GoSecure

December 2019

MDR RISK SUMMARY REPORT

Contents

Executive Summary

The following report supplies a brief summary of network and threat activity observed during the month of December. This information includes traffic analysis statistics as well as a summary of all event escalations.

If you have any questions regarding this report or its contents, please contact the Active Response Centre (ARC) at arc@gosecure.net.

Maintaining Your Security Coverage

To help maintain the security of your environment, we ask that you consider the following items and ensure that MDR is fully integrated with your internal processes.

Personnel Changes

When a member of your security team leaves your organization or transfers to another team, we ask that you inform the ARC so we can perform the following changes:

- Disable access to the MDR dashboard
- Issue a new Client ID to your organization
- Update your escalation path if required*

When a team member is added, please let us know if they require dashboard access, or if your escalation path will require updating.

*We highly recommend maintaining an email distribution list to help your team manage the list of personnel who receive communications from the ARC as these communications may contain sensitive information.

Endpoint Protection

To maintain endpoint protection, it is imperative that the latest Endpoint Detection & Response (EDR) sensor be installed on all applicable assets in your environment. To accomplish this, we recommend the following best practices:

- Integrate the latest EDR sensor into your golden images
- Include the latest EDR sensor within your patching processes, keeping in mind the requirements for patch-related pending reboots to be completed prior to sensor deployment
- Regularly cross reference your EDR deployment list (available from your client dashboard) with your asset management solution to ensure all endpoints are fully covered and reporting to our cluster, and that outdated entries in the EDR deployment list are removed

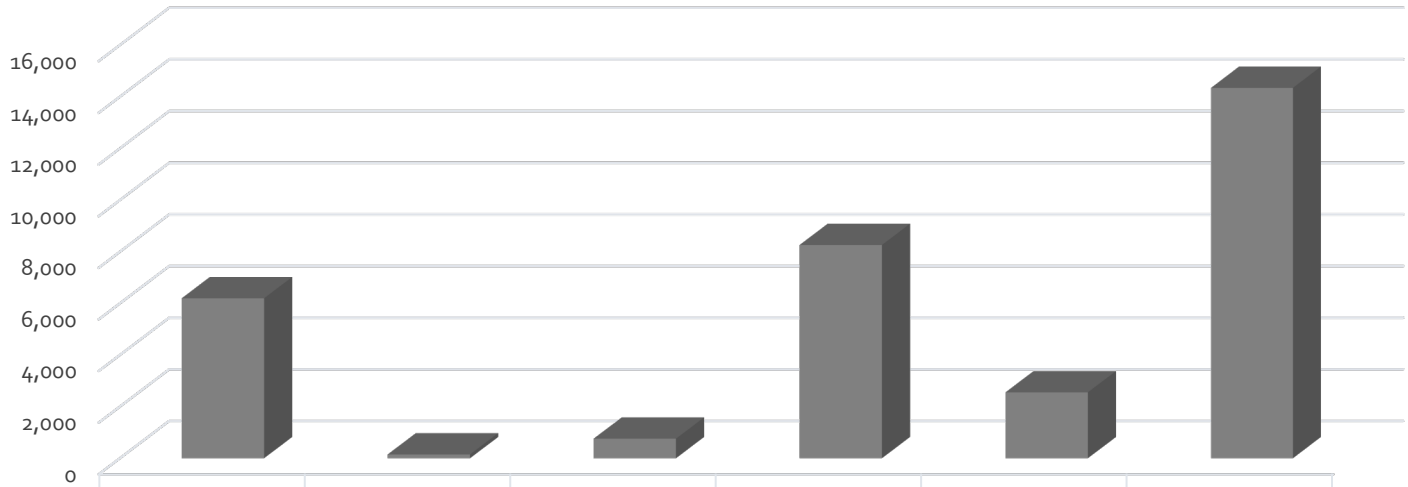
Infrastructure Updates

Following any alterations to critical infrastructure in your environment, we ask that you perform the following:

- Confirm your network spanning configuration to ensure the visibility of the ARC appliance has not been negatively affected
- Reference the logging sources page of the dashboard to ensure that the ARC is receiving logs from all required sources
- Provide updated network documentation to the ARC so we can update our situational awareness of your environment

Traffic Analysis

Below you will find a visual representation of the potentially malicious traffic observed during the month of December. After detection, all events are investigated to remove false positives and determine if the events pose a threat to your environment.



