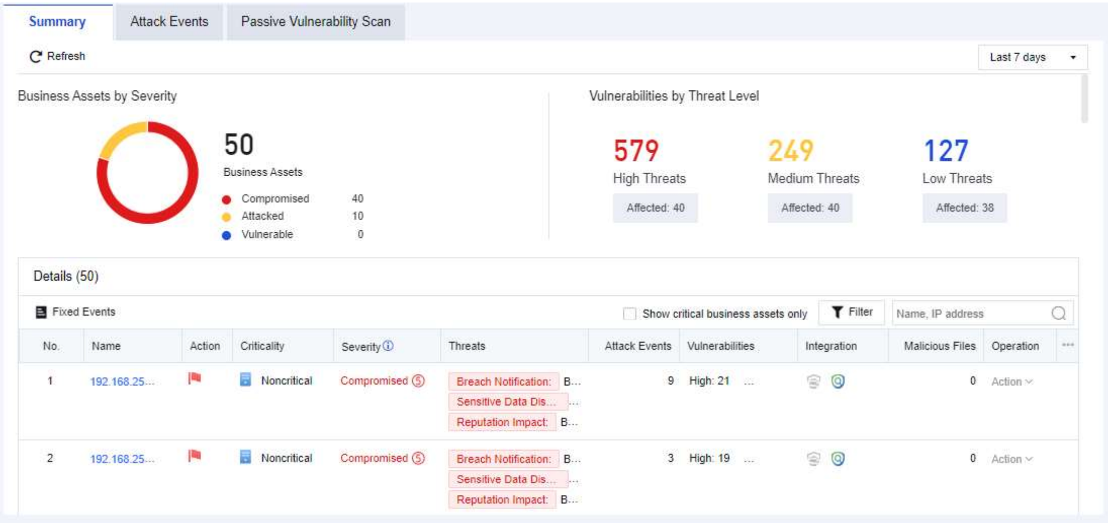
## 4.2.1. Summary of Business Asset Risks

It shows the security status from the dimension of business assets. You can check whether the business assets have intrusion risks or view the potential risks as shown below.



Business Assets by Severity

50 Business Assets

| | |
|---|---|
| ● Compromised | 40 |
| ● Attacked | 10 |
| ● Vulnerable | 0 |

Vulnerabilities by Threat Level

| 579 High Threats | 249 Medium Threats | 127 Low Threats |
|---|---|---|
| Affected: 40 | Affected: 40 | Affected: 38 |

Details (50)

| No. | Name | Action | Criticality | Severity | Threats | Attack Events | Vulnerabilities | Integration | Malicious Files | Operation |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 192.168.25... | | Noncritical | Compromised (5) | Breach Notification: B...<br>Sensitive Data Dis... ...<br>Reputation Impact: B... | 9 | High: 21 ... | | 0 | Action |
| 2 | 192.168.25... | | Noncritical | Compromised (5) | Breach Notification: B...<br>Sensitive Data Dis... ...<br>Reputation Impact: B... | 3 | High: 19 ... | | 0 | Action |

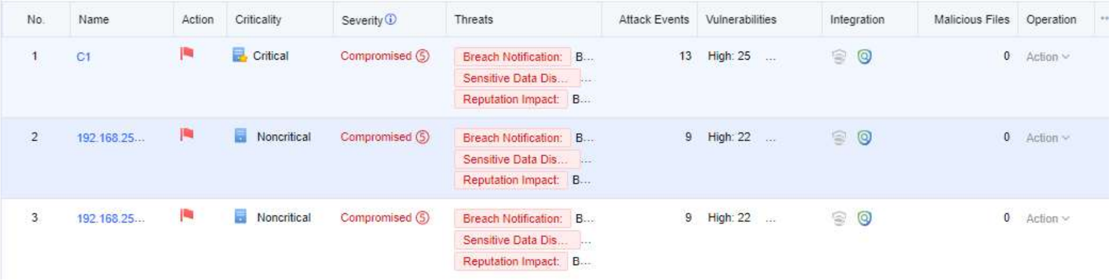
The description of risk levels is shown in the following table.

