

Cyber Threat Detection & Discovery Report

Incident Name	Cyber Smurfs Threat Detection & Discovery
Report Author	Cyber Smurfs
Report Date	Created - 20 JUN 23
Revision Dates	Last Revision - 23 JUN 23

Executive Summary

Over the past week, our AWS VPC has been the target of intrusion attempts by an adversary characterized as low-skilled, yet persistent and determined. This actor engaged in a series of noisy and broad-spectrum attacks, predominantly utilizing port scanning and brute force techniques, highlighting their desire to identify and exploit potential vulnerabilities. The adversary's tactics, techniques, and procedures (TTPs), although not sophisticated, were consistent, indicating a potential threat that requires appropriate attention and response.

In response to these intrusion attempts, we've enhanced our security measures to protect against similar incidents. Although no direct harm came to our systems or personnel during these attacks, they served as a glaring reminder of the constant threats in the digital landscape. We continue to monitor these threats and adapt our strategies to ensure the continued security of our VPC infrastructure. The remainder of this report provides an in-depth analysis of the observed adversary activities.

Description of Adversary

The adversary can be categorized as a low-skilled, persistent, and determined actor based on their intrusion attempts. The attacker repeatedly engaged in noisy and highly visible activities, primarily using port scanning and brute force attacks. The adversary's potential customer is likely to be a malicious actor interested in gaining unauthorized access to our systems for exploitation purposes, data theft, or a related illicit activity. The motivations behind these actions could range from curiosity or monetary gain, to potentially more damaging objectives like espionage or sabotage.

In terms of the intrusion kill chain, the reconnaissance phase was evident in the port scanning activities that occurred at different times. The noisy approach indicates a lack of finesse and stealth usually associated with more advanced adversaries. The weaponization and delivery phases were apparent in the brute force attacks aimed at our Metasploitable EC2 instance and Accounting2 EC2 instance.

Adversary's Capabilities

Despite the apparent low level of sophistication, the adversary displayed consistent use of recognized tactics, techniques, and procedures (TTPs). Despite the apparent low level of sophistication, the adversary displayed consistent use of recognized tactics, techniques, and procedures (TTPs). These included large scale port scanning as a method of identifying potential vulnerabilities within our system, as well as brute force attacks in an attempt to gain unauthorized access to our systems.

Overall, the adversary's capabilities are relatively limited, relying on brute force and simple scanning techniques. However, their persistence signals a potential threat that should not be overlooked. Continued monitoring and implementing stronger security measures can help mitigate any potential risks posed by such an actor.

Victims and Affected Assets

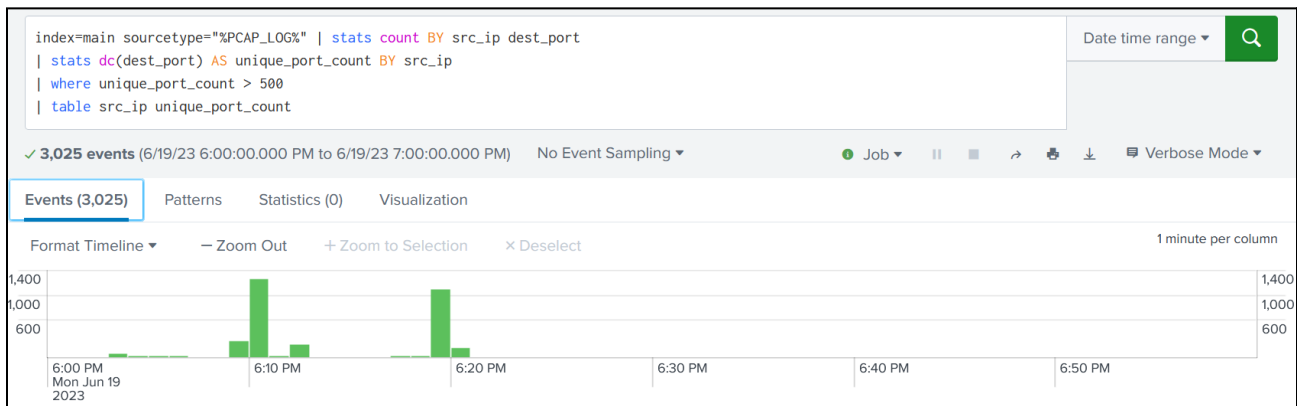
Although no personal identifiers or specific personnel within the organization were directly targeted or affected to our knowledge, the intrusion attempts represent a significant risk to the broader security and integrity of our systems. Therefore, while the adversary was not tremendously successful this time, these instances demonstrate the necessity of maintaining robust security measures to protect all individuals and assets connected to our network.

