TXShield

Advanced protection for endpoints and datacenter servers against zero-day attacks, without requiring patches

Highlights

- Advanced endpoint and server protection against malware, fileless threats and hacking
- ➢ Provides early insights on new attacks methods
- ➢ Performs testing on other enterprise systems to identify which ones have similar weaknesses and protects them
- ➢ Mitigates attacks against those newly discovered unpatched or exposed systems
- ➢ Detects and blocks APT and zero-day attacks without requiring patches
- ➢ Reduces the number of false or irrelevant security alert

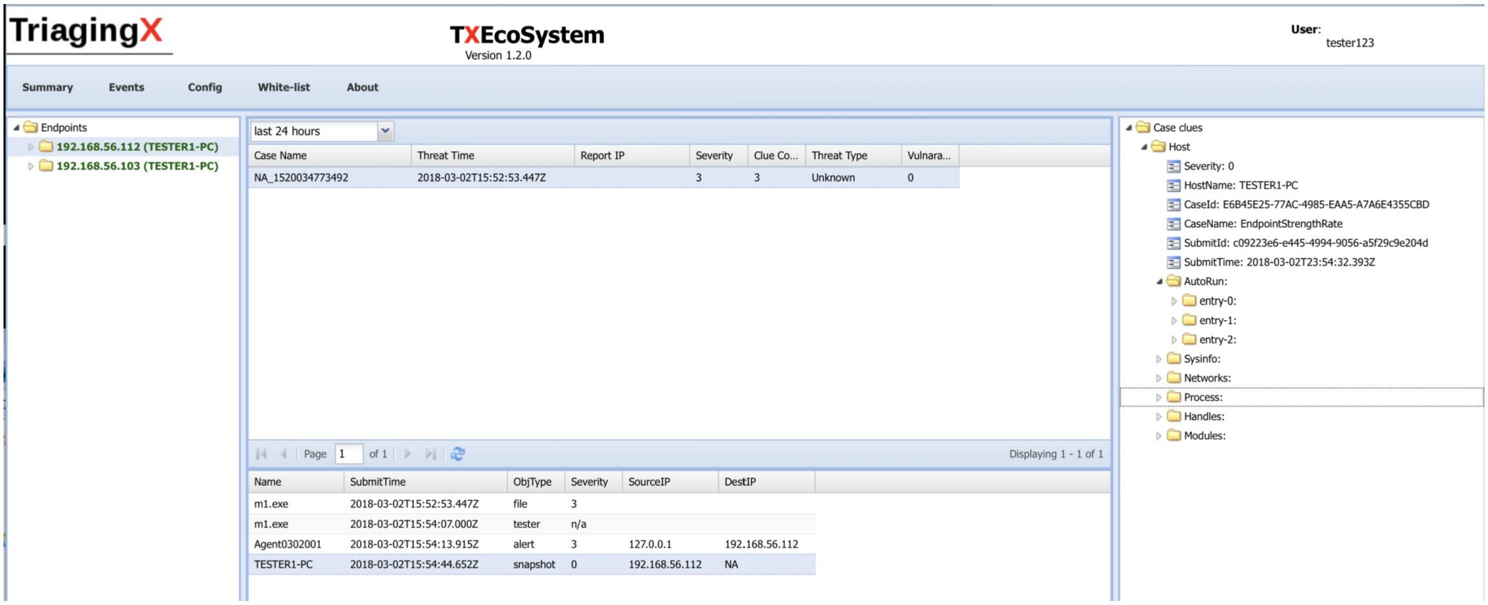
Overview

TXShield provides a real-time protection guard for datacenter servers and endpoint systems against known and zero-day attacks, either from hackers or malware, all without requiring rushed patch deployments.

It targets one of the major challenges in securing enterprise environments, how to reduce the asymmetric advantage enjoyed by attackers where they often only need to compromise one weakness, while defenders scramble to prioritize and fix scores of vulnerabilities.

TXShield aggregates and analyzes millions alerts and logs from IPS/FW/WAF/SIEM and endpoint systems, in order to protect against known attacks and automatically launch investigations on pre-attack reconnaissance and attacking incidences. It decodes the new attack method and conducts real-time penetration tests across the network to find the similar weaknesses in order to block a real attack, if such an attack is launched.

