Vectra Triage Report

Report Reference: VTR-

Report Date:



Findings

The Vectra Triage Service has identified the following metrics and potential improvements to your triage health.

Rules That Have Not Triggered in the Last 3 Months

There are rules on your system that have not triggered in at least 3 months. There are no active detections affected by these rules. The behavior may no longer be expected on your network or the rule has been consolidated elsewhere.

|  |  |  |
| --- | --- | --- |
| **Original Detection Name** | **ID** | **Rule Name** |
| «1\_detection\_name» | «1\_id» | «1\_rule\_name» |

**Recommendations**

Verify these rules are still required, and do not require additional tuning.

Rules That Have Not Triggered in the Last 6 Months

There are rules on your system that have not triggered in at least 6 months. There are no detections in the system that are affected by these rules. The behavior may no longer be expected on your network or the rule has been consolidated elsewhere.

|  |  |  |  |
| --- | --- | --- | --- |
| **Original Detection Name** | **ID** | **Rule Name** | |
|  |  |  |

**Recommendations**

All rules are candidates to be deleted.

Mark as Custom with Same Names, Rule Creation may be Beneficial (Past Month)

These detections were triaged through one time “Mark as Custom”. This can be highly useful for behaviors you understand are authorized but want to be alerted upon. This table may however identify a rule that you want to implement. “Mark as Custom” does not affect model learnings and detections triaged this way may continue to arise.

|  |  |  |
| --- | --- | --- |
| **Count** | **Original Detection Name** | **Rule Name** |
| «3\_count» | «3\_detection\_name» | «3\_rule\_name» |

**Recommendations**

These rules may be candidates for a permanent triage filter, though other detections here may represent behaviors that are desirable to be notified of regularly (e.g. administrative activities on sensitive systems). Consider creating triage filters for entries in this list.

Currently Active Detections Not Triaged by Rule

These are the detections currently active in Detect and contributing to Host Score.

|  |  |
| --- | --- |
| **Count** | **Detection Type** |
| «4\_count» | «4\_detection\_type» |

**Recommendations**

These are the most common untriaged detections in the environment. Similarities here indicate repeated behavior of external services including OpenDNS, Office365, GSuite, or Salesforce. Internal services including Adobe products, Cisco Wireless devices, Patch Management / Inventory, vulnerability scanners and others may also be observed here. Review these detections and create triage filters for expected and verified behaviors. Unexpected behaviors should be investigated to determine the cause.

Currently Active Detections Including Triaged

These are all active detections in Detect, including those not contributing to Host Score. This may help identify improperly scoped rules.

|  |  |
| --- | --- |
| **Count** | **Detection Type** |
| «5\_count» | «5\_detection\_type» |

**Recommendations**

N/A

Top 50 Source IPs of Currently Active Detection Type Not Caught by a Triage Rule

This table helps identify your noisiest machines on the network. This can either indicate a compromise or ongoing and expected behavior. In the latter case, one or more Custom Filter can usually be created. This table is expected to be fewer than 50 entries if there are fewer than 50 hosts with active detections.

|  |  |
| --- | --- |
| **Count** | **Source IP** |
| «6\_count» | «6\_source\_ip» |

**Recommendations**

Hosts in the above table can include print servers, administrative workstations, inventory and vulnerability scanners, and other hosts performing their expected roles. Review these detections and create triage filters for expected and verified behaviors. Unexpected behaviors should be investigated to determine the cause.

Top 50 Source IPs Divided by Active Detection Type Not Caught by a Triage Rule

This table helps identify your noisiest machines on the network by detection type. This usually indicated an ongoing and expected behavior. One or more Customer Filter can usually be created. This table is expected to be fewer than 50 entries if there are fewer than 50 hosts with active detections.

|  |  |  |
| --- | --- | --- |
| **Count** | **Detection Type** | **Source IP** |
| «7\_count» | «7\_detection\_type» | «7\_source\_ip» |

**Recommendations**

Similar to the previous table, this table focuses on hosts by detection type to help narrow down certain behaviors.

Top 50 Destination Domains Divided by Active Detection Type Not Caught by a Triage Rule

This table helps identify the most common destination domains of your active detections. This usually indicates a common behavior on your network that can be triaged on your system.

Common destinations include SaaS, and commonly used internal systems. This table is expected to be fewer than 50 entries if there are fewer than 50 unique destination domains.

|  |  |  |  |
| --- | --- | --- | --- |
| **Count** | **Detection Type** | **Destination Domain** | **Destination Port** |
| «8\_count» | «8\_detection\_type» | «8\_destination\_domain» | «8\_destination\_port» |

**Recommendations**

N/A

Top 50 Destination Domain Requests for Suspect Domain Activity

This tables identifies the most common suspicious domains detected on your network. Large detection counts may indicate a large-scale campaign. This table is expected to be fewer than 50 entries if there are fewer than 50 unique destination domains.

|  |  |  |  |
| --- | --- | --- | --- |
| **Count** | **Detection Type** | **Destination Domain** | **Response** |
| «9\_count» | «9\_detection\_type» | «9\_destination\_domain» | «9\_response» |

**Recommendations**

While these should be investigated, a suspicious domain will trigger on the host querying / connecting to the domain, as well as DNS servers (possibly including Active Directory domain controllers since they can function as DNS servers), firewalls, proxies, and other infrastructure. In most cases triage filters can be created for DNS servers and egress infrastructure, though other detections should be reviewed.

Top 50 Destination IPs Divided by Active Detection Type Not Caught by a Triage Rule

This table identified the most common destination IPs detected on your network. Large detection counts may indicate an expected behavior or misconfiguration. This table is expected to be fewer than 50 entries if there are fewer than 50 unique destination IPs.

|  |  |  |
| --- | --- | --- |
| **Count** | **Detection Type** | **Destination IP** |
| «10\_count» | «10\_detection\_type» | «10\_destination\_ip» |

**Recommendations**

N/A

Top 50 Destination Ports by Detection Type Not Caught by a Triage Rule

This table identifies the most common destination ports by detection type. Large detection counts may indicate an expected behavior. This table is expected to be fewer than 50 entries if there are fewer than 50 active detections.

|  |  |  |
| --- | --- | --- |
| **Count** | **Detection Type** | **Destination Port** |
| «11\_count» | «11\_detection\_type» | «11\_destination\_port» |

Whitelists

|  |  |
| --- | --- |
| **Rule Name** | **ID** |
| «12\_rule\_name» | «12\_id» |

Custom Filters with Any-Any

|  |  |
| --- | --- |
| **Rule Name** | **ID** |
| «13\_rule\_name» | «13\_id» |

Empty Groups

|  |  |
| --- | --- |
| **Group Name** | **ID** |
| «14\_group\_name» | «14\_id» |