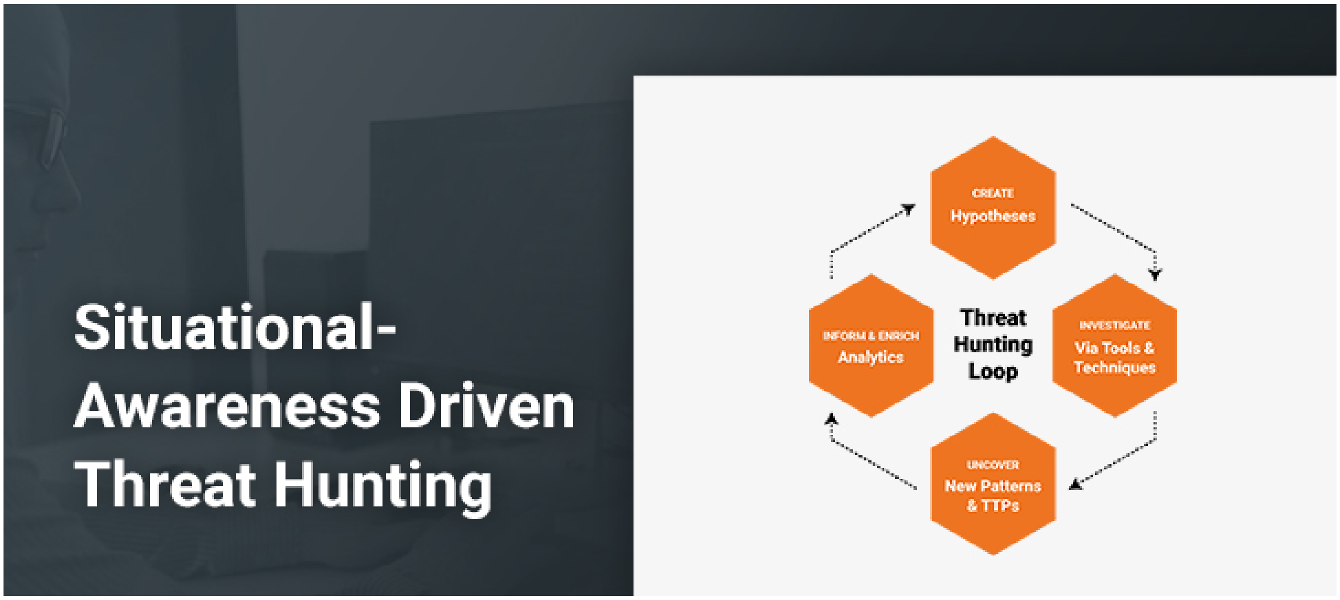
SITUATIONAL-AWARENESS DRIVEN THREAT HUNTING

(/blog/)



(/situational-awareness-driven-threat-hunting/)

December 19, 2017 by Ryan Nolette (https://sqrrl.com/author/ryan/)

SITUATIONAL-AWARENESS DRIVEN THREAT HUNTING

For this example, I will limit my search to just high-value targets, such as the domain admin accounts.

Authentication requests are used to identify accounts or users that are allowed to access the network and its resources. Similar to legitimate authentication, attackers may use compromised or distinct accounts to identify itself to a authentication server and may also use existing accounts in order to blend in with normal authentication traffic.

The process described herein may also be used to analyze authentication attempts.

After a successful asset discovery, adversaries try to exfiltrate data from the compromised network. The actual approach of the exfiltration depends on group’s tactics, data amount and other circumstances.

In order to gain access to desired data, the attacker will commonly abuse legitimate credentials/accounts that have been compromised. For this purpose, any of the most common techniques can be used, including most common tools, mimikatz PWdump, WCE etc, to steal credentials for authenticating to the compromised Domain Admin accounts. Attackers might limit themselves to certain account types which allow them to blend in and remain stealthy.

