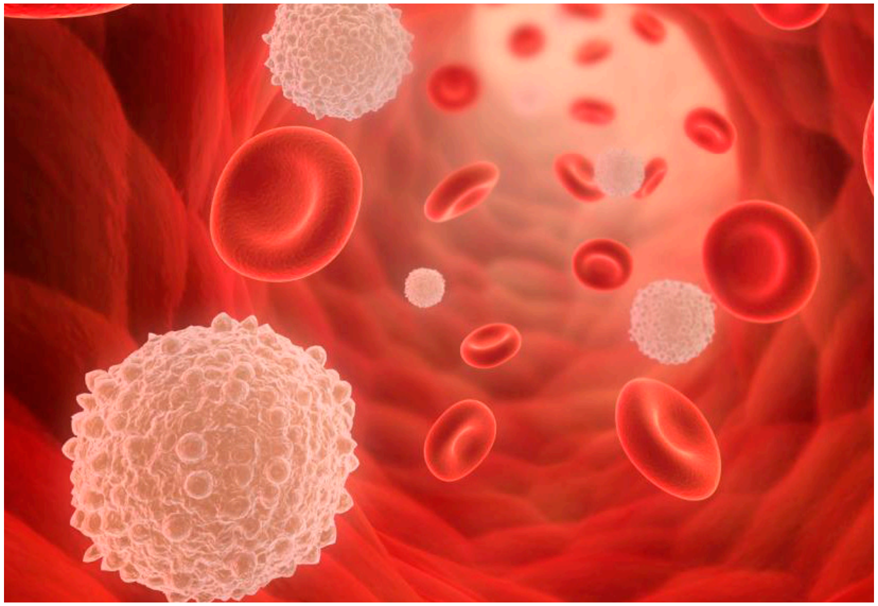
THREAT HUNTING PLAYBOOK

LEARN HOW TO EMBRACE A PROACTIVE SECURITY POSTURE

RANK

TABLE OF CONTENTS

INTRODUCTION:
BUILDING RESILIENCE



The human body has been said to be 'at war'.

Our bodies are constantly under attack from things that are trying to do it harm. These include toxins, bacteria, fungi, parasites and viruses. All of these can, under the right conditions, cause damage and destruction to parts of the body and if these were left unchecked, the human body would not be able to function. It is the purpose of the immune system to act as the body's own army, in defence against this constant stream of possible infections and toxins.

While we're all familiar with the immune system, it's less well-known that its ability to build resilience against attacks comes from two broad groups called the innate and the acquired immune systems. Each plays a specific role in building a robust security posture for the body.

The innate immune system is comprised of defences like the skin, lungs, eyes, stomach - all aimed at stopping the infection from getting into the body in the first place.

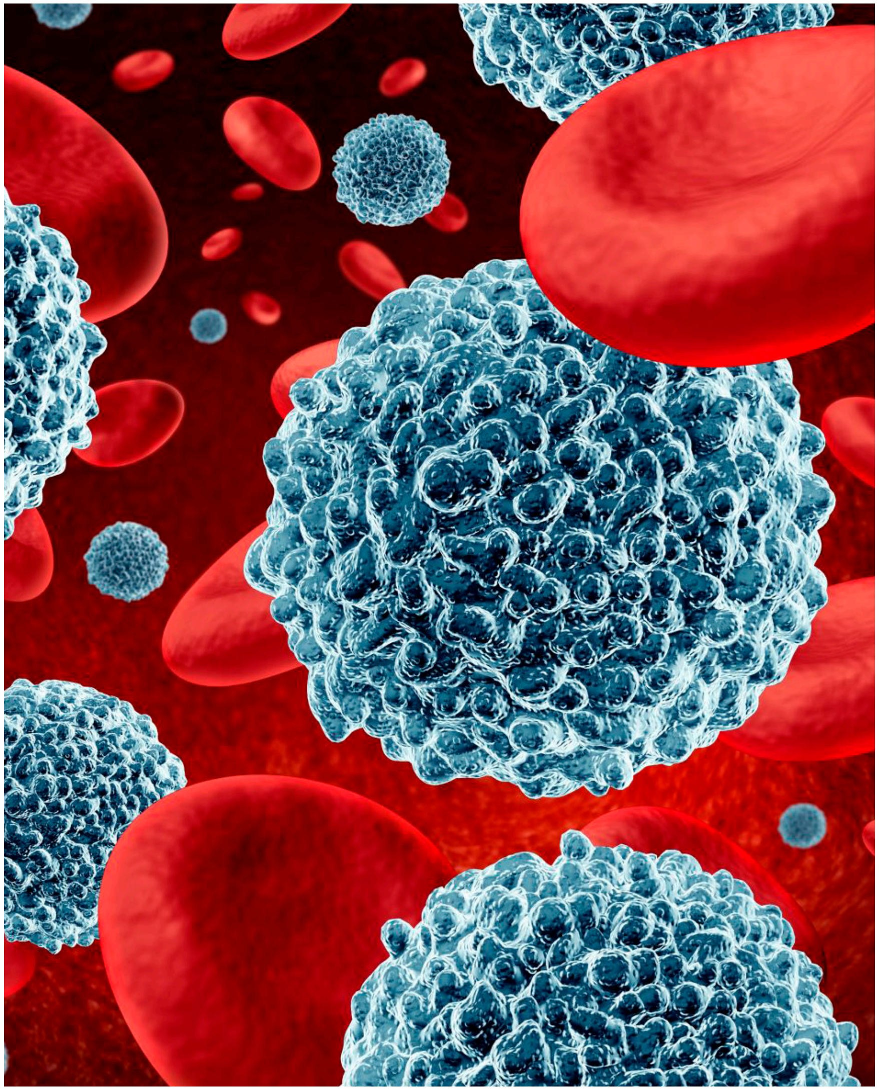
But our bodies are smart enough to know that infectious agents can and will get through the perimeter defenses, and so it has developed a second set of defenses. For example, our white blood cells exist to seek out and destroy foreign organisms.

