NetWitness® Platform

Picus Event Source Log Configuration Guide

NETWITNESS
Platform

Picus Integration Guide

Last Modified: Friday, July 19, 2024

Integration Product Information:

Partner Name: Picus Security

Website: https://www.picussecurity.com/

Versions: API v1.0

NetWitness Platform Product Information:

Supported On: NetWitness Platform 12.2.x and later

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on NetWitness Community. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Miscellaneous

This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at https://www.netwitness.com/standard-form-agreements/.

February, 2024

Contents

About Picus

Named a Cool Vendor by Gartner in 2019 and cited as one of the most innovative Breach and Attack Simulation (BAS) players by Frost&Sullivan in 2020, Picus Security offers a Complete Security Validation platform based on a transformative Breach and Attack Simulation (BAS) technology.

Picus Platform continually and on-demand assesses the readiness of security controls against changing adversarial techniques, tactics and procedures. Picus assessments reveal defensive capabilities across the prevention and detection stages holistically and provide customized detection content to close identified gaps swiftly. Becoming part of daily security operations with its extensive range of integrations, automated architecture, feature-rich UI, and advanced reporting, Picus empowers security professionals and maximizes the potential of security technologies. Picus works with a large number of enterprises from different industries around the globe.

About NetWitness

NetWitness is an Evolved SIEM and XDR platform that accelerates threat detection and response for organizations worldwide. NetWitness Platform delivers complete visibility combined with applied threat intelligence and user behavior analytics to detect, prioritize, investigate threats, and automate response. It can collect and analyze data across all capture points (logs, packets, netflow, Endpoint, and IoT) and computing platforms (physical, virtual and cloud), enriching data with threat intelligence and business context. This empowers security analysts to be more efficient and stay ahead of business-impacting threats.

NetWitness Platform Integration

Detection Analytics module communicates with NetWitness Platform using its following API calls.

API Type	Operation	API
REST	Search	/sdk/query
REST	Log Collection	/sdk/content
NW-API	Alert Collection	/rest/api/incidents

Prerequisites

The Detection Analytics module requires a Concentrator service user and the NetWitness Platform user. The concentrator service user is used to query and retrieve the Picus attack simulation-related logs. The NetWitness Platform user is used to query and retrieve the Picus attack simulation-related incidents through NW-API.

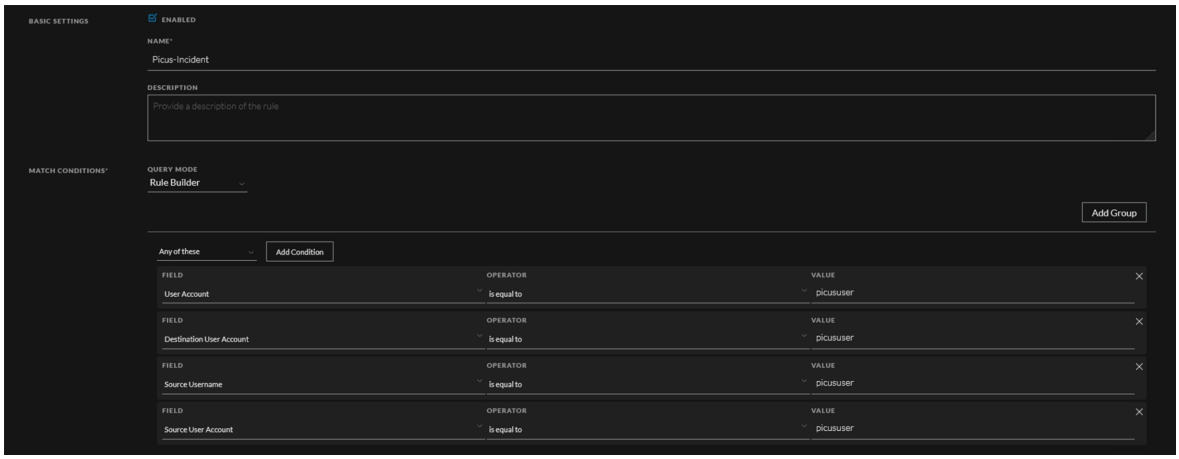
The Detection Analytics module also requires an incident rule to analyze the alerts on the NetWitness Platform. The alerts triggered by the incident rule will be analyzed. A sample incident rule is provided below.

IMPORTANT: The value for the Picus user in the sample rule can vary depending on the current environment.