EXAMPLE HUNT

Domain Admin Account Abuse Hunt (Windows Environment)	
What are you looking for? (Hypothesis)	**Hypothesis:** If we analyze Domain Admin account logon attempts seen in our network and look for outliers, then we may find attackers or abuse of legitimate credentials. **Look for:** • Spike in Domain Admin account logons
Investigation (Data)	**Datasets:** For identifying authentication activity, you will want to focus primarily on authentication system and event metadata, including: • Netflow (“flow” data in general) • Active Directory logs • Windows Security Event logs • Multi-Factor Authentication (MFA) logs (if windows hosts leverage MFA) • Additional UAC applications logs (if exists) • EDR tool logs (if exists)
Uncover Patterns and IOCs (Techniques)	1. For this hunt, the data set is a set of Domain Admin account logon events used in authentication to a system. 1. Identification of these username string formats may vary from network to network; however, it is recommend to start with a larger set of data (e.g., all username strings or a specific type of username string) and reduce the size of the set as required by the results of the hunt. 2. Take the output of step 1 and remove hosts as you confirm they are legitimately connecting to a destination. This should leave only unexplained authentication connections that need further analysis. 3. Take the results of step 2 and stack the data for what is useful to investigating your hypothesis 1. For example: destination IP, port used, connection duration/length, etc.
Inform and Enrich Analytics (Takeaways)	The destination IP addresses, account name, user ID, and impersonation level involved in the authentication activity you have discovered can be taken as IOCs and added to an indicator database in order to expand automated detection systems.

Always keep in mind that for each instance of a hunt, there will always be multiple different paths that a hunter can take to address a given hypothesis.

Hypothesis

A spike in Domain Admin account logon attempts may indicate an abuse of a Domain Admin account. If we analyze Domain Admin account logon attempts seen in our network and look for outliers, then we may find attackers or abuse of legitimate credentials.

The assumption made in this type of analysis is that the activity in question will not be "normal" or overly prevalent on the active network. Ideally, this will lead to identification of malicious or otherwise prohibited activity that was missed via other detection mechanisms, which the Domain Admin accounts can then be used to detect in the future.

Data: Windows Event Logs

Built-in data source connector for Windows event logs. Supports EVTX XML format for Windows 7/2008 and newer.

This hunt requires metadata that contains authentication requests. This data should include the domain used in the authentication requests, the source (endpoint, user, or IP address) of the authentication request, and the username requested in the authentication request.

We will first look at 4624 events (https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4624).

This is a highly valuable event since it documents each and every successful attempt to logon to the local computer regardless of logon type, location of the user or type of account. You can tie this event to logoff events 4634 and 4647 using Logon ID.

Additional events for consideration:

- 4672 Privileged account usage
- 4720 Account creation
- 4728 A member was added to a security enabled global group
  - We're looking specifically for a domain admin or enterprise admin groups
- 4776 local admin account (not logged on the DC).

Win2012 adds the Impersonation Level field as shown below.

Description Fields in 4624

Subject:

Identifies the account that requested the logon – NOT the user who just logged on. Subject is usually Null or one of the Service principals and not usually useful information. See New Logon for who just logged on to the system.

- Security ID
- Account Name
- Account Domain
- Logon ID

Logon Information:

- Logon Type: See below

Remaining logon information fields are new to Windows 10/2016

- Restricted Admin Mode: Normally “-“.”Yes” for incoming Remote Desktop Connections where the client specified /restrictedAdmin
- Virtual Account: Normally “No”. This will be Yes in the case of services configured to logon with a “Virtual Account”.
- Elevated Token: This has something to do with User Account Control but our research so far has not yielded consistent results.

Logon Type:

This is a valuable piece of information as it tells you **HOW** the user just logged on:

Logon Type	Description
2	Interactive (logon at keyboard and screen of system)
3	Network (i.e. connection to shared folder on this computer from elsewhere on network)
4	Batch (i.e. scheduled task)
5	Service (Service startup)
7	Unlock (i.e. unattended workstation with password protected screen saver)
8	NetworkCleartext (Logon with credentials sent in the clear text. Most often indicates a logon to IIS with “basic authentication”)
9	NewCredentials such as with RunAs or mapping a network drive with alternate credentials. This logon type does not seem to show up in any events. If you want to track users attempting to logon with alternate credentials see 4648 (http://www.ultimatewindowssecurity.com/wiki/SecurityLogEventID4648.ashx).
10	RemoteInteractive (Terminal Services, Remote Desktop or Remote Assistance)
11	CachedInteractive (logon with cached domain credentials such as when logging on to a laptop when away from the network)

Impersonation Level: (Win2012 only)

From MSDN

Anonymous	Anonymous COM impersonation level that hides the identity of the caller. Calls to WMI may fail with this impersonation level.
Default	Default impersonation.
Delegate	Delegate-level COM impersonation level that allows objects to permit other objects to use the credentials of the caller. This level, which will work with WMI calls but may constitute an unnecessary security risk, is supported only under Windows 2000.
Identify	Identify-level COM impersonation level that allows objects to query the credentials of the caller. Calls to WMI may fail with this impersonation level.
Impersonate	Impersonate-level COM impersonation level that allows objects to use the credentials of the caller. This is the recommended impersonation level for WMI calls.