The story of the human immune system shares many parallels with the challenges faced by today's enterprises. Just like the human body, enterprises are under constant attack with 230,000 new malware attacks launched every day. And just as the human body has multiple layers of security, progressive organizations are building resilience against these mounting threats by embracing a layered approach to security.

Security leaders are beginning to understand, just like the human body, that perimeter based defense systems are not ironclad and that threat actors will, eventually, get in. In response they're developing 'white blood cells' of their own in the form of new capabilities that will proactively hunt out threats and neutralize them.

Real time threat hunting has many benefits. It allows security analysts to focus on the most credible threats and to build a robust story around an event as it unfolds. CIOs are able to manage risk by arming the front line with tools, techniques and procedures to identify unknown and internal threats and increase team productivity.

This guide will help you to operationalize the real-time threat hunting methodology by unpacking which indicators of attack and compromise to monitor along with presenting threat hunting scenarios to further assist the SOC analyst in their threat hunt for a potential breach on their network.



INDICATORS OF THREAT ATTACKS

There are many indicators of compromise (IOC) and indicators of attack (IOA) that threat hunters look for. These IOCs/IOAs are signals on the network, that are forensic evidence of compromised activity, that could reveal a threat is imminent or has been successful. These IOCs, unusual activities, are footprints, that a threat hunter is searching for to prevent an imminent attack.

Here are some key indicators of compromise to monitor (in no particular order)[1]:

1. Unusual Outbound Network Traffic
2. Anomalies In Privileged User Account Activity
3. Geographical Irregularities
4. Other Log-In Red Flags
5. Swells In Database Read Volume
6. HTML Response Sizes
7. Large Numbers Of Requests For The Same File
8. Mismatched Port-Application Traffic
9. Suspicious Registry Or System File Changes
10. DNS Request Anomalies
11. Unexpected Patching Of Systems
12. Mobile Device Profile Changes
13. Bundles Of Data In The Wrong Places
14. Web Traffic With Unhuman Behavior
15. Signs Of DDoS Activity

[1] As reported by Dark Reading: https://www.darkreading.com/attacks-breaches/top-15-indicators-of-compromise/d/d-id/1140647?page_number=1

1.

UNUSUAL OUTBOUND NETWORK TRAFFIC

The threat hunter should look for suspicious traffic leaving the network.

Watch for activity within the network and look for traffic leaving your perimeter. Compromised systems will often call home to command-and-control servers, and this traffic may be visible before any real damage is done.

VASA Note: Out of the box, VASA will detect any unusual Outbound Network Traffic. Our Machine Learning Algorithms will generate Alerts for any anomalous event deviating from the standard user/ machine behaviours. The following are some of the built-in-detections. Customized rules can be created to address a specific scenario.

- Successful connections to and from servers with bad reputation. The reputation intelligence comes from multiple open source intelligence feeds - OSINT, OTX, MalwareDomainList.com, PhishTank. Paid intelligence feeds like Kasperky, DGA Archive etc. are supported if you have a license for the feeds.
- Outgoing traffic to TOR exit nodes.
- Excessive outgoing RDP connections from a host.
- Outgoing access to popular crypto currency mining domains.
- Non-proxy http access.
- Excessive NXDOMAIN responses to DNS queries on any host.
- External DNS servers being used.
- Non-standard DNS servers being used.
- Non-standard SMTP servers being used.
- External SMTP servers being used.
- RDP brute force attack – multiple RDP failures followed by a success.

2. ANOMALIES IN PRIVILEGED USER ACCOUNT ACTIVITY

A well-prepared attack is when attackers either escalate privileges of accounts they've already compromised or use that compromise to leapfrog into other accounts with higher privileges. Keeping tabs on unusual account behavior from privileged accounts not only watches out for insider attacks, but also account takeover. Watching for changes — such as time of activity, systems accessed, type or volume of information accessed — will provide early indication of a breach.