Table 5 Description of Risk Levels

| Risk Level | Note |
|---|---|
| **Compromised** | Existing data prove that the server has been hacked, such as embedment of web shell, backlink, etc. |
| **Attacked** | There is no data to prove that the server is hacked, but it will save the evidence of attack, including SQL injection, brute-force attack, web shell uploading, and other attack logs. |
| **Information collected** | There is no data to prove that the server is hacked, but the evidence of collecting information will be recorded. |
| **Reconnaissance** | There is no data to prove that the server is hacked, and there is no attack history, which indicates the server itself has reconnaissance. |

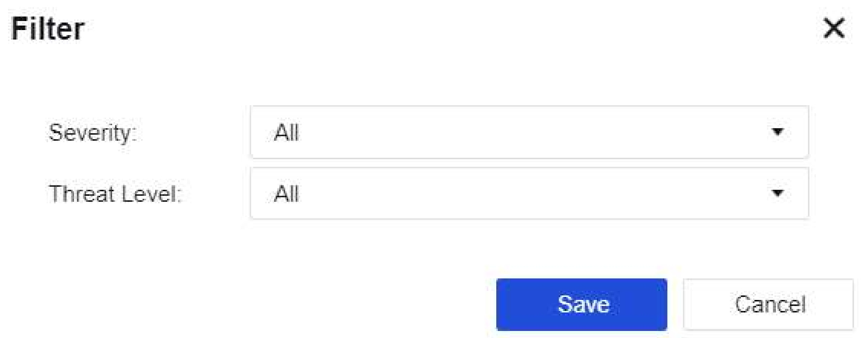
Key risks include compliance notification, sensitive data disclosure, reputation impact, and high/medium/low vulnerabilities. Vulnerability statistics are based on the real-time vulnerability analysis results.

You can only view the security status of core business assets by selecting **Show critical business assets only**. See the figure below.



| No. | Name | Action | Criticality | Severity | Threats | Attack Events | Vulnerabilities | Integration | Malicious Files | Operation |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | C1 | ⚑ | Critical | Compromised ⑤ | Breach Notification: B...<br>Sensitive Data Dis... ...<br>Reputation Impact: B... | 13 | High: 25 ... |  | 0 | Action ⌄ |
| 2 | 192.168.25... | ⚑ | Noncritical | Compromised ⑤ | Breach Notification: B...<br>Sensitive Data Dis... ...<br>Reputation Impact: B... | 9 | High: 22 ... |  | 0 | Action ⌄ |
| 3 | 192.168.25... | ⚑ | Noncritical | Compromised ⑤ | Breach Notification: B...<br>Sensitive Data Dis... ...<br>Reputation Impact: B... | 9 | High: 22 ... |  | 0 | Action ⌄ |

Click **Filter**. You can filter business assets by the comprehensive risk level and vulnerability level. See the figure below.

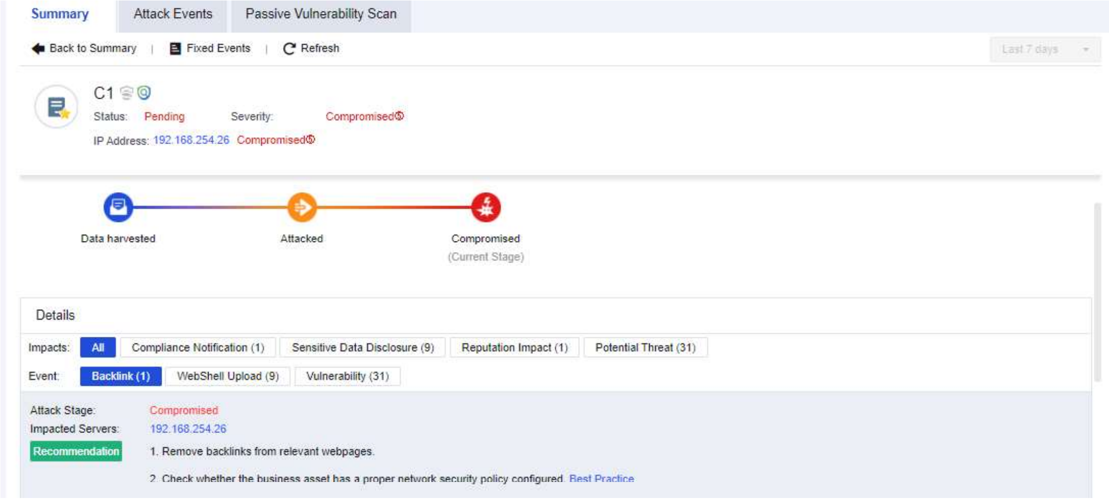


Filter

Severity: All

Threat Level: All

Click a business asset name. The following security details page will be displayed.



