Asset Criticality

The Asset Criticality feature in Crowdstrike allows users to track the relative importance of the assets in their environment. This guide describes the value of assigning criticality, various processes for assigning asset criticality, and how users can use that information to enrich Crowdstrike data.

Why Asset Criticality?

Unfortunately there will never be enough hours in the day to address every threat and vulnerability. This makes prioritization important, as users should be spending their time addressing the most serious threats on the most critical systems. This is where Asset Criticality comes in, allowing users to use knowledge about their own managed systems to determine which ones should be prioritized.

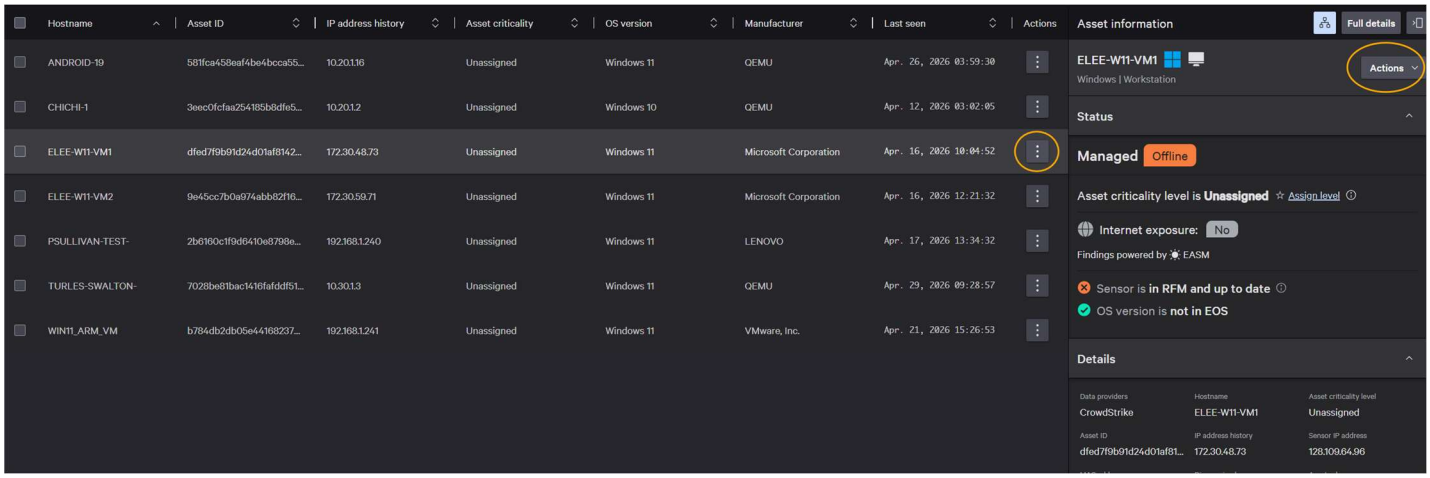
For instance, a Remote Code Execution vulnerability on two identical servers may be much more of a threat on a server storing Protected Health Information or one exposed directly to the Internet. Asset Criticality allows users to account for these types of details so they can quickly assess risk when time is of the essence.

There are four different criticality statuses that can be applied:
Unassigned: All assets are unassigned until they're assigned a criticality level
Noncritical: Most typical assets are noncritical (eg staff workstations)
High: Important assets such as servers or domain controllers
Critical: The most important assets such as internet-exposed assets or a central server

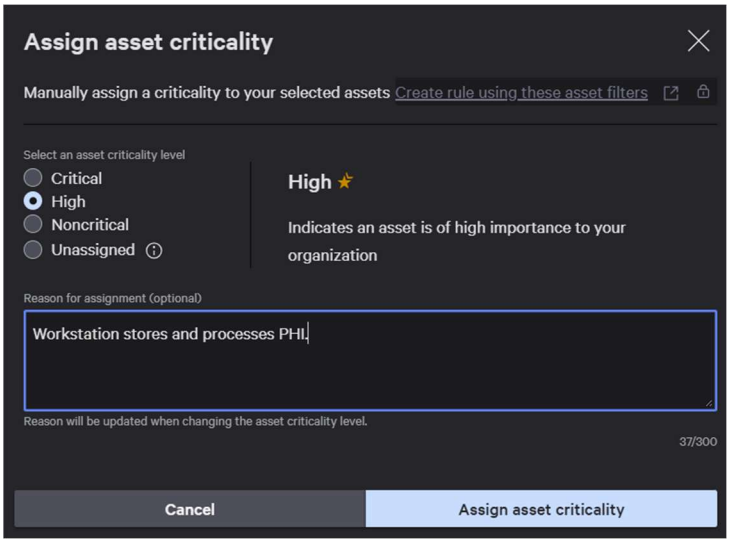
Assigning Asset Criticality Manually

Asset Criticality can be assigned manually or via defined rules. To manually assign, first go to Exposure Management>Managed Assets *(note criticality can also be manually assigned to unmanaged and unsupported assets, which may be useful when reviewing assets before they are added to Crowdstrike. This guide will focus on assigning criticality to managed assets, but the process is essentially the same).*

