# Monthly Security Report – February 2024

## Note:

This document serves as a sample of our Monthly Security Report, tailored for one of our clients. Originally classified, the document it has been reclassified to ”Unclassified” status with the express consent of the client involved.

All confidential information has been meticulously redacted to ensure privacy and security. As such, this version offers a glimpse into our standard reporting methodology, demonstrating the rigor and detail we apply to our security analysis on a regular basis.

It is important to note that in this specific instance, our role encompasses Security Monitoring, Detection, Analysis, and Recommendations. The responsibility for implementing the Response phase lies solely with the client.

Nevertheless, we also offer comprehensive services in Response, Containment, Isolation, and Eradication, standing ready to excel in these areas with our well-prepared and prolific capabilities.

# Table of Contents

# Executive Summary

As your committed Managed Detection and Response (MDR) service provider, HoundBytes is dedicated to ensuring the security and integrity of your digital assets. This executive summary outlines our key achievements in February 2024, demonstrating our ongoing commitment to enhancing your cybersecurity posture and delivering on our promises.

This month, our Security Operations Center (SOC) has been pivotal in addressing and mitigating a range of sophisticated cyber threats. Our continued investment in our infrastructure, including the integration of 3 new VPN servers, has significantly fortified our network security, enabling us to monitor and counteract cyber threats more effectively.

Our efforts have yielded a significant reduction in false-positive security alerts, streamlining security operations and ensuring that our focus remains on genuine threats. This enhancement has not only improved operational efficiency but also ensured that your security posture remains both resilient and responsive to the evolving cyber threat landscape.

A key highlight of our recent operations includes the detection and neutralization of the NetSupport RAT malware on an organizational laptop. This swift action prevented unauthorized access and potential data compromise, underscoring our commitment to protecting your organization from advanced security threats.

# Client-Centric Security Enhancements

With the strategic network expansion, the addition of new VPN servers has strengthened our network security, enhancing our ability to safeguard your digital assets from potential threats.

By focusing on threat detection, our refined monitoring protocols ensure that our vigilance is effectively targeted, minimizing distractions and maximizing the relevance of our security efforts.

Based on proactive Threat Mitigation, the rapid identification and neutralization of the NetSupport RAT malware exemplifies our proactive stance in safeguarding your organization against sophisticated cyber threats.

# Conclusion

The strategic enhancements and diligent efforts of HoundBytes' SOC reflect our unwavering commitment to providing superior cybersecurity services. Our focus on reducing false positives, along with our effective response to advanced malware, illustrates our dedication to enhancing your security and operational efficiency. Our promise is to maintain a vigilant, responsive, and robust defense against cyber threats, ensuring the safety and resilience of your digital environment. As we move forward, HoundBytes will continue to prioritize your security needs, deploying advanced measures to protect against the challenges of today and tomorrow.

# Security Operations Overview

The numbers for February: 40k+ (40,187 ) alerts generated which resulted in 39k (39,567) processed alerts:

**Severity levels**

| Levels | Count ↓ |
|---|---|
| Low | 29k+ |
| High | 3k+ |
| Medium | 3k+ |
| Critical | 2k+ |


39k+ processed alerts which entered under investigation in 412 cases with a total of 26,459 alerts and an average of 15 minutes in response, the rest were closed, acknowledged, or whitelisted as normal behavior.

However, some Cases response time appears to be longer because they require additional inputs from your system administrators or developers. Even after our team completed the investigation, these cases needed further verification or actions from other departments, which sometimes extended the response time.

## Alerts and investigations, Key Metrics and Performance Indicators

We received over 40k+ alerts in February, out of which 26,459 alerts needed investigation. This unusually high figure is largely attributed to the generation of noise from atypical system configurations and operations. The alerts span a broad range of categories, with a significant False-Positive portion originating from command-and-control beacon activities, along with several types of network traffic and system operations. The data suggests an imperative need to refine our alert configurations and review our system operations to enhance focus on actual security threats and minimize false alarms **and the whitelist procedures where Security Analysts worked on.**

Each of these investigations was carried out meticulously, ensuring that no stone was left unturned in our pursuit of maintaining your system's security.

# Cases

| Name | Tags | Alerts | Category | Created On | Closed On | Status | Severity |
|---|---|---|---|---|---|---|---|
| Multiple Alerts caused by SOC investigation | SOC Team | 5 | SOC_Investigation | Feb 29, 2024 @ 20:06:22 | Feb 29, 2024 @ 20:06:30.341 | Closed | Low |
| Multiple Scans (1 Packet, Event Duration 0) | scan | 3 | network | Feb 29, 2024 @ 19:59:15 | Feb 29, 2024 @ 19:59:25.390 | Closed | Low |
| System configuration - ***.***.eu | true-positive | 31 | Host Detection | Feb 29, 2024 @ 19:57:14 | Feb 29, 2024 @ 20:12:01.950 | Closed | Low |
| Multiple Discovery Alerts made by admins | true-positive | 18 | Host Detection | Feb 29, 2024 @ 19:13:15 | Feb 29, 2024 @ 20:12:05.358 | Closed | Low |

- Classified - Confidential -

| Name | Tags | Alerts | Category | Created On | Closed On | Status | Severity |
|---|---|---|---|---|---|---|---|
| Multiple discovery alerts made by *** | true-positive | 155 | Host Detection | Feb 29, 2024 @ 19:04:30 | Feb 29, 2024 @ 19:06:47.074 | Closed | Low |
| SMTP Scans (Out of Exception) | scan | 28 | network | Feb 29, 2024 @ 18:45:13 | Feb 29, 2024 @ 20:12:09.288 | Closed | Low |
| Multiple Alerts on desktop-*** - Windows | windows | 7 | Host Detection | Feb 29, 2024 @ 18:37:15 | Feb 29, 2024 @ 18:37:26.956 | Closed | Low |
| TI Hash | Threat-Intel | 12 | Host Detection | Feb 29, 2024 @ 17:25:31 | Feb 29, 2024 @ 17:26:19.530 | Closed | High |
| Multiple Scans (1 Packet, Event Duration 0) | scan | 3 | network | Feb 29, 2024 @ 15:24:48 | Feb 29, 2024 @ 15:25:02.060 | Closed | Low |
| SMB Scans on a Host | scan | 10 | network | Feb 29, 2024 @ 15:22:16 | Feb 29, 2024 @ 20:12:13.489 | Closed | Low |
| Multiple Alerts Involving a User | true-positive | 53 | Host Detection | Feb 29, 2024 @ 15:09:48 | Feb 29, 2024 @ 20:12:16.906 | Closed | Low |
| Alerts on desktop-***-Windows | windows | 1 | Host Detection | Feb 29, 2024 @ 11:12:49 | Feb 29, 2024 @ 11:17:00.525 | Closed | Low |
| SMTP Scans by Malicious Hosts | scan | 14 | network | Feb 29, 2024 @ 07:36:30 | Feb 29, 2024 @ 07:36:43.445 | Closed | Low |
| TI IP Address Indicator Match - 45.227.254.26 | Threat-Intel | 6 | network | Feb 29, 2024 @ 07:24:24 | Feb 29, 2024 @ 07:26:21.936 | Closed | Low |
| Multiple Scans (1 Packet, Event Duration 0) | scan | 6 | network | Feb 29, 2024 @ 03:03:02 | Feb 29, 2024 @ 07:18:38.958 | Closed | Low |
| Multiple Alerts Involving a User | true-positive | 9 | Host Detection | Feb 29, 2024 @ 02:14:05 | Feb 29, 2024 @ 07:20:24.177 | Closed | Low |
| SMTP Scans by Malicious Host | scan | 5 | network | Feb 29, 2024 @ 00:38:23 | Feb 29, 2024 @ 00:38:32.230 | Closed | Low |
| win11-vm test station alerts | SOC Team | 10 | — | Feb 29, 2024 @ 00:11:43 | Feb 29, 2024 @ 00:11:53.339 | Closed | Low |

- Classified - Confidential -

- Classified - Confidential -

| Name | Tags | Alerts | Category | Created On | Closed On | Status | Severity |
|---|---|---|---|---|---|---|---|
| Multiple Alerts Involving a User | true-positive | 9 | Host Detection | Feb 28, 2024 @ 21:07:54 | Feb 28, 2024 @ 21:08:05.652 | Closed | Low |
| SMTP Scans by Benign Host | scan | 6 | network | Feb 28, 2024 @ 20:40:39 | Feb 28, 2024 @ 20:41:16.276 | Closed | Low |
| Multiple Scans (1 Packet, Event Duration 0) | scan | 6 | network | Feb 28, 2024 @ 20:17:11 | Feb 28, 2024 @ 20:17:20.725 | Closed | Low |
| TI ***.***. - etcd | Threat-Intel | 12 | network | Feb 28, 2024 @ 17:49:04 | 17 minutes ago | Closed | Low |
| Multiple alerts - admins | — | 18 | Host Detection | Feb 28, 2024 @ 17:30:40 | Feb 28, 2024 @ 17:35:01.993 | Closed | Low |
| BAU ** & *** - admins | — | 12 | Host Detection | Feb 28, 2024 @ 17:20:01 | Feb 28, 2024 @ 17:24:28.753 | Closed | Low |
| razvanj multiple alerts | — | 16 | Host Detection | Feb 28, 2024 @ 17:11:30 | Feb 28, 2024 @ 17:17:59.732 | Closed | Low |
| SOC investigation | SOC Team | 5 | SOC_Investigation | Feb 28, 2024 @ 16:01:00 | Feb 28, 2024 @ 16:02:06.401 | Closed | Low |
| ***.***. backuppc | — | 10 | Host Detection | Feb 28, 2024 @ 14:45:22 | Feb 28, 2024 @ 14:46:23.941 | Closed | Low |
| SMTP scans out of exceptions | scan | 11 | true-positive | Feb 28, 2024 @ 14:15:04 | Feb 28, 2024 @ 14:23:31.085 | Closed | Low |
| ***.***. BAU | — | 12 | Host Detection | Feb 28, 2024 @ 13:26:40 | Feb 28, 2024 @ 14:43:56.258 | Closed | Low |
| desktop-*** browser | lovense | 13 | Host Detection | Feb 28, 2024 @ 12:36:22 | Feb 28, 2024 @ 12:49:33.749 | Closed | Low |
| *** BAU | enumeration | 30 | Host Detection | Feb 28, 2024 @ 11:37:09 | Feb 28, 2024 @ 11:41:53.246 | Closed | Low |
| ***docker | host | 2 | true-positive | Feb 28, 2024 @ 10:48:58 | Feb 28, 2024 @ 11:27:19.891 | Closed | Low |
| desktop-**** driver load | host | 1 | true-positive | Feb 28, 2024 @ 10:30:56 | Feb 28, 2024 @ 10:41:05.693 | Closed | Low |
| IPSEC Scans | scan | 4 | network | Feb 28, 2024 @ 05:09:26 | Feb 28, 2024 @ 05:09:42.281 | Closed | Low |
| Windows desktop-*** | windowslovense | 29 | Host Detection | Feb 28, 2024 @ 04:41:58 | Feb 28, 2024 @ 04:42:14.746 | Closed | Low |

- Classified - Confidential -

- Classified - Confidential -

| Name | Tags | Alerts | Category | Created On | Closed On | Status | Severity |
|---|---|---|---|---|---|---|---|
| SMTP Scans | scan | 5 | network | Feb 28, 2024 @ 04:23:35 | Feb 28, 2024 @ 06:07:55.898 | Closed | Low |
| Discovery processes | system-configuration | 4 | Host Detection | Feb 28, 2024 @ 04:16:01 | Feb 28, 2024 @ 07:28:22.087 | Closed | Low |
| Multiple Scans (1 Packet, Event Duration 0) | scan | 7 | network | Feb 28, 2024 @ 04:13:39 | Feb 28, 2024 @ 07:54:26.528 | Closed | Low |
| SMB Scans on a Host | scan | 6 | network | Feb 28, 2024 @ 04:10:09 | Feb 28, 2024 @ 04:10:21.288 | Closed | Low |
| SOC Investigation | SOC Team | 22 | SOC_Investigation | Feb 28, 2024 @ 03:54:35 | Feb 28, 2024 @ 06:07:50.021 | Closed | Low |
| CL_Utility.ps1 | false-positive | 1 | Host Detection | Feb 28, 2024 @ 00:41:39 | Feb 28, 2024 @ 00:47:27.056 | Closed | Low |
| System Administrator Activity - *** | system-configuration | 5 | Host Detection | Feb 28, 2024 @ 00:32:23 | Feb 28, 2024 @ 00:33:12.374 | Closed | Low |
| Multiple Alerts Involving a User | true-positive | 15 | Host Detection | Feb 27, 2024 @ 23:27:06 | Feb 28, 2024 @ 04:24:00.108 | Closed | Low |
| SMTP Scans by Malicious Host | scan | 6 | network | Feb 27, 2024 @ 18:55:37 | Feb 27, 2024 @ 18:55:45.237 | Closed | Low |
| TI IP Address Indicator Match - 45.227.254.26 | Threat-Intel | 12 | network | Feb 27, 2024 @ 17:19:33 | Feb 27, 2024 @ 17:19:46.052 | Closed | Low |
| SMB Scans on a Host | scan | 5 | network | Feb 27, 2024 @ 16:40:39 | Feb 27, 2024 @ 16:41:00.358 | Closed | Low |
| System Administrator Activity | system-configuration | 141 | Host Detection | Feb 27, 2024 @ 12:50:34 | Feb 27, 2024 @ 17:53:55.559 | Closed | Low |
| Multiple Scans (1 Packet, Event Duration 0) | scan | 6 | network | Feb 27, 2024 @ 11:54:32 | Feb 27, 2024 @ 17:53:51.619 | Closed | Low |
| Multiple Alerts Involving a User | true-positive | 11 | Host Detection | Feb 27, 2024 @ 11:05:09 | Feb 27, 2024 @ 16:06:15.855 | Closed | Low |
| WinRed Project Alerts | SOC Team | 47 | — | Feb 27, 2024 @ 10:13:05 | Feb 27, 2024 @ 17:53:59.267 | Closed | Low |