Attacks Discovered

19 JUN 23

Port Scanning (18:09 CT) - Between approximately 18:09:00 and 18:20:00 CDT port scanning was identified using the query below.

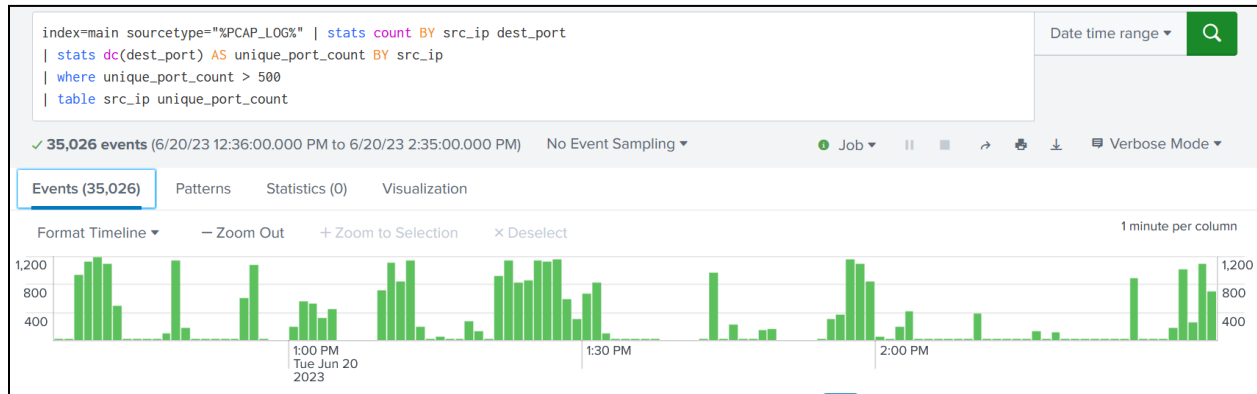
- Query searches the main index on 19 JUN for network traffic entries (%PCAP_LOG%) where the source IP has connected to more than 500 unique destination ports.
- 3025 log events were returned



20 JUN 23

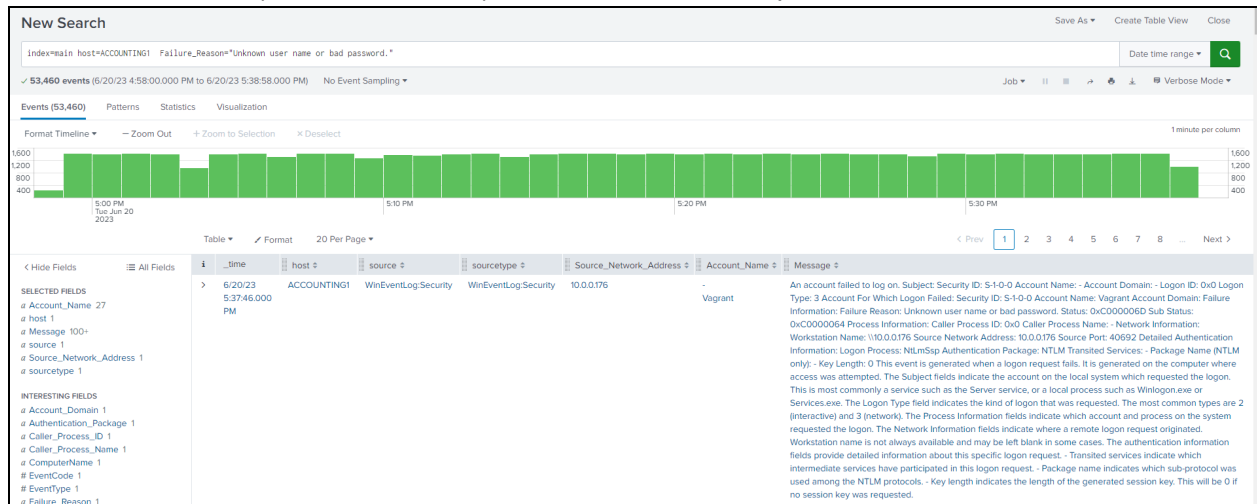
Port Scanning (20 Jun, 12:38 CT) - Between approximately 12:38:00 and ??:??:00 CDT port scanning was identified using the query below.