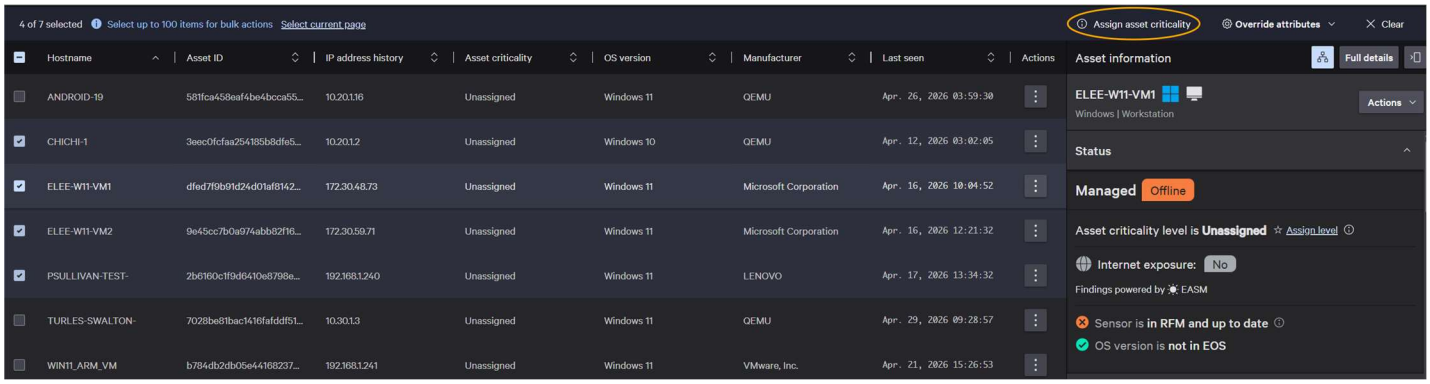
To categorize a single asset, locate the asset in the list and select the action menu by clicking the three dots in the 'Action column'. You can also click the asset to select and find the 'Actions' menu in the details view on the right side



This will open a window where users can set the criticality level and add an optional note to track the reason for assignment.



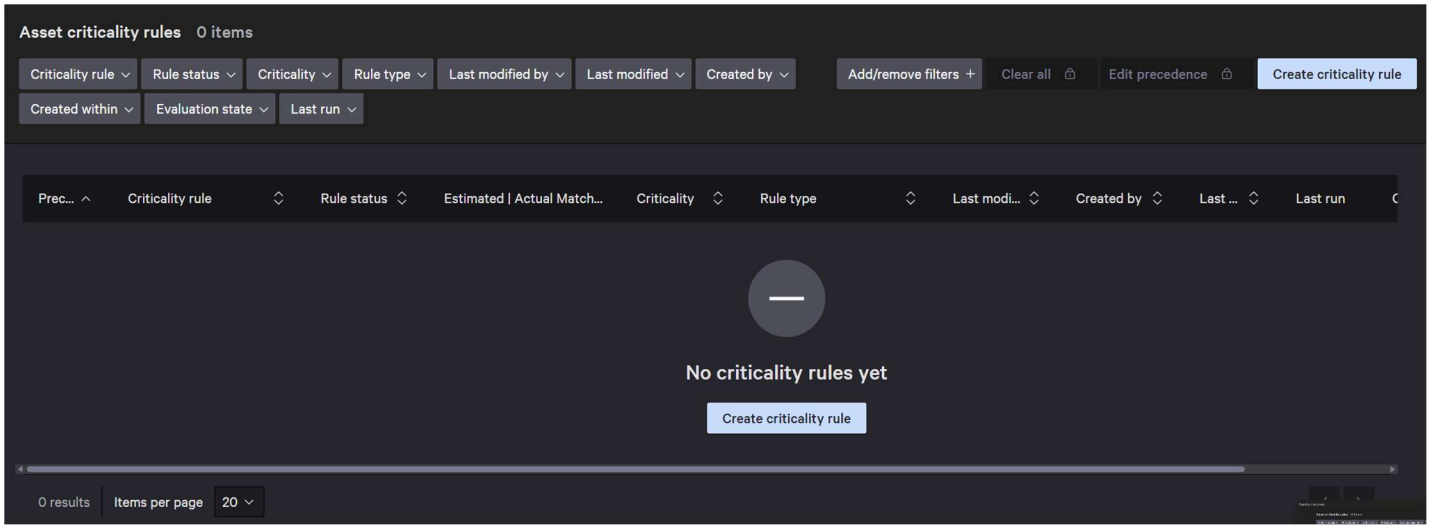
Up to 100 assets at once can be categorized by clicking the check box on the left and selecting ‘Assign asset criticality’.