- Classified - Confidential -

| Name | Tags | Alerts | Category | Created On | Closed On | Status | Severity |
|---|---|---|---|---|---|---|---|
| System Administrator Activity | system-configuration | 10 | Host Detection | Feb 27, 2024 @ 09:56:42 | Feb 27, 2024 @ 09:56:49.948 | Closed | Low |
| VM Configuration by System Administrator | system-configuration | 13 | Host Detection | Feb 27, 2024 @ 09:52:29 | Feb 27, 2024 @ 10:10:23.112 | Closed | Low |
| Oddjob PID file creation | system-configuration | 8 | Host Detection | Feb 27, 2024 @ 09:39:16 | Feb 27, 2024 @ 09:39:28.161 | Closed | Low |
| Multiple False Positive Discovery Alerts | false-positive | 5 | Host Detection | Feb 27, 2024 @ 07:04:41 | Feb 27, 2024 @ 07:05:51.729 | Closed | Low |
| SOC Investigation | false-positive | 32 | SOC_Investigation | Feb 27, 2024 @ 06:55:35 | Feb 27, 2024 @ 06:55:48.164 | Closed | Low |
| SMTP Scans (Out of Exceptions) | scan | 26 | network | Feb 27, 2024 @ 06:50:07 | Feb 27, 2024 @ 08:00:04.271 | Closed | Low |
| Multiple Scans (1 Packet, Event Duration 0) | scan | 3 | network | Feb 27, 2024 @ 06:00:02 | Feb 27, 2024 @ 06:00:18.658 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 17 | Host Detection | Feb 27, 2024 @ 05:56:36 | Feb 27, 2024 @ 07:39:29.134 | Closed | Low |
| SMB Scans on a Host | scan | 6 | network | Feb 27, 2024 @ 05:54:00 | Feb 27, 2024 @ 05:54:45.296 | Closed | Low |
| Suspicious System Commands Executed - numactl | system-configurationfalse-positive | 1 | Host Detection | Feb 27, 2024 @ 01:14:53 | Feb 27, 2024 @ 01:15:55.249 | Closed | Low |
| Multiple Scans (1 Packet, Event Duration 0) | scan | 3 | network | Feb 27, 2024 @ 00:14:05 | Feb 27, 2024 @ 00:14:19.849 | Closed | Low |
| Suspicious Network Connection Attempt by Root | dockerfalse-positive | 3 | network | Feb 26, 2024 @ 23:13:41 | Feb 26, 2024 @ 23:14:03.091 | Closed | Low |
| Multiple Scans (1 Packet, Event Duration 0) | scan | 27 | network | Feb 26, 2024 @ 16:02:07 | Feb 26, 2024 @ 19:24:13.106 | Closed | Low |

- Classified - Confidential -

| Name | Tags | Alerts | Category | Created On | Closed On | Status | Severity |
|---|---|---|---|---|---|---|---|
| SMTP Scan by SOC Team | SOC Team | 15 | SOC_Investigation | Feb 26, 2024 @ 15:57:58 | Feb 26, 2024 @ 15:58:11.373 | Closed | Low |
| TI Hash | Threat-Intel | 5 | Host Detection | Feb 26, 2024 @ 15:51:25 | Feb 27, 2024 @ 20:19:28.768 | Closed | High |
| Multiple Discovery processes | system-configuration | 32 | Host Detection | Feb 26, 2024 @ 15:06:23 | Feb 26, 2024 @ 18:39:38.289 | Closed | Low |
| SOC Investigation | SOC Team | 5 | Host Detection | Feb 26, 2024 @ 14:27:05 | Feb 26, 2024 @ 15:06:45.912 | Closed | Low |
| User & rabbitmq standard activity 2 | host | 49 | Host Detection | Feb 26, 2024 @ 14:25:17 | Feb 26, 2024 @ 18:39:12.869 | Closed | Low |
| SMTP Scans (Out of Exceptions) | networktrue-positive | 49 | network | Feb 26, 2024 @ 13:10:05 | Feb 26, 2024 @ 13:20:16.024 | Closed | Low |
| User & rabbitmq standard activity | host | 9 | Host Detection | Feb 26, 2024 @ 12:59:45 | Feb 26, 2024 @ 13:20:26.914 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 115 | network | Feb 26, 2024 @ 10:12:38 | Feb 26, 2024 @ 20:08:28.911 | Closed | Low |
| SOC Investigation | false-positive | 20 | SOC_Investigation | Feb 25, 2024 @ 19:43:44 | Feb 25, 2024 @ 19:58:12.332 | Closed | Low |
| Multiple False Positive Discovery Alerts | false-positive | 15 | Host Detection | Feb 25, 2024 @ 19:40:43 | Feb 25, 2024 @ 19:58:20.481 | Closed | Low |
| SMTP Scans 25 Feb | scan | 31 | network | Feb 25, 2024 @ 18:09:36 | Feb 25, 2024 @ 19:58:16.084 | Closed | Low |
| SMB Scans on a host | scan | 4 | network | Feb 25, 2024 @ 17:53:36 | Feb 25, 2024 @ 17:53:48.724 | Closed | Low |
| Multiple Scans (1 Packet, Event Duration 0) | scan | 3 | network | Feb 25, 2024 @ 16:39:13 | Feb 25, 2024 @ 16:40:26.320 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 68 | network | Feb 25, 2024 @ 15:19:25 | Feb 25, 2024 @ 19:28:06.684 | Closed | Low |
| Multiple Scans (1 Packet, Event Duration 0) | scan | 3 | network | Feb 25, 2024 @ 10:12:33 | Feb 25, 2024 @ 10:13:01.403 | Closed | Low |

- Classified - Confidential -

| Name | Tags | Alerts | Category | Created On | Closed On | Status | Severity |
|---|---|---|---|---|---|---|---|
| Multiple Scans (1 Packet, Event Duration 0) | scan | 3 | network | Feb 25, 2024 @ 04:18:16 | Feb 25, 2024 @ 04:18:47.475 | Closed | Low |
| Multiple Alerts Involving a User | true-positive | 23 | Host Detection | Feb 25, 2024 @ 01:11:41 | Feb 25, 2024 @ 07:51:31.983 | Closed | Low |
| SMTP Scans by Malicious Host | scan | 52 | network | Feb 24, 2024 @ 20:34:13 | Feb 24, 2024 @ 20:34:29.949 | Closed | Low |
| Multiple Scans (1 Packet, Event Duration 0) | scan | 6 | network | Feb 24, 2024 @ 20:28:55 | Feb 24, 2024 @ 20:29:20.607 | Closed | Low |
| Multiple Alerts Involving a User | true-positive | 69 | Host Detection | Feb 24, 2024 @ 20:26:28 | Feb 24, 2024 @ 23:56:05.858 | Closed | Low |
| TI IP Address Indicator Match - 45.95.147.236 | Threat-Intel | 121 | network | Feb 24, 2024 @ 20:16:52 | Feb 24, 2024 @ 23:58:08.775 | Closed | Low |
| Multiple Scans (1 Packet, Event Duration 0) | scan | 4 | network | Feb 24, 2024 @ 04:29:18 | Feb 24, 2024 @ 07:46:39.925 | Closed | Low |
| SMTP Scans 24 Feb | scan | 29 | network | Feb 24, 2024 @ 04:26:33 | Feb 24, 2024 @ 07:46:35.102 | Closed | Low |
| Multiple Discovery processes | false-positive | 18 | Host Detection | Feb 24, 2024 @ 04:10:03 | Feb 24, 2024 @ 07:46:31.128 | Closed | Low |
| TI IP Address Indicator Match - 45.95.147.236 | Threat-Intel | 24 | network | Feb 23, 2024 @ 22:46:56 | Feb 24, 2024 @ 04:10:35.327 | Closed | Low |
| Multiple Alerts Involving a User | discovery | 54 | Host Detection | Feb 23, 2024 @ 20:52:52 | Feb 24, 2024 @ 04:10:30.779 | Closed | Low |
| TI IP Address Indicator Match - 45.95.147.236 | Threat-Intel | 2 | network | Feb 23, 2024 @ 18:19:40 | Feb 23, 2024 @ 18:19:51.568 | Closed | Low |
| SMB Scans on a host | scan | 6 | network | Feb 23, 2024 @ 17:13:30 | Feb 23, 2024 @ 17:13:39.554 | Closed | Low |

- Classified - Confidential -

| Name | Tags | Alerts | Category | Created On | Closed On | Status | Severity |
|---|---|---|---|---|---|---|---|
| Multiple Scans (1 Packet, Event Duration 0) | scan | 3 | network | Feb 23, 2024 @ 15:49:59 | Feb 23, 2024 @ 15:50:21.876 | Closed | Low |
| Alerts Triggered by Microcode and Kernel Update | system-update | 501 | Host Detection | Feb 23, 2024 @ 14:33:23 | Feb 23, 2024 @ 15:50:40.505 | Closed | Low |
| SMTP Scans by Malicious Host | scan | 21 | network | Feb 23, 2024 @ 11:39:57 | Feb 23, 2024 @ 15:48:31.866 | Closed | Low |
| Program Uninstall on Windows endpoint | windows | 4 | network | Feb 23, 2024 @ 11:12:59 | Feb 23, 2024 @ 15:49:03.083 | Closed | Low |
| Multiple Alerts Involving a User | discoverytrue-positive | 61 | Host Detection | Feb 23, 2024 @ 09:50:15 | Feb 23, 2024 @ 17:00:24.500 | Closed | Low |
| Multiple Scans (1 Packet, Event Duration 0) | scan | 3 | network | Feb 23, 2024 @ 07:59:54 | Feb 23, 2024 @ 08:00:05.987 | Closed | Low |
| SMB Scans on a host | scan | 6 | network | Feb 23, 2024 @ 07:19:29 | Feb 23, 2024 @ 07:19:39.410 | Closed | Low |
| Multiple False Positive Discovery Alerts | false-positive | 6 | Host Detection | Feb 23, 2024 @ 03:10:00 | Feb 23, 2024 @ 03:10:13.862 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 62 | Host Detection | Feb 23, 2024 @ 03:05:32 | Feb 23, 2024 @ 07:58:54.226 | Closed | Low |
| SMTP Scans 23 Feb | scan | 22 | network | Feb 23, 2024 @ 02:00:40 | Feb 23, 2024 @ 02:03:41.891 | Closed | Low |
| Multiple Scans (1 Packet, Event Duration 0) | scan | 3 | network | Feb 23, 2024 @ 01:51:12 | Feb 23, 2024 @ 01:52:21.015 | Closed | Low |
| SOC Investigation | SOC Teamfalse-positive | 78 | SOC_Investigation | Feb 23, 2024 @ 01:22:30 | Feb 23, 2024 @ 01:25:12.182 | Closed | Low |
| TI IP Indicator Match - 45.227.254.26 & 45.95.147.236 | Threat-Intel | 286 | network | Feb 22, 2024 @ 20:53:45 | Feb 23, 2024 @ 03:04:11.711 | Closed | Low |

- Classified - Confidential -

- Classified - Confidential -

| Name | Tags | Alerts | Category | Created On | Closed On | Status | Severity |
|---|---|---|---|---|---|---|---|
| SMTP Scans Feb 22nd | scan | 14 | network | Feb 22, 2024 @ 19:41:30 | Feb 22, 2024 @ 19:42:23.132 | Closed | Low |
| Discovery processes | false-positive | 160 | Host Detection | Feb 22, 2024 @ 17:14:24 | Feb 22, 2024 @ 19:45:15.562 | Closed | Low |
| Enumeration of Kernel Modules | dracutfalse-positive | 634 | Host Detection | Feb 22, 2024 @ 14:38:41 | Feb 22, 2024 @ 17:13:33.657 | Closed | Low |
| Discovery processes by admin *** & *** | false-positive | 71 | Host Detection | Feb 22, 2024 @ 14:14:10 | Feb 22, 2024 @ 15:23:43.853 | Closed | Low |
| Multiple Scans (1 Packet, Event Duration 0) | scan | 8 | network | Feb 22, 2024 @ 12:48:26 | Feb 22, 2024 @ 19:45:21.830 | Closed | Low |
| Discovery processes by admin paulc | dockerfalse-positive | 4 | Host Detection | Feb 22, 2024 @ 12:20:19 | Feb 22, 2024 @ 12:45:32.391 | Closed | Low |
| SMTP Scans Feb 22nd | scan | 37 | network | Feb 22, 2024 @ 11:50:05 | Feb 22, 2024 @ 17:14:43.353 | Closed | Low |
| Discovery processes by admin ** | false-positive | 10 | Host Detection | Feb 22, 2024 @ 11:24:44 | Feb 22, 2024 @ 12:45:37.193 | Closed | Low |
| Discovery processes | false-positive | 188 | Host Detection | Feb 22, 2024 @ 10:47:04 | Feb 22, 2024 @ 12:45:46.810 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 74 | Host Detection | Feb 22, 2024 @ 10:34:50 | Feb 22, 2024 @ 10:39:50.766 | Closed | Low |
| Cron Job Created - *** | false-positive | 2 | Host Detection | Feb 21, 2024 @ 19:57:34 | Feb 21, 2024 @ 19:57:43.504 | Closed | Low |
| Multiple Scans (1 Packet, Event Duration 0) | scan | 3 | network | Feb 21, 2024 @ 18:41:48 | Feb 21, 2024 @ 18:42:30.910 | Closed | Low |
| SOC Investigation | false-positive | 92 | SOC_Investigation | Feb 21, 2024 @ 18:20:45 | Feb 21, 2024 @ 19:58:23.521 | Closed | Low |
| SMTP Scans 21 Feb | scan | 37 | network | Feb 21, 2024 @ 18:15:36 | Feb 21, 2024 @ 19:58:39.828 | Closed | Low |
| Multiple False Positive Discovery Alerts | false-positive | 33 | Host Detection | Feb 21, 2024 @ 17:52:13 | Feb 21, 2024 @ 19:58:18.628 | Closed | Low |

- Classified - Confidential -

- Classified - Confidential -

| Name | Tags | Alerts | Category | Created On | Closed On | Status | Severity |
|---|---|---|---|---|---|---|---|
| Noise by host *** | false-positive | 5 | Host Detection | Feb 21, 2024 @ 17:47:08 | Feb 21, 2024 @ 17:47:17.325 | Closed | Low |
| SMB Scans on a host | scan | 4 | network | Feb 21, 2024 @ 17:44:27 | Feb 21, 2024 @ 17:44:43.399 | Closed | Low |
| Multiple Scans (1 Packet, Event Duration 0) | scan | 3 | network | Feb 21, 2024 @ 14:28:11 | Feb 21, 2024 @ 14:30:00.897 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 71 | Host Detection | Feb 21, 2024 @ 14:23:27 | Feb 21, 2024 @ 19:58:14.744 | Closed | Low |
| SMTP Scans 21 Feb | scan | 17 | network | Feb 21, 2024 @ 05:49:42 | Feb 21, 2024 @ 05:49:56.817 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 19 | Host Detection | Feb 21, 2024 @ 01:56:18 | Feb 21, 2024 @ 03:23:38.528 | Closed | Low |
| Multiple Scans (1 Packet, Event Duration 0) | scan | 3 | network | Feb 21, 2024 @ 00:54:48 | Feb 21, 2024 @ 00:55:08.763 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 51 | Host Detection | Feb 20, 2024 @ 21:30:23 | Feb 21, 2024 @ 00:51:18.583 | Closed | Low |
| SMB Scans on a host | scan | 5 | network | Feb 20, 2024 @ 21:26:34 | Feb 20, 2024 @ 21:26:47.221 | Closed | Low |
| SMTP Scans 20 Feb | scan | 50 | network | Feb 20, 2024 @ 21:08:37 | Feb 21, 2024 @ 00:51:12.213 | Closed | Low |
| Multiple Scans (1 Packet, Event Duration 0) | scan | 3 | network | Feb 20, 2024 @ 20:54:44 | Feb 20, 2024 @ 20:54:55.046 | Closed | Low |
| TI IP Address Indicator Match - 45.227.254.26 | Threat-Intel | 12 | network | Feb 20, 2024 @ 20:38:49 | Feb 20, 2024 @ 21:08:53.519 | Closed | Low |
| Ionut - AnyDesk | hostfalse-positive | 1 | Host Detection | Feb 20, 2024 @ 16:53:01 | Feb 20, 2024 @ 17:22:02.235 | Closed | Low |
| Traian - admin - BAU | host | 50 | Host Detection | Feb 20, 2024 @ 16:07:40 | Feb 20, 2024 @ 16:13:04.027 | Closed | Low |
| TI - 91.215.85.17 | Threat-Intel | 8 | network | Feb 20, 2024 @ 15:48:38 | Feb 20, 2024 @ 15:58:43.209 | Closed | Low |

