# ANYWHERE Intrusion Detection

## Armor Knowledge Base

**Topics Discussed**

- Armor Knowledge Base

Review Widgets
Understand Intrusion Detection System (IDS)
Enable Trend Sub-Agent
- Recommendation Scans

Enable Intrusion Prevention Service
Export IDS Data
Log Search for Intrusion Detection

To fully use this screen, you must add the following permission to your account:

- Read IDS

You can use the **Intrusion Detection System** screen to view data from the host-based intrusion detection system (HIDS).

Intrusion Detection Systems (IDS) analyze network or host traffic and alert if that traffic matches signatures of known attacks. These events are correlated in our Security Information Event Management (SIEM) system, in combination with other security data, to alert on security threats.

This system provides an agent-based, intrusion detection service for network traffic analysis and reporting. Specifically, HIDS monitors for attack attempts.

HIDS policies focus on detecting OWASP top 10 events. Any observed attempts are delivered to Armor's advanced correlation engine for inspection and correlation with other collected logs.

## Review Widgets

| Widget | Description |
|---|---|
| **Top Signatures** | This widget displays the top 10 IDS events detected over the past 7 days, grouped together by signature. |
| **Top VMs** | This widget displays the top 10 IDS events detected over the past 7 days, grouped together by virtual machine. |

## Understand Intrusion Detection System (IDS)

This section displays details for all IDS events detected over the past 7 days.

| Column | Description |
|---|---|
| **Name** | This column displays the name of your virtual machine. |
| **Source IP** | This column displays the IP address of the signature. |
| **Source Port** | This column displays the port address of the signature. |
| **Destination IP** | This column displays the IP address of your virtual machine. |
| **Destination Port** | This column displays the port address of your virtual machine. |
| **Event Signature** | This column displays the the content of the signature. |
| **Event Timestamp** | This column displays the time and date when the event signature was detected. |
| **Count** | This column displays the number of event signatures that were detected. |

## Enable Trend Sub-Agent

As a prerequisite to installing Intrusion Prevention Services, you must install the Trend sub-agent. Use the following commands to manage the Trend sub-agent.

### Recommendation Scans

One of the features available in Agent 3.0 is Recommendation scans. Recommendation scans provide a good starting point for establishing a list of rules that you should implement. During a recommendation scan, the Armor Agent scans the operating system for installed applications, the Windows registry, open ports, and more. To take advantage of Recommendation scans, turn on Ongoing Recommendation scans in the Toolbox.

> Recommendation Scans work in tandem with the Auto-Apply configuration for IPS. The results of the Recommendation Scan can only be applied when Auto-Apply for the IPS service is turned on.

**Install Trend Sub-Agent:**

```
Windows: C:\.armor\opt\armor.exe trend install
Linux: /opt/armor/armor trend install
```

**Uninstall Trend Sub-Agent:**

```
Windows: C:\.armor\opt\armor.exe trend uninstall
Linux: /opt/armor/armor trend uninstall
```

**Trend Sub-Agent Status:**

```
Windows: C:\.armor\opt\armor.exe trend status
Linux: /opt/armor/armor trend status
```

**Turn On Recommended Scans:**

```
Windows: C:\.armor\opt\armor.exe trend ongoing-recommendation-scan on
Linux: /opt/armor/armor trend ongoing-recommendation-scan on
```

**Turn Off Recommended Scans:**

```
Windows: C:\.armor\opt\armor.exe trend ongoing-recommendation-scan off
Linux: /opt/armor/armor trend ongoing-recommendation-scan off
```

**Schedule a Recommended Scan (Runs on Next Trend Sub-Agent Heartbeat):**

```
Windows: C:\.armor\opt\armor.exe trend recommendation-scan
Linux: /opt/armor/armor trend recommendation-scan
```

**Set Recommendation Scan Interval:**

```
Windows: C:\.armor\opt\armor.exe trend set-recommendation-scan-interval <interval>
Linux: /opt/armor/armor set-recommendation-scan-interval <interval>
```

> Options are "24 Hours" "2 Days" "3 Days" "7 Days" "2 Weeks" "3 Weeks" "4 Weeks"

**Get Recommendation Scan Interval:**

```
Windows: C:\.armor\opt\armor.exe trend get-recommendation-scan-interval
Linux: /opt/armor/armor trend get-recommendation-scan-interval
```

**Trend Sub-Agent Help**

```
Windows: C:\.armor\opt\armor.exe trend help
Linux: /opt/armor/armor trend help
```

**Restart Trend:**

```
Windows: C:\.armor\opt\armor.exe trend service-restart
Linux: /opt/armor/armor trend service-restart
```

## Enable Intrusion Prevention Service

Use the following commands to manage the Intrusion Detection service.