VASA Note: RANK's VASA has built in support for this scenario. With the assumption that End Point Logs are being collected, upon privileges changes, VASA will trigger a High Risk Score Alert, indicating a possible malware detection.

3. GEOGRAPHICAL IRREGULARITIES

Geographical irregularities in log-ins and access patterns can provide good evidence that attackers are pulling strings from far away. For example, traffic between countries that a company doesn't do business with offers reason for pause.

Similarly, when one account logs in within a short period of time from different IPs around the world, that's a good indication of trouble.

VASA Note: By default, VASA creates a baseline behaviour for clusters of users and machines. When VASA detects geographical irregularities in log-ins, or from abnormal locations/IPs, or timeframes, VASA will trigger Alerts to signal the Anomaly detected.

4. OTHER LOG-IN RED FLAGS

Log-in irregularities and failures can provide excellent clues of network and system probing by attackers. Check for failed logins using user accounts that don't exist — these often indicate someone is trying to guess a user's account credentials and gain authorization Similarly, attempted and successful log-in activity after hours can provide clues that it isn't really an employee who is accessing data.

VASA Note: As in the previous section, VASA will generate Alerts for any unusual successful or unsuccessful login activity.

5. SWELLS IN DATABASE READ VOLUME

Once an attacker has made it into the network, they seek to exfiltrate information, there will be signs that someone has been mucking about data stores. One of them is a spike in database read volume.

VASA Note: VASA's built in intelligence will sense any anomaly in swells of Database Read Volumes, as well as any increase in SMB file transfers, and trigger the respective Alert.

6.

HTML RESPONSE SIZES

If attackers use SQL injection to extract data through a Web application, the requests issued by them will usually have a larger HTML response size than a normal request.

For example, if the attacker extracts the full credit card database, then a single response for that attacker might be 20 to 50 MB, where a normal response is only 200 KB.

VASA Note: VASA will detect any unusual HTML response size larger than a normal request.

7.

LARGE NUMBERS OF REQUESTS FOR THE SAME FILE

It takes a lot of trial and error to compromise a site — attackers have to keep trying different exploits to find ones that stick. And when they find signs that an exploit might be successful, they'll frequently use different permutations to launch it.

So while the URL they are attacking will change on each request, the actual filename portion will probably stay the same. So you might see a single user or IP making 500 requests for 'join.php,' when normally a single IP or user would only request that page a few times max.

VASA Note: Any unusual, or high frequency scanning of internal machines, is indicative of reconnaissance activity. Vasa will trigger an associated alert when it detects this behaviour.

8.

MISMATCHED PORT-APPLICATION TRAFFIC

Attackers often take advantage of obscure ports to get around more simple Web filtering techniques. So if an application is using an unusual port, it could be sign of command-and-control traffic masquerading as “normal” application behavior.

For example, if you notice several instances of infected hosts sending C&C communications masked as DNS requests over port 80. At first glance, these requests may appear to be standard DNS queries; however, it is not until you actually look at those queries that you see the traffic going across a nonstandard port. DNS does not use port 80.

VASA Note: Protocol Masquerading is a default detection available on VASA.

9.

SUSPICIOUS REGISTRY OR SYSTEM FILE CHANGES

One of the ways malware writers establish persistence within an infected host is through registry changes.

Creating a baseline is the most important part when dealing with registry-based IOCs. Defining what a clean registry is supposed to contain essentially creates the filter against which you will compare your hosts. Monitoring and alerting on changes that deviate outside the bounds of the clean ‘template’ can drastically increase security team response time.

Similarly, many attackers will leave behind signs that they’ve tampered with a host in system files and configurations.

What can happen is that the attacker will install packet-sniffing software to harvest credit card data as it moves around the network. The attacker targets a system that can watch the network traffic, then installs the harvesting tool. While the chances of catching the specific harvesting tool are slim — because they will be targeted and probably not seen before — there is a good chance to catch the changes to the system that houses the harvesting tool.

VASA Note: Assuming End Point Logs are being collected, VASA will detect any deviation from the baseline behaviours of the end points and trigger the associated Alert.

10. DNS REQUEST ANOMALIES

According to experts, one of the most effective red flags an organization can look for are tell-tale patterns left by malicious DNS queries.

Command-and-control traffic is often the most important traffic to an attacker because it allows them ongoing management of the attack and it needs to be secure so that security professionals can't easily take it over. The unique patterns of this traffic can be recognized and is a very standard approach to identifying a compromise.

Seeing a large spike in DNS requests from a specific host can serve as a good indicator of potentially suspect activity. Watching for patterns of DNS requests to external hosts, compared against geoIP and reputation data, and implementing appropriate filtering can help mitigate C&C over DNS.

VASA Note: VASA will trigger Alerts on any Abnormal DNS behavior such as high rate of DNS requests, DNS resolving to multiple IP's.