- Query searches the main index on 20 JUN for network traffic entries (%PCAP_LOG%) where the source IP has connected to more than 500 unique destination ports.
- 3025 log event were returned

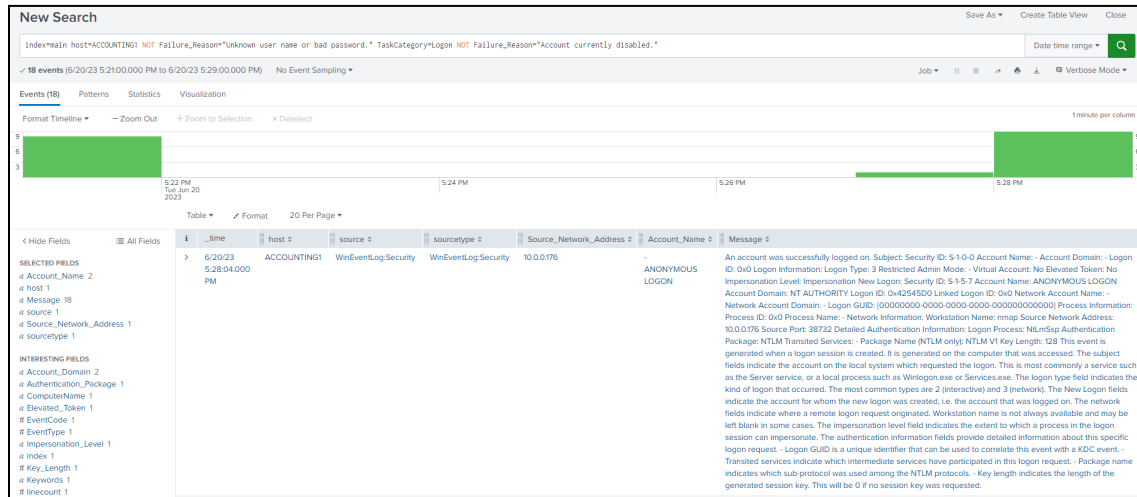


ACCOUNTING1 Investigation:

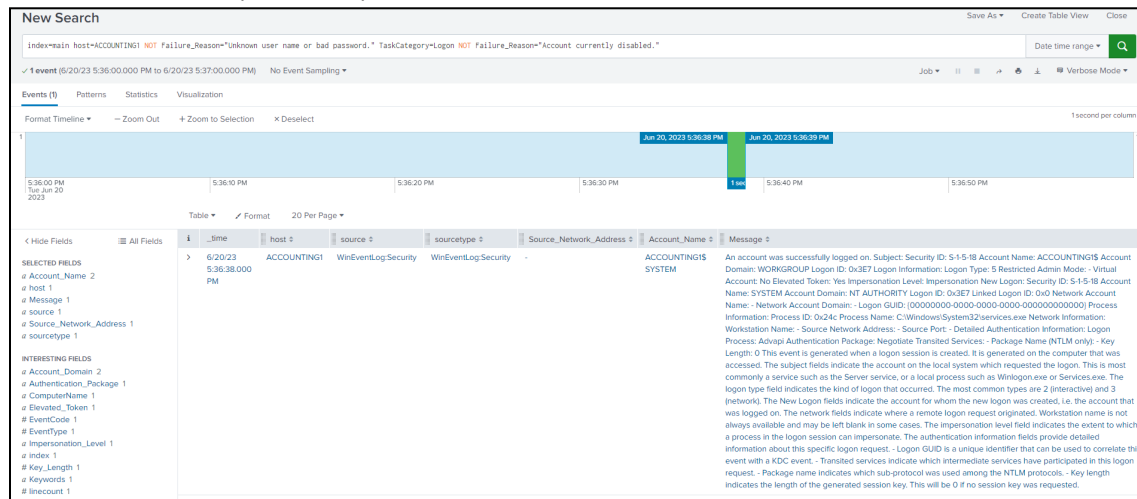
Brute Force Attack (16:58 - 17:38 CT) - 53,460 Failed attempts



