New and Changed Information

New and changed information in release 5.5.x

This table summarizes the feature updates and enhancements available in Cyber Vision release 5.5.x.

Table 1: Feature updates

Feature	Description
Intrusion detection alert type	Intrusion detection alert type monitors network traffic using the Snort intrusion detection system. It raises an alert when suspicious or malicious network activity is detected on monitored assets, based on Snort rules. For more information, see Alerts.
Inactive asset alert type	Inactive asset alert type detects assets that stop communicating due to failure or misconfiguration. You can define custom rules for the inactivity period to reduce manual monitoring. For more information, see Alerts.
Assets with unexpected external communications alert type	Assets with unexpected external communications alert type monitors asset communications. It raises an alert if an asset communicates to external IP addresses or domains. For more information, see Alerts.

Feature	Description
Custom properties	Cyber Vision supports custom properties at both the network and asset levels. You can view, add, and edit these properties, with strict validation rules enforced to maintain data integrity. This enhancement enables the addition of custom metadata to assets, facilitating more efficient emergency response and maintenance operations. For more information, see Add custom properties to an asset.
Bulk vulnerability acknowledgment for assets	Acknowledge or unacknowledge multiple vulnerabilities at once from the asset vulnerability table. This change removes manual processing, saving time for asset security. For more information, see Vulnerabilities.
Enhancement of sensor health monitoring	Monitor sensor health proactively with automated updates and deep insights. The sensor management system tracks each sensor's status and provides actionable updates, helping you resolve issues before they affect your operations. Use Advanced View to analyze performance trends and troubleshoot efficiently. For more information, see Sensor management frameworks.
Enhanced system connectivity and security settings	The system offers intuitive user interface based settings to simplify administrative workflow. Date and time settings allow for precise time synchronization for the center and connected sensors. DNS management streamlines system access. Proxy configurations ensure secure, controlled connectivity in isolated environments. For more information, see System settings.
Network based auto grouping	The network based auto grouping feature streamlines device management. It automatically organizes devices based on established network definitions. Groups are created and named according to your network names. You can use this feature for easier ISE API integration and device classification. For more information, see Create network groups.

Feature	Description
Asset vulnerability insights in the New UI	Cyber Vision Center matches asset properties against the knowledge database to detect vulnerabilities. You can view the matched asset properties in the New UI. This process provides clear, actionable insights into your security posture. For more information, see Vulnerability detection in Cyber Vision Center.
External IP country mapping	This feature maps the countries of external IP addresses your device connects with. It identifies geographical locations and helps prioritize which communications to investigate to improve network insight and security. For more information, see Communication maps.
ASN and ASN organization insights for external communications	This feature shows ASN (Autonomous System Number) and ASN Organization information for external communications. It helps identify traffic sources and network owners. Enables quick detection of suspicious communications and reduces investigation time. For more information, see Communication maps.

New and changed information in release 5.5.x