11. UNEXPECTED PATCHING OF SYSTEMS

Patching is generally a good thing, but if a system is inexplicably patched without reason, that could be the sign that an attacker is locking down a system so that other bad guys can't use it for other criminal activity.

12.

MOBILE DEVICE PROFILE CHANGES

As attackers migrate to mobile platforms, enterprises should keep an eye on unusual changes to mobile users' device settings. They also should watch for replacement of normal apps with hostile ones that can carry out man-in-the-middle attacks or trick users into giving up their enterprise credentials.

If a managed mobile device gains a new configuration profile that was not provided by the enterprise, this may indicate a compromise of the user's device and, from there, their enterprise credentials. These hostile profiles can be installed on a device through a phishing or spear-phishing attack.

VASA Note: If an Enterprise, has an MDM Solution in place, VASA can be integrated with the any MDM solution to provide insights on Mobile Devices.

13.

BUNDLES OF DATA IN THE WRONG PLACES

Attackers frequently aggregate data at collection points in a system before attempting exfiltration. If you suddenly see large gigabytes of information and data where they should not exist, particularly compressed in archive formats your company doesn't' use, this is a telltale sign of an attack.

In general, files sitting around in unusual locations should be scrutinized because they can point to an impending breach.

Files in odd places, like the root folder of the recycle bin, are hard to find looking through Windows, but easy and quick to find with a properly crafted Indicator of Compromise. Executable files in the temp folder is another one, often used during privilege escalation, which rarely has a legitimate existence outside of attacker activity.

14.

WEB TRAFFIC WITH UNHUMAN BEHAVIOR

Web traffic that doesn't match up with normal human behavior shouldn't pass the sniff test.

How often do you open 20 or 30 browser windows to different sites simultaneously? Computers infected with a number of different click-fraud malware families may generate noisy volumes of Web traffic in short bursts. Or, for instance, on a corporate network with a locked-down software policy, where everyone is supposed to be using one type of browser, an analyst might see a Web session in which the user-agent string which identifies the browser to the Web server indicates the use of a browser that's far removed from the standard corporate image, or maybe a version that doesn't even exist.

VASA Note: VASA will trigger Alerts for the above use case.

15.

SIGNS OF DDOS ACTIVITY

Distributed denial-of-service attacks (DDoS) are frequently used as smokescreens to camouflage other more pernicious attacks. If an organization experiences signs of DDoS, such as slow network performance, unavailability of websites, firewall failover, or back-end systems working at max capacity for unknown reasons, they shouldn't just worry about those immediate problems.

In addition to overloading mainstream services, it is not unusual for DDoS attacks to overwhelm security reporting systems, such as IPS/IDS or SIEM solutions. This presents new opportunities for cybercriminals to plant malware or steal sensitive data. As a result, any DDoS attack should also be reviewed for related data breach activity.

VASA Note: Vasa will trigger alerts for the above use case.

THREAT HUNTING SCENARIOS

Attacks on enterprise networks are coming from a growing number of different threats, faster than previously thought possible. Successful cyber attacks result in exposing sensitive customer data, an immediate loss of revenue, and a long-lasting damage to your brand.

SIEMs, IPS, IDS are computer-based technologies that help protect your network infrastructure. But the reality is the amount of data generated, across many sources, is very huge, and as it is today, is dispersed across multiple areas. With Machine Learning & Artificial Intelligence, these data sources, can all be combined into one single aggregated platform, which becomes more effective to support the Security Analyst. With Rank's Virtual Advisor to Security Analyst (VASA), we have pretty much done all the work of the security analyst, of looking at logs, searching through in a fine comb, and present anomaly detection. But not only that, we have also given the Analyst a Platform to hunt for threats in REAL TIME.

The following is a knowledge base of SQL queries, based on the Adversary Tactics, Techniques, and Common Knowledge (ATT&CK) adversary model, developed by MITRE. These SQL queries are based on MITRE's recommended analytics, and are meant to further assist the SOC analyst in their threat hunt for a potential breach on their network.

The knowledge base is broken down into:

- a ***Use Case*** label and the ***Tactic*** that the analytic detects
- a ***Hypothesis*** which explains the idea behind the analytic
- a ***VASA Note*** explaining relative feature in RANK's VASA
- a ***SQL Query*** description of how the analytic might be implemented

1.

USE CASE: Reg.exe called from Command Shell

Tactic: TTP

MITRE Reference: CAR-2013-03-001: Reg.exe called from Command Shell

Hypothesis: Registry modifications are often essential in establishing persistence via known Windows mechanisms. Many legitimate modifications are done graphically via regedit.exe or by using the corresponding channels, or even calling the Registry APIs directly. The built-in utility reg.exe provides a command-line interface to the registry, so that queries and modifications can be performed from a shell, such as cmd.exe. When a user is responsible for these actions, the parent of cmd.exe will likely be explorer.exe. Occasionally, power users and administrators write scripts that do this behavior as well, but likely from a different process tree. These background scripts must be learned so they can be tuned out accordingly.

