# Veramine Inc.

Cyber Security

APT Malware

Deception

SOC EDR

DLP

IR

# Veramine Outstanding Features

The followings are quite unique to Veramine

## Data Collection

1) Quality of collected data: Wide Variety. In Details. Relevance. Small Traffic. The collection of all security-related activities, some important Windows events, especially System Security and SMB data, is probably only offered by Veramine, as follows.

- Process: creation, image loads, command arguments; open, injection, remote process access, remote thread creation

- Registry: key access, value operations, Windows registry key when modify/create

- System Security: security tokens and flags, privileges, file security, binary policy violations, service tracking

- Network: protocols such as TCP and UDP, connections and ports, DNS cache monitoring, URL access

- User: logon sessions, privileges, using console, remote or local

- SMB: sessions and file access

- Binaries: all loaded binaries

2) Collection continuous in real time: Some other products only pull the data from an endpoint to the server as the admin requests

3) Flexible collection policies: The admin can select what data to collect. That's also good for under-powered machines

4) Adaptive filter: When sensor detects a repeating event pattern, or determines that a high-volume event is unlikely to be important for detection or analysis, it does not send it to server. This can filter out TB's of traffic being sent by sensor and processed by server. It's the reason we can collect so much stuff and still limit bandwidth to a small amount.

5) Providing raw data: We are willing to provide the raw collected data outside of the product.

## Detection

1) Aim to detect all attack tactics (kill chain: exploits, payloads, spreading, C&C, actions…) and techniques in https://attack.mitre.org/wiki/Technique_Matrix, the Attack Dictionary.

2) More collected data types allow more types of data analysis algorithms, that result in better Detection, especially for Behavior-based Detections. Examples

- SMB data allows detecting Lateral Movement and Insider Threat

- Precise Elevation of Privilege (EOP) detection by collecting security tokens

- Lsass process open allows detecting credentials and passwords dumping (Mimikatz)

- Command arguments allow detecting Malicious Powershell Fileless intrusion

- Unusual process migration and in-memory process injection

- Process loading binaries allows detecting Dll sideloading/planting

- Executables run after being recently downloaded from the internet

3) Combine Rule-based and Machine Learning. Examples of machine-learning detection algorithms:

- Process profiling: deviances from norms of process behavior

- User tracking: deviances from norms of user logon & logoff behavior

- Data exfiltration: deviances from historical and seasonal norms of network volume

- SMB tracking: deviances from normal SMB behaviors indicating lateral movement

Detection alerts could be sent over email for quick notifications. Detection could be also easily sorted by time through Veramine’s portal’s interactive dash board.

## Investigation

Yara Search on Memory: A killer unique Incident Response feature that only Veramine have. Sensor reports processes matching yara expression (per process, not only system match).

Yara Search on Files: Sensor intelligently uploads every binary loaded. Immediately scan every new file with Yara. Automatically block every Yara match.

Veramine enable search rules to be created and modified in order to search for attacks

Host or Process Memory dumps for forensics is at fingertips.

All collected data is searchable using very flexible logical expressions including process name, hash, command, IP etc. Each alert level of detection can be filtered and viewed separately.

All executable binaries are collected.

## Response Actions

VEDR has most Response Actions, from Binaries, Users, Hosts to Processes, whereas most other products just have Binary Blocking or Host Quarantine. Veramine could also guide response for some basic event.

- Host: Network Quarantine, Memory Dump, Yara Search on Memory, Start/Stop Monitoring, Sleep/Shutdown/Restart

- Process: Network Quarantine, Memory Dump, Yara Search on Memory, Suspend, Terminate

- User: Disable/Enable, Disconnect User Session

- Binary/Files: Network Quarantine, Block, Scan with Virus Total, Quarantine Files

## Deception

Uniquely offered by Veramine as an Active Defense approach, whereas most existing approaches are Passive Defense.

Deceptive services, processes, files, mutexes, events, listeners, credentials, shares, registries.

Capable of making every computer (physical or VM) a honeypot, in IT Systems.

Platform of Traps, put along the kill chain, to cheat, detect and prevent intrusions.

Track intruders' activities, and limit things they can do, with the traps.

E.g. WannaCry checks a mutex to decide if a system is already infected. We can set such a deceptive mutex.

## Performance

Only VEDR sensors can claim on average taking less than 1% CPU and 20 MB RAM.

On average, per host, network traffic is less than 30 MB / 1 day. It can be further tuned using collection policies which allows to configure which events are collected by sensors.

## Deployment

Installation, by just running "phantom -install", is so simple that VEDR can be deployed to several clients in various ways such as AD, SCCM or psexec. Update is also easy. Veramine agents could be started or stopped easily through Veramine's Portal.

As per conflicts - we shouldn't have any conflicts with a correctly designed security or AV product including McAfee AV, Kaspersky EPP, Trend Micro AV, Symantec AV etc. When implementing our sensor, we follow all rules and recommendation related to modules operating environment cooperation and compatibility.

Veramine sensors could also be deployed on both Windows and Linux. Veramine support Windows 7 and all newer Windows versions, Windows Server 2008 R2 and all newer Windows Server versions.

Veramine support most mainstream Linux distros released up to 5y ago, running kernel version 3.x and up, basically ubuntu, centos, fedora, gentoo, slackware etc...

Veramine EDR are easily integrated with popular SIEM such as Splunk, IBM Qradar, ArcSight, ELK using syslog/json.

Veramine also support reporting in csv format.