed

Next steps

- MiSecure Wiki - https://wiki.michit.org/en/public/misecure
- Support - CrowdStrike Support Portal
- Community - CrowdStrike Reddit
- Training - CrowdStrike University
    - Access to CrowdStrike University requires a CSU license for access and use.
- Recorded Webinars on Support Portal - Webinars
- Watch for emails from `cscommunication@michit.org`
    - Users will be periodically added to this email list after they are added as a user in Crowdstrike

☐	Completed

Additional Information

Fine Grained Access or Child CIDs

FGA (Fine Grained Access) is currently only applicable for segregating LEA's into only being able to view their own data when it applies to Host Groups, Host Management, and Real Time Response (RTR). This means that LEA's will still be able to view vulnerabilities, graphs, reports, etc. that contain information from across the entire CID. This level of access is subject to change as CrowdStrike refines FGA, but as it stands currently, FGA is limited.

For ISDs that would prefer to completely separate each LEA within CrowdStrike, the best solution for this is to purchase a child/sub CID of the ISD for the individual LEA. The same policies and configuration for the ISD/RESA CID will be set up within the LEA child CID by the Crowdstrike provisioning team.

Sensor Protection Policies

CrowdStrike's recommendation is those with MDR to avoid changing the policies applied to host groups. If a policy needs to be adjusted for whatever reason, you need to contact your Falcon Complete team first. If you make adjustments to a policy without their knowing, your breach prevention warranty provided by the Complete team will be void.

If you have EDR or XDR it is recommended that you contact the MiSecure team for assistance. Information will be available on the MichIT wiki regarding recommended policy settings.

Alerts

Should there be an incident in your CID that requires the intervention of the Falcon Complete team, they will only call from the following number: **+1-737-212-9729**

It is important that you & your team add that contact information to your phones, as we have gotten a few reports that cell providers are incorrectly marking that number as spam. It is also recommended that you allow that number to bypass any Do Not Disturb settings on your phone.

EDR Licensing

ISD/LEA's purchasing EDR licensing will be receiving a CID with their EDR licensing. We recommend that CID is placed under the ISD's CID, so that detection data flows upwards to the ISD CID then to the MiSecure CID.

User Roles

For the least privileged roles, there are a few read/view-only roles, where the user can not modify any settings. Those would be the

- Falcon Console Guest
- Falcon Analyst - Read Only
- Event Viewer.

For users that need control and action abilities with the CID, CrowdStrike provisioning has been setting up initial users with the following roles

- Dashboard Admin
- Endpoint Manager
- Exposure Assets Admin
- Falcon Security Lead
- Quarantine Manager
- Vulnerability Manager

These roles above work well without having to grant the all-powerful Falcon Administrator role.

CrowdStrike does allow you to create additional roles and their recommendation is to clone an existing role and add or remove the necessary permissions to fit your needs.

Real Time Responder Roles

Lastly, for specific roles to be cautious about assigning, the Real Time Responder roles have the ability to access the client directly via the Real Time Responder console built within the Falcon UI. The Real Time Responder console is only accessible to the roles below and should only be granted as necessary and with training to prevent issues on servers and workstations. It is recommended that you remove this role when it is no longer needed.

- Real Time Responder - Active Responder
- Real Time Responder - Administrator
- Real Time Responder - Read Only Analyst

Reduced Functionality Mode (RFM)

Reduced Functionality Mode occurs when the Windows/macOS/Linux workstation/server is updated to the most current updates from the vendor, before CrowdStrike has had a chance to verify and approve those updates for systems with the CrowdStrike Sensor installed. Commonly, you will see this happen with machines that update immediately on Microsoft's Patch Tuesday, the host details will show the machine in RFM. CrowdStrike generally approves all Microsoft updates within 48 hours, and macOS and Linux within 10 days.

You don't have to take any actions to fix or correct machines in RFM. As the most recent updates for all 3 OS's are approved by CrowdStrike, you will see the machines come out of RFM.