	Trojan and CNC	Phishing	Malicious Communication	Brute Force	Policy Violation	Scanning Activity
Network Events	6,197	146	756	8,261	2,553	14,342

Traffic Type Categorization

Trojan/CNC Activity: Network traffic indicating potential compromised endpoints including communication to known command and control servers.

Phishing Activity: Email and website attempts leveraging social engineering techniques to manipulate users into clicking a malicious link or devolving personal information and credentials.

Malicious Communication: External Exploit Attempts, Malware, Spyware, Adware, Tool Bars or various other Potentially Unwanted Programs.

Brute Force Attempts: Attempts to gain access to internal systems by employing repeat password-guessing techniques.

Policy Violations: General policy violations including TOR traffic, P2P activity, explicit content and user credentials showing up in plain text or Base64 in outbound traffic.

Scanning Activity: External vulnerability scanners and attempts to gain private information about your network.

Log Sources

During the month of December, we have received logs from **11 sources**. A comprehensive, live list of all log sources is available from your client dashboard.

Please note that clients are responsible for ensuring that all required logs sources are provided to the ARC for analysis. This list should be reviewed following any network changes to ensure that visibility has not been affected.

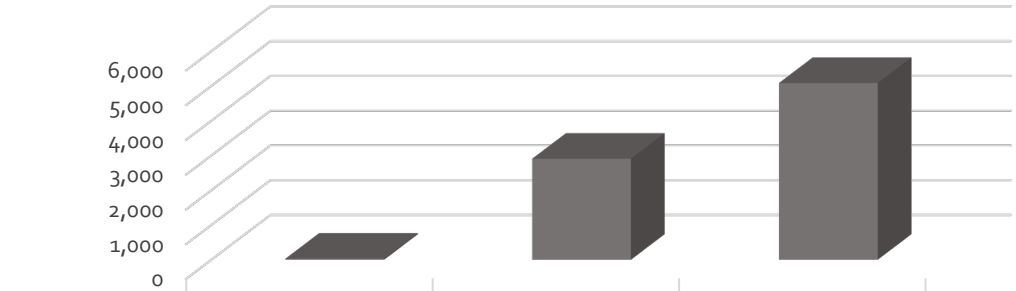
Log Sources No Longer Reporting

The following sources have stopped providing logs to our appliance within the last 6 months. Please let us know which of these systems can be removed from the list as decommissioned log sources. Any unexpected list entries should be examined to ensure continued monitoring via the LIDS service.

Source	IP Address	Last Modified Timestamp
FW-575	172.18.2.252	2019-10-30 15:14:32 UTC
FW-578	172.18.2.253	2019-10-30 15:03:13 UTC
FE-536	172.18.2.254	2019-10-30 15:03:03 UTC

Endpoint Detection & Response

There were over **322.7 million basic network events** analyzed for evidence of compromise during the month of December.



	Classifications	Traces	Key Events
Observed Events	30	2,906	5,084

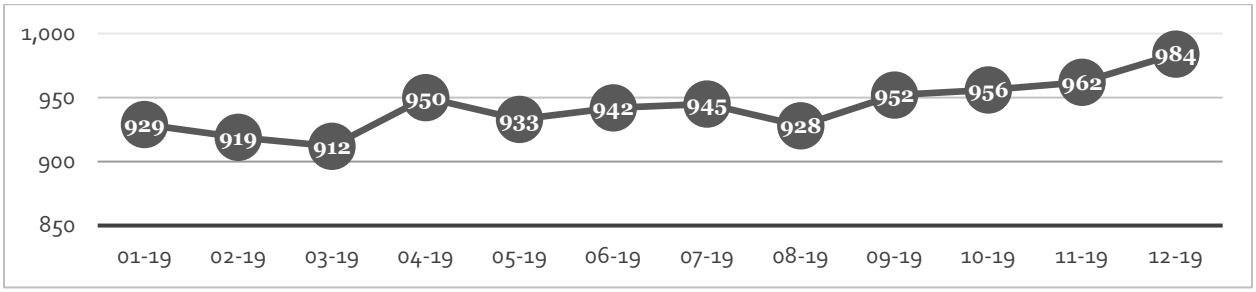
Classifications: Patterns of behavior characteristic of known malware families, techniques used by malware and other attempts to undermine endpoint integrity.

Traces: A set of related interactions starting from an origin event, following the evolution of activity over time. Used to provide context around suspicious interactions by exposing not only the suspicious interaction itself but the impact of that interaction on the operating system.

Key Events: Call out important interactions within a trace.

EDR Endpoint Count

At the time of this report there were **984 EDR sensors** installed in your environment. A detailed account of all currently monitored endpoints can be obtained from your client dashboard. Sensor deployment for your organization over time can be viewed in the below graph.

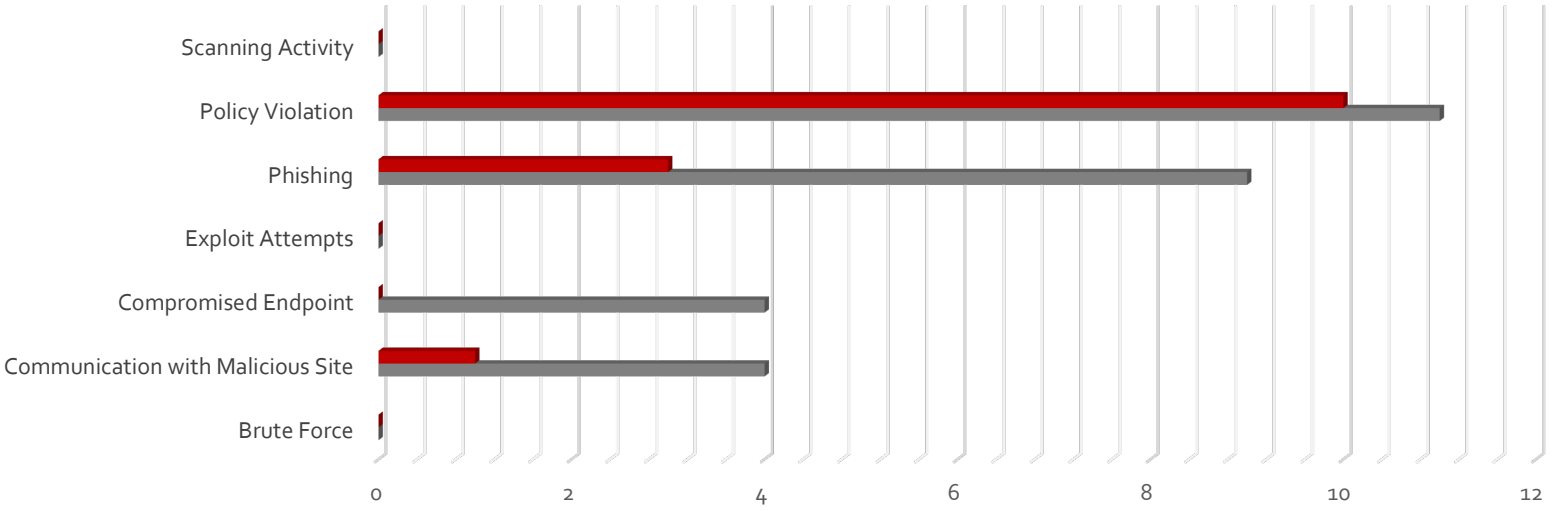


To ensure ongoing visibility, please ensure that the EDR sensor is included in your golden images and patching process.