- Classified - Confidential -

- Classified - Confidential -

| Name | Tags | Alerts | Category | Created On | Closed On | Status | Severity |
|---|---|---|---|---|---|---|---|
| SMTP scans, event.duration>0 | network | 28 | network | Feb 20, 2024 @ 15:29:47 | Feb 20, 2024 @ 15:37:28.469 | Closed | Low |
| Internet scans - duration 0 | network | 3 | network | Feb 20, 2024 @ 15:01:09 | Feb 20, 2024 @ 15:02:23.175 | Closed | Low |
| CL_Utility.ps1 | false-positive | 2 | Host Detection | Feb 20, 2024 @ 13:20:32 | Feb 20, 2024 @ 14:34:27.223 | Closed | Low |
| Multiple alerts translation-tool | false-positive | 125 | Host Detection | Feb 20, 2024 @ 10:31:47 | Feb 20, 2024 @ 10:38:40.942 | Closed | Low |
| IPSEC Scan 20 Feb | scan | 5 | network | Feb 20, 2024 @ 03:42:10 | Feb 20, 2024 @ 07:01:25.620 | Closed | Low |
| SMTP Scans | scan | 32 | network | Feb 20, 2024 @ 03:40:02 | Feb 20, 2024 @ 07:01:20.241 | Closed | Low |
| Cron Job Created - *** | false-positive | 6 | Host Detection | Feb 20, 2024 @ 01:41:20 | Feb 20, 2024 @ 01:41:39.948 | Closed | Low |
| SMB Scans on a host 20 Feb | scan | 7 | Host Detection | Feb 20, 2024 @ 00:36:58 | Feb 20, 2024 @ 06:14:06.743 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 39 | Host Detection | Feb 20, 2024 @ 00:29:50 | Feb 20, 2024 @ 00:30:02.688 | Closed | Low |
| SMB Scans on a host 19 Feb | scan | 4 | network | Feb 19, 2024 @ 18:59:46 | Feb 19, 2024 @ 18:59:59.442 | Closed | Low |
| Alerts on desktop-*** - Windows | windowsfalse -positive | 3 | Host Detection | Feb 19, 2024 @ 18:49:02 | Feb 19, 2024 @ 18:49:28.505 | Closed | Low |
| Multiple Scans (1 Packet, Event Duration 0) | scan | 5 | network | Feb 19, 2024 @ 18:39:25 | Feb 19, 2024 @ 18:39:32.353 | Closed | Low |
| SMTP Scans on a host 19 Feb | scan | 25 | network | Feb 19, 2024 @ 18:29:14 | Feb 19, 2024 @ 18:29:32.445 | Closed | Low |
| Cron Job Created - *** | false-positive | 12 | Host Detection | Feb 19, 2024 @ 18:21:20 | Feb 19, 2024 @ 18:21:38.901 | Closed | Low |
| Alerts Caused by Openvswitch Restart | system-confi guration | 238 | Host Detection | Feb 19, 2024 @ 16:46:22 | Feb 19, 2024 @ 18:56:26.673 | Closed | Low |

- Classified - Confidential -

- Classified - Confidential -

| Name | Tags | Alerts | Category | Created On | Closed On | Status | Severity |
|---|---|---|---|---|---|---|---|
| SMTP Scans 19 Feb | scan | 48 | network | Feb 19, 2024 @ 09:44:05 | Feb 19, 2024 @ 11:23:19.612 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 77 | Host Detection | Feb 19, 2024 @ 09:29:48 | Feb 19, 2024 @ 18:15:59.988 | Closed | Low |
| SMB Scans 19 Feb | scan | 5 | network | Feb 19, 2024 @ 04:49:44 | Feb 19, 2024 @ 04:49:54.175 | Closed | Low |
| Multiple Scan Alerts Discovery [Custom] | scan | 1 | network | Feb 19, 2024 @ 03:24:24 | Feb 19, 2024 @ 03:26:21.790 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 45 | Host Detection | Feb 19, 2024 @ 03:19:25 | Feb 19, 2024 @ 07:58:39.678 | Closed | Low |
| IPSEC Scans 19 Feb | scan | 71 | network | Feb 19, 2024 @ 03:17:37 | Feb 19, 2024 @ 08:00:46.736 | Closed | Low |
| SMTP Scans 19 Feb | scan | 321 | network | Feb 19, 2024 @ 03:14:24 | Feb 19, 2024 @ 08:00:43.797 | Closed | Low |
| Noise by host *** | false-positive | 28 | Host Detection | Feb 19, 2024 @ 02:12:54 | Feb 19, 2024 @ 07:55:01.138 | Closed | Low |
| Cron Job Created - *** | false-positive | 8 | Host Detection | Feb 19, 2024 @ 01:27:39 | Feb 19, 2024 @ 07:58:54.147 | Closed | Low |
| IPSEC Scans 18 Feb | scan | 21 | network | Feb 18, 2024 @ 23:27:24 | Feb 19, 2024 @ 00:41:25.251 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 24 | Host Detection | Feb 18, 2024 @ 23:18:32 | Feb 19, 2024 @ 00:39:34.912 | Closed | Low |
| SMTP Scans 18 Feb | scan | 148 | network | Feb 18, 2024 @ 23:12:59 | Feb 19, 2024 @ 00:41:30.097 | Closed | Low |
| SMB Scans 18 Feb | scan | 5 | network | Feb 18, 2024 @ 22:47:04 | Feb 18, 2024 @ 22:47:24.767 | Closed | Low |
| SMTP Scans 18 Feb | scan | 297 | network | Feb 18, 2024 @ 17:34:50 | Feb 18, 2024 @ 20:00:40.804 | Closed | Low |
| IPSEC Scans 18 Feb | scan | 72 | network | Feb 18, 2024 @ 17:32:46 | Feb 18, 2024 @ 20:00:47.035 | Closed | Low |
| Discovery processes | false-positive | 40 | Host Detection | Feb 18, 2024 @ 11:48:23 | Feb 18, 2024 @ 11:48:41.339 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 86 | Host Detection | Feb 18, 2024 @ 11:43:57 | Feb 18, 2024 @ 11:45:00.758 | Closed | Low |

- Classified - Confidential -

- Classified - Confidential -

| Name | Tags | Alerts | Category | Created On | Closed On | Status | Severity |
|---|---|---|---|---|---|---|---|
| SMTP Scans 18 Feb | scan | 703 | network | Feb 18, 2024 @ 11:38:47 | Feb 18, 2024 @ 13:29:26.069 | Closed | Low |
| SMB Scans 18 Feb | scan | 11 | Host Detection | Feb 18, 2024 @ 11:35:37 | Feb 18, 2024 @ 11:45:11.520 | Closed | Low |
| IPSEC Scans 18 Feb | scan | 305 | network | Feb 18, 2024 @ 11:32:16 | Feb 18, 2024 @ 13:29:21.217 | Closed | Low |
| TI IP Address Indicator Match - 45.227.254.26 | Threat-Intel | 12 | network | Feb 18, 2024 @ 11:26:58 | Feb 18, 2024 @ 11:45:06.216 | Closed | Low |
| SOC Investigation | false-positive | 6 | SOC_Investigation | Feb 17, 2024 @ 18:41:02 | Feb 17, 2024 @ 18:58:44.968 | Closed | Low |
| SMB Scans 17 Feb | scan | 5 | network | Feb 17, 2024 @ 18:17:23 | Feb 17, 2024 @ 19:56:21.295 | Closed | Low |
| IPSEC Scans 17 Feb | scan | 96 | network | Feb 17, 2024 @ 16:04:30 | Feb 17, 2024 @ 19:58:59.452 | Closed | Low |
| Testing new rule | false-positive | 7 | SOC_Investigation | Feb 17, 2024 @ 15:44:47 | Feb 17, 2024 @ 15:46:04.687 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 58 | Host Detection | Feb 17, 2024 @ 15:39:37 | Feb 17, 2024 @ 19:59:04.418 | Closed | Low |
| SMTP Scans 17 Feb | scan | 317 | network | Feb 17, 2024 @ 15:33:03 | Feb 17, 2024 @ 19:59:06.652 | Closed | Low |
| TI IP Address Indicator Match - 45.227.254.26 | Threat-Intelscan | 12 | network | Feb 17, 2024 @ 15:01:44 | Feb 17, 2024 @ 18:03:20.166 | Closed | Low |
| Cron Job Created - *** | false-positive | 16 | Host Detection | Feb 17, 2024 @ 12:36:48 | Feb 17, 2024 @ 19:57:46.502 | Closed | Low |
| SOC Investigation | false-positive | 6 | SOC_Investigation | Feb 17, 2024 @ 10:58:39 | Feb 17, 2024 @ 10:59:08.115 | Closed | Low |
| Noise by host *** | false-positive | 171 | Host Detection | Feb 17, 2024 @ 10:43:30 | Feb 17, 2024 @ 18:18:28.177 | Closed | Low |
| SMB Scans 17 Feb | scan | 11 | network | Feb 17, 2024 @ 10:36:51 | Feb 17, 2024 @ 15:46:08.791 | Closed | Low |
| TI IP Address Indicator Match - 45.227.254.26 | Threat-Intel | 12 | network | Feb 17, 2024 @ 07:00:18 | Feb 17, 2024 @ 10:38:10.703 | Closed | Low |
| SMTP Scans 17 Feb | scan | 361 | network | Feb 17, 2024 @ 04:12:58 | Feb 17, 2024 @ 10:31:21.063 | Closed | Low |
| IPSEC Scans 17 Feb | scan | 207 | network | Feb 17, 2024 @ 02:36:48 | Feb 17, 2024 @ 10:41:13.678 | Closed | Low |

- Classified - Confidential -

- Classified - Confidential -

| Name | Tags | Alerts | Category | Created On | Closed On | Status | Severity |
|---|---|---|---|---|---|---|---|
| Multiple Alerts Involving a User | false-positive | 67 | Host Detection | Feb 17, 2024 @ 01:18:33 | Feb 17, 2024 @ 10:32:39.321 | Closed | Low |
| Cron Job Created - *** | false-positive | 20 | Host Detection | Feb 17, 2024 @ 00:23:45 | Feb 17, 2024 @ 10:02:05.687 | Closed | Low |
| Alerts Triggered by Sysadmin File Modification | system-configuration | 2 | Host Detection | Feb 16, 2024 @ 23:45:39 | Feb 16, 2024 @ 23:45:50.192 | Closed | Low |
| Alerts on desktop-*** - Windows | windowsfalse-positive | 8 | Host Detection | Feb 16, 2024 @ 22:28:57 | Feb 16, 2024 @ 23:26:02.534 | Closed | Low |
| SMTP Scans 16 Feb | scan | 515 | network | Feb 16, 2024 @ 22:21:55 | Feb 16, 2024 @ 23:47:36.247 | Closed | Low |
| IPSEC Scans 16 Feb | scan | 45 | network | Feb 16, 2024 @ 22:14:28 | Feb 16, 2024 @ 23:47:33.192 | Closed | Low |
| Cron Job Created - *** | false-positive | 20 | Host Detection | Feb 16, 2024 @ 21:57:30 | Feb 16, 2024 @ 23:47:29.141 | Closed | Low |
| SMB Scans 16 Feb | scan | 36 | network | Feb 16, 2024 @ 21:47:18 | Feb 16, 2024 @ 23:47:26.156 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 96 | Host Detection | Feb 16, 2024 @ 21:41:54 | Feb 16, 2024 @ 23:47:22.352 | Closed | Low |
| TI IP Address Indicator Match - 45.227.254.26 | Threat-Intel | 12 | network | Feb 16, 2024 @ 21:27:02 | Feb 16, 2024 @ 21:27:21.197 | Closed | Low |
| TI IP Address Indicator Match - 91.215.85.17 | Threat-Intel | 22 | network | Feb 16, 2024 @ 21:12:36 | Feb 16, 2024 @ 21:12:47.020 | Closed | Low |
| Alerts Triggered by Microcode and Kernel Update | system-update | 882 | Host Detection | Feb 16, 2024 @ 20:42:44 | Feb 16, 2024 @ 21:03:08.876 | Closed | Low |
| Internet Scans | network | 86 | network | Feb 16, 2024 @ 11:25:27 | Feb 16, 2024 @ 11:26:52.441 | Closed | Low |
| TI 91.215.85.17 | network | 16 | network | Feb 16, 2024 @ 10:42:18 | Feb 16, 2024 @ 10:53:43.473 | Closed | Low |
| **client** admin *** (BAS) | host | 10 | Host Detection | Feb 16, 2024 @ 10:31:10 | Feb 16, 2024 @ 10:33:21.092 | Closed | Low |

- Classified - Confidential -

- Classified - Confidential -

| Name | Tags | Alerts | Category | Created On | Closed On | Status | Severity |
|---|---|---|---|---|---|---|---|
| HB SOC investigation | hostfalse-positive | 5 | SOC_Investigation | Feb 16, 2024 @ 10:27:53 | Feb 16, 2024 @ 10:28:27.152 | Closed | Low |
| *** well known crons | hostfalse-positive | 6 | Host Detection | Feb 16, 2024 @ 10:25:14 | Feb 16, 2024 @ 11:46:56.691 | Closed | Low |
| SMB scans | network | 16 | network | Feb 16, 2024 @ 10:16:04 | Feb 16, 2024 @ 10:19:29.653 | Closed | Low |
| SMTP scans | network | 45 | network | Feb 16, 2024 @ 10:12:46 | Feb 16, 2024 @ 10:14:48.023 | Closed | Low |
| noise **** | — | 365 | SOC_Investigation | Feb 16, 2024 @ 10:02:45 | Feb 16, 2024 @ 10:07:15.920 | Closed | Low |
| SMB Scans 16 Feb | scan | 10 | Host Detection | Feb 16, 2024 @ 05:02:34 | Feb 16, 2024 @ 07:42:10.234 | Closed | Low |
| SMTP Scans 16 Feb | scan | 424 | network | Feb 16, 2024 @ 04:58:53 | Feb 16, 2024 @ 07:42:05.357 | Closed | Low |
| IPSEC Scans 16 Feb | scan | 50 | network | Feb 16, 2024 @ 04:51:17 | Feb 16, 2024 @ 07:42:00.362 | Closed | Low |
| Cron Job Created - *** | file-modification | 2 | Host Detection | Feb 16, 2024 @ 02:42:35 | Feb 16, 2024 @ 02:42:50.013 | Closed | Low |
| SMB Scans 16th of Feb | scan | 10 | Host Detection | Feb 16, 2024 @ 02:38:43 | Feb 16, 2024 @ 02:39:05.385 | Closed | Low |
| Kernel Module Removal - *** | ksplice | 8 | Host Detection | Feb 16, 2024 @ 02:34:39 | Feb 16, 2024 @ 03:41:33.105 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 16 | Host Detection | Feb 15, 2024 @ 23:39:04 | Feb 15, 2024 @ 23:41:32.599 | Closed | Low |
| TI IP Address Indicator Match - 91.215.85.17 | Threat-Intel | 32 | network | Feb 15, 2024 @ 23:36:26 | Feb 15, 2024 @ 23:41:37.480 | Closed | Low |
| Discovery processes | false-positive | 22 | Host Detection | Feb 15, 2024 @ 22:36:44 | Feb 15, 2024 @ 23:37:44.871 | Closed | Low |
| Discovery processes - ***.***.com | false-positive | 40 | Host Detection | Feb 15, 2024 @ 22:12:41 | Feb 15, 2024 @ 22:12:59.321 | Closed | Low |

