Enabling Behavioral Analytics Using Micro Focus Interset

Access Manager uses Risk Service to assess the risk associated with an access attempt based on the contextual information. For example, the contextual information can be IP address and device information.

Risk Service uses deterministic, rule-based computation. It enables organizations to find threats quickly with known attack patterns and take appropriate actions.

Some threats are very complex and difficult to trace through rule-based computation. These unknown threats are unpredictable and do not leave any evidence behind. The evidence might be hidden within your data. These threats require a more sophisticated approach to anomaly detection using machine learning.

To enable the unknown threat or anomaly detection, **Risk Service** integrates with **Interset** and leverages its *User and Entity Behavioral Analytics* (UEBA) capability. Using the organization's data, Interset establishes the normal behavior for the organizational entities and then, using advanced analytics and machine learning, identifies the anomalous behaviors that constitute potential risks such as compromised accounts, insider threats, or other unknown cyber threats.

For more information about Access Manager Risk Service, see Risk-based Authentication (https://www.netiq.com/documentation/access-manager-45/admin/data/b1dg0omz.html).

For more information, see User and Entity Behavioral Analytics (https://www.microfocus.com/media/flyer/user-and-entity-behavioral-analytics-flyer.pdf).

The following are a few examples of anomalies in behavioral access control:

- A large number of session authentication successes and failures
- A large number of application access events
- A large number of distinct applications accessed
- Unusual application access events
- Unusual browser used during authentication
- Unusual working hours or working days

This integration enables Risk Service to perform the following actions by using behavioral analytics:

- Detect compromised account and bots
- Detect insider threats
- Detect compromised network, host, and devices
- Detect unknown threats

In This Guide:

- Prerequisites for the Integration
- Integrating Risk Service with Interset
- Troubleshooting Integrating Risk Service with Interset

1 Example Scenarios

The following are a few common scenarios where enabling behavioral analytics helps accelerate threat detection:

- Scenario: Compromised Account Detection
- Scenario: Insider Threats Detection
- Scenario: Accidental Insider Threats Detection
- Scenario: Compromised Network, Host, or Device Detection

1.1 Scenario: Compromised Account Detection

Albert works in a Healthcare organization. He browses news sites from his corporate computer. One day, he inadvertently clicks a malicious URL that injects the spyware script in his browser. The script starts accessing numerous sensitive applications and downloading the data.

Interset identifies a sudden increase in the number of access attempts and network lateral movements from Albert's system. Interset classifies this as high risk and shares his risk score with Risk Service. Access Manager blocks Albert from accessing any application.

1.2 Scenario: Insider Threats Detection

Daniel, a helpdesk engineer, accesses the sensitive data and explores various corporate resources from home at night. Interset detects the anomalous behavior and classifies Daniel as a high-risk user. Interset shares the risk score with Risk Service. Access Manager blocks access for Daniel before anything too malicious happens.

Olga, an engineer, is erroneously given access to a privileged application. She decides to browse that application from home on a weekend. Interset detects this privileged access abuse and increases her risk. Access Manager blocks Olga's access to the application.

Lucio, a system admin, has access to a service account with higher privileges. He uses that account's credentials to access the restricted data. Interset detects the account misuse as high risk and shares this information with Risk Service. Access Manager locks down this service account.

1.3 Scenario: Accidental Insider Threats Detection

Amrita, an HR professional, forgets to lock her computer. This allows a colleague to probe the sensitive data. Interset detects this account compromise with medium risk and results in the Access Manager multi-factor authentication requirement the next day. This stops the colleague from the subsequent attempt to steal the data.

1.4 Scenario: Compromised Network, Host, or Device Detection

Interset detects an unusual number of access requests from similar IPs or similar devices. The overall risk is high as the organization might be under a stealth attack or at risk of a DDOS attack.

Interset detects an increase in the number of identities. It also detects an unusual number of access requests from these identities. Interset increases the overall risk of this B2C organization as the attackers might be creating an excessive number of identities by using social login. Attackers could also launch a DDOS attack with these valid identities.

