Netsurion | EventTracker®

How to- Configure StealthINTERCEPT to forward logs to EventTracker

EventTracker v9.2 and above

Publication Date: August 4, 2020

Abstract

This guide helps you in configuring **StealthINTERCEPT** with EventTracker to receive **StealthINTERCEPT** events. In this guide, you will find the detailed procedures required for monitoring **StealthINTERCEPT.**

Scope

The configurations detailed in this guide are consistent with EventTracker version v9.2 or above and **StealthINTERCEPT.**

Audience

Administrators, who are assigned the task to monitor and manage **StealthINTERCEPT** events using **EventTracker.**

Table of Contents

1. Overview

StealthINTERCEPT monitors and prevents unwanted and unauthorized activities in real-time for active directory security and compliance. It inspects all active directory, exchange, and file system traffic at the source, it detects malicious and unintended changes in real-time to safeguard organization's credentials and unstructured data.

EventTracker's built-in knowledge pack enables you to gather business intelligence providing increased security, performance, availability, and reliability of your systems.

Through alerts, knowledge base solutions, and reports, EventTracker helps you correct problems before a disastrous failure occurs.

NOTE: Currently EventTracker supports only active directory monitoring by StealthINTERCEPT.

2. Prerequisites

- **EventTracker v9.2** or **above** should be installed.
- **Port 514** should be open.

3. Integrating StealthINTERCEPT with EventTracker

1. Log in to StealthINTERCEPT.
2. Open the **Administration** Console.
3. From the menu bar, select **Configuration → Alerts**.
4. Click **the SIEM tab**.
5. Click the button in front of **Disabled** to toggle the setting to **Enabled**.

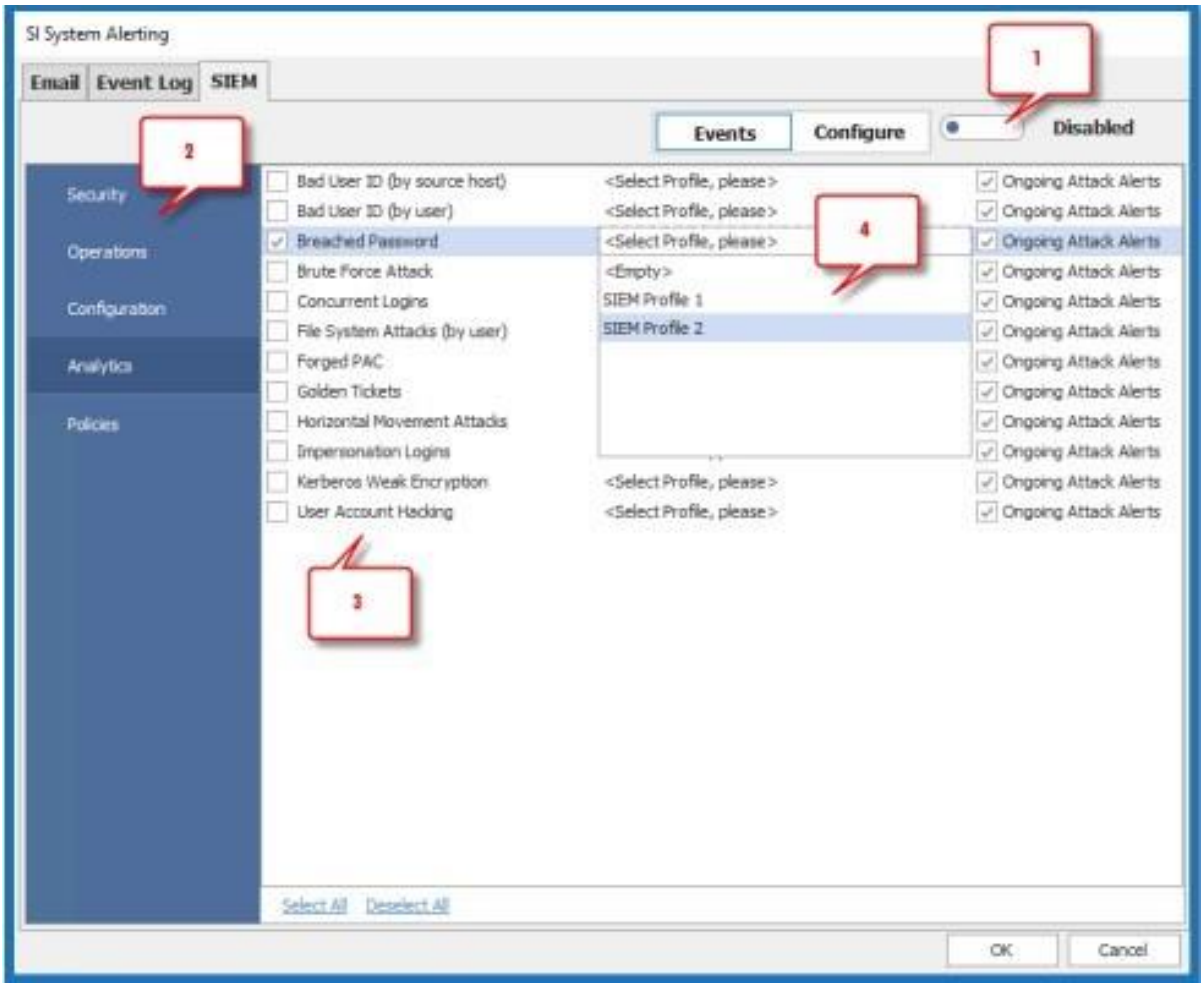

Figure 1

6. Click **Configure** in the SI System Alerting window.
7. Enter the **Protocol**.
8. Enter the **IP address** of the EventTracker in the Host Address field.
9. In the **Port** field, enter **514**.
10. From the Mapping File drop-down lists, select the "**Generic CEF format**".
11. Click **Events** and select the event types that you want for SIEM reporting.
12. Select the event category (Security, Operations, Configuration, Analytics, Policies) from the list on the left.
13. Check the event/incident/policy that triggers SIEM notifications from the center list.
14. Select the new Configured SIEM Profile to send alerts to.
15. Click OK to apply the new configuration.