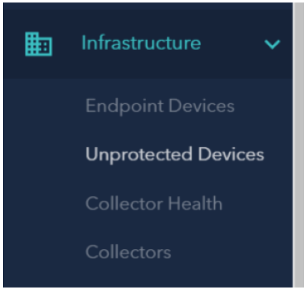
Barracuda XDR Release Notes — February 2024

https://campus.barracuda.com/doc/110560373/

Easily identify unprotected devices using the Unprotected Devices page

The new **Unprotected Devices** page displays the devices in your environment that aren't under the protection of the Barracuda XDR agent.

You can find this page in the XDR Dashboard by clicking **Infrastructure** > **Unprotected Devices**.



For a device to appear on the **Unprotected Devices** page, it must be:

- Not protected by the Barracuda XDR agent
- Compatible with the Barracuda XDR agent
- On a subnet that has at least two devices protected by the Barracuda XDR agent

Also on this page, you can export a .CSV file of information on the unprotected devices, including their **Hostname**, **Local IP**, **External IP**, **OS Type**, **OS Version**, **MAC Address**, and time they were last seen, so you can easily protect them.

For more information, see Working with the Unprotected Devices page.

Find your account more easily

Companies and MSPs who have multiple accounts can now find them more easily in the **Account** dropdown.

In the **Account** dropdown at the top right corner of each page, instead of being limited to scrolling through the list to find your account name, you can also start typing the name. The list is filtered in real-time.

Removal of unhelpful alerts

ConnectWise/Autotask/ServiceNow tickets only alert the Partner if relevant activities occur in XDR.

This enhancement cuts down on ticket fatigue and clutter by no longer generating Partner updates unless new information is actually added to the ticket (Such as a new comment from the SOC team, ticket status update, etc.)

This lets Partners focus on tickets that truly matter instead of wasting time clearing out tickets for things such as internally facing changes and updates.

New automated detection rules

The following rules have been added:

Google Workspaces Unencrypted File Shared Externally This detection rule flags potential security incidents involving sensitive data being moved outside the organization without proper encryption. It triggers an alert when a user downloads more than 20 unencrypted files within a 15-minute window, suggesting the possibility of data exfiltration by either an internal or external threat actor. Such activity is a strong indicator of a data breach and aligns with the MITRE ATT&CK framework under the tactic of Exfiltration (TA0010). Upon detection, SOAR automatically performs further analysis, including enrichment and threat intelligence checks, to assess the severity of the incident. This includes verifying whether VPNs were utilized for the downloads and identifying the IP addresses involved in the activity. This comprehensive approach helps in the swifti dentification and mitigation of potential data exfiltration threats.

Fortigate Brute Force Authentication User Attempt This detection rule signals a potential brute force attack, identifying when a single IP address unsuccessfully attempts to log into the same user account 50 times across various destinations within a half-hour period. Triggered alarms initiate an automatic SOAR response, conducting IP threat intelligence investigations to dissect the attack’s anonymity measures, including the use of proxies, TOR exit nodes, and VPNs. This activity is further analyzed for context and origin through ASN information and comprehensive threat intelligence lookups. Aligned with the MITRE ATT&CK™ framework’s Initial Access (TA0001) category.

Barracuda IDS: Abnormal Rule High Count This detection rule Is a fully automated ML rule designed to monitor and identify unusually high traffic volumes against specific rule signatures within an organization’s network. This rule specifically targets signatures that are classified as Major or Critical, with a severity level of 1, indicating they are of significant importance and potential impact. The underlying hypothesis of this rule is that spikes in the activity levels of these high-criticality signatures could signal a potential threat or malicious activity within the network. By focusing on these critical indicators, the rule aims to detect and flag activities that could compromise network security or integrity. This approach aligns with the MITRE ATT&CK™ framework under Credential Access (TA0006), suggesting that such abnormal traffic patterns could be indicative of attempts to gain unauthorized access to credentials or sensitive information, thus posing a direct threat to the organization's cybersecurity posture.

Barracuda IDS: High Destination Bytes This ML rule is a fully automated designed to monitor and identify anomalously large volumes of data being transferred to a destination IP address from any source within an organization. This rule calculates the total sum of destination bytes transferred and compares it across the entire population of source IPs within the organization to pinpoint unusual spikes or high transfer volumes. Such detection is crucial because it could indicate data exfiltration activities, where sensitive or critical information is being illicitly transferred outside the organization. This rule's effectiveness in identifying potential data leaks or unauthorized data transfer aligns with the MITRE ATT&CK™ framework's Exfiltration category (TA0010), aiming to safeguard against threats that attempt to extract data, thereby mitigating the risk of data breaches and securing the organization's digital assets.

Okta: Push Deny And Security Threat This automated ML detection for Okta factor authentication failures and identifies threats such as password spraying and invalid credential use. This rule is specifically tailored to monitor and flag events where an authentication attempt has been explicitly denied (e.g., through a push denial in a multi-factor authentication setup) or where patterns indicative of malicious activities, such as widespread attempts to gain access using multiple passwords (password spraying) or attempts with known invalid credentials, are detected. By focusing on these authentication-related anomalies and threats, the rule aids in preventing unauthorized access to credentials and sensitive information, aligning with the MITRE ATT&CK™ framework's Credential Access category (TA0006).

Microsoft 365: Conditional Access Policy Block from New Location This ML rule is designed to automatically detect and alert when a user's login attempt is blocked due to a conditional access policy triggered by an attempt from a new country. This detection is critical as it suggests that while an attacker may possess valid user credentials, the access attempt is being thwarted by pre-set policies aimed at preventing unauthorized access from unfamiliar locations. The implication of such detections is significant because it points to the possibility of compromised credentials being used in an attempt to gain unauthorized access to the organization's data or systems. The MITRE ATT&CK™ category is Initial Access (TA0001).

Figures