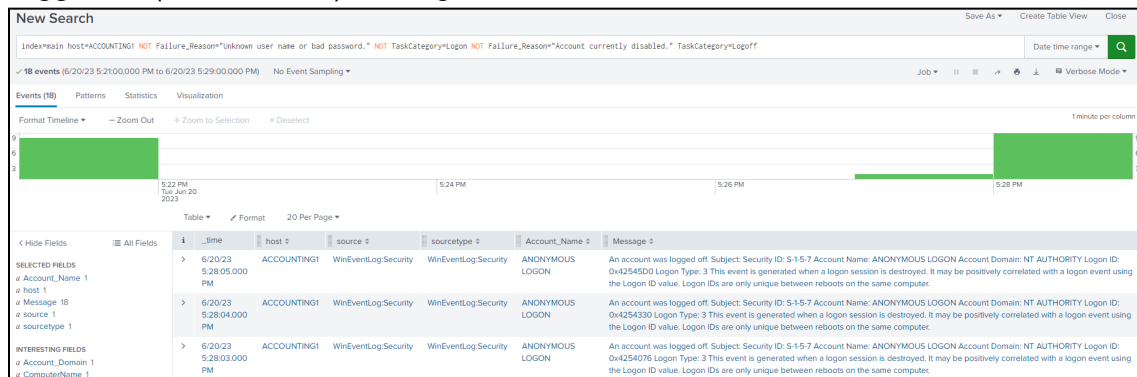
Successful Logins (17:21 - 17:29 CT) - 18 successful logins



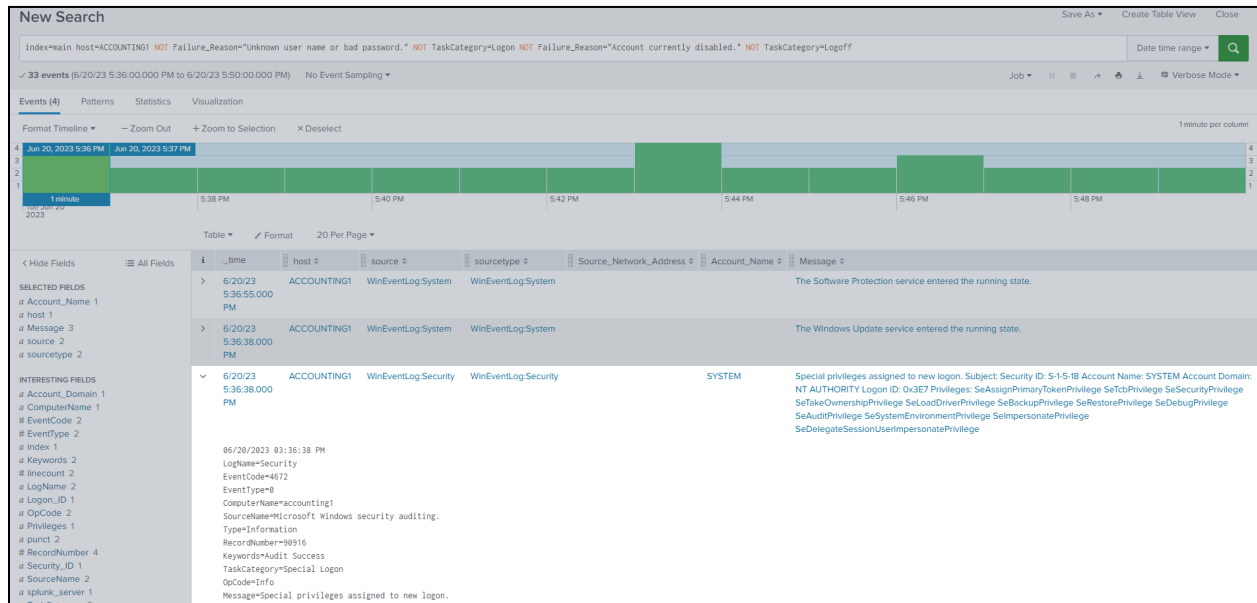
Successful Login (17:36 CT) - 1 successful Login