Alert and Observed Threat Summary

The threat activity summary demonstrates new potential threats observed interacting with your environment during the month of December.

The following graph serves to represent new threats only and does not show activity from sources previously investigated or alerted on. The numbers displayed are based on the volume of sources found, not the amount of activity seen from each of those sources.



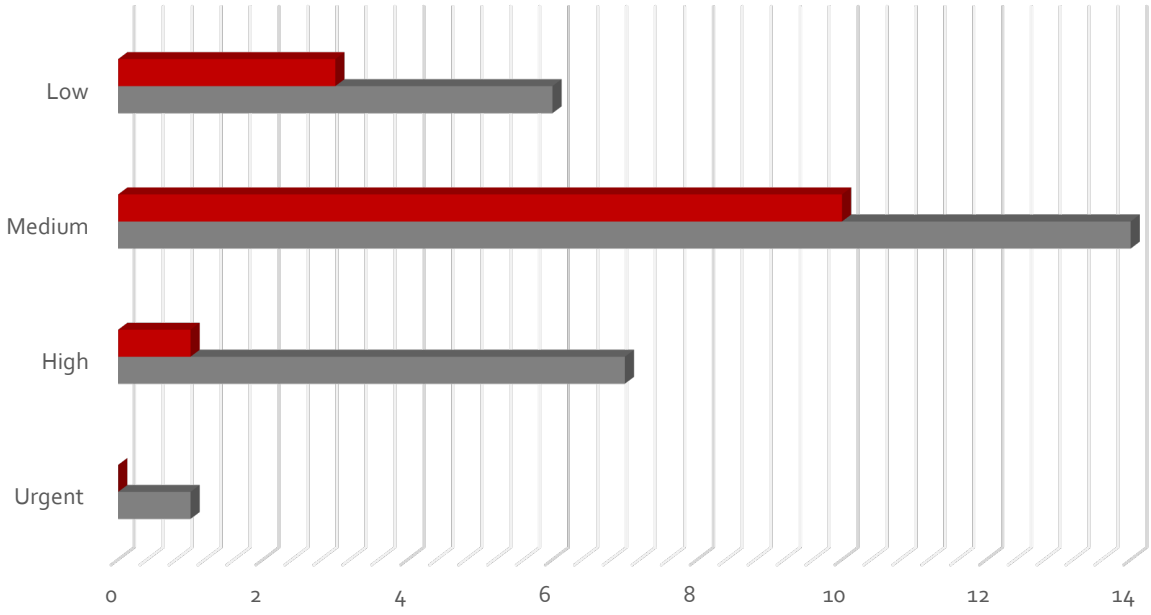
	Brute Force	Communication with Malicious Site	Compromised Endpoint	Exploit Attempts	Phishing	Policy Violation	Scanning Activity
Alerts	0	1	0	0	3	10	0
Deep Dive	0	4	4	0	9	11	0

A "**Deep Dive**" is a security incident investigation that occurs when in-depth analysis is required to validate a potential threat and/or determine the impact of an incident that occurred. Only new threats spawn unique deep dives. If multiple events are related or the incidents follow the same pattern, they are collected in the same deep dive record to assist in ongoing pattern analysis.

The "**Alerts**" metric represents the alerts that have been escalated to your team divided by the type of activity observed.

Threat Priority

The following chart depicts Alerts and Observed Threats for the month of December divided by priority level.



	Urgent	High	Medium	Low
Alerts	0	1	10	3
Deep Dive	1	7	14	6

Urgent: High impact threats that cannot be mitigated by GoSecure. This includes successful phishing attacks and the compromise of endpoints where EDR is not installed. These events should be addressed by your security team as soon as possible.

High: High impact incidents such as the presence of a malicious file/email or compromised endpoints which have been placed in quarantine. Although these events should be dealt with as soon as possible, the threat is not spreading or actively exfiltrating data.

Medium: Potential threats including exploit and phishing attempts, recon scans and brute force activity. This activity should be addressed when resources are available.

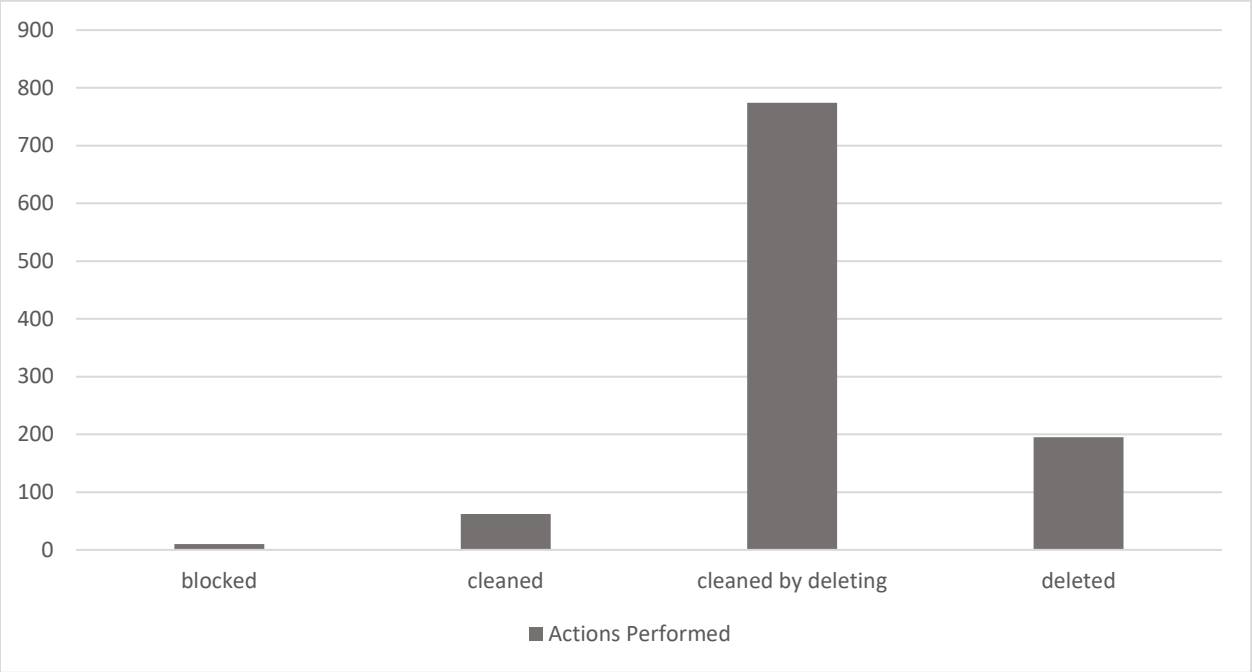
Low: These events expose your organization to risk and increase the likelihood of a future compromise. Events in this category include policy violations, potentially unwanted programs and user credentials visible in clear text. These events should be addressed to reduce risk to your organization.