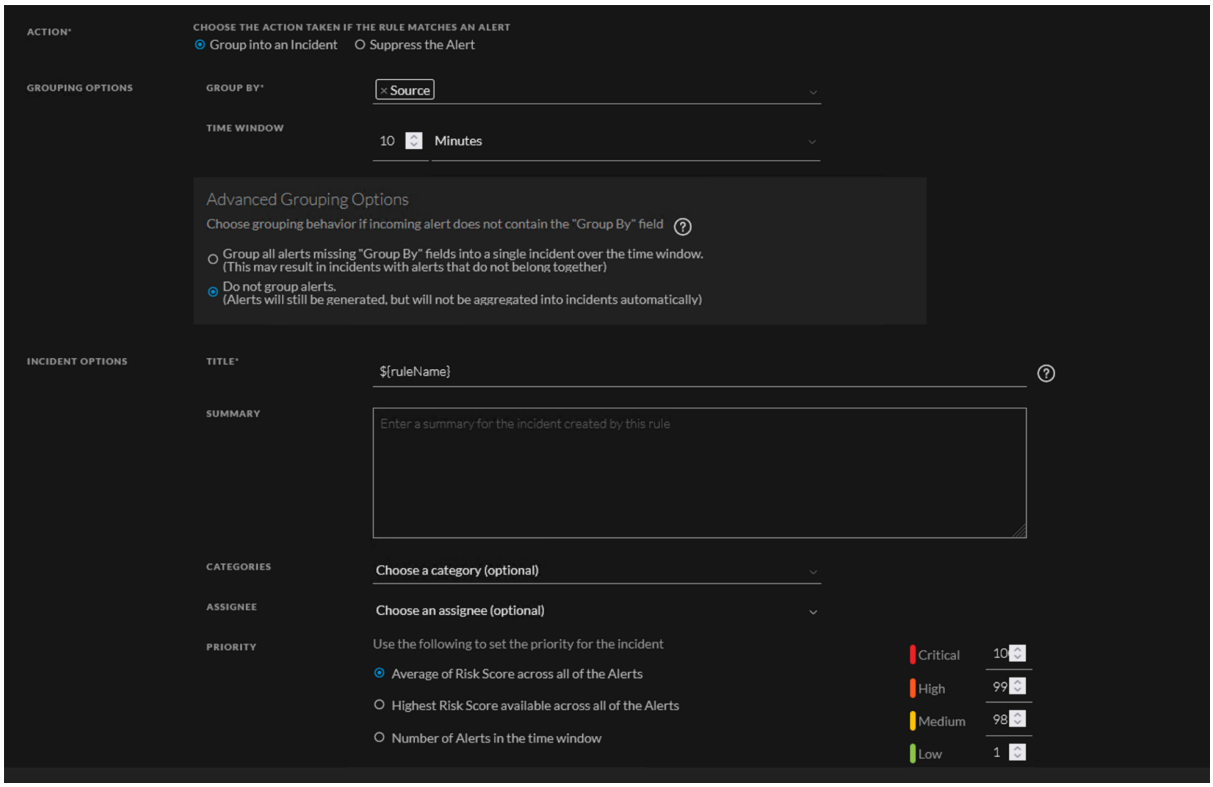
Settings

1. Add the following fields for any of these option and set their value to the Picus user under the **Match Conditions**.
   - User Account
   - Destination User Account
   - Source Username

- Source User Account



2. Set the **Source** for the **Group By** option and set the **Time Window** value under the **Grouping Options** less than the total analysis interval that will be configured at the Alert Based step of the NetWitness integration process.
3. Under **Incident Options**, set the **${ruleName}** in the **Title** field.



NetWitness Integration Process

The NetWitness integration process consists of the following steps

1. Access
2. Vendor Based
3. OS Based
4. Alert Based

Warning: Picus provides a predefined field mapping at the Vendor Based and OS Based steps. As log source indexing mechanisms may vary, it is important to review and adjust the field mapping according to the current NetWitness log source configuration.

Access

1. Enter the concentrator service user credentials that are used to authenticate to the NetWitness Concentrator and make API calls.
2. Enter the system IP Address or Host Name on which the concentrator service is hosted.
3. Enter a listening port number for the concentrator service's API on the system. The default API port number is **50105**.

   Note: The Concentrator service's port number is different from the concentrator service's API port number. The default concentrator service's port number is **50005**. The concentrator service's API port number can be obtained by adding one hundred to the configured value for the concentrator service's port number.
4. Select one of the available communication protocols, which are HTTP or HTTPS.
5. Select any available Picus Integration Peer, that will be responsible for the communication.
6. Enter a Concurrent Assessment Limit for the Picus Integration Peer when it makes the API calls.
7. Click **Login** to verify that the information provided is correct.