- Classified - Confidential -

- Classified - Confidential -

| Name | Tags | Alerts | Category | Created On | Closed On | Status | Severity |
|---|---|---|---|---|---|---|---|
| Abnormal Process ID File Created by PHP-FPM | false-positive | 3 | Host Detection | Feb 15, 2024 @ 19:23:47 | Feb 15, 2024 @ 19:23:56.626 | Closed | Low |
| Alerts on desktop*** - Windows | windowsfalse-positive | 4 | Host Detection | Feb 15, 2024 @ 15:09:33 | Feb 15, 2024 @ 15:10:07.815 | Closed | Low |
| IPSEC Scans 15 Feb | scan | 25 | network | Feb 15, 2024 @ 15:00:50 | Feb 15, 2024 @ 15:01:33.806 | Closed | Low |
| SMTP Scans 15 Feb | scan | 137 | network | Feb 15, 2024 @ 14:54:58 | Feb 15, 2024 @ 14:55:42.612 | Closed | Low |
| TI IP Address Indicator Match - 45.227.254.26 | Threat-Intel | 6 | network | Feb 15, 2024 @ 14:51:09 | Feb 15, 2024 @ 14:51:19.330 | Closed | Low |
| SMB Scans 15 Feb | scan | 18 | network | Feb 15, 2024 @ 14:46:57 | Feb 15, 2024 @ 14:47:05.574 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 29 | Host Detection | Feb 15, 2024 @ 14:44:55 | Feb 15, 2024 @ 14:45:11.200 | Closed | Low |
| TI IP Address Indicator Match - 91.215.85.17 | Threat-Intel | 12 | network | Feb 15, 2024 @ 14:38:23 | Feb 15, 2024 @ 14:39:10.139 | Closed | Low |
| Alerts Triggered by Kernel Update | system-updatefalse-positive | 986 | Host Detection | Feb 15, 2024 @ 12:10:41 | Feb 15, 2024 @ 14:31:39.910 | Closed | Low |
| SOC Investigation | false-positive | 11 | SOC_Investigation | Feb 15, 2024 @ 06:45:22 | Feb 15, 2024 @ 06:46:58.249 | Closed | Low |
| IPSEC Scans 15 Feb | scan | 40 | network | Feb 15, 2024 @ 06:42:07 | Feb 15, 2024 @ 07:53:56.290 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 55 | Host Detection | Feb 15, 2024 @ 06:34:00 | Feb 15, 2024 @ 06:34:14.437 | Closed | Low |
| SMTP Scans 15 Feb | scan | 142 | network | Feb 15, 2024 @ 06:31:22 | Feb 15, 2024 @ 07:53:59.114 | Closed | Low |
| TI IP Address Indicator Match - 91.215.85.17 | scan | 2 | network | Feb 15, 2024 @ 02:39:47 | Feb 15, 2024 @ 02:40:39.586 | Closed | Low |
| SMB Scans 15 Feb | scan | 4 | network | Feb 15, 2024 @ 01:26:12 | Feb 15, 2024 @ 04:54:15.844 | Closed | Low |

- Classified - Confidential -

- Classified - Confidential -

| Name | Tags | Alerts | Category | Created On | Closed On | Status | Severity |
|---|---|---|---|---|---|---|---|
| IPSEC Scans 15 Feb | scan | 99 | network | Feb 15, 2024 @ 01:20:27 | Feb 15, 2024 @ 01:45:35.466 | Closed | Low |
| SMTP Scans 15 Feb | scan | 153 | network | Feb 15, 2024 @ 01:11:41 | Feb 15, 2024 @ 01:12:50.092 | Closed | Low |
| SMB Scans | scan | 6 | Host Detection | Feb 14, 2024 @ 18:06:28 | Feb 14, 2024 @ 19:11:40.088 | Closed | Low |
| SMTP Scans | scan | 73 | network | Feb 14, 2024 @ 18:04:35 | Feb 14, 2024 @ 19:27:08.407 | Closed | Low |
| IPSEC Scans | scan | 73 | network | Feb 14, 2024 @ 18:02:57 | Feb 14, 2024 @ 19:27:02.781 | Closed | Low |
| **client** Admins | host | 13 | Host Detection | Feb 14, 2024 @ 17:51:38 | Feb 14, 2024 @ 17:54:12.056 | Closed | Low |
| SystemD Service created - False/Pos | false-positive | 1 | — | Feb 14, 2024 @ 16:47:57 | Feb 14, 2024 @ 17:54:06.330 | Closed | Low |
| SOC Team false positive | false-positive SOC Team | 17 | Host Detection | Feb 14, 2024 @ 14:45:22 | Feb 14, 2024 @ 17:53:28.782 | Closed | Low |
| Suspicious File Created / Modified | file-modificationfalse-positive | 7 | Host Detection | Feb 14, 2024 @ 14:18:03 | Feb 14, 2024 @ 17:27:12.091 | Closed | Low |
| **client** admins BAS | host | 31 | Host Detection | Feb 14, 2024 @ 13:09:36 | Feb 14, 2024 @ 13:12:41.527 | Closed | Low |
| IPSEC Scans 14th of Feb | scan | 228 | network | Feb 14, 2024 @ 11:12:41 | Feb 14, 2024 @ 11:15:52.282 | Closed | Low |
| SMTP Scans 14th of Feb | scan | 186 | network | Feb 14, 2024 @ 11:07:56 | Feb 14, 2024 @ 11:13:05.025 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 74 | Host Detection | Feb 14, 2024 @ 10:45:41 | Feb 14, 2024 @ 11:08:50.263 | Closed | Low |
| SMB Scans 14th of Feb | scan | 31 | network | Feb 14, 2024 @ 10:36:32 | Feb 14, 2024 @ 10:37:24.602 | Closed | Low |
| TI IP Address Indicator Match - 91.215.85.17, 5.181.80.126 | Threat-Intel | 36 | network | Feb 14, 2024 @ 10:30:05 | Feb 14, 2024 @ 10:33:02.577 | Closed | Low |

- Classified - Confidential -

| Name | Tags | Alerts | Category | Created On | Closed On | Status | Severity |
|---|---|---|---|---|---|---|---|
| Multiple False Positive Discovery Alerts | false-positive | 147 | Host Detection | Feb 13, 2024 @ 18:19:47 | Feb 13, 2024 @ 18:27:45.566 | Closed | Low |
| Component Object Model Hijacking - desktop-pm5vjpg | windowsfalse -positive | 2 | Host Detection | Feb 13, 2024 @ 16:35:56 | Feb 13, 2024 @ 16:40:41.614 | Closed | Low |
| TI IP Address Indicator Match - 45.227.254.26 | Threat-Intel | 6 | network | Feb 13, 2024 @ 15:34:24 | Feb 13, 2024 @ 15:35:01.474 | Closed | Low |
| Multiple False Positive Discovery Alerts | false-positive | 46 | Host Detection | Feb 13, 2024 @ 14:31:50 | Feb 13, 2024 @ 14:43:17.397 | Closed | Low |
| SOC Investigation | false-positive | 27 | Host Detection | Feb 13, 2024 @ 14:18:35 | Feb 13, 2024 @ 14:21:46.346 | Closed | Low |
| IPSEC Scans 13 Feb | scan | 96 | network | Feb 13, 2024 @ 14:14:41 | Feb 13, 2024 @ 18:54:07.825 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 32 | Host Detection | Feb 13, 2024 @ 14:00:52 | Feb 13, 2024 @ 14:02:25.042 | Closed | Low |
| SMTP Scans 13 Feb | scan | 196 | network | Feb 13, 2024 @ 13:44:39 | Feb 13, 2024 @ 18:54:11.371 | Closed | Low |
| SMB Scans 13 Feb | scan | 6 | network | Feb 13, 2024 @ 12:51:04 | Feb 13, 2024 @ 12:51:13.808 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 25 | Host Detection | Feb 13, 2024 @ 07:01:05 | Feb 13, 2024 @ 07:01:15.022 | Closed | Low |
| SMTP Scans 13 Feb | scan | 49 | network | Feb 13, 2024 @ 06:47:24 | Feb 13, 2024 @ 06:47:38.217 | Closed | Low |
| IPSEC Scans 13 Feb | scan | 110 | network | Feb 13, 2024 @ 06:37:23 | Feb 13, 2024 @ 06:42:05.672 | Closed | Low |
| SMB Scans 13 Feb | scan | 5 | network | Feb 13, 2024 @ 02:17:51 | Feb 13, 2024 @ 02:18:09.251 | Closed | Low |
| TI IP Address Indicator Match - 91.215.85.17 | Threat-Intel | 4 | network | Feb 13, 2024 @ 01:01:14 | Feb 13, 2024 @ 01:01:34.673 | Closed | Low |
| SMB Scans 12 Feb | scan | 4 | network | Feb 12, 2024 @ 21:23:53 | Feb 12, 2024 @ 21:27:56.065 | Closed | Low |
| Abnormal Process ID File created by qemu | false-positive qemu | 1 | Host Detection | Feb 12, 2024 @ 21:18:02 | Feb 12, 2024 @ 21:18:35.491 | Closed | Low |

- Classified - Confidential -

| Name | Tags | Alerts | Category | Created On | Closed On | Status | Severity |
|---|---|---|---|---|---|---|---|
| SMTP Scans 12 Feb | scan | 293 | network | Feb 12, 2024 @ 21:08:53 | Feb 12, 2024 @ 21:10:16.334 | Closed | Low |
| IPSEC Scans 12 Feb | scan | 51 | network | Feb 12, 2024 @ 20:54:05 | Feb 12, 2024 @ 20:54:25.196 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 40 | Host Detection | Feb 12, 2024 @ 20:11:55 | Feb 12, 2024 @ 20:12:08.269 | Closed | Low |
| TI 91.215.85.17 | Threat-Intel | 48 | Host Detection | Feb 12, 2024 @ 17:11:32 | Feb 12, 2024 @ 18:00:02.021 | Closed | Low |
| paulc standard linux activity | — | 5 | Host Detection | Feb 12, 2024 @ 16:58:38 | Feb 12, 2024 @ 17:00:05.749 | Closed | Low |
| BAS *** svs activity | — | 7 | Host Detection | Feb 12, 2024 @ 16:42:57 | Feb 12, 2024 @ 16:54:59.436 | Closed | Low |
| Multiple alerts Involving a User | — | 15 | Host Detection | Feb 12, 2024 @ 16:27:48 | Feb 12, 2024 @ 16:54:22.536 | Closed | Low |
| IPSEC Scans 12th Feb | scan | 93 | network | Feb 12, 2024 @ 14:30:40 | Feb 12, 2024 @ 14:50:22.504 | Closed | Low |
| **** docker | docker | 25 | Host Detection | Feb 12, 2024 @ 14:25:16 | Feb 12, 2024 @ 14:27:38.502 | Closed | Low |
| SMTP scans 12th Feb | scan | 192 | network | Feb 12, 2024 @ 13:01:50 | Feb 12, 2024 @ 13:57:21.198 | Closed | Low |
| SMTP Scans 12 Feb | scan | 103 | network | Feb 12, 2024 @ 06:15:10 | Feb 12, 2024 @ 06:20:22.533 | Closed | Low |
| IPSEC Scans 12 Feb | scan | 37 | network | Feb 12, 2024 @ 06:11:22 | Feb 12, 2024 @ 06:11:52.030 | Closed | Low |
| Auth Keys File Modification by System Administrator | system-configuration | 1 | Host Detection | Feb 11, 2024 @ 23:29:41 | Feb 11, 2024 @ 23:30:08.536 | Closed | Low |
| Cron Job Created - ** | file-modification | 4 | Host Detection | Feb 11, 2024 @ 23:22:28 | Feb 11, 2024 @ 23:23:21.527 | Closed | Low |
| TI IP Address Indicator Match - 91.215.85.17 | Threat-Intel | 8 | network | Feb 11, 2024 @ 23:18:30 | Feb 12, 2024 @ 06:11:48.016 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 18 | Host Detection | Feb 11, 2024 @ 23:08:23 | Feb 11, 2024 @ 23:10:14.334 | Closed | Low |

- Classified - Confidential -

- Classified - Confidential -

| Name | Tags | Alerts | Category | Created On | Closed On | Status | Severity |
|---|---|---|---|---|---|---|---|
| Auth Keys File Modification by System Administrator | system-configuration | 1 | Host Detection | Feb 11, 2024 @ 19:21:41 | Feb 11, 2024 @ 19:22:04.512 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 21 | Host Detection | Feb 11, 2024 @ 18:12:38 | Feb 11, 2024 @ 18:12:53.146 | Closed | Low |
| SMB Scans 11 Feb | scan | 6 | network | Feb 11, 2024 @ 17:54:38 | Feb 11, 2024 @ 17:55:05.136 | Closed | Low |
| TI IP Address Indicator Match - 45.227.254.26 | Threat-Intel | 6 | network | Feb 11, 2024 @ 14:00:19 | Feb 11, 2024 @ 14:03:17.192 | Closed | Low |
| IPSEC Scans 11 Feb | scan | 67 | network | Feb 11, 2024 @ 12:29:32 | Feb 11, 2024 @ 12:29:59.477 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 18 | Host Detection | Feb 11, 2024 @ 11:23:27 | Feb 11, 2024 @ 11:23:39.133 | Closed | Low |
| SMTP Scans 11 Feb | scan | 61 | network | Feb 11, 2024 @ 10:07:06 | Feb 11, 2024 @ 10:07:45.849 | Closed | Low |
| TI IP Address Indicator Match - 91.215.85.17 | Threat-Intel | 6 | network | Feb 11, 2024 @ 10:03:46 | Feb 11, 2024 @ 10:03:55.931 | Closed | Low |
| IPSEC Scans 11 Feb | scan | 82 | network | Feb 11, 2024 @ 05:04:10 | Feb 11, 2024 @ 07:54:53.179 | Closed | Low |
| SMTP Scans 11 Feb | scan | 202 | network | Feb 11, 2024 @ 04:49:39 | Feb 11, 2024 @ 07:54:57.434 | Closed | Low |
| SMB Scans 11 Feb | scan | 20 | network | Feb 11, 2024 @ 04:33:41 | Feb 11, 2024 @ 04:33:51.323 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 41 | Host Detection | Feb 11, 2024 @ 04:29:55 | Feb 11, 2024 @ 04:30:12.579 | Closed | Low |
| TI IP Address Indicator Match - 91.215.85.17 & 45.227.254.26 | Threat-Intel | 14 | network | Feb 11, 2024 @ 04:03:02 | Feb 11, 2024 @ 05:26:04.380 | Closed | Low |
| SMB Scans 10 Feb | scan | 6 | network | Feb 10, 2024 @ 22:48:42 | Feb 10, 2024 @ 23:11:02.690 | Closed | Low |
| SOC Investigation | false-positive | 30 | network | Feb 10, 2024 @ 22:14:24 | Feb 10, 2024 @ 22:17:27.312 | Closed | Low |