SQL Query:

```
select source.name, data.process.cmd, count(*) AS
hostcount from network-events where type = 'sysmon'
AND data.process.action = 'launch' AND data.process.
image.file = 'reg.exe' AND data.process.parentImage.file =
'cmd.exe' AND

(data.process.cmd LIKE '%add%' OR data.process.cmd LIKE
'%delete%' OR data.process.cmd LIKE '%copy%' OR data.
process.cmd LIKE '%restore%' OR data.process.cmd LIKE
'%load%' OR data.process.cmd LIKE '%import%') order by
hostcount DESC
```

2.

USE CASE: Simultaneous Logins on a Host

Tactic: Situational Awareness

MITRE Reference: CAR-2013-02-008: Simultaneous Logins on a Host

Hypothesis: Multiple users logged into a single machine at the same time, or even within the same hour, do not typically occur in networks we have observed.

VASA Note: VASA has built in anomaly detection for excessive log-ins. The analyst can also run the following SQL Queries:

SQL Query:

```
select source.name, count(distinct `data.login.user`) as
uniqueUserLogins, timeInterval(date, '1h') from network-events
where type = 'winevent' AND data.winevent.EventID = 4624 AND
data.winevent.LogonType IN (2, 3, 9, 10) AND data.login.status =
'success'
group by source.name
having uniqueUserLogins > 1
```

SQL Query:

```
select `data.login.user`, count(distinct source.name) as
uniqueMachineLogins, timeInterval(date, '1h')
from network-events
where type = 'winevent' AND data.winevent.EventID = 4624 AND
data.winevent.LogonType IN (2, 3, 9, 10) AND data.login.status =
'success'
group by `data.login.user`
having uniqueMachineLogins > 1
```

3.

USE CASE: Quick execution of a series of suspicious commands

Tactic: TTP

MITRE Reference: CAR-2013-04-002: Quick execution of a series of suspicious commands

Hypothesis: Certain commands are frequently used by malicious actors and infrequently used by normal users. By looking for execution of these commands in short periods of time, we can not only see when a malicious user was on the system but also get an idea of what they were doing.

VASA Note: We already generate Alerts on this use case. The Analyst can dig a bit deeper by writing SQL query:

SQL Query:

```
select source.name, count(date) as numSuspiciousCommnds , timeInterval(date, '30m')
from network-events
where type = 'sysmon' AND data.process.image.file IN ('arp.exe', 'at.exe', 'attrib.exe', 'cscript.exe', 'dsquery.exe', 'hostname.exe', 'ipconfig.exe', 'mimikatz.exe', 'nbstat.exe', 'net.exe', 'netsh.exe', 'nslookup.exe', 'ping.exe', 'quser.exe', 'qwinsta.exe', 'reg.exe', 'runas.exe', 'sc.exe', 'schtasks.exe', 'ssh.exe', 'systeminfo.exe', 'taskkill.exe', 'telnet.exe', 'tracert.exe', 'wscript.exe', 'xcopy.exe')
group by source.name
having numSuspiciousCommnds > 1
```

4.

USE CASE: Processes Spawning cmd.exe

Tactic: Situational Awareness

MITRE Reference: CAR-2013-02-003: Processes Spawning cmd.exe

Hypothesis: The Windows Command Prompt (cmd.exe) is a utility that provides a command line interface to Windows operating systems. It provides the ability to run additional programs and also has several built-in commands such as dir, copy, mkdir, and type, as well as batch scripts (.bat).

Typically, when a user runs a command prompt, the parent process is explorer.exe or another instance of the prompt. There may be automated programs, logon scripts, or administrative tools that launch instances of the command prompt in order to run scripts or other built-in commands. Spawning the process cmd.exe from certain parents may be more indicative of malice.

For example, if Adobe Reader or Outlook launches a command shell, this may suggest that a malicious document has been loaded and should be investigated. Thus, by looking for abnormal parent processes of cmd.exe, it may be possible to detect adversaries.

VASA Note: Already exists as anomaly detection, assuming end point logs through sysmon are being captured and sent to VASA. SOC analyst can lookup the Process report on the VASA dashboard. Specifically, the hunter looks if cmd.exe is being spawned, and what parent process has spawned cmd.exe. Finally, the Analyst can dig a bit deeper by writing SQL query:

SQL Query:

```
select * from network-events where data.process.image.file = 'cmd.exe'
AND data.process.parentImage.file != 'explorer.exe' AND data.process.
action = 'launch'
```

5.

USE CASE: RDP Connection Detection

Tactic: Lateral Movement

MITRE Reference: CAR-2013-07-002: https://car.mitre.org/wiki/CAR-2013-07-002

Hypothesis: The Remote Desktop Protocol (RDP), built in to Microsoft operating systems, allows a user to remotely log in to the desktop of another host. It allows for interactive access of the running windows, and forwards key presses, mouse clicks, etc. Network administrators, power users, and end-users may use RDP for day-to-day operations. From an adversary's perspective, RDP provides a means to laterally move to a new host. Determining which RDP connections correspond to adversary activity can be a difficult problem in highly dynamic environments but will be useful in identifying the scope of a compromise.

