Barracuda XDR Release Notes — September 2022

https://campus.barracuda.com/doc/98211448/

Customer Features

This release of Barracuda XDR includes the following new or improved Customer features:

New Integrations

Our Open XDR model has added monitoring for the following:

- Barracuda CloudGen Firewall
- Microsoft Defender for Endpoint

Barracuda CloudGen

Collect and analyze Barracuda CloudGen logs to better identify threats and intrusions.

Setup

Microsoft Defender for Endpoint 🟡

Bring SKOUT insight into your endpoint protection logs for analysis and alerting.

Setup

SentinelOne Enhancements

SentinelOne enhancements for this release include the following:

- An updated SentinelOne agent has been pushed to all existing installs.
- USB device blocking has been enabled for Endpoint Security customers who have the managed offering, limiting their attack surface.

Additional Rules

The following additional rules have been added to existing integrations:

- Several firewall rules looking for activities to/from suspicious regions
- Detections looking for brute force authentication across a variety of devices
- Additional ML detections within AWS, OKTA, and CrowdStrike

Expanded SOAR Capabilities

To allow Barracuda XDR to communicate compromise indicators quickly, and to ensure you receive all the information needed for mitigation, this release features expanded SOAR capabilities, automating the investigations and queries performed by our security professionals including:

- Several firewalls
- Windows Server
- Windows Server Machine Learning detections
- Microsoft 365
- Threat intelligence enrichment

If you have any questions, please contact partnersuccess@barracudamsp.com

Figures

1. Barracuda_MSP_XDR.png
2. Screen Shot 2022-10-04 at 2.44.29 PM.png
3. Screen Shot 2022-10-04 at 2.43.28 PM.png