- Classified - Confidential -

- Classified - Confidential -

| Name | Tags | Alerts | Category | Created On | Closed On | Status | Severity |
|---|---|---|---|---|---|---|---|
| TI IP Address Indicator Match - 91.215.85.17 & 45.95.147.236 | Threat-Intel | 22 | network | Feb 10, 2024 @ 20:30:33 | Feb 10, 2024 @ 22:06:59.174 | Closed | Low |
| SMTP Scans | scan | 65 | network | Feb 10, 2024 @ 18:32:26 | Feb 10, 2024 @ 22:06:46.380 | Closed | Low |
| IPSEC Scans | scan | 188 | network | Feb 10, 2024 @ 18:28:32 | Feb 10, 2024 @ 22:06:35.792 | Closed | Low |
| Process Discovery | system-configuration | 61 | Host Detection | Feb 10, 2024 @ 18:13:58 | Feb 10, 2024 @ 18:17:53.946 | Closed | Low |
| Process Discovery via Built-In Application | system-configuration | 103 | Host Detection | Feb 10, 2024 @ 18:07:02 | Feb 10, 2024 @ 18:10:19.285 | Closed | Low |
| SMB Scan 10th of Feb | scan | 12 | network | Feb 10, 2024 @ 16:53:30 | Feb 10, 2024 @ 17:08:20.955 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 78 | Host Detection | Feb 10, 2024 @ 12:28:32 | Feb 10, 2024 @ 12:28:56.980 | Closed | Low |
| SMB Scan 10th of Feb | scan | 9 | network | Feb 10, 2024 @ 12:21:26 | Feb 10, 2024 @ 12:21:51.620 | Closed | Low |
| Cron Job Created - *** | file-modification | 14 | Host Detection | Feb 10, 2024 @ 12:19:53 | Feb 10, 2024 @ 12:20:07.706 | Closed | Low |
| IPSEC Scans 10th of Feb | scan | 147 | network | Feb 10, 2024 @ 12:15:17 | Feb 10, 2024 @ 12:29:00.694 | Closed | Low |
| SMTP Scans 10th of Feb | scan | 267 | network | Feb 10, 2024 @ 12:09:44 | Feb 10, 2024 @ 12:29:04.140 | Closed | Low |
| TI IP Address Indicator Match | Threat-Intel | 36 | network | Feb 10, 2024 @ 12:04:51 | Feb 10, 2024 @ 12:15:31.145 | Closed | Low |
| SOC Investigation | false-positive | 21 | Host Detection | Feb 9, 2024 @ 18:20:03 | Feb 9, 2024 @ 18:24:23.559 | Closed | Low |
| IPSEC Scans 09 Feb | scan | 89 | network | Feb 9, 2024 @ 18:08:12 | Feb 9, 2024 @ 19:59:34.424 | Closed | Low |
| SMTP Scans 09 Feb | scan | 69 | network | Feb 9, 2024 @ 17:58:44 | Feb 9, 2024 @ 19:59:37.355 | Closed | Low |

- Classified - Confidential -

- Classified - Confidential -

| Name | Tags | Alerts | Category | Created On | Closed On | Status | Severity |
|---|---|---|---|---|---|---|---|
| Multiple Alerts Involving a User | false-positive | 37 | Host Detection | Feb 9, 2024 @ 17:31:36 | Feb 9, 2024 @ 17:32:09.566 | Closed | Low |
| TI IP Address Indicator Match - 91.215.85.17 | Threat-Intel | 24 | network | Feb 9, 2024 @ 14:18:49 | Feb 9, 2024 @ 18:34:22.689 | Closed | Low |
| Multiple False Positive Discovery Alerts | false-positive | 150 | Host Detection | Feb 9, 2024 @ 10:26:19 | Feb 9, 2024 @ 10:49:16.907 | Closed | Low |
| Multiple alerts made by a *** | false-positive | 516 | Host Detection | Feb 9, 2024 @ 09:30:20 | Feb 9, 2024 @ 09:43:38.281 | Closed | Low |
| SMTP Scans 09 Feb | scan | 27 | network | Feb 9, 2024 @ 06:09:53 | Feb 9, 2024 @ 06:10:15.039 | Closed | Low |
| IPSEC Scans 09 Feb | scan | 43 | network | Feb 9, 2024 @ 05:05:49 | Feb 9, 2024 @ 05:06:09.271 | Closed | Low |
| Multiple Alerts on desktop-pm5vjpg - Windows | windowsfalse -positive | 11 | Host Detection | Feb 8, 2024 @ 20:47:04 | Feb 8, 2024 @ 21:23:32.514 | Closed | Low |
| SMTP Scans 08 Feb | scan | 199 | network | Feb 8, 2024 @ 20:40:13 | Feb 8, 2024 @ 20:42:21.649 | Closed | Low |
| IPSEC Scans 08 Feb | scan | 51 | network | Feb 8, 2024 @ 20:36:20 | Feb 8, 2024 @ 20:36:33.220 | Closed | Low |
| Cron Job Created - *** | file-modificati on | 8 | Host Detection | Feb 8, 2024 @ 20:31:37 | Feb 8, 2024 @ 20:31:53.487 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 74 | Host Detection | Feb 8, 2024 @ 20:29:34 | Feb 8, 2024 @ 20:29:42.885 | Closed | Low |
| SMB Scans 08 Feb | scan | 23 | network | Feb 8, 2024 @ 20:26:55 | Feb 8, 2024 @ 20:27:30.045 | Closed | Low |
| TI IP Address Indicator Match - 45.227.254.26 & 45.95.147.236 | Threat-Intel | 10 | network | Feb 8, 2024 @ 20:20:21 | Feb 8, 2024 @ 20:20:45.300 | Closed | Low |
| TI IP Address Indicator Match - 91.215.85.17 | Threat-Intel | 44 | network | Feb 8, 2024 @ 20:12:51 | Feb 8, 2024 @ 20:13:21.289 | Closed | Low |
| Cron Job Investigation | Es-agent | 4 | — | Feb 8, 2024 @ 14:45:57 | Feb 8, 2024 @ 20:32:02.906 | Closed | Low |

- Classified - Confidential -

- Classified - Confidential -

| Name | Tags | Alerts | Category | Created On | Closed On | Status | Severity |
|---|---|---|---|---|---|---|---|
| TI IP Port 25 Russia | Threat-Intel | 34 | — | Feb 8, 2024 @ 13:25:32 | Feb 8, 2024 @ 20:31:59.071 | Closed | Low |
| Cron Job Created - cs3458 | file-modification | 2 | Host Detection | Feb 8, 2024 @ 07:16:56 | Feb 8, 2024 @ 07:17:18.605 | Closed | Low |
| TI IP Address Indicator Match | Threat-Intel | 18 | network | Feb 8, 2024 @ 07:14:23 | Feb 8, 2024 @ 07:14:45.836 | Closed | Low |
| SMB Scan 8th of Feb | scan | 16 | network | Feb 8, 2024 @ 07:10:58 | Feb 8, 2024 @ 07:11:07.343 | Closed | Low |
| SMTP Scans 8th of Feb | scan | 72 | network | Feb 8, 2024 @ 07:09:45 | Feb 8, 2024 @ 07:14:57.059 | Closed | Low |
| IPSEC Scans 8th of Feb | scan | 52 | network | Feb 8, 2024 @ 07:08:10 | Feb 8, 2024 @ 07:14:51.101 | Closed | Low |
| SMB Scan 8th of Feb | scan | 4 | network | Feb 8, 2024 @ 01:29:26 | Feb 8, 2024 @ 01:29:44.235 | Closed | Low |
| SMTP Scans 8th of Feb | scan | 127 | network | Feb 8, 2024 @ 01:23:16 | Feb 8, 2024 @ 01:29:59.457 | Closed | Low |
| IPSEC Scans 8th of Feb | scan | 63 | network | Feb 8, 2024 @ 01:05:37 | Feb 8, 2024 @ 01:19:38.694 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 24 | Host Detection | Feb 8, 2024 @ 01:00:54 | Feb 8, 2024 @ 01:01:49.600 | Closed | Low |
| TI IP Address Indicator Match | Threat-Intel | 12 | network | Feb 8, 2024 @ 00:57:56 | Feb 8, 2024 @ 01:01:59.555 | Closed | Low |
| IPSEC Scans 07 Feb | scan | 43 | network | Feb 7, 2024 @ 19:17:00 | Feb 7, 2024 @ 19:17:22.277 | Closed | Low |
| SMTP Scans 07 Feb | scan | 65 | network | Feb 7, 2024 @ 15:59:40 | Feb 7, 2024 @ 16:00:08.667 | Closed | Low |
| Suspicious Network Connection Attempt by docker | dockerfalse-positive | 3 | network | Feb 7, 2024 @ 11:39:48 | Feb 7, 2024 @ 11:39:59.897 | Closed | Low |
| Cron Job Created - *** | file-modification | 14 | Host Detection | Feb 7, 2024 @ 11:28:56 | Feb 7, 2024 @ 11:29:23.001 | Closed | Medium |

- Classified - Confidential -

| Name | Tags | Alerts | Category | Created On | Closed On | Status | Severity |
|---|---|---|---|---|---|---|---|
| Multiple Alerts Involving a User | false-positive | 24 | Host Detection | Feb 7, 2024 @ 11:25:23 | Feb 7, 2024 @ 11:25:37.619 | Closed | Low |
| SMB Scans 07 Feb | scan | 5 | network | Feb 7, 2024 @ 10:59:01 | Feb 7, 2024 @ 10:59:50.043 | Closed | Low |
| TI IP Address Indicator Match | scanThreat-Intel | 8 | network | Feb 7, 2024 @ 10:54:30 | Feb 7, 2024 @ 10:56:18.176 | Closed | Low |
| SMB Scans 07 Feb | scan | 6 | network | Feb 7, 2024 @ 07:08:37 | Feb 7, 2024 @ 07:54:59.155 | Closed | Low |
| TI IP Address Indicator Match | Threat-Intelscan | 20 | network | Feb 7, 2024 @ 04:44:57 | Feb 7, 2024 @ 07:57:17.260 | Closed | Low |
| SOC Investigation | false-positive | 123 | SOC_Investigation | Feb 7, 2024 @ 04:27:59 | Feb 7, 2024 @ 06:06:46.125 | Closed | Low |
| IPSEC Scans 07 Feb | scan | 141 | network | Feb 7, 2024 @ 04:18:40 | Feb 7, 2024 @ 07:57:23.771 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 46 | Host Detection | Feb 7, 2024 @ 04:11:32 | Feb 7, 2024 @ 07:57:20.241 | Closed | Low |
| SMTP Scans 07 Feb | scan | 145 | network | Feb 7, 2024 @ 04:07:07 | Feb 7, 2024 @ 07:57:13.968 | Closed | Low |
| Suspicious JAVA Child Process - wget spider | false-positive | 1 | Host Detection | Feb 7, 2024 @ 03:52:42 | Feb 7, 2024 @ 03:53:16.581 | Closed | Low |
| Abnormal Process ID or Lock File Created | system-configuration | 7 | Host Detection | Feb 6, 2024 @ 22:04:42 | Feb 6, 2024 @ 22:04:51.914 | Closed | Low |
| TI IP Address Indicator Match | Threat-Intel | 159 | network | Feb 6, 2024 @ 21:15:41 | Feb 7, 2024 @ 02:26:34.896 | Closed | Low |
| Enumeration of Kernel Modules dracut | dracutsystem-update | 827 | Host Detection | Feb 6, 2024 @ 18:35:12 | Feb 6, 2024 @ 19:12:09.682 | Closed | Low |
| Potential Shadow File Read | file-modificationfalse-positive | 1 | Host Detection | Feb 6, 2024 @ 14:30:42 | Feb 6, 2024 @ 14:33:02.663 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 35 | Host Detection | Feb 6, 2024 @ 11:34:38 | Feb 6, 2024 @ 14:33:10.760 | Closed | Low |

- Classified - Confidential -

| Name | Tags | Alerts | Category | Created On | Closed On | Status | Severity |
|---|---|---|---|---|---|---|---|
| TI IP Address Indicator Match | Threat-Intel | 221 | network | Feb 6, 2024 @ 11:06:29 | Feb 6, 2024 @ 18:42:09.787 | Closed | Low |
| IPSEC Scans 6th of Feb | scan | 170 | network | Feb 6, 2024 @ 10:32:59 | Feb 6, 2024 @ 18:42:23.304 | Closed | Low |
| SMTP Scans 6th of Feb | scan | 312 | network | Feb 6, 2024 @ 10:28:06 | Feb 6, 2024 @ 18:42:18.099 | Closed | Low |
| *** investigation | file-modificationThreat-Intel | 44 | Host Detection | Feb 6, 2024 @ 10:22:08 | Feb 6, 2024 @ 16:36:22.714 | Closed | Medium |
| SMB Scan 6th of Feb | scan | 11 | network | Feb 6, 2024 @ 09:17:33 | Feb 6, 2024 @ 09:18:26.971 | Closed | Low |
| SMB Scan 5th of Feb | scan | 9 | network | Feb 5, 2024 @ 18:02:30 | Feb 5, 2024 @ 18:03:04.639 | Closed | Low |
| TI IP Address Indicator Match - 91.215.85.17 | Threat-Intel | 12 | network | Feb 5, 2024 @ 17:24:56 | Feb 5, 2024 @ 18:03:26.450 | Closed | Low |
| SMTP Scans 5th of Feb | scan | 76 | network | Feb 5, 2024 @ 11:29:16 | Feb 5, 2024 @ 14:46:47.760 | Closed | Low |
| IPSEC Scans 5th of Feb | scan | 93 | network | Feb 5, 2024 @ 11:23:14 | Feb 5, 2024 @ 14:46:52.689 | Closed | Low |
| Multiple Alerts Involving a User | false-positive Es-agent | 15 | Host Detection | Feb 5, 2024 @ 11:11:27 | Feb 5, 2024 @ 11:26:26.328 | Closed | Low |
| TI IP Address Indicator Match - 91.215.85.17 | Threat-Intel | 18 | network | Feb 5, 2024 @ 10:48:51 | Feb 5, 2024 @ 13:20:22.346 | Closed | Low |
| SMTP Scans 05 Feb | scan | 106 | network | Feb 5, 2024 @ 06:43:47 | Feb 5, 2024 @ 06:44:43.861 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 11 | Host Detection | Feb 5, 2024 @ 02:58:29 | Feb 5, 2024 @ 02:58:43.293 | Closed | Low |
| SMB Scans 05 Feb | scan | 4 | network | Feb 5, 2024 @ 02:56:15 | Feb 5, 2024 @ 02:56:29.492 | Closed | Low |
| IPSEC Scans 04 Feb | scan | 147 | network | Feb 4, 2024 @ 20:36:09 | Feb 4, 2024 @ 20:37:15.499 | Closed | Low |