Thomas, an engineer, has malware running on his laptop. This malware uses his account to snoop the resources on the network. Interset detects the infected host by considering unusual access patterns and endpoint threat patterns. Interset determines the user as high risk. Access Manager blocks his access.

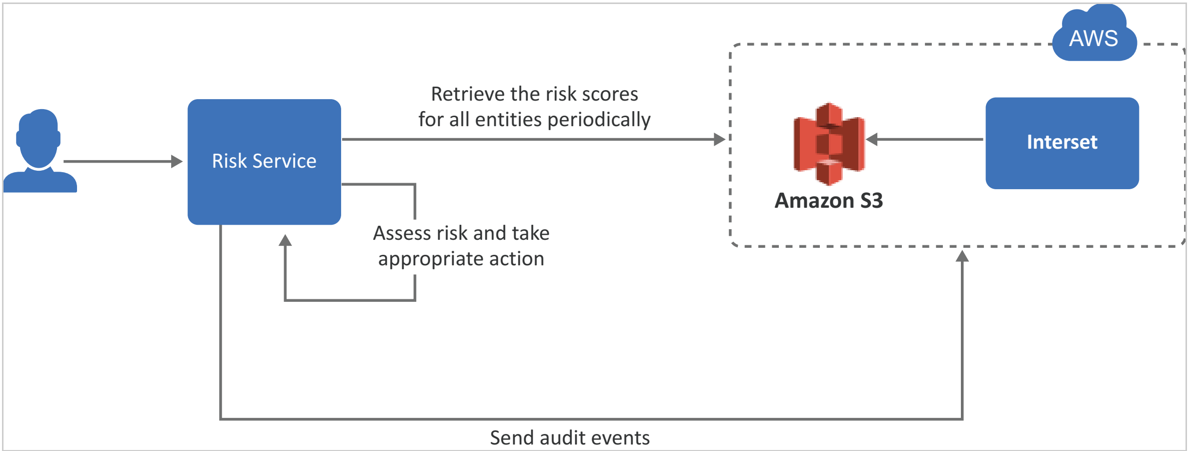
2 How It Works

Access Manager Risk Service periodically fetches risk scores for all entities from Interset. When a user tries to access a protected resource, Risk Service uses the risk score for assessing the risk.

While configuring Interset, you need to configure it to receive data from various applications used in your organization. Interset analyzes the behavior of entities and users using this data. In addition to this, you can configure to send the following Access Manager audit events to Interset:

- User Session Authenticated
- User Session Authentication Failed
- Intruder Lockout
- Access Denied
- Federation Assertion
- Application Access

The following diagram illustrates how this integration works:


AWS
Risk Service
Retrieve the risk scores for all entities periodically
Amazon S3
Interset
Assess risk and take appropriate action
Send audit events

1. A user tries to log in to a protected resource.
2. Risk Service checks the behavioral risk score for this user in the risk score cache.

   Risk Service keeps retrieving the latest behavioral risk scores for all entities at a regular interval and updates the cache.
3. Risk Service assesses the score and takes appropriate action.
4. (Optional) Access Manager sends the audit events to Interset for the behavior analysis purpose.

3 Prerequisites for the Integration

- ❒ An ArcSight Intelligence *(formerly Interset)* account on AWS is available. For more information, see ArcSight Intelligence (https://www.microfocus.com/en-us/products/arcsight-intelligence/overview).
- ❒ AWS S3 URL to access Interest is available.
- ❒ AWS region name is available.
- ❒ AWS access key ID and secret access key required to access the AWS S3 URL are available.
- ❒ (Optional) The Interset syslog connector URL is available.
- ❒ (Optional) The syslog connector certificate is available.
- ❒ Access Manager 4.5 Service Pack 3 or later is installed and configured (on-premises or on the cloud).

  This integration is not supported on Windows.

NOTE: Interset syslog connector URL and syslog connector certificate are required only when you want to send Access Manager audit events to Interset.

