Threat Research

Threat Research is generated from a set of rules that are applied to the inspection engine to detect threats and malicious activity. This page allows you to view these rules. Once a day, Multicloud Defense searches for new or modified rules for network intrusion and includes or removes rules and known malicious sources from the internal library. This action is automated. Included in this function is the act of downloading and validating the new list of IP addresses as sources and implementing them in new rulesets. These rulsesets are then deployed.

The rules have a variety of ways in which they are organized such as policy, class, application, ruleset library date, and other parameters. If you are interested in understanding more about a rule that has tripped (e.g., detected a threat or malicious activity), use the **Threat Research** page to view more details about the rule. The following parts of each of the page are available for your use:

Search Bar

The search bar at the top of the window allows you to search each page under threat research for any singular dientifying facet: a known IP address, action, rule name, gateway name, attack type, or profile name. If you find a specific field value by scrolling, you can **Add to Search** to facilitate an easier search experience.

Note that the searches are isolated to each page, and you cannot cross-search the different types of threat research. See the section below for more details.

View Details

Each of the facets under threat research offer the ability to **View Details** of a singular incident or attack. The values provided in these details differ between the types of threat research, but can be valuable if you want to finetune your policies, security profiles, rules or rulesets.

Add to Search

For any of the types of research available here, you can click on any one value within a row and automatically have the option to **Add to Search**. This automatically applies the selected value to the search bar at the top of the window and filteres the viewing window to the content in the search bar. You can do this multiple times and the values you select compound into a complex search request.

Network Intrusion

Network intrusion refers to any unauthorized activity on your network. Note that this tabl does not include the built-in rules to the IDS/IPS engine or any affiliated information from these rules; these rules are designated for detection only; the remainder of the IDS/IPS rules are configured to protect and perform actions based on the varying levels of intrusion or attack.

The Network Intrusion page displays the following:

- **Gateway Names** - the names of the affected gateways that processed the malicious source.
- **Profile Names** - the names of the security profiles triggered by the malicious source.
- **IPS Policy** - the policy within Multicloud Defense triggered by the event or attack.
- **IPS Class** - the type of attack as deteremined by the database of attack signatures traffic is compared against.
- **IPS Category** - the IPS signature category triggered by the event or attack.
- **Rule ID** - the rule ID as documented internally within Multicloud Defense that was triggered by the event or attack.
- **Services Impacted** - the type of web service affected by the event or attack.
- **Impact** - the severity level of impact, known or assumed, by the event or attack.
- **Message** - the contents of the event that has been identified as an attack.
- **Rule Content** - content of the rule triggered by the event or attack.
- **CVSS Score** - Common Vulnerability Scoring System (CVSS) is a framework that assigns a numerical score to the severity of an information security vulnerability. CVSS scores range from 0 to 10, with 10 being the most severe.
- **CVEs** - Common Vulnerabilities and Exposures (CVE) is a glossary that classifies vulnerabilities. Is there is a CVE associated with the type of attack or event, the internal library automatically generates its value here.
- **References** - If publicly available, this link directs you to the original announcement and categorization of the CVE.

Web Protection

The Web Application Firewall (WAF) research is displayed as "Web Protection" This lets you secure your devices against web threats and helps you regulate unwanted content. The Web Protection page displays the following:

- **Gateway Names** - the names of the affected gateways that processed the malicious source.
- **Profile Names** - the names of the security profiles triggered by the malicious source.
- **CRS Category** - the Core Rule Set (CRS) category identified per set of generic attack detection rules.

- **Inspection Type** - the type of inspection Multicloud Defense peformed on the traffic that encapsulated the attack or event.
- **Attack Type** - the type of unauthorized attack traversed over a network.
- **Platform** - the platform type identified from the attack or event.
- **Lanuage** - the noted web developtment language detected from the event.

Malicious Sources

Malicious sources are any type of code or packet that causes harm to a network. The Malicious Sources page dispalys the following:

- **Gateway Names** - the names of the affected gateways that processed the malicious source.
- **Profile Names** - the names of the security profiles triggered by the malicious source.
- **Malicious Sources Action** - the action taken when the malicious source was identified.
- **Impact** - the impact of the malicious material deteremined by how it is ranked within the library.
- **Malicious Source IP** - the IP address where the malicious source originates from.