C1

Status: Pending Severity: Compromised

IP Address: 192.168.254.26 Compromised

Details

Impacts: All | Compliance Notification (1) | Sensitive Data Disclosure (9) | Reputation Impact (1) | Potential Threat (31)

Event: Backlink (1) | WebShell Upload (9) | Vulnerability (31)

Attack Stage: Compromised

Impacted Servers: 192.168.254.26

Recommendation 1. Remove backlinks from relevant webpages.

2. Check whether the business asset has a proper network security policy configured. Best Practice

As shown in the above figure, the upper part is a summary of business asset risks. Details include the current impacts on the business assets and the specific event types bringing such impacts (Webshell file access, Webshell backdoor, botnet, internal vulnerabilities, external attacks, etc.).

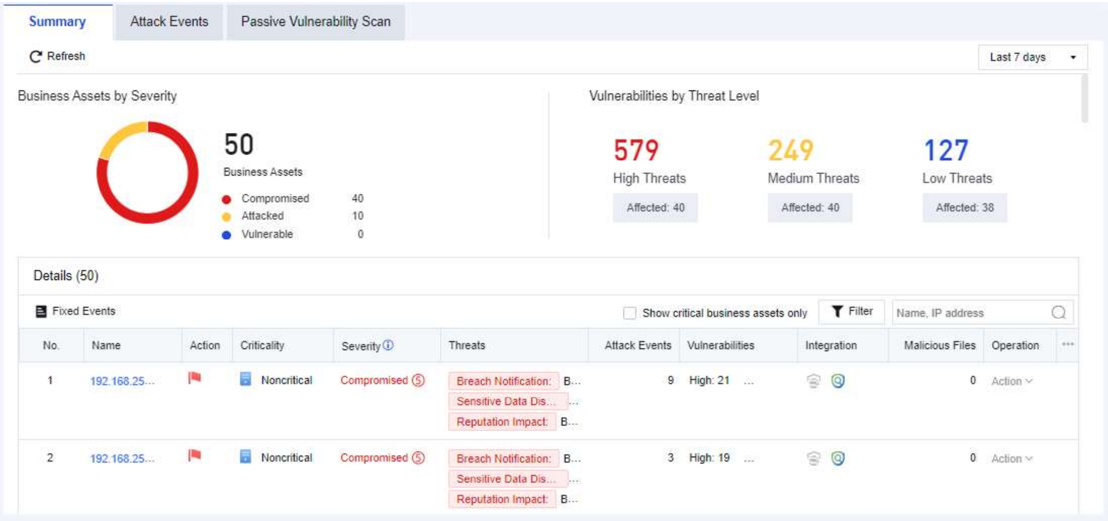
The risk level is **Compromised**. You can also see the impacted servers, recommendations, and proof.

### Configuration Case

In an enterprise, the NGAF has generated many business asset risk warnings, so admin must verify whether the mentioned business asset actually has such risks.

**Operation Steps:**

Step 1. Click **Summary** to check which business assets have risks. If they have compromised, you need to check the status of business assets first, as shown below.