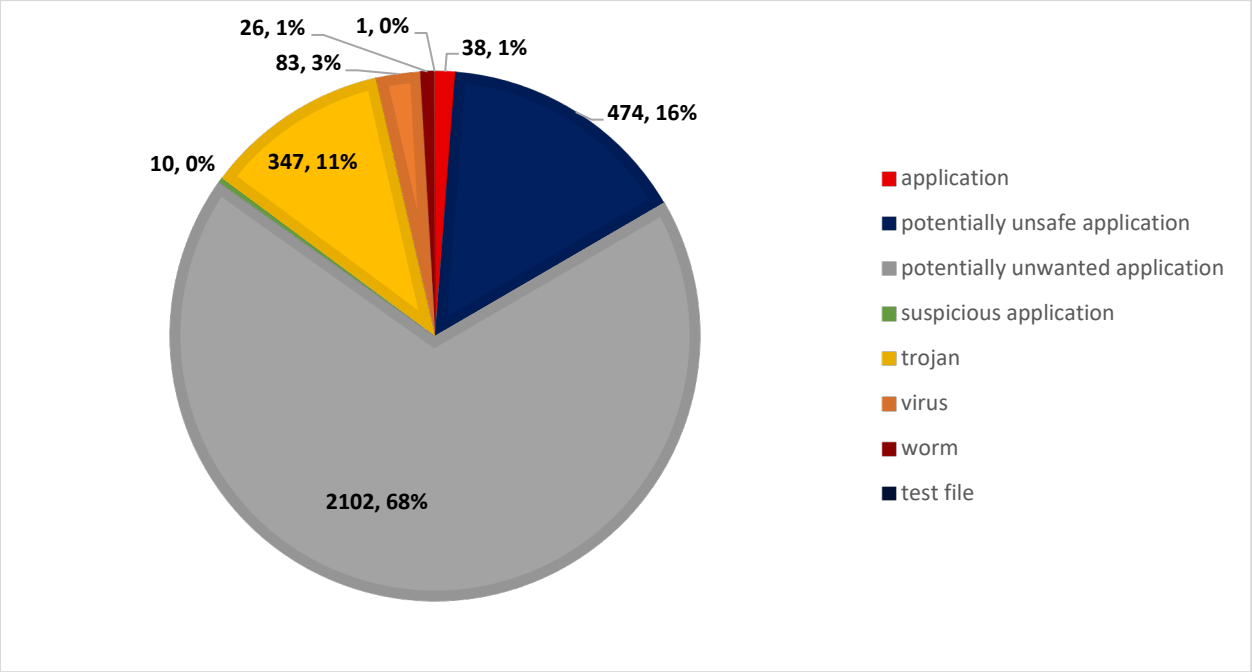
ESET Anti-virus

There were over **30.5 million items scanned** by ESET during the month of December.

Of those, **4151** were determined to be potential threats and **3082** were actioned. Please note, multiple potential threats may be handled by a single action.

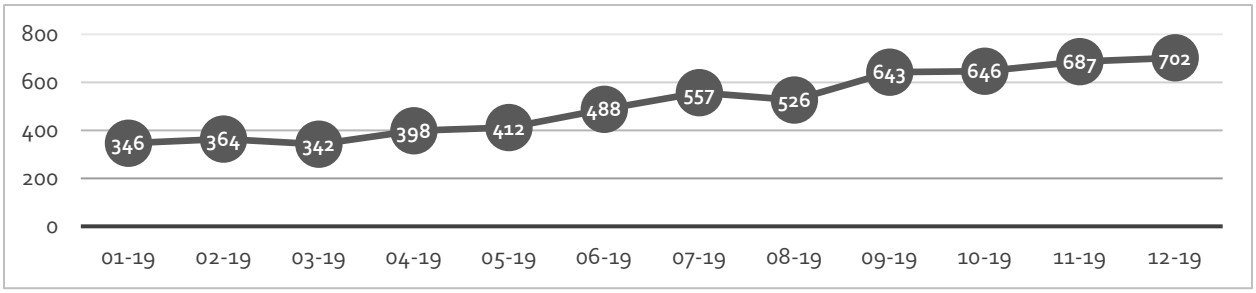
The following charts depict the actions taken and types of items actioned by ESET in December:





ESET Endpoint Count

At the time of this report there were **702 ESET anti-virus agents** installed in your environment. Agent deployment for your organization over time can be viewed in the below graph.



To ensure ongoing visibility, please ensure that the ESET agent is included in your golden images and patching process.