4 Integrating Risk Service with Interset

To integrate Risk Service with Interset, perform the following actions:

1. Configure Interset in Access Manager
2. Modify the External Parameters Rule
3. Add BehavioralAnalyticsRule to a Risk Policy

Configure Interset in Access Manager

1 Click Policies > Risk-based Policies > Behavioral Analytics.

2 Select Integrate with Interset.

3 Specify the following details under **Read Behavioral Analytics Data from Interset**:

Field	Description
Interset Data URL	The AWS S3 bucket URL from where you want to get the Interset data.
AWS Region	The AWS region where Interset is deployed.
Access Key ID	The AWS access key ID to access the Interset URL.
Secret Access Key	The AWS secret access key to access the Interset URL.
Update every	The interval for syncing the data from Interset. The recommended value is 360 minutes (sync four times a day).

NOTE: To prevent disruption of service, ensure that Access Key ID and Secret Access Key specified here are up to date when these are rotated as per AWS guidelines.

4 (Optional) If you want to send Access Manager audit events to Interset, specify the following details under **Send Events to Interset**:

Field	Description
Enable	Select this option to enable sending audit events to Interset. See Audit Events Supported for Behavioral Analytics.
Interset Syslog Connector URL	Specify the URL of the AWS Interset syslog connector in the `domain:port` format. Identity Server and Access Gateway send audit events to this syslog server.
Syslog Connector Certificate	Upload the syslog connector certificate. This certificate validates and secures the connection to the syslog connector.

5 Click OK.

6 Continue with "Modify the External Parameters Rule" on page 5.

Modify the External Parameters Rule

When you configure Behavioral Analytics, Access Manager creates an `External Parameters` rule automatically with the appropriate values. The name of the rule is **BehavioralAnalyticsRule**. You can modify this rule if required.

1 Policies > Risk-based Policies > Rules.

2 Click BehavioralAnalyticsRule.

This rule is configured with the default behavior to consider any user with Interset score less than 50 as a low-risk user. You can modify this rule to change how the score from Interset is interpreted. You can modify Negate Result and the value for the score (the default value for the score condition is < 50). Do not modify any other field.

Field	Details
Negate Result	Select this option to reverse the result of the rule evaluation.
Parameters Set 1	Modify the value for the score parameter, if required.

NOTE: This rule retrieves GET requests that return simple JSON responses. To perform advanced operations, such as GET that returns nested data and POST, you must create a custom class to retrieve details from an external provider. For more information, see User Information Methods and Creating an Authentication Class in the NetIQ Access Manager 4.5 SDK Guide.

Add BehavioralAnalyticsRule to a Risk Policy

You can add `BehavioralAnalyticsRule` to an existing risk policy or you can create a new policy and add it.

1 To add it to an existing policy:

- **1a** Click **Policies** > **Risk-based Policies** > **Risk Policies**.
- **1b** Click the policy to which you want to add this rule.
- **1c** Under **Policy Rules**, click **Actions** > **Add Existing Rule**.
- **1d** In **Risk Rule**, select `BehavioralAnalyticsRule`.

2 To add it to a new policy:

- **2a** Click **Policies** > **Risk-based Policies** > **Risk Policies** > **Create Risk Policy**.
- **2b** Under **Policy Rules**, click **Actions** > **Add Existing Rule**.
- **2c** In **Risk Rule**, select `BehavioralAnalyticsRule`.

3 Create an authentication method and a contract for the authentication class associated with the risk policy to use the behavioral analytics capability.

See Configuring a Method for an Authentication Class (https://www.netiq.com/documentation/access-manager-45/admin/data/b1e08ogt.html#riskmethod) and Configuring a Contract for an Authentication Class (https://www.netiq.com/documentation/access-manager-45/admin/data/b1e08ogt.html#riskcontract).

For more information about configuring a risk policy, see Configuring a Risk Policy (https://www.netiq.com/documentation/access-manager-45/admin/data/b1e08ogt.html#riskgroup) in the Administration Guide (https://www.netiq.com/documentation/access-manager-45/admin/data/bookinfo.html).