**Turn On Detect Mode:**

```
Windows: C:\.armor\opt\armor.exe ips detect
Linux: /opt/armor/armor ips detect

Optional Parameters
Windows: C:\.armor\opt\armor.exe ips detect auto-apply-recommendations=on
Linux: /opt/armor/armor ips detect auto-apply-recommendations=on

Windows: C:\.armor\opt\armor.exe ips detect auto-apply-recommendations=off
Linux: /opt/armor/armor ips detect auto-apply-recommendations=off
```

> The Auto-Apply configuration for IPS works in tandem with Recommendation Scans. Only after a Recommendation Scan is run will there be policies to Auto-Apply.

**Turn On Prevent Mode:**

```
Windows: C:\.armor\opt\armor.exe ips prevent
Linux: /opt/armor/armor ips prevent

Optional Parameters
Windows: C:\.armor\opt\armor.exe ips prevent auto-apply-recommendations=on
Linux: /opt/armor/armor ips prevent auto-apply-recommendations=on

Windows: C:\.armor\opt\armor.exe ips prevent auto-apply-recommendations=off
Linux: /opt/armor/armor ips prevent auto-apply-recommendations=off
```

**Turn Off Prevent Mode:**

```
Windows: C:\.armor\opt\armor.exe ips off
Linux: /opt/armor/armor ips off
```

**List of Available IPS Rules:**

```
Windows: C:\.armor\opt\armor.exe ips list-available-rules
Linux: /opt/armor/armor ips list-available-rules
```

**List of Assigned IPS Rules on Policy:**

```
Windows: C:\.armor\opt\armor.exe ips list-assigned-rules
Linux: /opt/armor/armor ips list-assigned-rules
```

**Assign IPS Rules:**

```
Windows: C:\.armor\opt\armor.exe ips assign-rules
Linux: /opt/armor/armor ips assign-rules
```

**Un-Assign IPS Rule:**

```
Windows: C:\.armor\opt\armor.exe ips unassign-rule
Linux: /opt/armor/armor ips unassign-rule
```

**Intrusion Detection Help**

```
Windows: C:\.armor\opt\armor.exe ips help
Linux: /opt/armor/armor ips help
```

## Export IDS Data

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Intrusion Detection.**
3. (Optional) Use the filter function to customize the data displayed.
4. Below the table, click **CSV**.
    - You have the option to export all of the data (**All**), or only the data that appears on the current screen (**Current Set**).

## Log Search for Intrusion Detection

Users can search for HIDS events in Log Search. For instructions on how to access and use Log Search, please see our documentation here.

An example of HIDS logs can be seen below:

| | |
|---|---|
| t parsed.trendmicro.action | IDS:Reset |
| t parsed.trendmicro.category | Intrusion Prevention |
| t parsed.trendmicro.cn1 | 108395 |
| t parsed.trendmicro.cn1_label | Host ID |
| t parsed.trendmicro.cn3 | 0 |
| t parsed.trendmicro.cn3_label | DPI Packet Position |
| t parsed.trendmicro.count | 1 |
| t parsed.trendmicro.cs2 | ACK PSH |
| t parsed.trendmicro.cs2_label | TCP Flags |
| t parsed.trendmicro.cs3 | DF 0 |
| t parsed.trendmicro.cs3_label | Fragmentation Bits |
| t parsed.trendmicro.cs5 | 0 |
| t parsed.trendmicro.cs5_label | DPI Stream Position |
| t parsed.trendmicro.cs6 | 0 |
| t parsed.trendmicro.cs6_label | DPI Flags |
| t parsed.trendmicro.description | Multiple SSH Connections Detected (ATT&CK T1498.001, T1110) |
| t parsed.trendmicro.ds_frame_type | IP |
| t parsed.trendmicro.ds_tenant | Primary |
| t parsed.trendmicro.ds_tenant_id | 0 |
| t parsed.trendmicro.dst_ip | 198.98.49.181 |
| t parsed.trendmicro.dst_mac | 00:00:00:00:00:00 |
| t parsed.trendmicro.dst_port | 37432 |
| t parsed.trendmicro.dvchost | 1024__dcf895a4-e43b-4fa7-8d6d-9a0ef2c46f43 |
| t parsed.trendmicro.name | Multiple SSH Connections Detected (ATT&CK T1498.001, T1110) |
| t parsed.trendmicro.out | 0 |
| t parsed.trendmicro.proto | tcp |
| t parsed.trendmicro.severity | 6 |
| t parsed.trendmicro.src_ip | 172.31.34.105 |
| t parsed.trendmicro.src_mac | 0A:DA:ED:94:3E:9E |
| t parsed.trendmicro.src_port | 22 |

For a full list of Log Search fields and descriptions, please visit our glossary here.



Was this helpful?

Your Rating: 

Results:  14 rates