New Logon:

The user who just logged on is identified by the Account Name and Account Domain. You can determine whether the account is local or domain by comparing the Account Domain to the computer name. If they match, the account is a local account on that system, otherwise a domain account.

Field	**Description**
Security ID	the SID of the account
Account Name	Logon name of the account
Account Domain	Domain name of the account (pre-Win2k domain name)
Logon ID	a semi-unique (unique between reboots) number that identifies the logon session just initiated. Any events logged subsequently during this logon session will report the same Logon ID through to the logoff event 4647 or 4634.
Logon GUID	Supposedly you should be able to correlate logon events on this computer with corresponding authentication events on the domain controller using this GUID. Such as linking 4624 on the member computer to 4769 on the DC. But the GUIDs do not match between logon events on member computers and the authentication events on the domain controller.

Process Information:

Field	**Description**
Process ID	is the process ID specified when the executable started as logged in 4688.
Process Name	identifies the program executable that processed the logon. This is one of the trusted logon processes identified by 4611

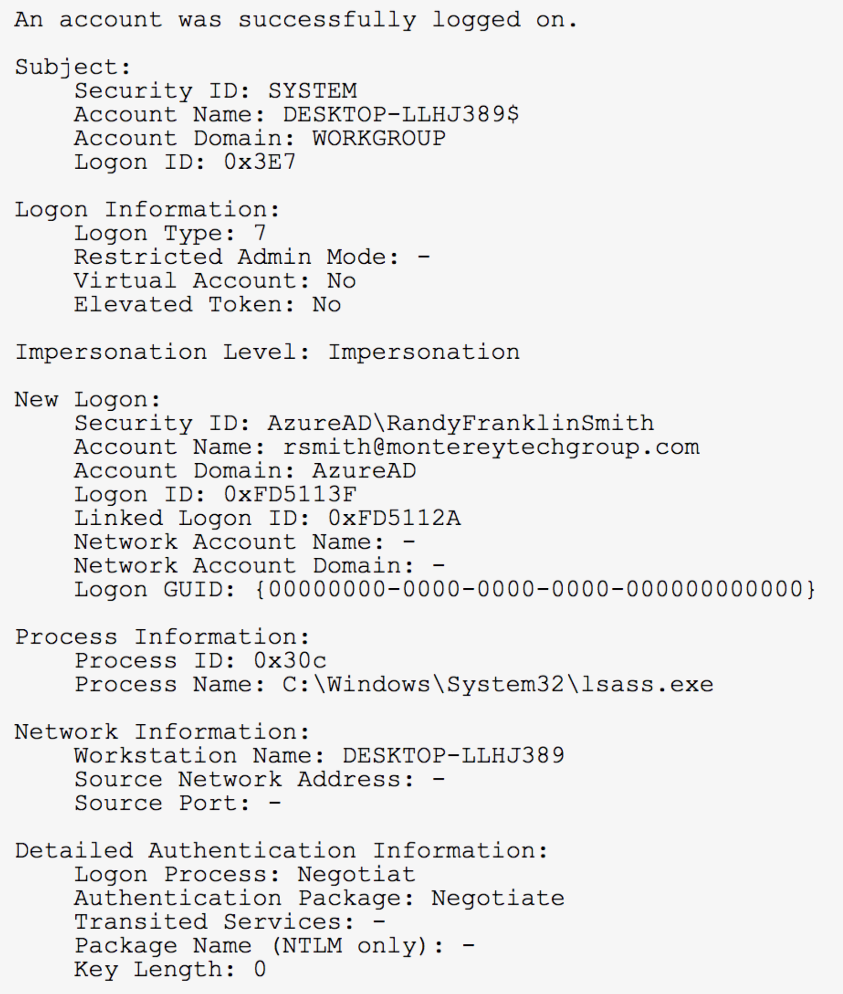
Network Information:

This section identifies WHERE the user was when he logged on. Of course if logon is initiated from the same computer this information will either be blank or reflect the same local computers.

