Detection and Response Dashboard

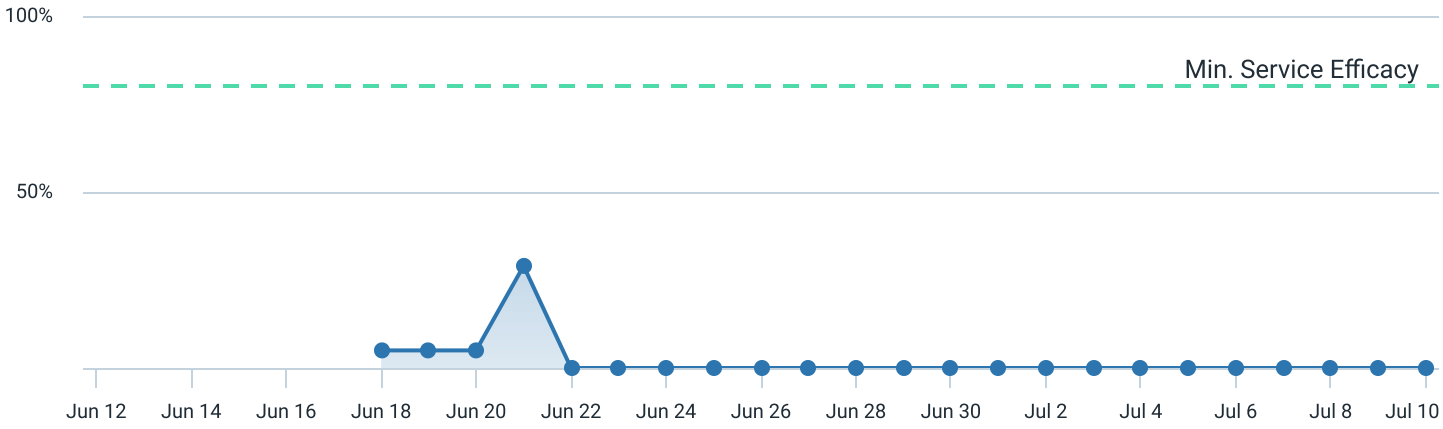
June 11, 2025 04:59 PM UTC - July 11, 2025 04:59 PM UTC