Report



Case Name	Threat Time	Report IP	Severity	Clue Co...	Threat Type	Vulnara...
NA_1520034773492	2018-03-02T15:52:53.447Z		3	3	Unknown	0

Name	SubmitTime	ObjType	Severity	SourceIP	DestIP
m1.exe	2018-03-02T15:52:53.447Z	file	3		
m1.exe	2018-03-02T15:54:07.000Z	tester	n/a		
Agent0302001	2018-03-02T15:54:13.915Z	alert	3	127.0.0.1	192.168.56.112
TESTER1-PC	2018-03-02T15:54:44.652Z	snapshot	0	192.168.56.112	NA

Case clues
Host
Severity: 0
HostName: TESTER1-PC
CaseId: E6B45E25-77AC-4985-EAA5-A7A6E4355CBD
CaseName: EndpointStrengthRate
SubmitId: c09223e6-e445-4994-9056-a5f29c9e204d
SubmitTime: 2018-03-02T23:54:32.393Z
AutoRun:
entry-0:
entry-1:
entry-2:
Sysinfo:
Networks:
Process:
Handles:
Modules:

TXShield

Deployment

TriagingX Analyzer Server

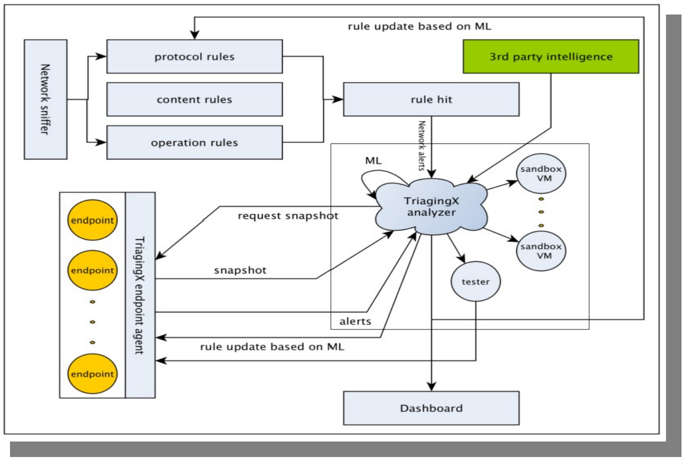
- Physical/VM server with minimum of 16 cores, 32G RAM, 2T HD, 2x1G NIC

TriagingX Network Sniffer (Option)

- Physical/VM server with minimum of 4 cores, 16G RAM, 200G HD

Download iso image from TriagingX support

Install and configure the systems



TriagingX Client

- Deliver installation package to each system that will be protected by Advanced Security Ecosystem
- Activate the installation package, msi, file to automatically complete the installation procedure
- Agent will automatically launch

Operation

- TriagingX's proactive agent installed on each business endpoint, workstation or server, constantly monitors suspicious behaviors and early indicators of attacks, sending this data to the analyzer server for correlation analysis.
- Other inputs, such as syslog, SIEM, system events and third party intelligence can also be sent to the analyzer server for integrated analysis.
- TriagingX's optional network sniffer, sitting on switch's span port, constantly monitors suspicious network contents, protocol violations, early attack indicators, also sends data to the server for correlation analysis.
- TriagingX Analyzer server automatically connects to multiple Sandboxes to perform behavior analysis on suspicious files and URLs
- Using the web based GUI interface the threat hunter can also acquire a snapshot from a remote endpoint system that is involved in triage process.

Specifications

Target System :	Windows 7, 8, 10, 2008R2
Analyzer Server :	Physical or VMWare Server (ISO Image contains Centos 7.0)
3rd Party Intelligence :	RestAPI (VT)
Report Format :	PDF

About TriagingX, Inc

TriagingX is headquartered in Silicon Valley. Our team successfully created the first-generation malware sandbox that is being used by many fortune 500 companies for daily malware analysis. We have recently designed and built the advanced security Ecosystem that provides complete protection for endpoint systems and datacenter servers against zero-day attacks, without requiring any patches. We are targeting security's root problem in order to help our clients always stay ahead of the attacker.