EventTracker
Actionable Security Intelligence

EventTracker Intrusion Detection System

OVERVIEW

An Intrusion Detection System (IDS) plays an essential role in IT security by detecting potentially malicious activity within your network. But in order for an IDS to be effective, you need expert staff with disciplined processes so that the system is consistently tuned and configured.

But organizations already short on IT resources and time won't get any value out of an IDS if they don't have time to review what it's telling them. So, they trust EventTracker Intrusion Detection System to actively monitor their environment for unusual patterns and suspicious behavior.

Our customers enjoy:

Continuous monitoring:
Our expert staff manage your IDS service from our 24x7 Security Operations Center (SOC).

Complete and current knowledge library:
EventTracker's Knowledge Center is constantly updated by our own security experts to ensure that we are aware of any emerging threats.

Real-time alerting and escalation:
Alerts are generated in real-time and integrated into your customized EventTracker Incidents dashboard, which can launch notifications to designated personnel.

EventTracker
Actionable Security Intelligence

As a valuable component that is available as part of our managed service, SIEMphonic, our Intrusion Detection System:

More effective:
We configure, tune and maintain available rules to monitor your network, to ensure maximum ROI.

Able to respond to threats more quickly:
Our expert staff, working 24x7, review your IDS/IPS alerts in real-time and notify you immediately if there is any suspicious activity. We will then provide you remediation recommendations, so you spend less time fixing any issues.

Constantly updated:
Our IDS/IPS are integrated with numerous threat intelligence feeds, so they are constantly tuned to look for emerging threats that pose a risk to your network.

The Intrusion Detection System/ET-IPS service offering also includes the maintenance of Snort for signature, engine and platform updates.

SPECIFICATIONS

- Virtual Appliance on VMWare ESX 5.0 or higher
- CPU – 2.8 GHz minimum
- Memory – 4 GB
- VM Controller – LSI Logic RAID
- VM Hard Drive – SCSI type
- Disk – 60 GB
- Network Adaptor – 1