Generated on July 11, 2025

Estimated Agent Coverage

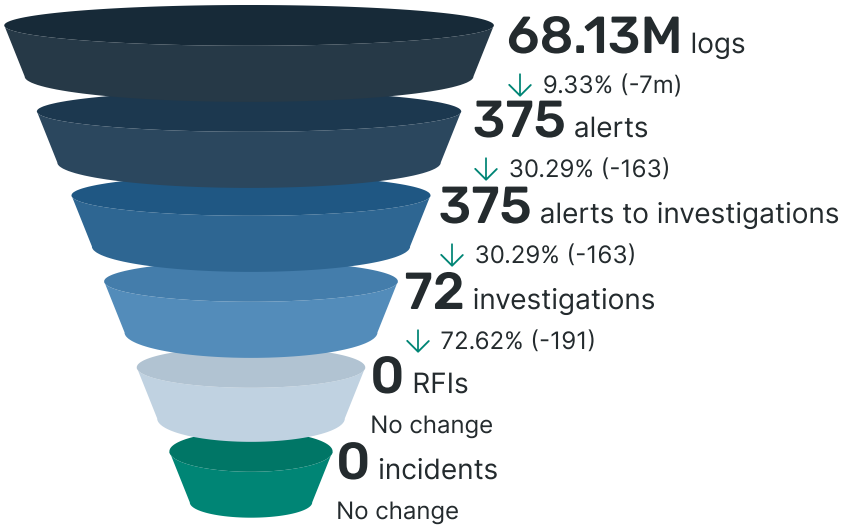
Powered by Surface Command

Assets with an Insight Agent 0%



Threat Pipeline

How alerts are progressing through qualifying stages



Detection and Response Dashboard

June 11, 2025 04:59 PM UTC - July 11, 2025 04:59 PM UTC

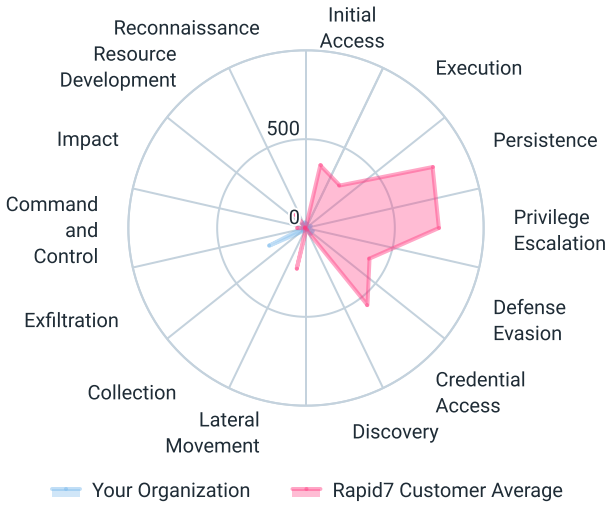
Generated on July 11, 2025

Incidents

Incidents **0** No change

No incident within the last year

Alerts By MITRE Tactic



Detection and Response Dashboard

June 11, 2025 04:59 PM UTC - July 11, 2025 04:59 PM UTC

Generated on July 11, 2025

Alerts Generated

↓ 30.29% (-163) from previous 30 days

2,259 Alerts Closed

↑ 431.52% (+1.8k) from previous 30 days

263 Investigations Closed

↑ 3.13% (+8) from previous 30 days

38 Critical and High Investigations Closed

↓ 56.32% (-49) from previous 30 days

0 Incidents Created

No change from previous 30 days

Detection and Response Dashboard

June 11, 2025 04:59 PM UTC - July 11, 2025 04:59 PM UTC

Generated on July 11, 2025

Top 5 Alert Types

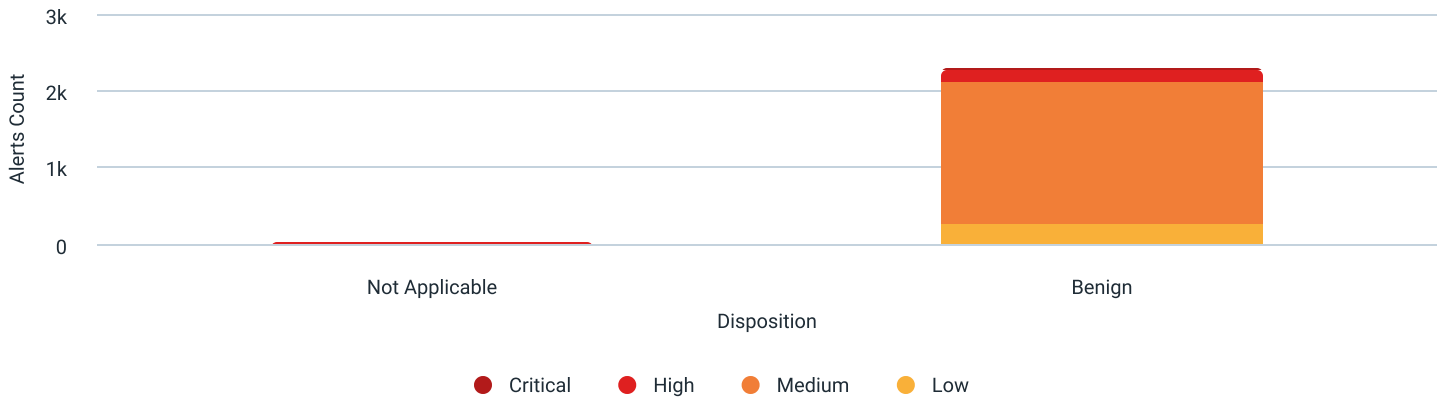
The types of alerts that occur most frequently in your environment.

Alert Type	Trend	Alerts	Priority
ET MALWARE Covenant Framework HTTP Beacon		224	
Endpoint Detection - On-Access Scanning Detected Malware		15	
AWS CloudTrail - Creating Access Keys		10	
Attacker Technique - Reg.exe disabling the User Access Control (UAC) remote restriction		7	
Amazon GuardDuty - PrivilegeEscalation:Kubernetes/PrivilegedContainer		7	