4.1 Audit Events Supported for Behavioral Analytics

You can send the following audit events to Interset:

- NIDS: User Session Was Authenticated (002e000a)
- NIDS: User Session Authentication Failed (002e000c)
- NIDS: Intruder Lockout (002e0017)
- NIDS: Issued a Federation Assertion (002E0102)
- Access Gateway: Access Denied (0x002e0505)
- Access Gateway: Application Accessed (002E0514)

To send these events to Interset, you must enable these on Administration Console. See Enabling Identity Server Audit Events and Enabling Access Gateway Audit Events. After enabling these events, you must restart Identity Server and Access Gateway.

Access Manager converts the format of events to CEF before sending to Interset.

5 Troubleshooting Integrating Risk Service with Interset

- Section 5.1, “Unable to Connect to Interset Server,” on page 7
- Section 5.2, “Issues with Sending Audit Events to Interset,” on page 8
- Section 5.3, “Interset Integration Has Stopped Working,” on page 8

5.1 Unable to Connect to Interset Server

If Identity Server cannot connect to Interset S3, its health turns yellow and the following message is displayed:

```
Unable to connect to the Interset Server
```

This issue might occur due to wrong access key ID, wrong secret access key, or wrong S3 URL.

Perform the following steps:

1. Click **Auditing** > **General Logging**.
2. In the Identity Servers section, select the `catalina.out`.
3. Search for messages similar to the following in `catalina.out`:

   When the access key ID is wrong

   ```
   ERROR ueba connector: The AWS Access Key Id you provided does not exist in our
   records. (Service: Amazon S3; Status Code: 403; Error Code: InvalidAccessKeyId;
   Request ID: 996002BD9C6E82FE; S3 Extended Request ID: K1JPq0z/
   37k5PwmZoW3YaJnXQb2JxzEKmwm+VkHOL5dRFs19K06D0bMkhFkG1iT20RKnUUvC7ag=; Proxy:
   null)
   ```

   When the secret access key is wrong

   ```
   ERROR ueba connector: The request signature we calculated does not match the
   signature you provided. Check your key and signing method. (Service: Amazon S3;
   Status Code: 403; Error Code: SignatureDoesNotMatch; Request ID:
   4NDJFW0P5MEQ9XFP; S3 Extended Request ID: D9kS/DoIEszYmdkT/
   8x3CN4wv5l537KxCqTvyx24WUyrZu/OoMK4x51YY+/wCWgISFOdaAlOCLI=; Proxy: null)
   ```

   When the Interset data URL is wrong

   ```
   ERROR ueba connector: The specified bucket does not exist (Service: Amazon S3;
   Status Code: 404; Error Code: NoSuchBucket; Request ID: 94C64A2074EACE59; S3
   Extended Request ID:
   KNhoKC7spYBq2kKhlnKHB9JNXNsOLNrAMlc+R7apUppt28Q9Z7+gdSQybrgb1brBoHXwMdC91QI=;
   Proxy: null)
   ```

   When the health check failed

   ```
   <amLogEntry> 2020-07-28T10:52:21Z DEBUG NIDS Application:

   Method: NIDPServletContext.healthCheckInterset

   Thread: RMI TCP Connection(375)-127.0.0.1

   Failed to connect to interset server </amLogEntry>
   ```

5.2 Issues with Sending Audit Events to Interset

1. Check the connectivity between Access Manager and Interset syslog server by using the following command:

   ```
   netstat -na | grep <port configured for sending events>
   ```

   This is the same port that is configured as part of **Interset Syslog Connector URL**.

2. Log in to Interset S3 and verify if the events are received at the S3 bucket.

   The following are a few sample AWS CLI S3 commands:

   - **To list all files in the S3 bucket:** `#aws s3 ls s3://<S3 bucket name>`
   - **To copy a file to the local disk:** `aws --profile <profile name> s3 sync s3://<S3 bucket name> <local directory>`

     Many compressed files in the `.gz` format are copied to the local directory specified in the command. You can pick any file to see the content. For example, `zcat 2020-07-30-08-56-16.done.cef.gz`. The files contain Access Manager events. Some files might contain Interset syslog connector system events in addition to Access Manager events.

5.3 Interset Integration Has Stopped Working

The Interset administrator might have rotated the AWS Access Keys. Check with the Interset administrator and update the keys in the `Behavioral Analytics` UI of Access Manager.

Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see https://www.microfocus.com/about/legal/.