TXHunter – Endpoint Threat Hunting

THREAT HUNTING

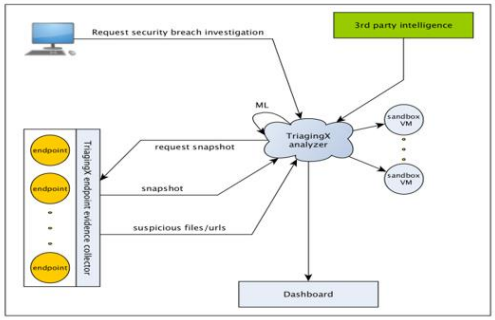
TXHunter integrates with SIEM & SOC workflow systems via RestAPI to selected endpoint systems to investigate and pass the behavioral data back.

IT SUPPORT

TXHunter enables IT support teams to remotely investigate unstable systems to identify if they have been compromised by malware before requiring re-imaging or system updates.

SECURITY OPERATIONS

TXHunter enables security teams to verify in minutes, whether high value laptops have been compromised while off the corporate network.



- Performs endpoint desktop or server breach investigations remotely with no permanent agent required. A continuous monitoring option available for systems that need to be baselined.
- The real-time threat hunting tool gathers the attack evidence, including memory, log and suspicious objects (PE, document files and URL's) in order to do automatic incident analysis
- Detects APT's, backdoors, spyware, hidden processes and rootkits, unusual network connections, mis-configurations and past abnormal activities

TXHunter is a new generation of machine-assisted hunters used for conducting highly focused threat incident investigations remotely. You only need to tell TXHunter which endpoints you want to investigate, download the disposable run-time agent to gather the data and wait for the analysis.

The agent takes a snapshot of the suspicious system and automatically conducts an incident investigation. If the investigation process identifies suspicious files or URL links, it will automatically launch the built-in sandbox capabilities for a behavior analysis. It is also integrated with third party engines and intelligence, to provide additional context on the detected objects.

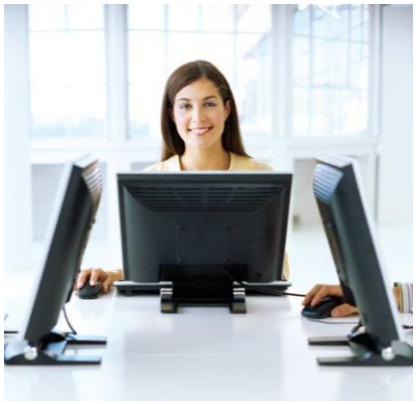
In about 5 to 10 minutes, TXHunter provides a straight and clear answer whether the endpoint has been infected or hacked, the severity level of that action and all supporting data.

"*Effective Incident Investigation requires speed of deployment and accuracy of the hunting tools. Using TXHunter we were able to establish the scope and severity of the attack on a critical server in our customer's environment in near real-time*"

Bill D. Global Risk Management Solutions, USA

TriagingX Inc.

Features and Benefits



Information Security teams who are investtigating potential breaches are often required to deploy endpoint detection response (EDR) sensors across the network environment to try and pick up evidence of system breaches or data exposure. This is the equivalent of casting a wide net to try and collect as many fish as possible, but not knowing exactly where they are, or what they are.

In contrast , by leveraging the TXHunter solution, incident response (IR) teams are able to quickly deploy a disposable client to suspect systems to promptly identify the presence of unknown and suspicious files on critical production Windows servers or endpoint systems. This allows the IR team to determine the extent and severity of the incident for risk analysis and remediation as early in the investigation process as possible

* Future releases will support Linux Server and Android OS platforms

TXSHIELD

Protects endpoint and datacenter systems against zero-day attacks without requiring patches.

TXSANDBOX

Analyzes unknown file and URL links according to their behaviors to detect new malware.

TRIAGINGX

We focus on the detection of zero day attacks, which are often unknown to traditional security solutions. Led by the team that successfully created the first generation malware sandbox used by many Fortune 500 companies for daily malware analysis.

For more information on any of our products or services please visit us on the Web at: www.triagingx.com

System Requirements

- **Target Systems:**
  Windows 7 SP1, Windows 8.1 , Windows 10
  Windows Server 2008 R2, 2012, 2016
- **Analyzer Server:**
  Deployable on Physical Server, VMWare/ESXi , Virtual Box , Cloud (ISO Image contains Centos 7.2)
- **Snapshot Data:**
  ~3 MB in size. Data sent in secured container transmitted via Windows Sockets API
- **3rd Party Intelligence:**
  Can run in isolated mode for sensitive networks, or configured to use intelligence data via RestAPI (VT)
- **Report Format:**
  HTML, PDF, JSON

DATA CATEGORIES COLLECTED

System Information
Process Information
Network Connections
Auto-Run Information
Event Information
Policy Information
File Information
Driver Information
Kernel Information

TriagingX Inc.

6050 Hellyer Ave, Suite 150-6
San Jose, CA 95138
tel: +1 408.568.7372
support@triagingx.com
www.triagingx.com