MCNC Managed Endpoint Protection Service
CrowdStrike End User Role Updates (2023)

Brief Summary of Changes

1) **New permissions added to Exposure Management (formerly Discover and Spotlight).** Examples include: the ability to create and modify application groups, assign asset criticality, and update the status on unmanaged and unsupported assets.
2) **New permissions added to Host Management.** Examples include: the ability to manually remove/hide hosts from the console as well as network contain assets.
3) **Additional permissions added to User Management.** Additional ability related to viewing and updating users in your environment.
4) A few changes have been added to remove some permissions tied to endpoint management that could compromise service if changed, such as updating host groups.

Detailed Summary of Changes

1) **Application Groups** - Admins can now create application groups in Exposure Management to categorize applications. These groups can be used as a data source for scheduled reports. *Example: An application group is created for all applications required on a managed asset, and admins could be alerted via an emailed report whenever a managed asset is missing one or more of those applications. Alternatively, an application group can be set up for applications that should never be installed on a managed asset, and admins could be alerted whenever a 'blocklisted' application is installed.*
2) **Asset Criticality** - Admins can now assign criticality to managed assets (Critical/High/Non-Critical) which they can use to monitor and report on the most important systems in your environment. *Example: Domain Controllers and other mission-critical servers can be marked as 'Critical', and a daily scheduled report could be generated for all new vulnerabilities on Critical assets, while vulnerabilities on Non-Critical assets could be sent out weekly instead.*
3) **Passive Discovery Management** - Previously all devices with the CrowdStrike agent were doing Passive Discovery by default. This could lead to noise in the Exposure Management - Assets tool, as devices that frequently go off site will generate entries in the Unmanaged and Unsupported assets list whenever they connect to a new wireless network. Admins can now configure Passive Discovery rules to allow or restrict specific groups and/or network prefixes from doing Passive Discovery. *Example:*

Some users constantly take their laptops off-network to work, so a group is created for these devices and this group is restricted from doing Passive Discovery. (Note that only MCNC has permissions to create or edit asset groups, so admins should open a SecOps ticket with the requested group changes before they update the Passive Discovery configuration)

4) **Asset Triage** - Admins can now review Unmanaged and Unsupported assets and update their status to indicate the investigation results. Assets can be reassigned as Unmanaged or Unsupported, recommend sensor installation, or simply mark as reviewed. Admins can use this status to follow up as needed. *Example: A review of the unmanaged assets screen found 5 devices that should have CrowdStrike installed (mark as 'Recommend sensor install'), 2 printers that can't actually run the CrowdStrike sensor (mark as 'Move to unsupported'), and 9 assets that don't belong to the organization (mark as 'reviewed only').*
5) Host removal - Admins will now have the ability to manually remove/hide hosts from the console rather than submitting a request to MCNC or waiting for 45 days of inactivity. **Important note:** While removing hosts from host management does not impact the protection of the sensor, it could delay or prevent MCNC from responding effectively to detections because detections for assets in the trash are suppressed. Please make sure to only remove/hide hosts from Host Management if you are sure they are no longer active.
6) **Network Containment** - Admins will now have the ability to Network Contain (and Uncontain) assets in Host Management. Network containment isolates individual hosts from all network activity, other than that to and from CrowdStrike's servers. This can be useful if an asset is believed to be compromised, as it would prevent lateral movement of the threat to other devices on your network as well as potential C&C or data loss to an external malicious server. **Important note:** Network containing a host (particularly a Domain Controller or other mission-critical server) has the potential to cause issues throughout your network and should only be done with an understanding of the potential risks involved. Please contact MCNC SecOps if you have any questions or concerns.
7) **Installation Tokens** - Admin can now update Installation token settings, including requiring a token for installation. This can be helpful if your CID has been exposed, either accidentally or by necessity, as requiring an Installation Token (which can be

rotated or disabled at will or on a set schedule) will prevent unauthorized users from being able to add devices to your CrowdStrike console even if they have your CID and an agent installer, which is usually all they would need.

8) **Removed Access** - *Host Groups* - Admins can no longer create, change, or delete host groups. *Sensor Update Policies* - Admins can no longer create, change, or delete Sensor Update Policies. *Direct CrowdStrike Support* - Admins can no longer directly message the CrowdStrike Overwatch team in the console

For support regarding these changes, please contact secops@mcnc.org.