How-To Guide

Integrate Linux with Netsurion Open XDR

Publication Date

September 12, 2023

Abstract

This guide provides instructions to configure and integrate Linux with Netsurion Open XDR to retrieve its logs via Syslog Integration and forward them to Netsurion Open XDR.

Note:

The screen/ figure references are only for illustration purpose and may not match the installed product UI.

Scope

The configuration details in this guide are consistent with Linux and Netsurion Open XDR 9.3 or later.

Audience

This guide is for the administrators responsible for configuring and monitoring Linux in Netsurion Open XDR.

Table of Contents

1 Overview

Linux is a family of open-source Unix-like operating systems based on the Linux kernel, an operating system kernel. An operating system is software that manages all the hardware resources associated with your desktop or laptop.

Netsurion Open XDR manages logs retrieved from Linux. The alerts, reports, dashboards, and saved searches in Netsurion Open XDR are enhanced by capturing important and critical activities in Linux.

2 Prerequisites

- Administrative or Root access to Linux console.
- Syslog port (for example, 514) must be set to allow in the firewall.
- Must have the Auditd service enabled and running.

3 Integrating Linux with Netsurion Open XDR

Linux can be integrated to Netsurion Open XDR via syslog by using Linux Log Forwarder.

> **Note**
>
> To get the Linux Log Forwarder package, contact your Netsurion Account Manager.

Refer the Configure Linux Log Forwarder document for integrating the Linux using Linux Log Forwarder.

4 System Extraction

Perform the following process for System extraction.

1. In **Netsurion Open XDR**, hover over the **Admin** menu and click **Manager.**
2. In the **Manager** interface, go to **syslog/ Virtual Collection Point** > **syslog,** hover over the **Gear** icon located adjacent to it, and then click **Extract device id** for extracting the system name.
3. Hover over the **Gear** icon and click the **Extract device Id** for extracting the system name using the below regex:
   - Fill in the following details,

   For Linux Log Forwarder Integration

   a. **Regular expression:** `Hostname:(?P<Computer>[^,]+)\,\sTenant:(?P<Tenant>[^,]+)`
   b. **Token Name:** Computer~Tenant
4. Click the **Update** button to save the extraction logic details.

5 Data Source Integration (DSI) in Netsurion Open XDR

After the logs are received by Netsurion Open XDR, configure the Data Source Integrations in Netsurion Open XDR.

The Data Source Integrations package contains the following files for **Linux**.

- Categories_Linux.iscat
- Alerts_Linux.isalt
- Reports_Linux.etcrx
- KO_Linux.etko
- Dashboards_Linux.etwd
- Templates_Linux.ettd

Note

Refer the How To Configure DSI guide for the procedures to configure the above DSIs in Netsurion Open XDR.

5.1 Alerts

Name	Description
Linux: User or group deleted	Generated when a user or group has been deleted.
Linux: Code injection by ld.so preload detected	Generated when any code injection by dynamic linkers like ld.so.preload is detected.
Linux: Interactive terminal spawned	Generated when someone spawned interactive shell using scripts.
Linux: Potential disabling of SELinux detected	Generated when someone disabled the SElinux configuration.
Linux: Suspicious process activity detected	Generated when someone executed suspicious commands related to network.
Linux: Sensitive files compression detected	Generated when someone compressed critical configuration files like ssh key files, bash files, and more.
Linux: Sudoers configuration file changed or modified	Generated when a sudoers configuration file is modified.
Linux: Symlink to critical system configuration files detected	Generated when someone linked critical configuration files like passwd, sudoers, and more.
Linux: Command history cleared	Generated when command history has been deleted in the host.

5.2 Reports

Name	Description
Linux - Login and logout activities	Provides details about all login and log out activities and their status.
Linux - User and group management	Provides details about all user and group management activities such as add user, delete user, change user permission, and more.
Linux - User Command execution	Provides details about all command execution activity by a user.
Linux - Root activities	Provides details about all root level commands status and related information such as a username, command, and more.

5.3 Dashboards

Name	Description
Linux - Login by geo location	Displays the geo location of the login event.
Linux - Critical root activities	Displays the data about critical root activities.
Linux - Login activities by source IP	Displays the data about all login related activities by source IP.
Linux - User management activities	Displays the data about user related activities by username.

5.4 Saved Searches

Name	Description
Linux - Sudoers configuration file modification	Provides details when someone tries to change the configuration in sudoers file.
Linux - User password modification	Provides details about user password change activities.
Linux - Login and logout activities	Provides detailed overview of user login and logout activities.
Linux - User and group management	Provides detailed overview of activities performed by any user, such as add user, delete user, group add, group delete, and more.
Linux - Root activities	Provides details about all root activities performed on Linux.
Linux - User command execution	Provides detailed overview of commands that were executed in user shell.

About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our Open XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's 24x7 SOC operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers managed threat protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection & Response (MXDR). Learn more at www.netsurion.com.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

Use the form to submit your technical support tickets. Or reach us directly at 1 (877) 333-1433

Managed XDR Enterprise Customers	SOC@Netsurion.com
Managed XDR Enterprise MSPs	SOC-MSP@Netsurion.com
Managed XDR Essentials	Essentials@Netsurion.com
Software-Only Customers	Software-Support@Netsurion.com

https://www.netsurion.com/support