Anomalous Login Detection in EventTracker
Abstract

This document gives a brief overview of the features that are introduced in EventTracker version 9.1 and above.

Audience

EventTracker SIEM users who wish to know about the Anomalous Login Detection feature that is added in EventTracker v9.1 and above.
# Table of Contents

1. Introduction to Anomalous Login................................................................. 3

2. Configuring Anomalous Login Detection..................................................... 3
1. Introduction to Anomalous Login

Anomalous Login is a method of attack such as a brute force attack by which the attacker is identifying the user name and password of the system or web page randomly. By generating the user name or password from a remote location, it can be compromised over time. From an unknown source, an attacker can try this by simulating a random number of passwords.

EventTracker agent is introducing a new kind of capability to identify Anomalous Login activity. Anomalous Login identification is based on user name and IP address.

- Prevention
  - Creation of new firewall rules for the Public IP address.
  - Adding the Public IP address to the EventTracker block list.

2. Configuring Anomalous Login Detection

1. Go to EventTracker Agent Configuration-> Network connections -> Advanced.
2. **Anomalous Login Detection Configuration** window opens.

3. Check the option "**Detect anomalous login activity**" to enable Anomalous Login Detection. Make sure that the "**Threshold to generate critical level event**" is greater than "**Threshold to generate information and warning level events**".

4. Event ID 3527 will be generated if logon threshold crosses information, warning and critical level with log levels information, warning and critical respectively.
Anomalous Login Detection will occur only when the threshold crosses the critical level that is entered.

- Block IP address in the Windows firewall.
- Add the IP address to the local unsafe list.
- Generate event if logon success is detected from the same user/IP address after the critical threshold level is crossed.

5. If the “Block IP address in Windows firewall” option is enabled, then the IP address will be added to the Windows firewall rule and generates an Event ID 3529.
6. If “Add the IP address to local unsafe list” option is enabled, the IP address will be added to the anomalous_data.bin file, which is in the following EventTracker installed path %ET_INSTALL_PATH%\Prism MicroSystems\EventTracker\Agent\Cache. When the IP address gets added to the Anomalous_data.bin file, Event ID 3530 will be generated.

7. If the “Generate event if logon success is detected from the same user/IP address after the critical threshold level is crossed” option is enabled then it will generate Event ID 3528, if the logon success happens from the same user/IP address after the critical threshold level is crossed.

8. If we provide “Unblock IP address after __ days” option, the IP address added in the Windows firewall or unsafe list will be unblocked after the enforcement period and it will generate Event ID 3529 for unblocking the rule and Event ID 3530 for unblocking the IP address.