How-To Guide

Configure Remote Workforce Threat Detection (RWTD) in Netsurion Open XDR

Publication Date:

May 26, 2023

Abstract

This guide provides instructions to configure RTWD Data Source Integration (DSI) in 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 Netsurion Open XDR 9.4 or later.

Audience

This guide is for the administrators responsible for configuring the RWTD in Netsurion Open XDR.

Table of Contents

1 Overview

Professionals working outside the office require a remote connection to the organizational network. To facilitate this, a VPN is used which may increase the risk associated with an organization's network in terms of social engineering and brute force attacks. To combat the rapid increase in the remote workforce threat, Netsurion Open XDR generates alerts using firewall devices and SSO descriptions. Alerts can be configured for Remote Workforce Threat Detection.

The dashboards and alerts in Netsurion Open XDR are enhanced by tracking possible attacks, suspicious activities, or any other threat noticed.

The following products are currently supported for RWTD DSIs.

VPN	• Cisco ASA Firewall • FortiGate Firewall • Palo Alto Firewall • Sophos XG Firewall • WatchGuard XTM Firewall • Firewall SonicWall UTM Firewall
Cloud suite	• Google Workspace • Microsoft 365
Authenticators	• OKTA SSO • DUO Security • Azure AD • Windows

2 Prerequisites

- PowerShell 5.0 must be installed in the Netsurion Open XDR console.

3 Configuring RWTD in Netsurion Open XDR

- Customers using Netsurion Open XDR 9.4 can install the Netsurion Remote Workforce Threat Detection feature add-on package NS94U23-8009 to configure features related to RWTD.
- This utility has a configuration file named **SuspiciousLogin.config** under the install path **installpath\ScheduledActionScripts\Suspicious Login** which determines the behavior of the RWTD utility.

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
    <AlertConfiguration>
        <alert Name='cisco asa firewall: vpn login activities'>
            <activities>
                <Simult available='True'/>
                <multiuser available='True'/>
                <blacklist available='True'/>
            </activities>
            <regex>User\s(?&lt;Username&gt;.*?)\sIP(?&lt;LoginIP&gt;.*?)\sanyconnect</regex>
        </alert>
```

Note

Refer the **SuspiciousLogin.config** file for any error related files and for more information about the events related to RWTD.

4 Data Source Integrations (DSIs) 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. These files can be found in the install location: **installpath\KnowledgePacks\RWTD\Configuration.**

Alerts	▪ Alerts_Essential RWTD.isalt ▪ Alerts_RWTD.isalt
Dashboard	▪ Dashboards_Authenticator.etwd ▪ Dashboards_CloudSuite.etwd ▪ Dashboards_EssentialRWTD.etwd ▪ Dashboards_VPN.etwd
Machine Learning	▪ ML_Essential RWTD.isrule ▪ ML_RWTD.isrule

Knowledge Objects	▪ KO_Fortinet Fortigate.etko ▪ KO_GoogleWorkspace.etko ▪ KO_OKTASSO.etko ▪ KO_RWTD.etko

Note

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

Data Source Integrations Details

4.1 Alerts

Name	Description
Cisco ASA Firewall: VPN login activities	Base alert for CISCO ASA to trigger the RTWD Suspicious Login remedial action script.
Duo Security: Login activities	Base alert for Duo Security to trigger the RTWD Suspicious Login remedial action script.
FortiGate firewall: VPN login activities	Base alert for FortiGate firewall to trigger the RTWD Suspicious Login remedial action script.
FortiGate firewall: VPN tunnel up connections	Base alert for FortiGate firewall related to VPN tunnel up connections to trigger the RTWD Suspicious Login remedial action script.
Google Workspace: Login activities	Base alert for Google Workspace to trigger the RTWD Suspicious Login remedial action script.
Microsoft 365: Login activities	Base alert for Microsoft 365 to trigger the RTWD Suspicious Login remedial action script.
Okta SSO: Login activities	Base alert for Okta SSO to trigger the RTWD Suspicious Login remedial action script.
Palo Alto firewall: VPN login activities	Base alert for Palo Alto firewall to trigger the RTWD Suspicious Login remedial action script.
SonicWall firewall: VPN login activities	Base alert for SonicWall firewall to trigger the RTWD Suspicious Login remedial action script.
Sophos XG firewall: VPN login activities	Base alert for Sophos XG firewall to trigger the RTWD Suspicious Login remedial action script.

Name	Description
WatchGuard XTM firewall: VPN login activities	Base alert for WatchGuard XTM firewall to trigger the RTWD Suspicious Login remedial action script.
Suspicious multiple account login attempts from same IP address	Generated when attempts related to multiple accounts are detected from a same IP address.
Login activity from blacklisted location	Generated when a login is detected from a blacklisted country.
Geographically improbable access detected	Generated when login attempts are detected from locations separated by a large distance in a very short span of time.

4.2 Dashboards

Name	Description
Authenticator- Login Activities by User	Provides insights on login activities from authenticator-based products based on users.
Authenticator- Login Activities by System Type	Provides insights on login activities from authenticator-based products based on system type.
Authenticator- Login Activities by Country	Provides insights on login activities from authenticator-based products based on detected countries.
Authenticator- Login Success Trend	Provides a trend view on successful logins from authenticator-based products.
Authenticator- Login Failure Trend	Provides a trend view on login failures from authenticator-based products.
Authenticator- Login Failed by Country	Provides insights on login failures from authenticator-based products based on detected countries.
Authenticator- Login Activities by Device Type	Provides insights on login activities from authenticator-based products based on device type.
Authenticator- Login Activities by Browser	Provides insights on login activities from authenticator-based products based on browser type.
Authenticator- Admin Activities	Provides insights on login activities from authenticator-based products related to admins.
Authenticator- Login failed by User	Provides insights on login failures from authenticator-based products based on users.
Login activities by Source Country	Provides insights on login activities from cloud suites based on source country name.
Login by User	Provides insights on login activities from cloud suites based on users.

Name	Description
Login failed by Country	Provides insights on login failures from cloud suites based on country name.
Login failed by User	Provides insights on login failures from cloud suites based on uses.
Login Failure Trend	Provides a trend of login failures from cloud suites related products.
Login Success Trend	Provides a trend of successful logins from cloud suites related products.
VPN Login by User	Provides insights on logins related to VPN based products based on users.
VPN Login by Geolocation	Provides insights on logins related to VPN based products based on geolocation.
VPN Login by IP address	Provides insights on logins related to VPN based products based on IP addresses.
VPN Login failed by User	Provides insights on login failures related to VPN based products based on users.
VPN Login failed by geolocation	Provides insights on login failures related to VPN based products based on geolocation.
VPN Login Success Trend	Provides a trend of successful logins from VPN related products.
VPN Login failed Trend	Provides a trend of login failures from VPN related products.
VPN Login failed by IP Address	Provides insights on login failures related to VPN based products based on IP Addresses.

4.3 Machine Learning Rule

Name	Description
Admin activities by New User and IP	Facilitates to understand login patterns related to Admins in Exchange, SharePoint, and Azure Active Directory related environments.

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-Support@Netsurion.com
Software-Only Customers	Software-Support@Netsurion.com

https://www.netsurion.com/support