VASA Note: We already generate Alerts on this use case.

SQL Query:

If you are collecting network traffic run:

```
Select source.name, destination.name, count(*) from network-events,
where type = 'rdp'
```

If we are not collecting network traffic run:

```
Select source.name, destination.name, count(*) from network-events,
where destination.port = '3389'
```

6.

USE CASE: All Logins Since Last Boot

Tactic: Analytics

MITRE Reference: CAR-2015-07-001: https://car.mitre.org/wiki/CAR-2015-07-001

Hypothesis: Once a credential dumper like **mimikatz** runs, every user logged on since boot is potentially compromised, because the credentials were accessed via the memory of **lsass.exe.** When such an event occurs, this analytic will give the forensic context to identify compromised users. Those users could potentially be used in later events for additional logons.

VASA Note: This has a pre-requisite — the NxLog configuration has to be changed to include EventID 6005 (which indicates when the machine was rebooted). Assuming we receive the EventID - 6005 to VASA: currently this will be a 2 step process:

SQL Query #1:

This query will give you the most recent time the machine was restarted:

```
select max(`date`) from network-events where data.winevent.EventID
= 6005 AND source.name = 'enter your machine name here'
```

SQL Query #2:

Take the date that you get above and find all login events after that date on that machine using:

```
select * from network-events where data.winevent.EventID = 4624
AND data.login.machine.name = 'mohan-rank' AND inInterval(`date`,
1529668613000, 'now')
```

7.

USE CASE: RPC Activity

Tactic: Lateral Movement

MITRE Reference: CAR-2014-05-001: https://car.mitre.org/wiki/CAR-2014-05-001

Hypothesis: Microsoft Windows uses its implementation of Distributed Computing Environment/Remote Procedure Call (DCE/RPC), which it calls Microsoft RPC, to call certain APIs remotely.

A Remote Procedure Call is initiated by communicating to the RPC Endpoint Mapper, which exists as the Windows service RpcEptMapper and listens on the port 135/tcp. The endpoint mapper resolves a requested endpoint/interface and responds to the client with the port that the service is listening on. Since the RPC endpoints are assigned ports when the services start, these ports are dynamically assigned from 49152 to 65535. The connection to the endpoint mapper then terminates and the client program can communicate directly with the requested service.

RPC is a legitimate functionality of Windows that allows remote interaction with a variety of services. For a Windows environment to be properly configured, several programs use RPC to communicate legitimately with servers. The background and benign RPC activity may be enormous, but must be learned, especially peer-to-peer RPC between workstations, which is often indicative of Lateral Movement.

According to ATT&CK, adversaries frequently use RPC connections to remotely

- Create, modify, and manipulate services
- Schedule Tasks
- Query & Invoke Remote Launched Executables over RPC.

7.

USE CASE: RPC Activity (continued)

SQL Queries:

An equivalent method to the MITRE Framework would be too look for:

- **All established RPC calls between internal machines**

```
select * from network-events where type = 'dce_rpc' AND destination.port >= 49152 AND source.port >= 49152 AND source.routingMode != 'LOOPBACK' AND source.internal = true AND destination.internal = true
```

- **You can further slice and dice this data. For example, you could view the number of rpc calls made between hosts by rpc endpoints. You can sort by the count column to check outliers.**

```
select source.name, destination.name, data.dce_rpc.endpoint, count(*)
from network-events where type = 'dce_rpc'
AND destination.port >= 49152 AND source.port >= 49152 AND source.routingMode != 'LOOPBACK' AND source.internal = true AND destination.internal = true
```

- **Machines that receive the most RPC calls:**

```
select destination.name, count(*) from network-events where type = 'dce_rpc' AND destination.port >= 49152 AND source.port >= 49152 AND source.routingMode != 'LOOPBACK' AND source.internal = true AND destination.internal = true
```

- **Machines that make the most RPC calls:**

```
select source.name, count(*) from network-events where type = 'dce_rpc' AND destination.port >= 49152 AND source.port >= 49152 AND source.routingMode != 'LOOPBACK' AND source.internal = true AND destination.internal = true
```

- **RPC endpoints receiving the most calls:**

```
select data.dce_rpc.endpoint, count(*) from network-events where type = 'dce_rpc' AND destination.port >= 49152 AND source.port >= 49152 AND source.routingMode != 'LOOPBACK' AND source.internal = true AND destination.internal = true
```

- **RPC operations:**

```
select data.dce_rpc.operation, count(*) from network-events where type = 'dce_rpc' AND destination.port >= 49152 AND source.port >= 49152 AND source.routingMode != 'LOOPBACK' AND source.internal = true AND destination.internal = true
```

8.