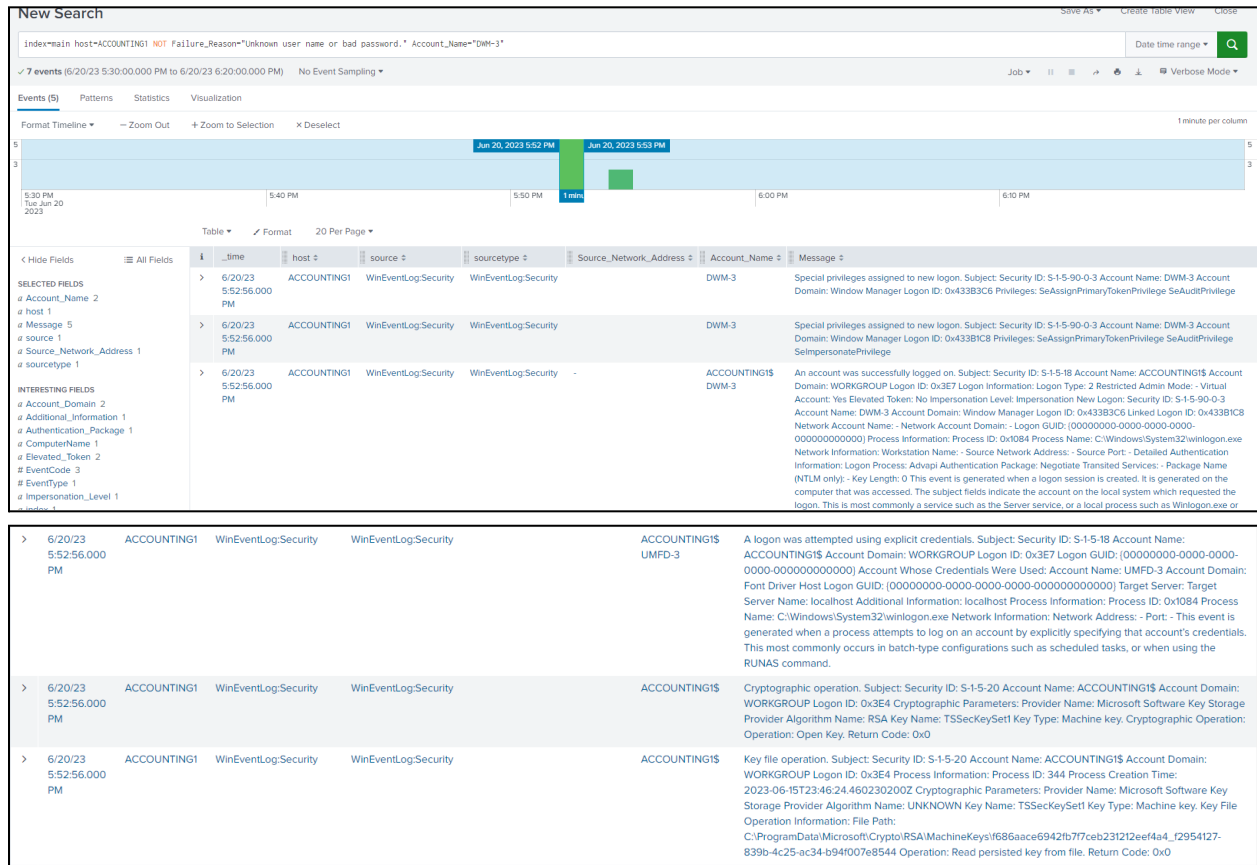
Logged off (17:21 - 17:29) - 18 log off events.



New Account Created (17:36 CT) - New account created *accounting1* with special privileges. (?)



New Account Created (5:52 CT) - New account created DWM-3



>	6/20/23 6:56:39.000 PM	ACCOUNTING1	WinEventLog:Security	WinEventLog:Security	SYSTEM	Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Privileges: SeAssignPrimaryTokenPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege		
>	6/20/23 6:56:39.000 PM	ACCOUNTING1	WinEventLog:Security	WinEventLog:Security	ACCOUNTING1\$ SYSTEM	An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: ACCOUNTING1\$ Account Domain: WORKGROUP Logon ID: 0x3E7 Logon Information: Logon Type: 5 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x24c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi 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 accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly 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 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. 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.	Add to search 3 events Exclude from search 171 events	Account Name: ACCOUNTING1\$ Logon Type: 5 Restricted Admin Impersonation New Logon: NT AUTHORITY Logon ID: 0x3E7

New Account Created (18:56) - New account created called SYSTEM (?)