Closed Alerts by Priority and Disposition

Disposition is the decision taken on the alert by analysts

Malicious **0** No change



Detection and Response Dashboard

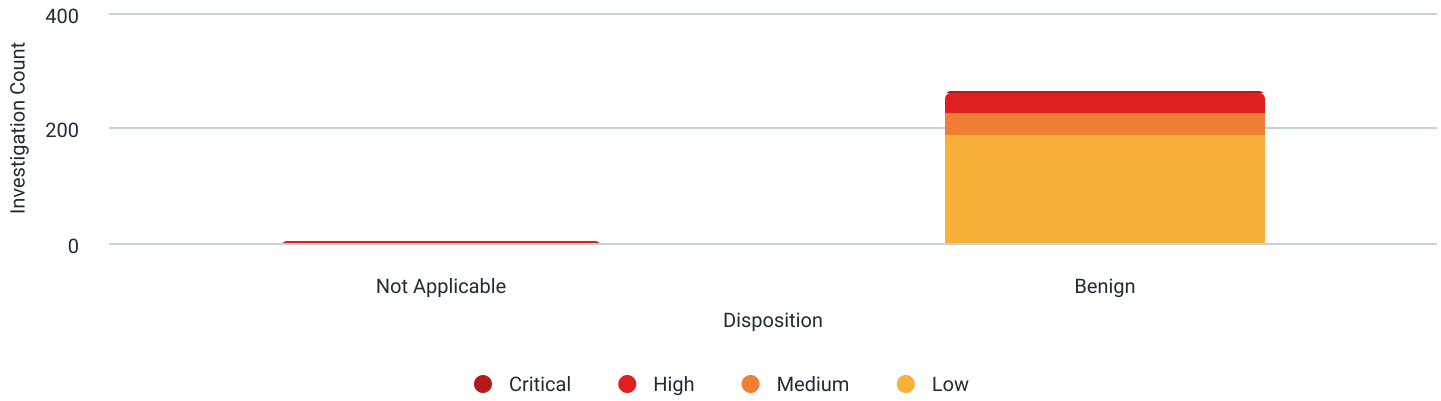
June 11, 2025 04:59 PM UTC - July 11, 2025 04:59 PM UTC

Generated on July 11, 2025

Closed Investigations by Priority and Disposition

Disposition is the decision taken on the investigation by analysts

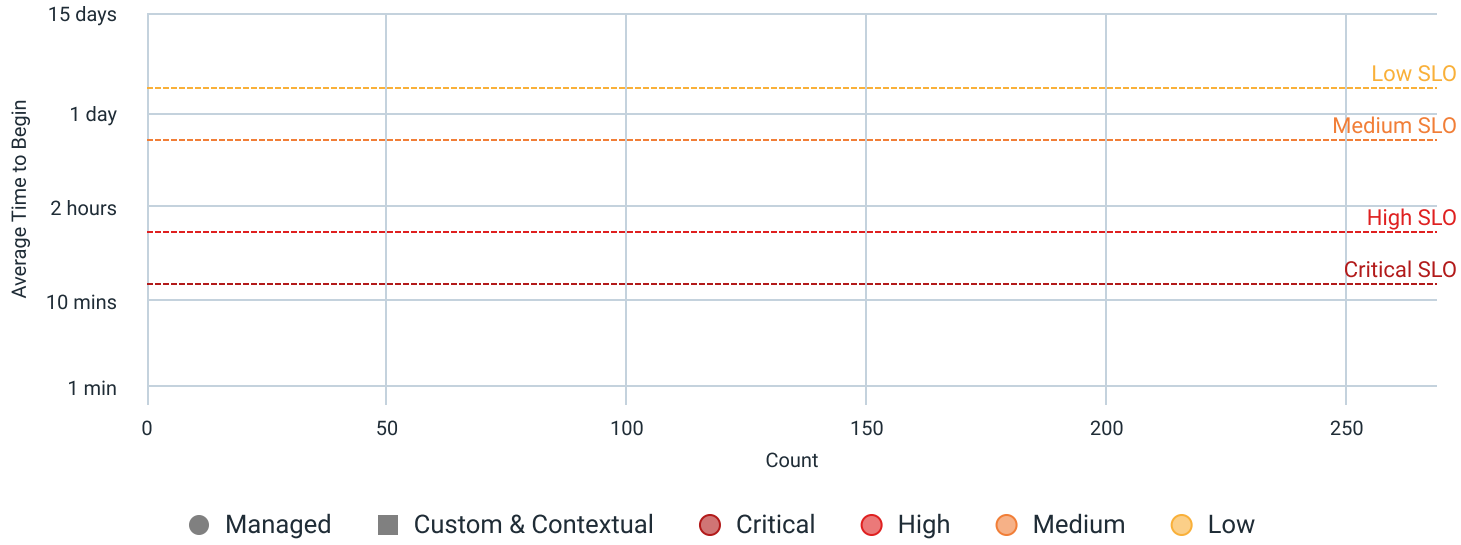
Malicious **0** No change



Mean Time to Begin Alert Investigation

How quickly are analysts investigating potential threats and are they achieving SLOs?

Managed N/A Custom & Contextual N/A



Detection and Response Dashboard

June 11, 2025 04:59 PM UTC - July 11, 2025 04:59 PM UTC

Generated on July 11, 2025

2,747 Admin Users

↓ 35.5% (-1.5k)
from previous 30 days

1 Users with Non-Expiring Passwords

— No change
from previous 30 days

0 Service Accounts with Non-Expiring...

No change
from previous 30 days

Risky User Permissions Over Time

Total Risky Permissions ↓ 35.71% (-1.5k)