USE CASE: Remote Desktop Logon

Tactic: Lateral Movement

MITRE Reference: CAR-2016-04-005: https://car.mitre.org/wiki/CAR-2016-04-005

Hypothesis: A remote desktop logon, through RDP, may be typical of a system administrator or IT support, but only from select workstations. Monitoring remote desktop logons and comparing to known/approved originating systems can detect lateral movement of an adversary.

Note: Detection already exists in VASA as a rule.

```
rdp:
  filters:
    partition: source.name
    category: suspicious-login
    interesting: machine:source.name
    expression: type = winevent AND data.winevent.EventID = [4624,
4634] AND data.winevent.LogonType = 10 AND source.name

  triggers:
    score: 65
    description: Suspicious Remote Login detected on host
    message: "Suspicious remote login activity detected on host {source.
name}"
    killchain: ["Exploitation"]
    context:
      graph:
        - taf_remote_login_destination(type:internal_ip, id:{source.name})
        - taf_remote_login_user(type:user, id:{source.name})
```

9.

USE CASE: User Activity from Clearing Event Logs

Tactic: Defense Evasion

MITRE Reference: CAR-2016-04-002:
https://car.mitre.org/wiki/CAR-2016-04-002

Hypothesis: It is unlikely that event log data would be cleared during normal operations, and it is likely that malicious attackers may try to cover their tracks by clearing an event log. When an event log gets cleared, it is suspicious. Alerting when a “Clear Event Log” is generated could point to this intruder technique. Centrally collecting events has the added benefit of making it much harder for attackers to cover their tracks. Event Forwarding permits sources to forward multiple copies of a collected event to multiple collectors, thus enabling redundant event collection. Using a redundant event collection model can minimize the single point of failure risk.

Note: Detection already exists in VASA as a rule.

```
eventlogclear:
  filters:
    partition: source.name
    category: suspicious-host-activity
    interesting: machine:source.name
    expression: type = winevent AND (data.winevent.EventID = 106
OR data.winevent.EventID = 104) AND source.name

  triggers:
    score: 65
    description: Windows Event Log cleared on host
    message: "Event Log was cleared on host {source.name}. Could be
indicative of malware."
    killchain: ["C2"]

auditlogclear:
  filters:
    partition: source.name
    category: suspicious-host-activity
    interesting: machine:source.name
    expression: type = winevent AND (data.winevent.EventID = 1102
OR data.winevent.EventID = 1100) AND source.name

  triggers:
    score: 65
    description: Audit Log cleared on host
    message: "Audit Log was cleared on host {source.name}. Could be
indicative of malware."
    killchain: ["C2"]
```

10.

USE CASE: User Activity from Stopping Windows Defensive Services

Tactic: Defense Evasion

MITRE Reference: CAR-2016-04-003:
https://car.mitre.org/wiki/CAR-2016-04-003

Hypothesis: Spyware and malware remain a serious problem and Microsoft developed security services, Windows Defender and Windows Firewall, to combat this threat. In the event Windows Defender or Windows Firewall is turned off, administrators should correct the issue immediately to prevent the possibility of infection or further infection and investigate to determine if caused by crash or user manipulation.

SQL Query:

Ensure that NxLog is configured to receive EventID 7036. Then the query is simply:

select * **from** network-events **where data**.winevent.EventID = 7036

Note: Detection already exists in VASA as rules.

```
firewallchanges:
  filters:
    partition: source.name
    category: suspicious-host-activity
    interesting: machine:source.name
    expression: type = winevent AND data.winevent.EventID = [2004,
2005, 2006, 2033, 2009] AND source.name

  triggers:
    score: 65
    description: Windows Firewall changes detected
    message: "Firewall changes detected on host {source.name}. Could
be indicative of a compromise."
    killchain: ["C2"]

defender:
  filters:
    partition: source.name
    category: suspicious-host-activity
    interesting: machine:source.name
    expression: type = winevent AND data.winevent.EventID = [1005,
1006, 1008, 1010, 3002, 5008] AND source.name

  triggers:
    score: 65
    description: Windows Defender Alert
    message: "Windows Defender Alerts detected on host {source.
name}."
    killchain: ["Installation"]
```

11.

USE CASE: Successful Local Account Login

Tactic: Lateral Movement

MITRE Reference: CAR-2016-04-004: https://car.mitre.org/wiki/CAR-2016-04-004

Hypothesis: The successful use of Pass The Hash for lateral movement between workstations would trigger event ID 4624, with an event level of Information, from the security log. This behavior would be a LogonType of 3 using NTLM authentication where it is not a domain logon and not the ANONYMOUS LOGON account.

SQL Query:

select * **from** network-events **where type** = 'winevent' AND **data**.winevent.EventID = 4624 AND **data**.winevent.TargetUserName != 'ANONYMOUS LOGON' AND **data**.winevent.AuthenticationPackageName = 'NTLM'

12.