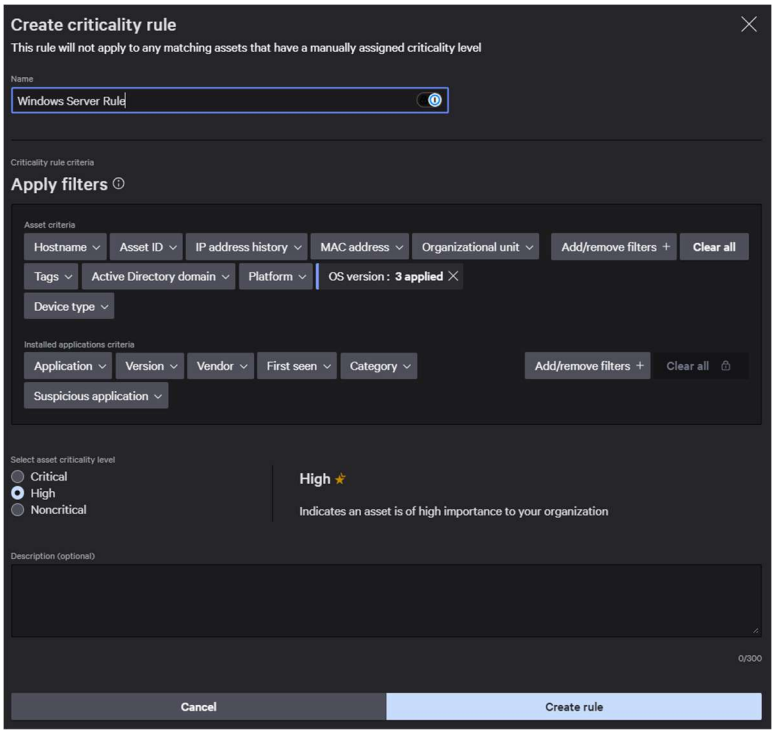
Asset Criticality Rules

For larger scale deployments Crowdstrike can automatically set Asset Criticality based on user-created rules. These rules are configured based on factors including hardware, OS versions, Organizational Unit, or assets with specific applications installed.

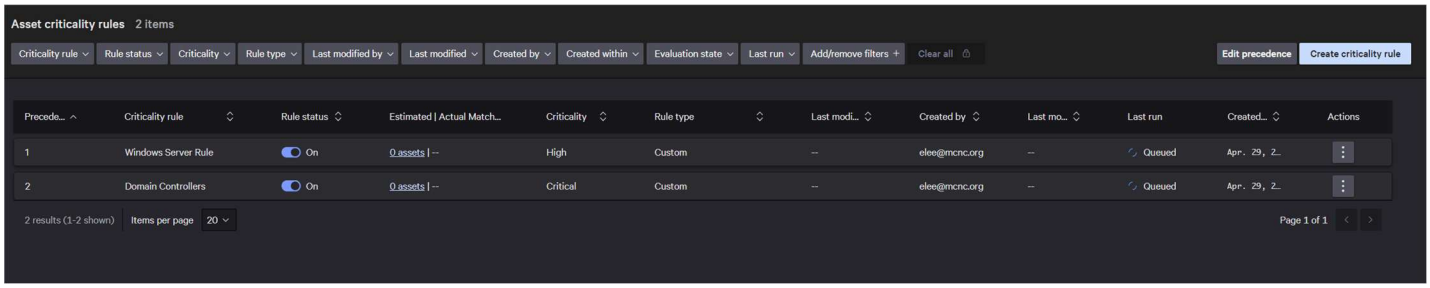
Go to Exposure Management>Setup>Asset Criticality Rules. Start by creating a new rule.



Name the rule and start applying filters to narrow the scope until it fits your needs. In this example assets running Windows Server OS will be set to ‘High’. This rule will only categorize assets that have not been manually assigned, preventing rules from overwriting any review work that has already been completed.



Once rules have been created they can be edited, disabled, or moved up or down in precedece. Since assets can only have one criticality level assigned, assets that fit more than one criticality rule will be assigned criticality based on the highest precedence rule that applies.



Using Asset Criticality

Once Asset Criticality has been set on your assets this information can be used to enrich data in other areas of Crowdstrike including Exposure Management, Dashboards, and Reports. One recommended use for this information is within Vulnerability Management. Using the 'Asset Criticality' filter along with other VM filters allow users to quickly highlight issues on the most important assets in their environment. Here's an example of using VM filters to show critical alerts on assets marked as critical: