EXECUTIVE SUMMARY REPORT

Date **Dec 19 12:00:00 AM** to **Dec 19 11:59:59 PM**

Please review this security report completely. Some unsafe processes or communications with bad reputed IP addresses may have been terminated by EventTracker sensors, to protect your systems from a potential security breach in accordance with the MDR guidance you provided to EventTracker. It is possible that the terminations were in response to a "false positive" due to an improperly categorized process hash or reputation lookup. If you would like to get more information or have questions regarding your MDR guidance or threat analysis data interpretation, email us at essentials-support@eventtracker.com

104	97	7	0
Total number of alerts during this period	Potential Cyber Breaches	Indicators of Compromise	Potential Insider Threats

Potential Cyber Breaches

This section lists all unsafe communications and processes.
Stopping lateral movement of malware/breach: When EventTracker detects a potentially unsafe process or connection to a bad IP address on a system, the threat is communicated to other systems protected by the siem-at-the-edge services.

Terminated connections to reputed BAD IP address(es).

Description: Below listed processes were observed connecting to bad IP address.

Recommendation: Review the processes listed below and confirm if they are legitimate or should continue to be part of the Unsafe List.

0 INCIDENTS: SHOW

Terminated processes with black-listed hash.

Description: Below listed processes were observed having black listed hash .

Recommendation: Review the processes listed below and confirm if they are legitimate or should continue to be part of the Black List.

0 INCIDENTS: SHOW

New process connected to site / IP address with a bad reputation.

Description: New Processes listed below were observed connecting to bad IP address.

Recommendation: Review the processes listed below and confirm if they are legitimate or should be part of the Black List.

0 INCIDENTS: SHOW

New TCP entry point opened.

Description: New TCP port(s) have been opened.

Recommendation: Must be reviewed and authorized/blocked.

97 INCIDENTS: SHOW

Unsafe Process / DLL executed.

Description: Process (EXE)/DLL with Suspicious Hash has been executed.

Recommendation: Please evaluate the impact. If required isolate the system(s) from your network.

0 INCIDENTS: SHOW

Indicators of Compromise

Critical Incidents to be reviewed for indications of compromise. If you find this activity suspicious, you may need to communicate with your end users and take appropriate steps to improve threat awareness. If you need more information on a particular activity, please contact your security analyst or email us at essentials-support@eventtracker.com

USB Activities

Description: The following users have inserted mass storage device(s) and perfomed the activities.

Recommendation: If they are authorized users, please let us know so we can update our safe list.

5 INCIDENTS: SHOW

New service started.

Description: System(s) have been modified. New service has been started. This is indicative of compromise and should be reviewed immediately.

Recommendation: If you determine that a service might be suspicious isolate the affected system from your network pending remediation.

0 INCIDENTS: SHOW

New software has been installed on your network.

Description: The unknown or unapproved software is installed in one/multiple system(s) in your environment.

Recommendation: It is important to review software and publisher/vendor. If the software is authorized, notify essentials-support@eventtracker.com and we will update your approved safe list.

2 INCIDENTS: SHOW

Out of Ordinary activities from IP address(es).

Description: Sudden and Out of ordinary IP address activity on your network requires attention.

Recommendation: Please review why there is a sudden and significant increased activity from the below IP address(es).

0 INCIDENTS: SHOW

Potential Insider Threats

This section highlights changes in your user activities. You need to quickly review the following critical/major changes in user activities.

Out of Ordinary activities from a/multiple user(s)

Description: Sudden and Out of Ordinary user activity requires attention.

Recommendation: Please review why there is a sudden and significant increased activity from a particular user(s).

0 INCIDENTS: SHOW

User (s) added to admin group.

Description: Administrator has enormous power in customer enterprise. You need to be fully aware of who has been set to have admin privileges.

Recommendation: Please review the user(s) added to admin group by the administrator.

0 INCIDENTS: SHOW

User Affinity.

Description: Behavior based unusual logon - critical review for Inside threat.

Recommendation: Why did the "New User" log into the system - Is it a valid activity?

0 INCIDENTS: SHOW

User Created.

Description: The following user(s) has been created.

Recommendation: Make sure all users are created by system administrator. Make sure there are no phantom users or unknown users.

0 INCIDENTS: SHOW

Multiple logon failures by user (s) (>10).

Description: Multiple logon failures from multiple user(s).

Recommendation: Please investigate. Excessive logon failure from a user(s) represents either serious misconfiguration or a serious inside threats.

0 INCIDENTS: SHOW

Multiple logon failures from a/multiple remote IP address(es).

Description: Multiple logon failures from multiple remote IP address(es).

Recommendation: Please investigate. Excessive logon failure from a IP address(es) represents either serious misconfiguration or a serious inside threats.

0 INCIDENTS: SHOW

Total number of incidents during this period

This section highlights number of incidents during this period

6 INCIDENTS: SHOW