USE CASE: Debuggers for Accessibility Applications

Tactic: Execution, Persistence, Privilege Escalation

MITRE Reference: CAR-2014-11-003: https://car.mitre.org/wiki/CAR-2014-11-003

Hypothesis: The Windows Registry location “HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options” allows for parameters to be set for applications during execution. One feature used by malicious actors is the “Debugger” option. When a key has this value enabled, a Debugging command line can be specified. Windows will launch the Debugging command line, and pass the original command line in as an argument.

Adversaries can set a Debugger for Accessibility Applications. The analytic looks for the original command line as an argument to the Debugger.

When the strings “sethc.exe”, “utilman.exe”, “osk.exe”, “narrator.exe”, and “Magnify.exe” are detected in the arguments, but not as the main executable, it is very likely that a Debugger is set.

SQL Query:

```
select * from network-events where type = 'sysmon' AND
data.process.action = 'launch' AND textMatches(data.
process.cmd, '.* .*(sethc|utilman|osk|narrator|magnify)\.exe')
```

13.

USE CASE: User Logged in to Multiple Hosts

Tactic: Lateral Movement

MITRE Reference: CAR-2013-02-012: https://car.mitre.org/wiki/CAR-2013-02-012

Hypothesis: Most users use only one or two machines during the normal course of business. User accounts that log in to multiple machines, especially over a short period of time, may be compromised. Remote logins among multiple machines may be an indicator of lateral movement.

SQL Query:

```
select timeInterval(date, '1h'), `data.login.user`,
count(distinct data.login.machine.name) as machinecount
from network-events where data.winevent.EventID = 4624
having machinecount > 1
```

14.

USE CASE: Service Search Path Interception

Tactic:

MITRE Reference: CAR-2014-07-001: https://car.mitre.org/wiki/CAR-2014-07-001

Hypothesis: According to ATT&CK, an adversary may escalate privileges by intercepting the search path for legitimately installed services. As a result, Windows will launch the target executable instead of the desired binary and command line. This can be done when there are spaces in the binary path and the path is unquoted. Search path interception should never happen legitimately and will likely be the result of an adversary abusing a system misconfiguration. With a few regular expressions, it is possible to identify the execution of services with intercepted search paths.

SQL Query:

```
select data.process.cmd, data.process.image.file from network-events where
type = 'sysmon' AND data.process.action = 'launch' AND data.process.
parentImage.file = 'services.exe' AND NOT textMatches(data.process.cmd,
'\".*') AND textMatches(data.process.cmd, '.* .*') AND NOT textMatches(data.
process.image.path, '.* .*')
```

Now, once you have the above results, you can add additional filters to filter out processes known to you to reduce the list so that you can visually compare the command line and the file that was executed. If the file executed is not in the command line then it is a problem.

e.g. filtering can be done using:

```
select data.process.cmd, data.process.image.file from network-events where
type = 'sysmon' AND data.process.action = 'launch' AND data.process.
parentImage.file = 'services.exe' AND NOT textMatches(data.process.cmd,
'\".*') AND textMatches(data.process.cmd, '.* .*') AND NOT textMatches(data.
process.image.path, '.* .*') AND data.process.image.file != 'svchost.exe' AND
data.process.image.file != 'upfc.exe'
```

SUMMARY CHART

Indicators of Compromise	RANK
Unusual Outbound Network Traffic	✓
Anomalies in Priviledged User Account Activity	✓
Geographical Irregularities	✓
Other Log-in Red Flags	✓
Swells in Database Read Volume	✓
HTML Response Sizes	✓
Large Numbers of Requests For The Same File	✓
Mismatched Port-Application Traffic	✓
Suspicious Registry or System File Changes	✓
DNS Request Anomalies	✓
Unexpected Patches of Systems	✓
Mobile Device Profile Changes	✓
Bundles of Data In The Wrong Places	✓
Web Traffic With Unhuman Behaviour	✓
Signals of DDoS Activity	✓

LEARN MORE

For additional details on arming security analysts with the right tools to become Threat Hunters capable of preventing today's known threats, and tomorrow's unknown risks, visit the Rank Software website at **www.ranksoftwareinc.com**.

Rank Software helps security professionals re-establish confidence in their enterprise security posture in an increasingly complex and hostile cyber landscape.

Leading businesses around the world choose RANK Software to help them improve their security posture.

Here are some of the reasons why:

- Reduce Risk. Lower the risk of a successful cyber attack.
- Control Cost. Increase efficiency of security professionals.
- Faster Response. Identify and act on threats in real time.
- Stay Ahead. Future proof your enterprise security posture.
- Improve Alignment. Enable your business to address emerging threats.

Next gen security analytics for the zero-day world.

VASA by RANK Software brings all the pieces of your threat hunting strategy together in one place. Ingest billions of signals from across your business. Enrich them with powerful context and behavioural analysis. Identify the most credible threats. Investigate on one screen and reduce false positives.