Business Assets by Severity

50
Business Assets

| | |
|---|---|
| ● Compromised | 40 |
| ● Attacked | 10 |
| ● Vulnerable | 0 |

Vulnerabilities by Threat Level

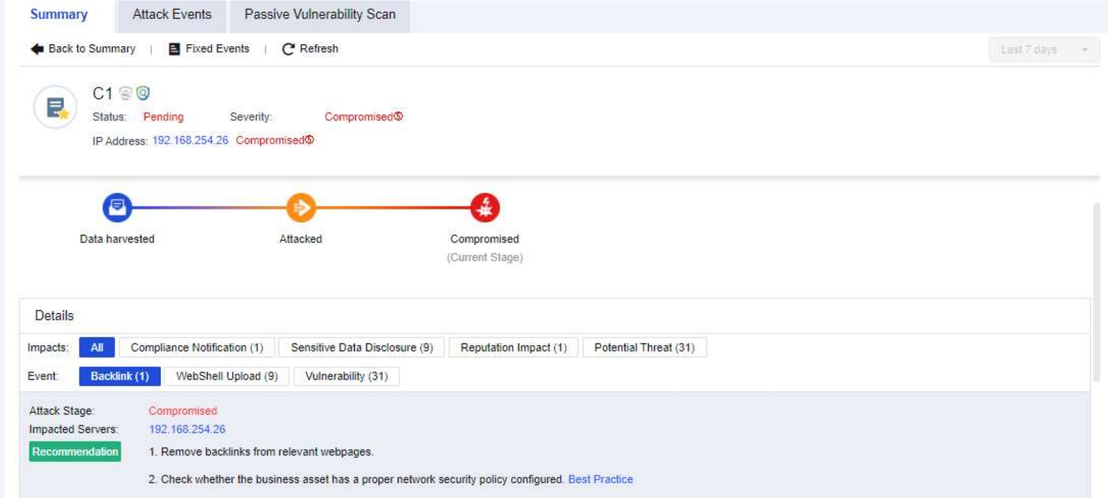
| 579 High Threats | 249 Medium Threats | 127 Low Threats |
|---|---|---|
| Affected: 40 | Affected: 40 | Affected: 38 |

Details (50)

Fixed Events □ Show critical business assets only Filter Name, IP address

| No. | Name | Action | Criticality | Severity | Threats | Attack Events | Vulnerabilities | Integration | Malicious Files | Operation |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 192.168.25... | | Noncritical | Compromised | Breach Notification: B...<br>Sensitive Data Dis... ...<br>Reputation Impact: B... | 9 | High: 21 ... | | 0 | Action |
| 2 | 192.168.25... | | Noncritical | Compromised | Breach Notification: B...<br>Sensitive Data Dis... ...<br>Reputation Impact: B... | 3 | High: 19 ... | | 0 | Action |

Step 2. Click the business asset name to view the specific status of the business asset, as shown below.



C1

Status: Pending Severity: Compromised

IP Address: 192.168.254.26 Compromised

Details

Impacts: All | Compliance Notification (1) | Sensitive Data Disclosure (9) | Reputation Impact (1) | Potential Threat (31)

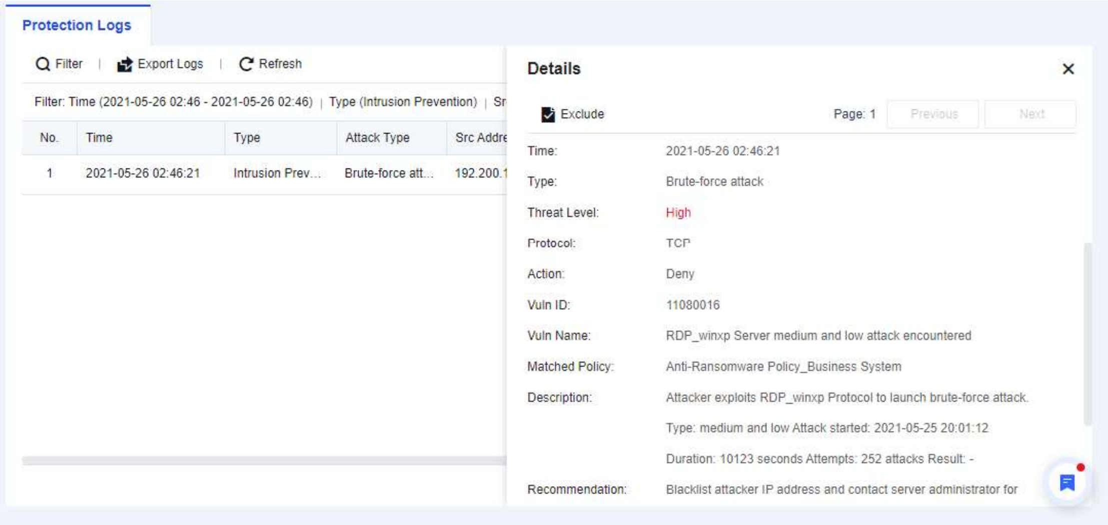
Event: Backlink (1) | WebShell Upload (9) | Vulnerability (31)

Attack Stage: Compromised

Impacted Servers: 192.168.254.26

Recommendation
1. Remove backlinks from relevant webpages.
2. Check whether the business asset has a proper network security policy configured. Best Practice

Step 3. View the corresponding events and click **Log** to analyze and judge the detection logs, and confirm whether the events are normal access, as shown below.