Field	**Description**
Workstation Name	the computer name of the computer where the user is physically present in most cases unless this logon was intitiated by a server application acting on behalf of the user. Workstation may also not be filled in for some Kerberos logons since the Kerberos protocol doesn't really care about the computer account in the case of user logons and therefore lacks any field for carrying workstation name in the ticket request message.
Source Network Address	the IP address of the computer where the user is physically present in most cases unless this logon was intitiated by a server application acting on behalf of the user. If this logon is initiated locally the IP address will sometimes be 127.0.0.1 instead of the local computer's actual IP address. This field is also blank sometimes because Microsoft says "Not every code path in Windows Server 2003 is instrumented for IP address, so it's not always filled out."
Source Port	identifies the source TCP port of the logon request which seems useless since with most protocols source ports are random

Example authentication event

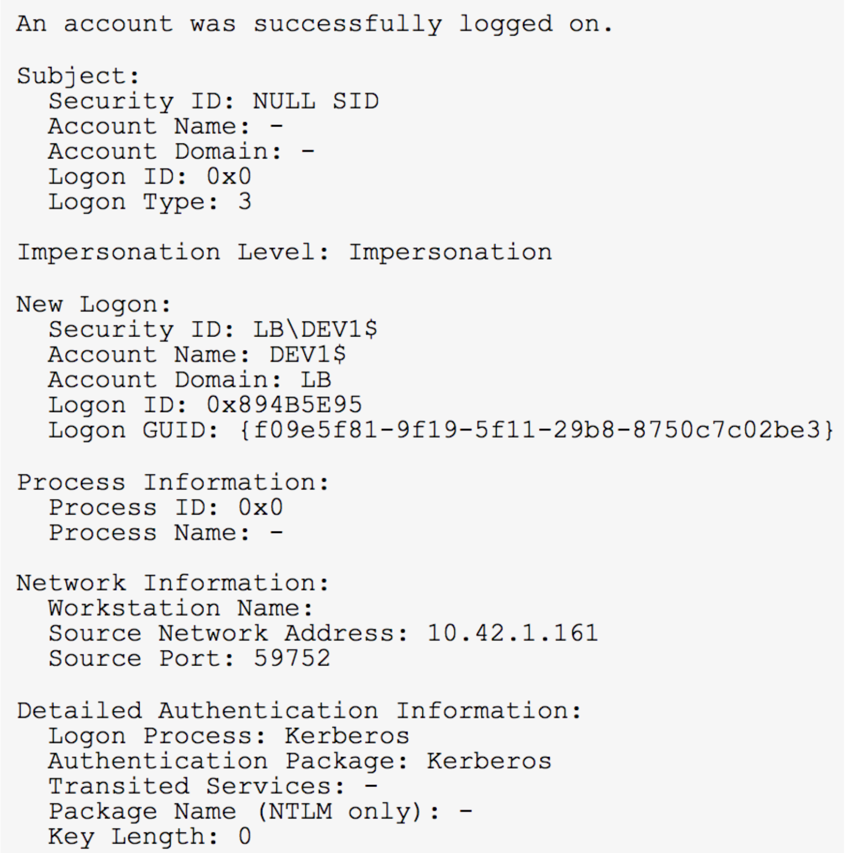
Windows 10 and 2016



```
An account was successfully logged on.

Subject:
    Security ID: SYSTEM
    Account Name: DESKTOP-LLHJ389$
    Account Domain: WORKGROUP
    Logon ID: 0x3E7

Logon Information:
    Logon Type: 7
    Restricted Admin Mode: -
    Virtual Account: No
    Elevated Token: No

Impersonation Level: Impersonation

New Logon:
    Security ID: AzureAD\RandyFranklinSmith
    Account Name: rsmith@montereytechgroup.com
    Account Domain: AzureAD
    Logon ID: 0xFD5113F
    Linked Logon ID: 0xFD5112A
    Network Account Name: -
    Network Account Domain: -
    Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:
    Process ID: 0x30c
    Process Name: C:\Windows\System32\lsass.exe

Network Information:
    Workstation Name: DESKTOP-LLHJ389
    Source Network Address: -
    Source Port: -

Detailed Authentication Information:
    Logon Process: Negotiat
    Authentication Package: Negotiate
    Transited Services: -
    Package Name (NTLM only): -
    Key Length: 0
```

(https://sqrrl.com/media/Screen-Shot-2017-11-20-at-11.41.05-AM.png)