- Classified - Confidential -

- Classified - Confidential -

| Name | Tags | Alerts | Category | Created On | Closed On | Status | Severity |
|---|---|---|---|---|---|---|---|
| SMTP Scans 04 Feb | scan | 233 | network | Feb 4, 2024 @ 20:29:44 | Feb 4, 2024 @ 20:31:22.401 | Closed | Low |
| SMB Scans 04 Feb | scan | 10 | network | Feb 4, 2024 @ 20:24:39 | Feb 4, 2024 @ 20:24:47.704 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 54 | Host Detection | Feb 4, 2024 @ 20:22:20 | Feb 4, 2024 @ 20:22:40.483 | Closed | Low |
| TI IP Address Indicator Match - 91.215.85.17 | Threat-Intel | 54 | network | Feb 4, 2024 @ 20:17:40 | Feb 4, 2024 @ 20:17:58.246 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 31 | Host Detection | Feb 4, 2024 @ 07:14:42 | Feb 4, 2024 @ 07:52:18.002 | Closed | Low |
| IPSEC Scans 04 Feb | scan | 90 | network | Feb 4, 2024 @ 07:11:48 | Feb 4, 2024 @ 07:52:14.727 | Closed | Low |
| SMTP Scans 04 Feb | scan | 155 | network | Feb 4, 2024 @ 07:08:03 | Feb 4, 2024 @ 07:52:11.597 | Closed | Low |
| TI IP Address Indicator Match - 91.215.85.17 | Threat-Intel | 22 | network | Feb 4, 2024 @ 04:17:06 | Feb 4, 2024 @ 07:52:08.551 | Closed | Low |
| SOC Investigation | false-positive | 157 | Host Detection | Feb 4, 2024 @ 01:07:16 | Feb 4, 2024 @ 01:18:12.128 | Closed | Low |
| SMTP Scans 03 Feb | scan | 126 | network | Feb 3, 2024 @ 23:22:59 | Feb 4, 2024 @ 00:34:28.698 | Closed | Low |
| TI IP Address Indicator Match | Threat-Intel | 45 | network | Feb 3, 2024 @ 23:01:13 | Feb 4, 2024 @ 00:42:38.202 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 81 | Host Detection | Feb 3, 2024 @ 22:37:27 | Feb 4, 2024 @ 00:42:44.259 | Closed | Low |
| SMB Scans 03 Feb | scan | 25 | network | Feb 3, 2024 @ 22:31:44 | Feb 3, 2024 @ 23:26:39.010 | Closed | Low |
| IPSEC Scans 03 Feb | scan | 210 | network | Feb 3, 2024 @ 22:23:31 | Feb 4, 2024 @ 00:42:47.973 | Closed | Low |
| TI IP Address Indicator Match | Threat-Intelscan | 274 | network | Feb 3, 2024 @ 20:47:23 | Feb 3, 2024 @ 22:04:07.282 | Closed | Low |
| SMTP Scans 3rd of Feb | scan | 73 | network | Feb 3, 2024 @ 06:34:18 | Feb 3, 2024 @ 08:04:43.224 | Closed | Low |

- Classified - Confidential -

- Classified - Confidential -

| Name | Tags | Alerts | Category | Created On | Closed On | Status | Severity |
|---|---|---|---|---|---|---|---|
| IPSEC Scans 3rd of Feb | scan | 138 | network | Feb 3, 2024 @ 06:18:40 | Feb 3, 2024 @ 08:04:37.283 | Closed | Low |
| SMB Scans 3rd Feb | scanfalse-positive | 14 | network | Feb 3, 2024 @ 01:07:02 | Feb 3, 2024 @ 03:17:41.613 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 10 | Host Detection | Feb 3, 2024 @ 01:04:13 | Feb 3, 2024 @ 01:04:23.907 | Closed | Low |
| IPSEC Scans 3rd of Feb | scan | 101 | network | Feb 3, 2024 @ 00:26:50 | Feb 3, 2024 @ 03:17:53.553 | Closed | Low |
| SMTP Scans 2nd of Feb | scan | 161 | network | Feb 2, 2024 @ 22:45:56 | Feb 3, 2024 @ 03:18:00.515 | Closed | Low |
| TI IP Address Indicator Match - 45.95.147.236 | Threat-Intel | 73 | network | Feb 2, 2024 @ 20:38:06 | Feb 2, 2024 @ 21:21:40.761 | Closed | Low |
| SOC Investigation | false-positive | 50 | Host Detection | Feb 2, 2024 @ 18:30:08 | Feb 2, 2024 @ 18:30:34.326 | Closed | Low |
| Potential Shadow File Read | file-modificationfalse-positive | 27 | Host Detection | Feb 2, 2024 @ 18:24:31 | Feb 2, 2024 @ 18:38:56.354 | Closed | Low |
| SMB Scans 02 Feb | scan | 17 | network | Feb 2, 2024 @ 16:22:59 | Feb 2, 2024 @ 17:15:59.039 | Closed | Low |
| False positive Discovery Alerts | false-positive | 133 | Host Detection | Feb 2, 2024 @ 16:15:12 | Feb 2, 2024 @ 16:22:05.119 | Closed | Low |
| SOC Investigation | false-positive | 63 | Host Detection | Feb 2, 2024 @ 14:25:37 | Feb 2, 2024 @ 14:26:35.653 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 34 | Host Detection | Feb 2, 2024 @ 14:18:47 | Feb 2, 2024 @ 14:19:06.259 | Closed | Low |
| SMTP Scans 02 Feb | scan | 94 | network | Feb 2, 2024 @ 12:14:53 | Feb 2, 2024 @ 18:38:07.965 | Closed | Low |
| IPSEC Scans 02 Feb | scan | 85 | network | Feb 2, 2024 @ 12:08:51 | Feb 2, 2024 @ 18:38:12.080 | Closed | Low |
| IPSEC Scans 2 Feb | scan | 30 | network | Feb 2, 2024 @ 05:49:19 | Feb 2, 2024 @ 05:49:38.660 | Closed | Low |

- Classified - Confidential -

- Classified - Confidential -

| Name | Tags | Alerts | Category | Created On | Closed On | Status | Severity |
|---|---|---|---|---|---|---|---|
| SMTP Scans 2 Feb | scan | 118 | network | Feb 2, 2024 @ 05:45:11 | Feb 2, 2024 @ 05:46:42.826 | Closed | Low |
| SMB Scans 2 Feb | scan | 5 | network | Feb 2, 2024 @ 01:00:59 | Feb 2, 2024 @ 01:01:16.976 | Closed | Low |
| Abnormal PID File Created by qemu | false-positive qemu | 5 | Host Detection | Feb 1, 2024 @ 23:50:05 | Feb 1, 2024 @ 23:50:16.313 | Closed | Low |
| TI IP Address Indicator Match - 45.95.147.236 | Threat-Intelscan | 24 | network | Feb 1, 2024 @ 21:46:49 | Feb 1, 2024 @ 21:47:10.123 | Closed | Low |
| Multiple Alerts Caused by root | false-positive | 26 | Host Detection | Feb 1, 2024 @ 20:53:22 | Feb 1, 2024 @ 20:54:41.082 | Closed | Low |
| SMTP Scans 01 Feb part 2 | scan | 83 | network | Feb 1, 2024 @ 19:38:42 | Feb 1, 2024 @ 23:25:05.901 | Closed | Low |
| IPSEC Scans 01 Feb part 2 | scan | 137 | network | Feb 1, 2024 @ 19:34:48 | Feb 1, 2024 @ 23:25:02.426 | Closed | Low |
| SOC Investigation | false-positive | 386 | Host Detection | Feb 1, 2024 @ 19:30:09 | Feb 1, 2024 @ 19:54:55.519 | Closed | Low |
| Multiple Alerts Involving a User | false-positive | 100 | Host Detection | Feb 1, 2024 @ 13:52:21 | Feb 1, 2024 @ 15:29:21.245 | Closed | Low |
| Multiple False Positive alerts triggered by sysadmin | false-positive | 115 | Host Detection | Feb 1, 2024 @ 13:13:53 | Feb 1, 2024 @ 13:18:57.581 | Closed | Low |
| SOC Investigation | false-positive | 56 | Host Detection | Feb 1, 2024 @ 12:37:30 | Feb 1, 2024 @ 12:38:08.086 | Closed | Low |
| SMB Scans 01 Feb | scan | 15 | network | Feb 1, 2024 @ 12:26:13 | Feb 1, 2024 @ 12:27:39.820 | Closed | Low |
| IPSEC Scans 01 Feb | scan | 156 | network | Feb 1, 2024 @ 12:20:24 | Feb 1, 2024 @ 15:29:18.055 | Closed | Low |
| SMTP Scans 01 Feb | scan | 303 | network | Feb 1, 2024 @ 12:06:35 | Feb 1, 2024 @ 15:29:15.144 | Closed | Low |
| TI IP Address Indicator Match - 45.95.147.236 | Threat-Intelscan | 114 | network | Feb 1, 2024 @ 10:53:43 | Feb 1, 2024 @ 10:54:19.024 | Closed | Low |

- Classified - Confidential -

## Cases conclusion

The security incident report for February 2024 reveals a comprehensive array of alerts across various categories, notably involving scans, true-positive detections, false-positives, SOC investigations, and threat intelligence matches. A significant portion of the incidents pertains to network scans (e.g., SMTP, SMB, IPSEC Scans) and host detections involving system configurations and user activities. The majority of alerts were classified as low severity, with a few high-severity instances related to threat intelligence hashes and IP address indicator matches. Notably, several incidents were flagged as false positives, indicating effective but overly cautious detection mechanisms. The report underscores the importance of continuous monitoring and analysis to discern legitimate threats from benign activities, ensuring both proactive threat detection and minimizing disruptions from false alarms.

# Security Analysis

Throughout February, our Security Operations Center (SOC) team tackled a broad range of cybersecurity challenges, engaging in detailed threat analysis across several key investigations. Their commitment was focused on enhancing our digital security and proactive defense measures. The team, equipped with advanced security tools, worked on identifying and mitigating potential threats to protect our network and data assets. Below, we provide a summarized overview of their efforts, showcasing the strategic steps taken to fortify our defenses against cyber threats and ensure the ongoing security of our organization's digital environment.

## Investigations into Network Attacks

Our network monitoring systems detected an extensive range of IP addresses executing scans against our network hosts. A substantial portion of these were identified as harboring malicious intent. In response, our team conducted comprehensive evaluations for exposed ports on the affected hosts and undertook detailed analysis of system logs. This meticulous approach was aimed at tracing the origins and understanding the methodologies of these incursions, ensuring robust defense mechanisms against potential threats.

## Process Investigations on Hosts

A substantial part of our investigative work centered on understanding the origins and purposes of various processes running on our hosts. In many instances, these processes were initiated by our

employees as part of regular server maintenance. Our SOC team's proactive log reviews and investigations helped clarify most alerts of this nature, distinguishing between legitimate administrative activities and potential security concerns.

For processes triggered by automated systems, we conducted a thorough review and subsequently whitelisted several this month, recognizing them as safe and necessary for our operations. Additionally, a smaller number of alerts related to employee workstations required specialized investigation using tools like osquery, highlighting the complexity of distinguishing between benign and malicious activities in diverse server environments and configurations.

These efforts underline the intricate and time-consuming nature of our security investigations, particularly when navigating the complexities of server configurations and services. Our team's dedication to dissecting and understanding each alert ensures the security and integrity of our digital infrastructure, even in the face of sophisticated and covert threats.

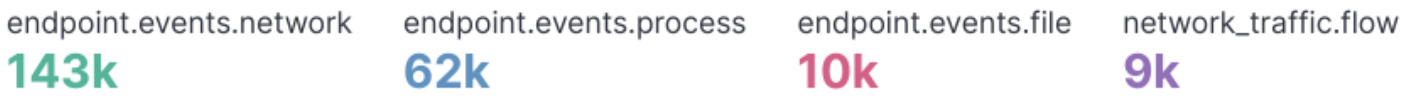
# Metrics

**Network events**: 5.9 Billions (averaging 2.385,64 per second).

**Network DNS+Flow events**: 414.810.566 (averaging 165,55 per second)

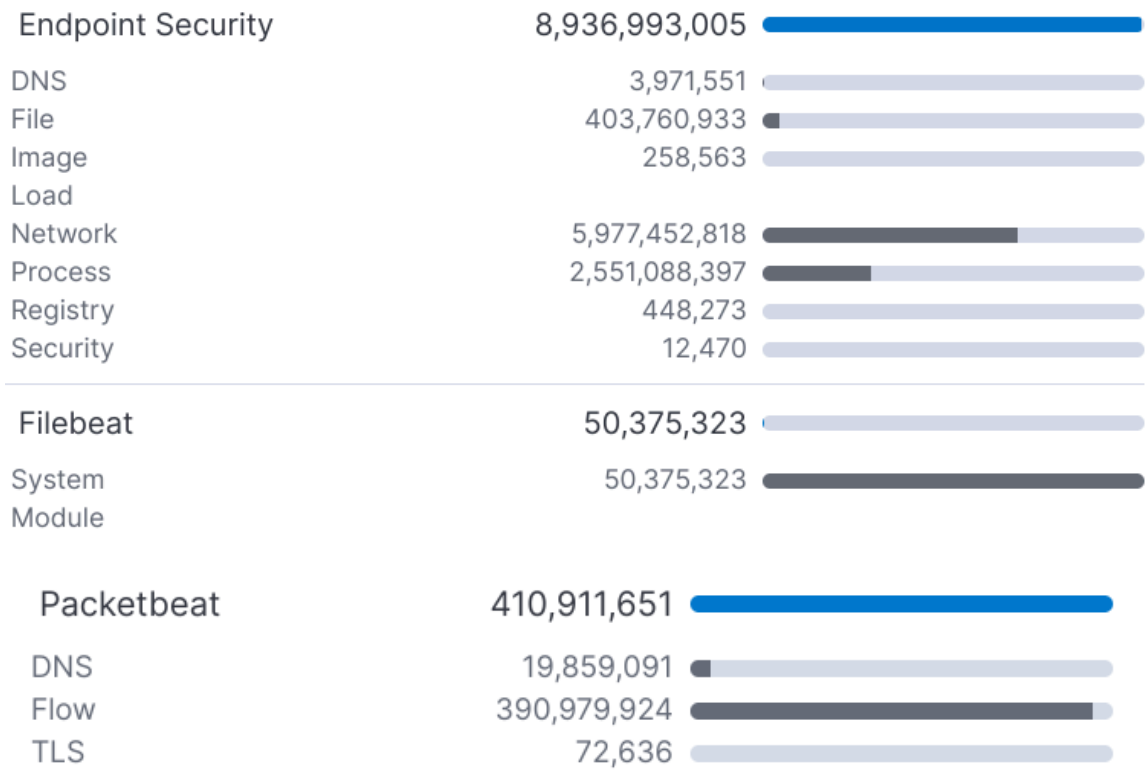
We maintained 1034 active rules throughout the month, with the following log rates:

