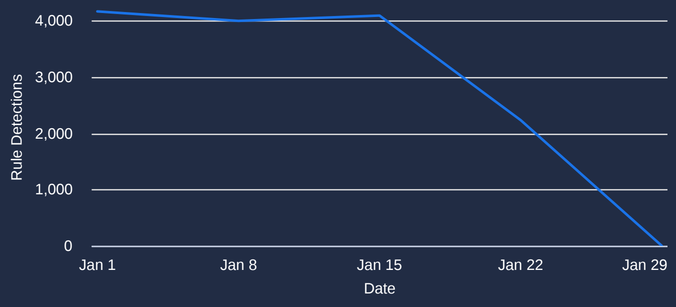
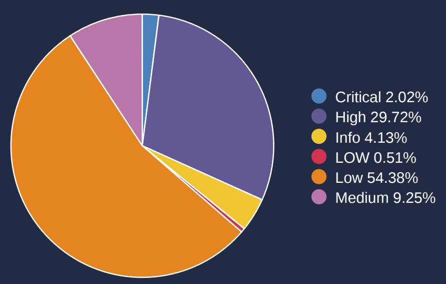
# Rule Detections

Time is in the last 1 month

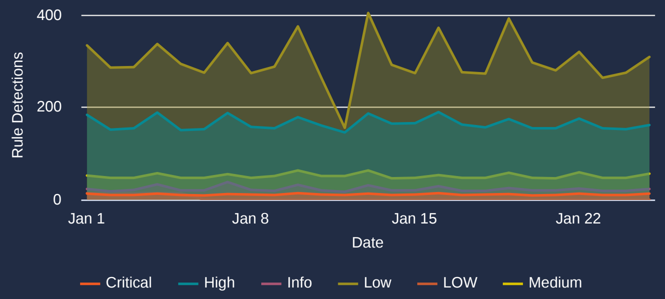
## Rule Detections Over Time



## Rule Detections by Severity



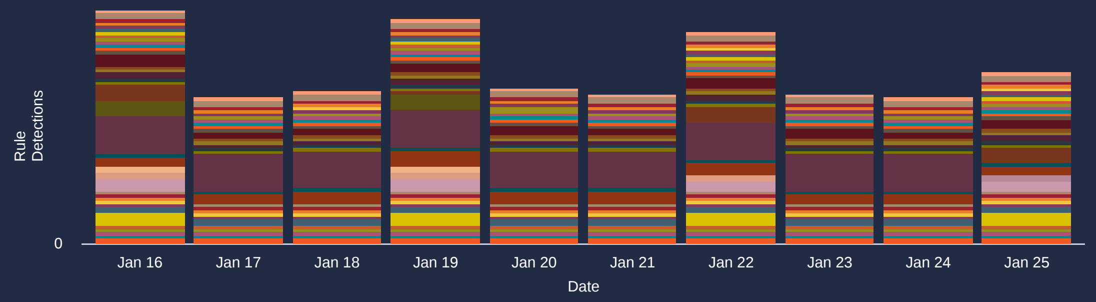
## Rule Detections by Severity Over Time



## Top 10 Rule Names by Detections

| rule_name | Count for Drill |
|---|---|
| active | 503 |
| gcti_malicious_file_process_launch | 498 |
| info_bat | 365 |
| whois_expired_domain_accessed | 289 |
| aws_guardduty_tor_network_activity_detected | 288 |
| gcti_tor_exit_nodes | 225 |
| SCC: BigQuery Extraction with DLP Context | 192 |
| gcti_tor_exit_nodes | 153 |
| GCP Multi-Project Billing Disabled | 125 |
| geoip_user_login_from_multiple_states_or_countries | 125 |

## Rule Detections by Name Over Time



## Top 10 Users by Rule Detections

| User Name with Link | Rule Detections |
|---|---|
| ∅ | 2,706 |
| admin | 1,666 |
| admin@my-demo-project.iam.gserviceaccou… | 1,129 |
| lisawalker | 834 |
| arn:aws:iam::127632175811:root | 729 |
| Administrator | 685 |
| user | 612 |
| SYSTEM | 513 |
| oscar.wild | 456 |
| admin@myexamplecompany.com | 427 |

## Top 10 Asset Names by Rule Detections

| Hostname | Rule Detections |
|---|---|
| ∅ | 5,810 |
| serhatg.local | 2,114 |
| 188.26.220.193 | 1,026 |
| wins-d19 | 908 |
| oscar.wild.desktop | 456 |
| wrk-shasek.stackedpads.local | 391 |
| prod-linux | 336 |
| activedir.stackedpads.local | 298 |
| win-server.lunarstiiiness.com | 295 |
| milton-waddams-pc | 249 |

## Top 10 IPs by Rule Detections

| detection.assets.asset_ip_address | Rule Detections |
|---|---|
| ∅ | 10,117 |
| 79.116.179.124 | 724 |
| 79.116.213.193 | 482 |
| 104.198.226.161 | 389 |
| 79.154.246.114 | 325 |
| 98.43.161.174 | 244 |
| 79.116.179.125 | 181 |
| 209.182.77.149 | 166 |
| 10.164.0.28 | 134 |
| 73.69.155.20 | 133 |

Generated by Looker on January 25, 2024 at 12:16 PM PST