Vendor Based

1. Define NetWitness indices for each log source.
2. Select one or more available vendors from the Vendors list. If a specific vendor is not available, it can be added using the **+ Add New Vendor**. The option also enables to specify of custom queries for the particular vendor.
3. Enter an early time in seconds. This option sets the analysis start time earlier than an attacks actual start time to address time synchronization issues.

   Caution: Entering a high early time may affect the NetWitness's performance. Entering a low early time may result in false-negative results.
4. Enter a delay time in seconds. The delay time is the duration of a log created and delivered to the NetWitness. The Detection Analytics module will query the attack simulation logs based on the provided delay time.

> **Caution:** Entering a high delay time may affect the NetWitness's performance. Entering a low delay time may result in false-negative results.

5. Expand the **Advanced Field Mapping** configuration. Review and adjust the predefined field mappings for the vendors. The **Name** and **Action** fields are mandatory.
6. Click **Test** to verify that the information provided is correct. Once the information is all correct, the **Test** will become **Next**.

OS Based

1. Define NetWitness indices for the Microsoft Windows OS logs.
2. **Picus** provides a predefined query for the Microsoft Windows OS logs. It can be edited accordingly.
3. Enter an early time in seconds. This option sets the analysis start time earlier than an attacks actual start time to address time synchronization issues.

   > **Caution:** Entering a high early time may affect the NetWitness's performance. Entering a low early time may result in false-negative results.

4. Enter a delay time in seconds. The delay time is the duration of a log created and delivered to NetWitness Platform. The Detection Analytics module will query the attack simulation logs based on the provided delay time.

   > **Caution:** Entering a high delay time may affect the NetWitness's performance. Entering a low delay time may result in false-negative results.

5. Expand the **Advanced Field Mapping** configuration. Review and adjust the predefined field mappings for the Microsoft Windows OS logs. The **Name** and **Action** fields are mandatory.
6. Click **Test** to verify that the information provided is correct. Once the information is all correct, the **Test** will become **Next**.

Alert Based

1. Enter the NetWitness Platform user credentials that will be used to query and retrieve the Picus attack simulation-related incidents through NW-API. Optionally, the credentials provided at the Access step can be used by checking the **Use the previous login credentials used in the access step** checkbox.
2. Enter the system IP Address or Host Name on which NetWitness Platform is hosted.
3. Enter a listening port number for NetWitness Platform on the system.
4. Select one of the available communication protocols, which are HTTP or HTTPS (default port).
5. Enter the Incident Rule's name created on NetWitness Platform for the Detection Analytics module to analyze the alerts.

6. Toggle on or off the **Enable auto-delete** setting that automatically deletes the incidents triggered by the incident rule at regular intervals to reduce the high volume of incidents in the NetWitness Platform **Respond** page.
7. Enter an early time in seconds. This option sets the analysis start time earlier than an attacks actual start time to address time synchronization issues.

   Caution: Entering a high early time may affect the NetWitness's performance. Entering a low early time may result in false-negative results.

8. Enter a delay time in seconds. The delay time is the duration of a log created, delivered to NetWitness Platform, and NetWitness Platform creates the alert.

   Caution: Entering a high delay time may affect the NetWitness's performance. Entering a low delay time may result in false-negative results.

9. Click **Test** to verify that the information provided is correct. Once the information is all correct, the **Test** will become **Save**.
10. Click **Save** to finish the NetWitness Platform Integration.

Getting Help with NetWitness Platform

Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness:

- See the documentation for all aspects of NetWitness here: https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation.
- Use the **Search** and **Create a Post** fields in NetWitness Community portal to find specific information here: https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions.
- See the NetWitness Knowledge Base: https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base.
- See the documentation for Logstash JDBC input plugin here: https://www.elastic.co/guide/en/logstash/current/plugins-inputs-jdbc.html.
- See Troubleshooting section in the guides.
- See also NetWitness® Platform Blog Posts.
- If you need further assistance, Contact NetWitness Support.

Contact NetWitness Support

When you contact NetWitness Support, please provide the following information:

- The version number of the NetWitness Platform or application you are using.
- Logs information, even source version, and collection method.
- If you have problem with an event source, enable **Debug** parameter (set this parameter to **On** or **Verbose**) and collect the debug logs to share with the NetWitness Support team.

Use the following contact information if you have any questions or need assistance.

NetWitness Community Portal	https://community.netwitness.com In the main menu, click **Support > Case Portal > View My Cases**.
International Contacts (How to Contact NetWitness Support)	https://community.netwitness.com/t5/support/ct-p/support
Community	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions

Feedback on Product Documentation

You can send an email to feedbacknwdocs@netwitness.com to provide feedback on NetWitness Platform documentation.