**Log rate per minute**



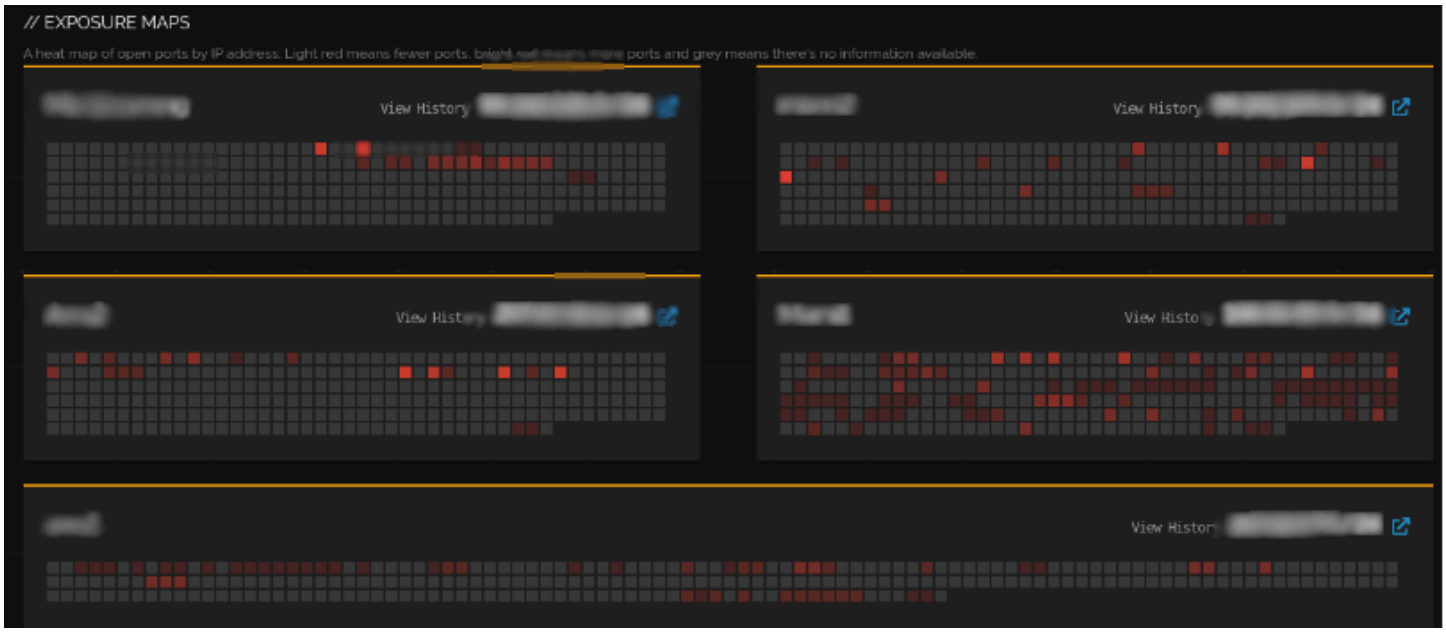
# Alerts

**Our security systems generated the following alerts by category:**



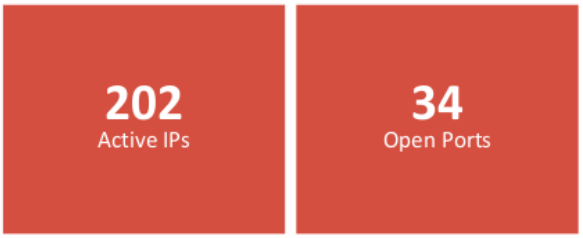

The security overview highlights that the majority of events are network-related, suggesting extensive data transmission that could be vulnerable to cyber threats. Process activities also form a massive portion, indicating active endpoint usage which requires vigilant monitoring. Other events, including file changes and DNS queries, although less frequent, are crucial for detecting potential security breaches and ensuring the integrity of the system.

# Operations




## Internet Facing

The network security overview reveals that we have 227 active IP addresses and 35 open ports across our system. The exposure maps visualize where open ports are concentrated, with some IPs showing more open ports than others. This information is crucial as eachopen port could be a potential entry point for security threats. Our immediate focus should be to review these open ports to confirm they are necessary for business operations and ensure they are secured.

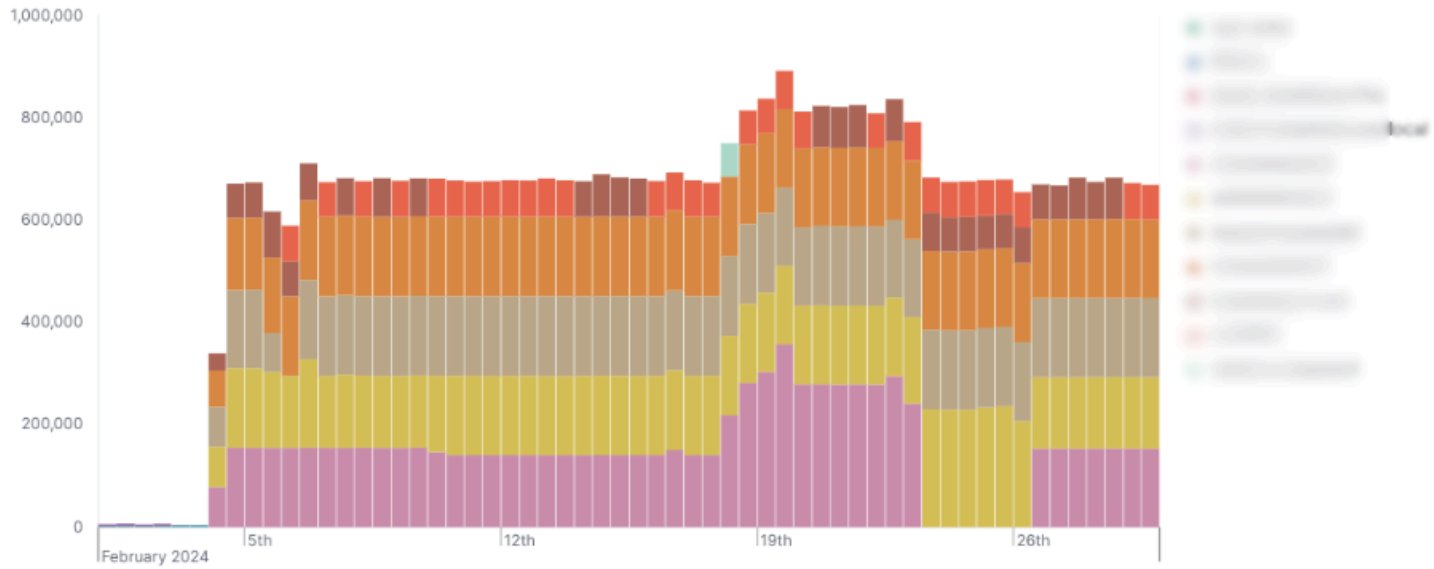



- Classified - Confidential -

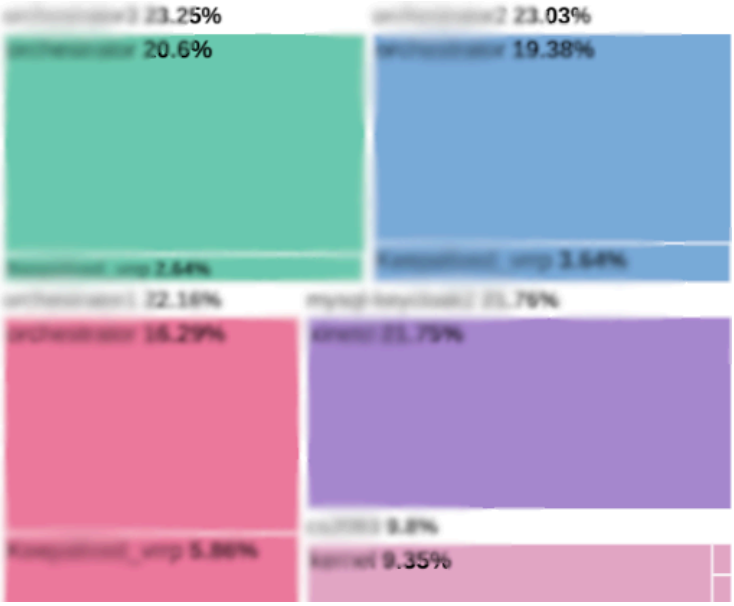
# Open ports per internet facing servers:

| IP addresses | Hostname | Ports |
|---|---|---|
| *.*.*.* | **.***.com | 25, 80, 110, 143, 587, 993, 995 |
| *.*.*.* | **.***.com | 25, 80, 110, 143, 587, 993, 995 |
| *.*.*.* | **.***.com | 111, 123, 443, 1935, 8083, 8086, 8087, 8088 |
| *.*.*.* | **.***.com | 111, 123, 443, 1935, 8083, 8086, 8087 |
| *.*.*.* | **.***.com | 111, 443, 1935, 8083, 8086, 8087, 8089 |
| *.*.*.* | **.***.com | 21, 80, 111, 443, 3306 |
| *.*.*.* | **.***.com | 111, 443, 1935, 8083, 8086, 8087, 8089 |
| *.*.*.* | **.***.com | 111, 443, 1935, 8051, 8086, 8087, 9443 |
| *.*.*.* | **.***.com | 111, 123, 8081, 9100, 10250 |
| *.*.*.* | **.***.com | 111, 123, 8081, 9100, 10250 |
| *.*.*.* | **.***.com | 111, 443, 1935, 8086, 8087, 9443 |
| *.*.*.* | **.***.com | 111, 123, 8081, 9100, 10250 |
| *.*.*.* | **.***.com | 25, 111, 123, 3306, 8080 |
| *.*.*.* | **.***.com | 111, 123, 8081, 9100, 10250 |
| *.*.*.* | **.***.com | 111, 8081, 9100, 10250 |
| *.*.*.* | **.***.com | 111, 8081, 9100, 10250 |
| *.*.*.* | **.***.com | 53, 80, 123, 443 |
| *.*.*.* | **.***.com | 443, 1935, 7400, 8088 |
| *.*.*.* | **.***.com | 443, 1935, 7400, 9302 |
| *.*.*.* | **.***.com | 80, 111, 123, 443 |

# Syslog events by hostnames




- Classified - Confidential -

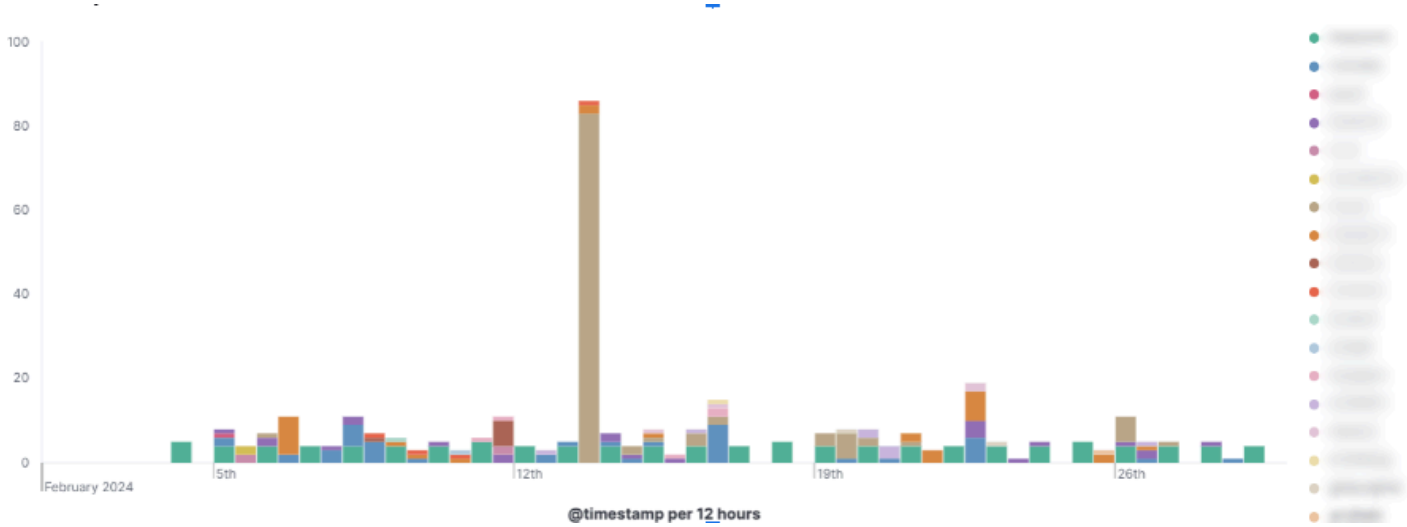



# Access Management

In February, our diligent oversight of security measures led to the processing of 20 User Access Management tickets, affirming that system access is securely restricted to authorized personnel only.

- Classified - Confidential -

## Sudo commands by user




While essential for administrative tasks, its potent capabilities necessitate stringent oversight. By monitoring sudo operations on a per-user basis, we gain unparalleled visibility into how, when, and by whom these elevated privileges are being utilized across our network.

This proactive approach to monitoring sudo operations enhances our security in several key areas:

Increased accountability, by associating sudo operations with individual users, we foster a culture of accountability.

Proactive Threat Detection, enables the early detection of potential security threats, minimizing their impact.

Operational Integrity which assures that privileged operations are conducted in line with our security policies and compliance requirements.

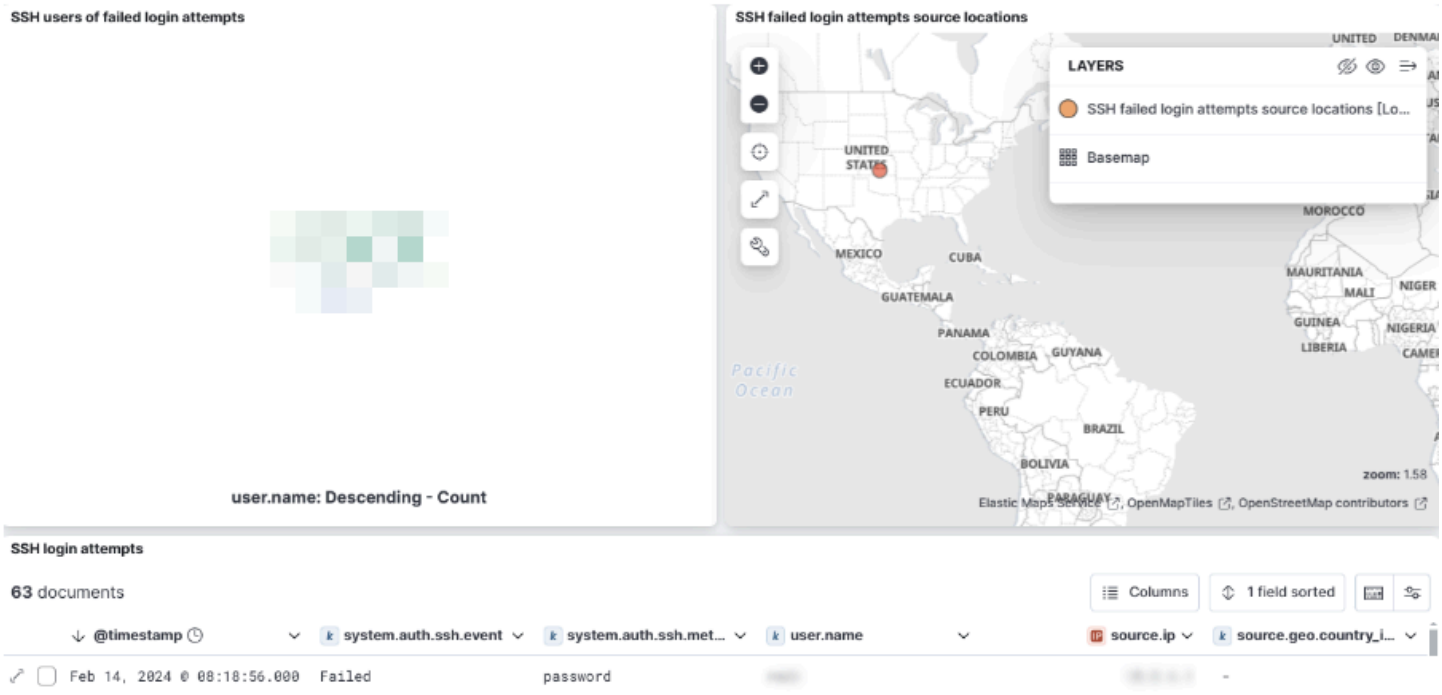
## SSH Access

In summary, our security strategy includes comprehensive monitoring of all SSH login attempts. This encompasses successful logins via public keys, accepted and postponed logins, as well as failed and invalid attempts, ensuring a thorough oversight of access to our systems:


In alignment with the findings and recommendations outlined in our preceding security assessment, we've strategically implemented a comprehensive monitoring system, augmented by meticulously crafted security protocols and real-time alerts. This advanced framework is designed to vigilantly oversee live activities within our network, providing a robust defense mechanism against potential cyber threats, whether they originate from malicious actors or arise due to unintentional human errors or automated system anomalies.