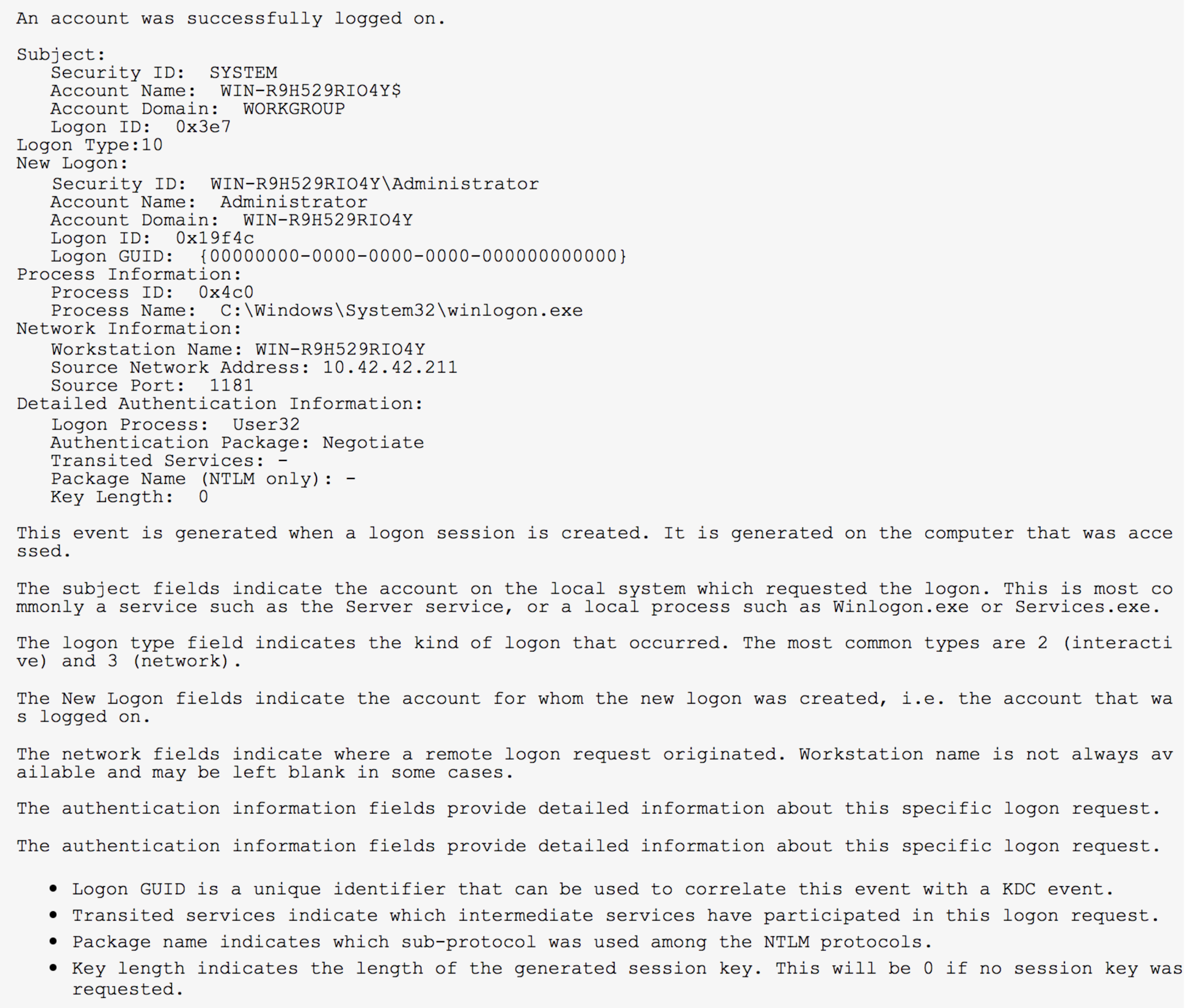
Win2008



```
An account was successfully logged on.

Subject:
  Security ID: NULL SID
  Account Name: -
  Account Domain: -
  Logon ID: 0x0
  Logon Type: 3

Impersonation Level: Impersonation

New Logon:
  Security ID: LB\DEV1$
  Account Name: DEV1$
  Account Domain: LB
  Logon ID: 0x894B5E95
  Logon GUID: {f09e5f81-9f19-5f11-29b8-8750c7c02be3}

Process Information:
  Process ID: 0x0
  Process Name: -

Network Information:
  Workstation Name:
  Source Network Address: 10.42.1.161
  Source Port: 59752

Detailed Authentication Information:
  Logon Process: Kerberos
  Authentication Package: Kerberos
  Transited Services: -
  Package Name (NTLM only): -
  Key Length: 0
```

(https://sqrrl.com/media/Screen-Shot-2017-11-20-at-11.41.30-AM.png)