Filter: Time (2021-05-26 02:46 - 2021-05-26 02:46) | Type (Intrusion Prevention) | Sr

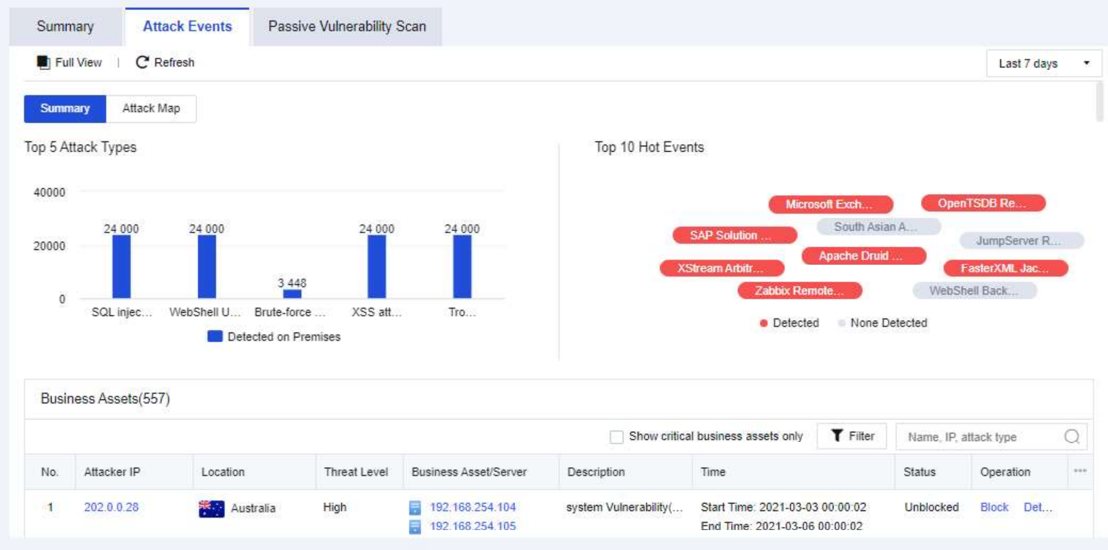
| No. | Time | Type | Attack Type | Src Addre |
|---|---|---|---|---|
| 1 | 2021-05-26 02:46:21 | Intrusion Prev... | Brute-force att... | 192.200.1 |

| | |
|---|---|
| Time: | 2021-05-26 02:46:21 |
| Type: | Brute-force attack |
| Threat Level: | High |
| Protocol: | TCP |
| Action: | Deny |
| Vuln ID: | 11080016 |
| Vuln Name: | RDP_winxp Server medium and low attack encountered |
| Matched Policy: | Anti-Ransomware Policy_Business System |
| Description: | Attacker exploits RDP_winxp Protocol to launch brute-force attack.<br>Type: medium and low Attack started: 2021-05-25 20:01:12<br>Duration: 10123 seconds Attempts: 252 attacks Result: - |
| Recommendation: | Blacklist attacker IP address and contact server administrator for |

Step 4. If it is a false positive, you can add it as an exceptional case through the analysis and judgment based on logs to generate no alarm later.

## 4.2.2 Summary of Attack Events

The **Attack Events** page displays the security data from the dimension of business asset security. You can see the TOP 5 attack types and attack map as shown below.



| No. | Attacker IP | Location | Threat Level | Business Asset/Server | Description | Time | Status | Operation |
|---|---|---|---|---|---|---|---|---|
| 1 | 202.0.0.28 | Australia | High | 192.168.254.104<br>192.168.254.105 | system Vulnerability(... | Start Time: 2021-03-03 00:00:02<br>End Time: 2021-03-06 00:00:02 | Unblocked | Block Det... |

### Attack Types

It mainly displays the TOP 5 attack types detected recently as shown below.