The diagram below illustrates our integrated security architecture, showcasing the dynamic interplay between our monitoring capabilities, security rules, and alert mechanisms. This cohesive approach ensures that our digital environment remains under constant surveillance, enabling us to swiftly identify and mitigate risks, thereby safeguarding our operational integrity and maintaining the trust of our stakeholders

- Classified - Confidential -




# VPN visibility

In line with our commitment to bolster network security and enhance visibility across our virtual private network (VPN) infrastructure, we've taken significant strides beyond just integrating additional VPN concentrators in Miami. As promised on our last report, we've successfully integrated and are now actively monitoring the following VPN concentrators:

- ***.***.net
- ***.***.net
- ***.***.com

This expansion allows us unprecedented full visibility and comprehensive tracking capabilities of each user's activity across our network. We are now equipped to monitor the city from which a user connects, providing approximate geo-location data. Additionally, we've developed sophisticated tools for gathering detailed statistics related to departmental VPN usage, the duration of connections, and other in-depth technical logs that offer insights into the behavior of our network users.

- Classified - Confidential -

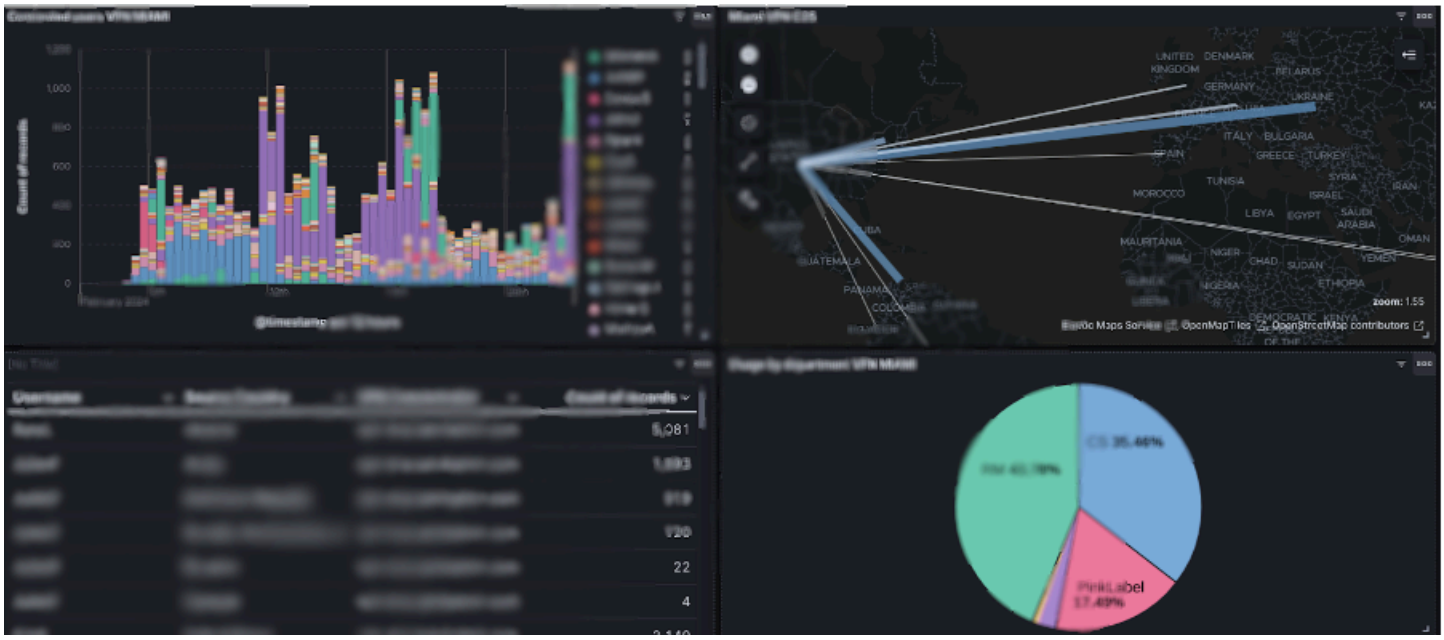
# VPN Security Monitoring

To take advantage of this wealth of information, our team has meticulously designed and implemented dashboards for each VPN concentrator. These dashboards display an array of amazing statistics and visualizations, offering a granular view of the network's health and usage patterns. The ability to analyze data at this level empowers our security team to identify potential security threats swiftly and devise effective countermeasures.

In February, we further augmented our security framework by intensifying the monitoring of VPN access points across the board. By diligently tracking every VPN event and analyzing this data against our advanced security baseline, we have gained valuable insights into the typical usage patterns and potential vulnerabilities within our network. Our proactive approach to security monitoring has enabled us to successfully visualize VPN activity over time, revealing trends and anomalies that could indicate security risks.

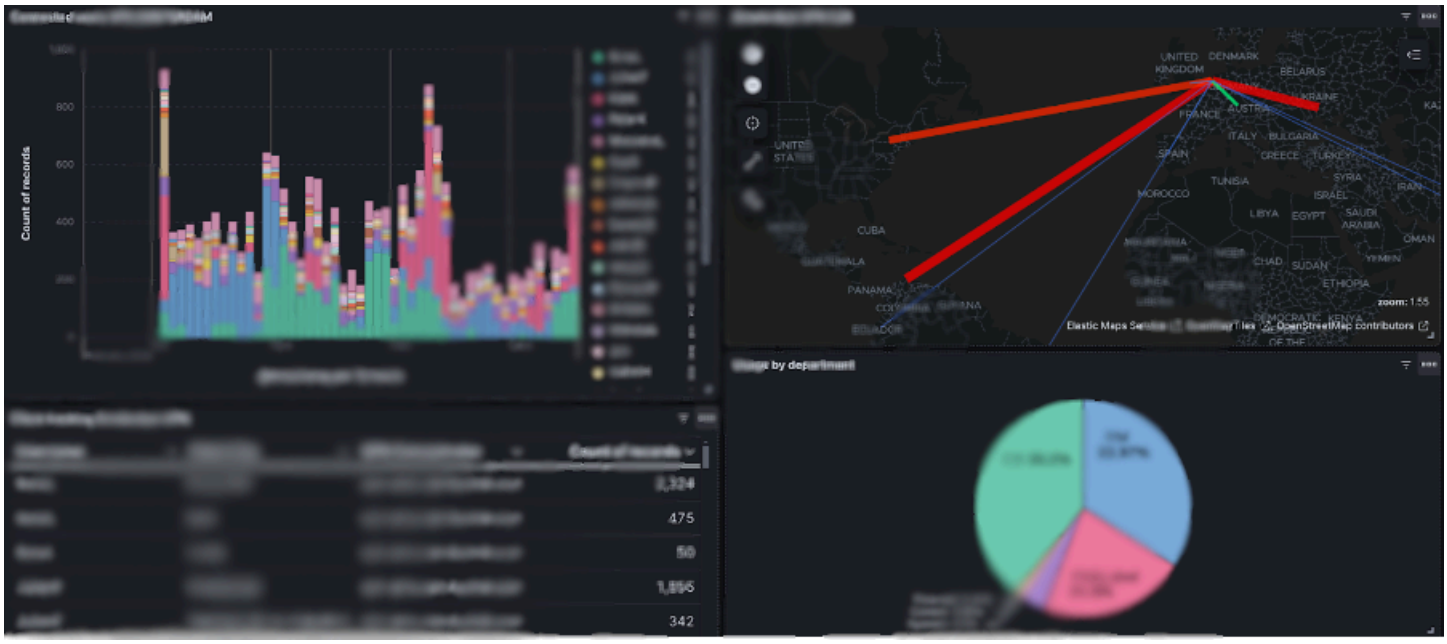
Leveraging the data gleaned from our enhanced monitoring efforts, we are in the process of formulating and implementing new security rules aimed at bolstering our defensive posture. These rules are designed to detect and prevent malicious activities more effectively, ensuring the integrity and reliability of our network. By continuously refining our security measures and leveraging state-of-the-art technologies, we are committed to maintaining a secure and resilient network infrastructure that supports the needs of our organization and protects our valuable data assets.

***:



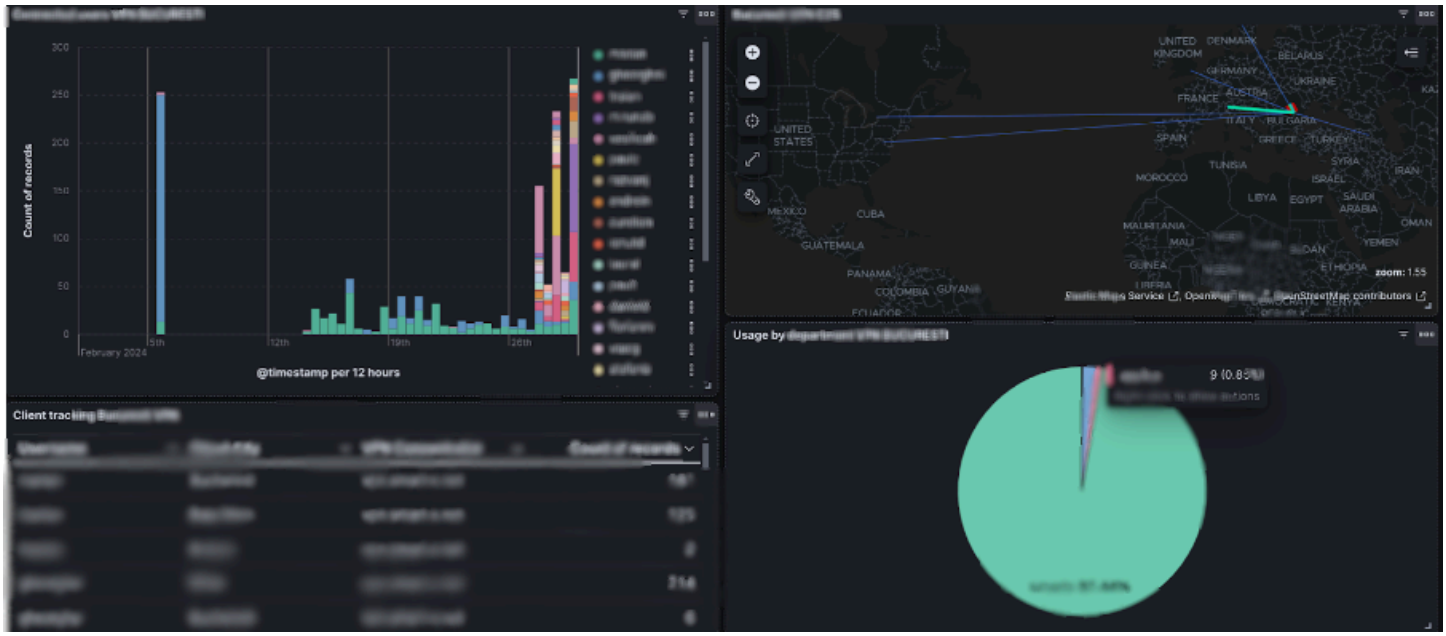

- Classified - Confidential -

***:


Count of records
UNITED KINGDOM
DENMARK
BELARUS
FRANCE
ITALY
BULGARIA
SPAIN
GREECE
TURKEY
SYRIA
TUNISIA
MOROCCO
ISRAEL
IRAN
LIBYA
EGYPT
SAUDI ARABIA
CUBA
PANAMA
CHAD
SUDAN
ETHIOPIA
OMAN
YEMEN
zoom: 1.55
Elastic Maps Service
OpenStreetMap contributors
475
342

- Classified - Confidential -

*** **client**:




- Classified - Confidential -

- Classified - Confidential -

******:


# Proactive Threat Hunting

Our proactive threat hunting identified multiple security issues:

## Threat hunting:

https://*****.atlassian.net/browse/SEC-1610

https://*****.atlassian.net/browse/SEC-1611

## Security engineering: -

## User Access Management:

https://*****.atlassian.net/browseUAM-4326 , also UAM-4327 & UAM-4328

https:///*****.atlassian.net/browse/UAM-4324

- Classified - Confidential -

https:///*****.atlassian.net/browse/UAM-4315

# Security Notes

In our pursuit to enhance the security of your digital infrastructure, we've scrutinized the network's threat environment, identifying key areas needing urgent improvement. Among these, activities involving etcd servers within Docker containers have emerged as a critical concern. It's important to note that etcd is a distributed key-value store essential for storing data across a network of machines, ensuring data consistency and availability even during network partitions or machine failures.

The challenge with Dockerized etcd instances lies in the insufficient logging of internet activities, limiting our capability to investigate alerts comprehensively. Without detailed logs, our security team's ability to monitor, analyze, and mitigate potential threats is significantly compromised.

To address this, we recommend that your administration team implements or offer a logging mechanism for these Docker container instances, specifically those running etcd servers. Proper logging and auditing are crucial for an enhanced security monitoring framework, enabling us to conduct in-depth investigations and respond effectively to security incidents.

Moving forward, our focus will be on refining detection mechanisms to reduce false positives, bolstering threat intelligence integration, securing exposed services, and tightening Docker configurations. Improved communication about system changes will also reduce unnecessary alerts, optimizing our Security Operations Center (SOC) operations.

Investing in these areas will substantially improve our capacity to detect and respond to genuine threats, thereby strengthening our network's defense against cyber threats. Immediate action on these recommendations is essential for a more secure and resilient network infrastructure.

## Minimization of Public Exposure

We strongly recommend reducing the threat surface presented by public IP addresses. Critical systems and services that do not require public internet access should be transitioned to a Local Area Network (LAN) or a secured private cloud environment. This strategic move will significantly decrease the vulnerability of your systems to external threats and unauthorized access.