Win2012



```
An account was successfully logged on.

Subject:
   Security ID:  SYSTEM
   Account Name:  WIN-R9H529RIO4Y$
   Account Domain:  WORKGROUP
   Logon ID:  0x3e7
Logon Type:10
New Logon:
   Security ID:  WIN-R9H529RIO4Y\Administrator
   Account Name:  Administrator
   Account Domain:  WIN-R9H529RIO4Y
   Logon ID:  0x19f4c
   Logon GUID:  {00000000-0000-0000-0000-000000000000}
Process Information:
   Process ID:  0x4c0
   Process Name:  C:\Windows\System32\winlogon.exe
Network Information:
   Workstation Name: WIN-R9H529RIO4Y
   Source Network Address: 10.42.42.211
   Source Port:  1181
Detailed Authentication Information:
   Logon Process:  User32
   Authentication Package: Negotiate
   Transited Services: -
   Package Name (NTLM only): -
   Key Length:  0

This event is generated when a logon session is created. It is generated on the computer that was acce
ssed.

The subject fields indicate the account on the local system which requested the logon. This is most co
mmonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.

The logon type field indicates the kind of logon that occurred. The most common types are 2 (interacti
ve) and 3 (network).

The New Logon fields indicate the account for whom the new logon was created, i.e. the account that wa
s logged on.

The network fields indicate where a remote logon request originated. Workstation name is not always av
ailable and may be left blank in some cases.

The authentication information fields provide detailed information about this specific logon request.

The authentication information fields provide detailed information about this specific logon request.

  • Logon GUID is a unique identifier that can be used to correlate this event with a KDC event.
  • Transited services indicate which intermediate services have participated in this logon request.
  • Package name indicates which sub-protocol was used among the NTLM protocols.
  • Key length indicates the length of the generated session key. This will be 0 if no session key was
    requested.
```

(https://sqrrl.com/media/Screen-Shot-2017-11-20-at-11.41.17-AM.png)

Technique: Define Your Data Set

For this hunt, the data set is a set of Domain Admin account logon events used in authentication to a system. Identification of these username string formats may vary from network to network; however, it is recommended to start with a larger set of data (e.g., all username strings or a specific type of username string) and reduce the size of the set as required by the results of the hunt.

Any username string seen in an authentication request can be considered for inclusion in the dataset. However, you may want to consider defining the activity group based upon known legitimate username strings. By filtering out these strings, outliers will be more noticeable. (However, keep in mind that filtering out legitimate username strings will not help you identify attackers who are maliciously using legitimate username strings!)

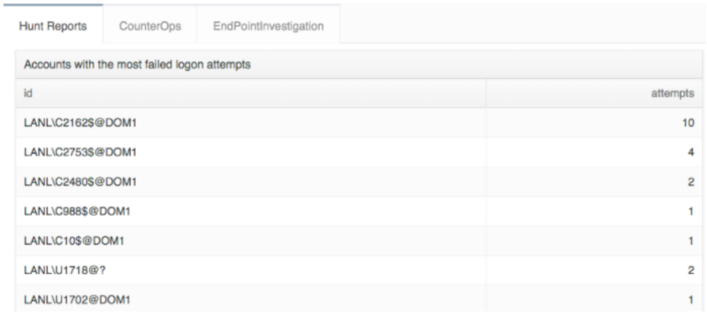
A query like this can be used to filter the results and would be one method for reducing your data set.
Find all users not meeting corporate naming convention and sort based on count
select TargetUserName, count(*) as count from Sqrrl_WindowsEvents WHERE TargetUserName NOT LIKE '%@DOM1' GROUP BY TargetUser
Find all users with a domain/realm that isn't known
MATCH Account From CounterOps WHERE Account.username NOT LIKE '%@DOM1' and ts_interval_sum(ts_flatten(Account.logonAttempts.
Find all users with failed login attempts (4625 windows event id) and sort based on count
SELECT TargetUserName, count(*) as failCount FROM Sqrrl_WindowsEvents where EventID=4625 group by TargetUserName order by failCo

Additional Sqrrl Uses

The queries identified in the prior section can all be used as starting points for exploration in the behavior graph. However, one of the goals of hunting is to reduce the amount of repetition and to re-apply what was learned on a hunt. As such, there are two additional mechanisms within Sqrrl that we can use to monitor spikes in Domain Admin account activity.

Hunt Reports

We can turn each of our example candidate investigation queries into a hunt report in order to get quick snapshots to aid in the identification of additional candidates on a regular basis. Hunt Reports are particularly well suited for data stacking.



