

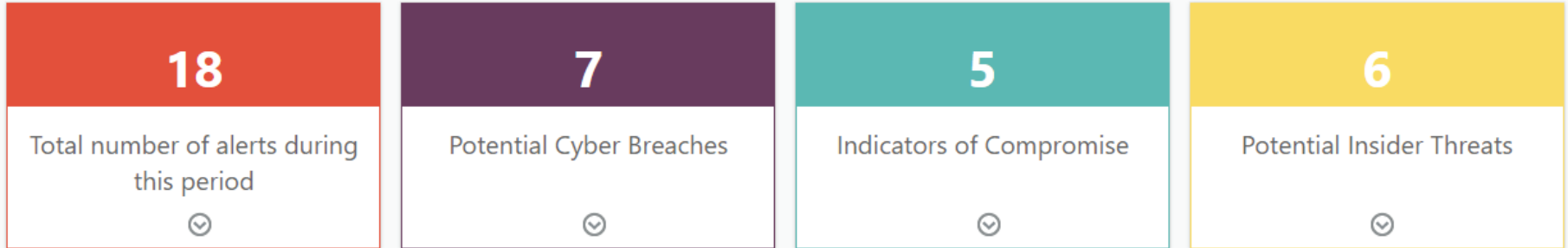
# Security Summary Report

Dashboard / Executive Summary

Site: PRI-SVR16-VM01 Published Report: Intech Essentials Sec Print

Date: May 25 12:00:00 AM to May 25 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 Netsurion sensors to protect your systems from a potential security breach, in accordance with the MDR guidance you provided to Netsurion. 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@netsurion.com



## Potential Cyber Breaches

This section lists all unsafe communications and processes. Stopping lateral movement of malware/breach: When Netsurion 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 Essentials services.

### Process has been terminated by Netsurion

**Description:** Process(es) listed, were observed connecting to IP address(es) with BAD reputation or not in the safe list or present in the unsafe list and connections were terminated.

**Recommendation:** Review the process(es) listed and confirm if they are legitimate or should continue to be part of the 'unsafe' list.

3 INCIDENTS: SHOW

### Critical potential breach from an unsafe IP.

**Description:** New processes listed, were observed connecting to IP address(es) with BAD reputation.

**Recommendation:** Review the process(es) listed and confirm if they are legitimate or should be part of the 'unsafe' list.

1 INCIDENTS: SHOW

### Process connected to an unsafe IP.

**Description:** Process(es) listed were observed connecting to unsafe IP address(es).

**Recommendation:** Please review the IP address(es) listed and if confirmed as unsafe and/or redundant, block these IP address(es).

1 INCIDENTS: SHOW

### **New TCP entry point opened.**

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

**Recommendation:** The new TCP port(s) that are listed, must be reviewed and either authorized or blocked.

2 INCIDENTS: SHOW

### **Anomalous login detected, critical threshold exceeded.**

**Description:** Repeated failed login attempts, which exceeded the critical threshold for a user or from an IP address was observed.

**Recommendation:** Investigate the user/IP activity to identify the root cause for the failed login attempts.

0 INCIDENTS: SHOW

### **Stopping anomalous login activity by adding to block list.**

**Description:** Repeated failed login attempts, which exceeded the critical threshold from an IP address was observed and stopped.

**Recommendation:** Action has been taken by EventTracker by adding the IP address to the block list (if windows firewall is enabled), OR IP address is added to the local IP block list file. If IP address is valid and to be allowed, remove from it from the blocked list in the windows firewall or in the local IP blocked list file.

0 INCIDENTS: SHOW

### **Successful login after anomalous login failure attempts.**

**Description:** Successful logon activities were, observed, all after multiple anomalous logon failed attempts.

**Recommendation:** Block access to the network for the user credential temporarily, until a thorough investigation into the login activity is completed.

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@netsurion.com](mailto:essentials@netsurion.com)

### USB activities.

**Description:** Users have inserted mass storage device(s) and performed the various listed activities.

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

1 INCIDENTS: SHOW

### Anomalous activities from an IP address.

**Description:** Repeated and multiple anomalous IP address activities on your network, requires your attention.

**Recommendation:** Do review, why there is sudden and significant increased anomalous activities from the listed IP address (es).

1 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:** Undertake an investigation, 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:** Listed new software has been installed in one/multiple system(s) in your network environment.

**Recommendation:** It is important to review the installed software and its publisher/vendor. If the software is authorized, notify [essentials@netsurion.com](mailto:essentials@netsurion.com) and we will update the approved safe list for your environment.

3 INCIDENTS: SHOW

### New windows network process activity.

**Description:** Listed new windows network process activity was observed on the system.

**Recommendation:** Do review the process activity and check if it is legitimate or not.

0 INCIDENTS: SHOW

### Unsafe process found.

**Description:** Listed unsafe process(es) were found on the system(s) specified.

**Recommendation:** Do review the process(es) and if it is (they are) trusted, notify [essentials@netsurion.com](mailto:essentials@netsurion.com) and the SOC team will add to the "safe" list.

0 INCIDENTS: SHOW

### Unsafe dormant process detected.

**Description:** Listed unsafe dormant process(es) were found on the system(s) specified.

**Recommendation:** Do review the listed dormant process(es) and if it is (they are) trusted, notify [essentials@netsurion.com](mailto:essentials@netsurion.com) and the SOC team will add to the "safe" list.

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.

### Anomalous activities from a user or multiple user(s).

**Description:** Repeated failed login attempts, for a user/multiple users has been observed and requires immediate attention.

**Recommendation:** Do review, why there is/are sudden and increased anomalous activity/activities from particular user(s).

1 INCIDENTS: SHOW

### User created.

**Description:** New user(s) has/have been created.

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

1 INCIDENTS: SHOW

### User(s) added to admin group.

**Description:** "Administrator" has extensive abilities in a customer enterprise. You need to be fully aware of which user has been provided with admin privileges. Also confirm that these privileges were provided by a system administrator.

**Recommendation:** Do review the user(s) added to "admin group" by the administrator.

2 INCIDENTS: SHOW

### User affinity.

**Description:** Logon(s) contrary to behavior, was observed - critical review for "insider threat".

**Recommendation:** Why did the "New User" log into the listed system(s)? Is it a valid activity? Confirm with the user.


2 INCIDENTS: SHOW

## Total number of incidents during this period

This section highlights number of incidents during this period

22 INCIDENTS: SHOW

*The information provided in this report is intended solely for the use of designated employees or agents of Intech. While every reasonable effort is made to ensure that the information provided in this report is accurate, no guarantees for the currency or accuracy of the information are made. The information herein is provided without any representation or endorsement made and without warranty of any kind, whether express or implied, including but not limited to the implied warranties of satisfactory quality, fitness for a particular purpose, non-infringement, compatibility, security and accuracy.*

TLP:AMBER  Limited disclosure, restricted to participants' organizations.