Accounts with the most failed logon attempts

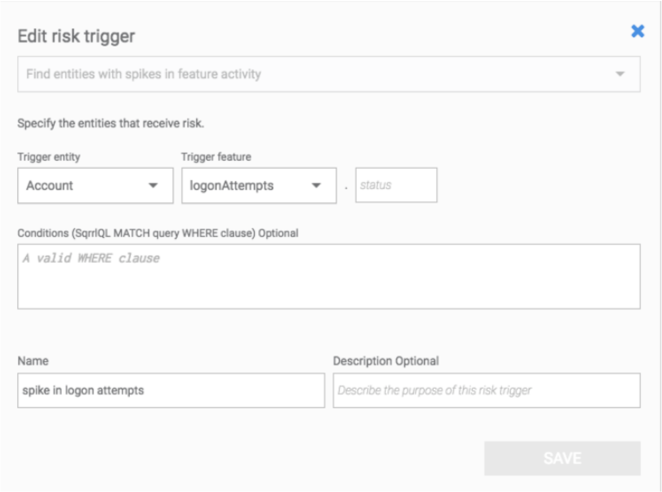
id	attempts
LANL\C2162$@DOM1	10
LANL\C2753$@DOM1	4
LANL\C2480$@DOM1	2
LANL\C988$@DOM1	1
LANL\C10$@DOM1	1
LANL\U1718@?	2
LANL\U1702@DOM1	1

(https://sqrrl.com/media/1-15.png)

Risk Triggers

While Hunt Reports assist with making data from certain hunts readily available, we can make use of Risk Triggers to identify observations of interest with respect to accounts and automatically use those to help bubble up entities of interest.

In one of our above examples, we determined that short usernames may be suspicious relative to others. As a result, I may want to create a Risk Trigger for entities observed using short usernames.



Edit risk trigger

Find entities with spikes in feature activity

Specify the entities that receive risk.

Trigger entity: Account

Trigger feature: logonAttempts . status

Conditions (SqrrlQL MATCH query WHERE clause) Optional: A valid WHERE clause

Name: spike in logon attempts

Description Optional: Describe the purpose of this risk trigger

(https://sqrrl.com/media/2-15.png)

Triggers also provide a good area to make use threat intelligence data that may be collected from any number of sources. Perhaps a relevant threat was recently observed using malware that made use of a specific username.

And as always, remember my motto, Flag it, Tag it, and Bag it.

For more threat hunting insight:

- Read Ryan's blog post (https://sqrrl.com/finding-evil-when-hunting-for-lateral-movement/) on threat hunting for lateral movement
- Watch our podcast (https://www.youtube.com/watch?v=N7JvE9nBCJs)on endpoint and network threat hunting

- Check out our training session (http://info.sqrrl.com/building-a-threat-hunting-team-david-bianco) on building a threat hunting team
- View our webinar (http://info.sqrrl.com/threat-hunting-lateral-movement)with Carbon Black on how to threat hunt for lateral movement

(http://info.sqrrl.com/sqrrl-enterprise-demo-request)

(http://info.sqrrl.com/trial)

(https://sqrrl.com/threat-hunter-profile-jordan-wigley/)

December 14, 2017 by Sqrrl Team (https://sqrrl.com/author/george/)

THREAT HUNTER PROFILE: JORDAN WIGLEY (HTTPS://SQRRL.COM/THREAT-HUNTER-PROFILE-JORDAN-WIGLEY/)

Name
Jordan Wigley

Organization
Fortune 50 Company

Years Hunting
5

Preferred Datasets

Full packet capture, Proxy logs, DNS logs, Endpoint data

Preferred Hunting Techniques

Baselining, Outlier analysis, Behavioral analysis

Preferred Tools

NetWitness, Splunk, Wireshark

READ MORE
(https://sqrrl.com/threat-hunter-profile-jordan-wigley/)

(https://sqrrl.com/going-offense-seed-hunt/)

December 12, 2017 by Matthew Hosburgh ()

GOING ON THE OFFENSE TO SEED THE HUNT (HTTPS://SQRRL.COM/GOING-OFFENSE-SEED-HUNT/)

Varying degrees of attacking back have been hotly debated (http://www.slate.com/articles/technology/future_tense/2017/10/hacking_back_the_worst_idea_in_cybersecurity_rises_again.html for years. Everything from fear of retaliation to collateral damage. Proponents claim that what we as a security collective have been doing for years is simply not working. The truth is, breach after breach is reported despite the millions, if not billions, of dollars spent by organizations to secure their assets. I will not try to solve the debate here; however, as a threat hunter, there are certain areas of Offensive Countermeasures, or Active Defense, that can readily be used to track down an adversary—and hopefully before any real damage occurs.

READ MORE
(https://sqrrl.com/going-offense-seed-hunt/)

Next Post

Browse by Topic

Featured Defenders ▴▾

Featured Posts

Top #InfoSec Twitter Accounts (From A Threat Hunter's Perspective)

By Danny Akacki
(/top-infosec-twitter-accounts/)

Is Threat Hunting-As-A-Service (THaaS) for you?

By Luis Maldonado
(/threat-hunting-service-thaas/)

Threat Hunting for Uncategorized Proxy Events

By Chris Sanders
(/cyber-threat-hunting-sqrrl-uncategorized-proxy-events/)

Threat Hunting for Lateral Movement

By Brandon Baxter
(/threat-hunting-lateral-movement-identifying-pivot-points/)

Threat Hunting for Evidence of Eavesdropping

By Matthew Hosburgh
(/hunting-evidence-eavesdropping/)

Threat Hunting Starting Points: Web Shells

By James Bower
(/3-threat-hunting-starting-points-web-shells-edition/)

Subscribe to Blog

Email Address

SUBSCRIBE

Resources

Webinar

Threat Hunting for Misbehaving PowerShells
(http://info.sqrrl.com/threat-hunting-for-misbehaving-powershells)

eBook

Hunt Evil: Your Practical Guide to Threat Hunting
(http://info.sqrrl.com/practical-guide-to-threat-hunting-ebook)

Whitepaper

The Who, What, Where, When, Why and How of Effective Threat Hunting
(http://info.sqrrl.com/sqrrl-sans-hunting-white-paper)

Whitepaper

Technical Guide: Nuts and Bolts of Sqrrl's Threat Hunting Platform
(http://info.sqrrl.com/sqrrl-product-paper-0)

points-web-shells-edition/)

Watch Overview

(https://www.youtube.com/watch?v=VI_zLBc4KQM&t&width=640&height=480)

(https://twitter.com/SqrrlData)
(https://www.facebook.com/SqrrlData)
(https://plus.google.com/116795302724746825954/posts)
(https://www.linkedin.com/company/sqrrl)
(http://www.youtube.com/user/sqrrldata)

SQRRL NEWSLETTER

Subscribe to our mailing list

PRODUCT (/PRODUCT/SQRRL-ENTERPRISE)

Sqrrl Enterprise (Https://Sqrrl.Com/Product/Sqrrl-Enterprise/)

Technology (Https://Sqrrl.Com/Product/Architecture/)

Architecture (Https://Sqrrl.Com/Product/Architecture/)

Security Behavior Graph (Https://Sqrrl.Com/Product/Behavior-Graph/)

User And Entity Behavior Analytics (Https://Sqrrl.Com/Product/User-And-Entity-Behavior-Analytics-Ueba/)

Test Drive VM (Http://Info.Sqrrl.Com/Trial-Software-Vm-1)

SOLUTIONS (/SOLUTIONS/USE-CASES/)

Use Cases (Https://Sqrrl.Com/Solutions/Use-Cases/)

Cyber Threat Hunting (Https://Sqrrl.Com/Solutions/Cyber-Threat-Hunting/)

Cyber Incident Investigation (Https://Sqrrl.Com/Solutions/Cyber-Incident-Response-And-Investigation/)

GET A DEMO (HTTP://INFO.SQRRL.COM/SQRRL-ENTERPRISE-DEMO-REQUEST)

PARTNERS (HTTPS://SQRRL.COM/THE-SQRRL-PARTNER-PROGRAM/)

Threat Hunting Ecosystem (Https://Sqrrl.Com/The-Sqrrl-Partner-Program/)

Technology (/Partners/Technology)

Sales (/Partners/Sales)

BLOG (/BLOG/)

SERVICES (/SERVICES/SQRRL-ENTERPRISE-SUPPORT/)

Sqrrl Enterprise Support (Https://Sqrrl.Com/Services/Sqrrl-Enterprise-Support/)

CONTACT US (HTTPS://SQRRL.COM/COMPANY/CONTACT-US/)

RESOURCES (/RESOURCES/)

Datasheets (/Resources/#Datasheet)

EBooks (/Resources/#Ebook)

Quick Reads (/Resources/#Quick-Read)

Reports (/Resources/#Report)

Videos (/Resources/#Video)

Webinars (/Resources/#Webinar)

Whitepapers (/Resources/#Whitepaper)

COMPANY (/COMPANY/OVERVIEW/)

Overview (Https://Sqrrl.Com/Company/Overview/)

Team (/Company/Team/Management)

Advisors (Https://Sqrrl.Com/Company/Team/Adviso

Blog (Http://Blog.Sqrrl.Com)

News Room (Https://Sqrrl.Com/Company/News/)

Careers (Https://Sqrrl.Com/Company/Careers/)

Contact Us (Https://Sqrrl.Com/Company/Contact-Us/)