>	6/20/23 6:56:39.000 PM	ACCOUNTING1	WinEventLog:Security	WinEventLog:Security		SYSTEM	Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Privileges: SeAssignPrimaryTokenPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege
>	6/20/23 6:56:39.000 PM	ACCOUNTING1	WinEventLog:Security	WinEventLog:Security	-	ACCOUNTING1\$ SYSTEM	An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: ACCOUNTING1\$ Account Domain: WORKGROUP Logon ID: 0x3E7 Logon Information: Logon Type: 5 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x24c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi 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 accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly 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 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. 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.
>	6/20/23 6:56:39.000 PM	ACCOUNTING1	WinEventLog:Security	WinEventLog:Security		SYSTEM	Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Privileges: SeAssignPrimaryTokenPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege
>	6/20/23 6:56:39.000 PM	ACCOUNTING1	WinEventLog:Security	WinEventLog:Security	-	ACCOUNTING1\$ SYSTEM	An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: ACCOUNTING1\$ Account Domain: WORKGROUP Logon ID: 0x3E7 Logon Information: Logon Type: 5 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x24c Process Name: C:\Windows\System32\services.exe Network Information:

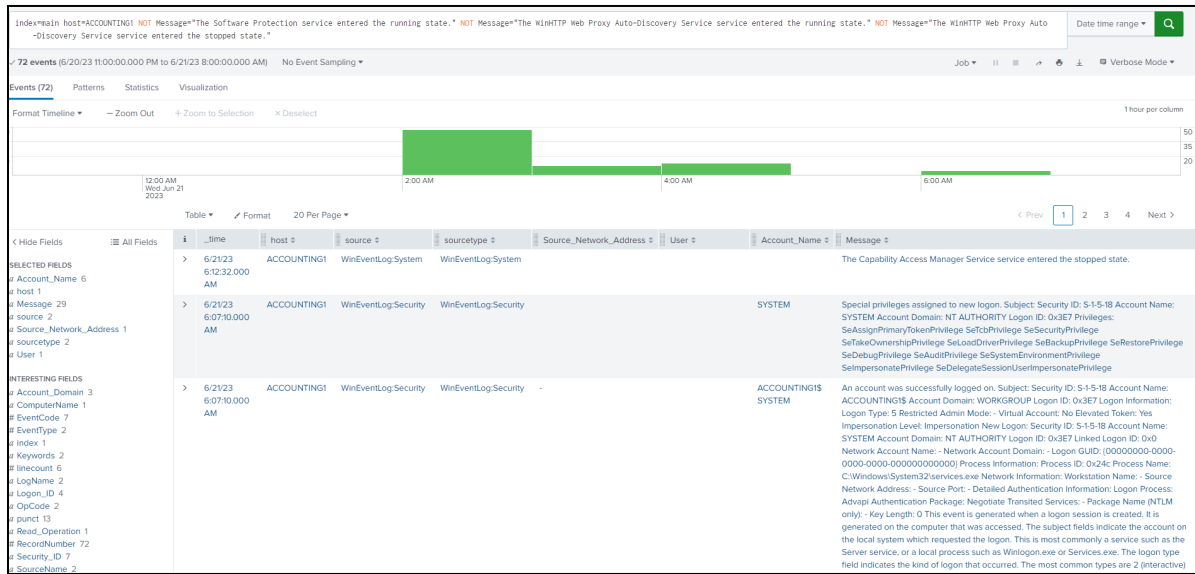
21 JUN 23

ACCOUNTING1 Investigation

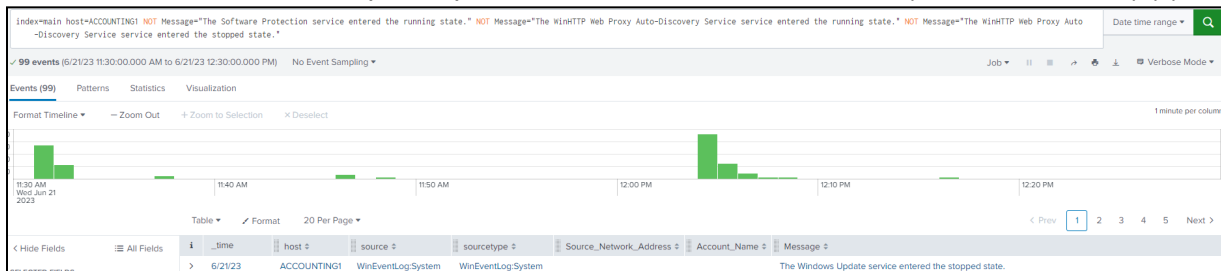
Credentials were read (Throughout the day)

>	6/21/23 2:46:29.000 AM	ACCOUNTING1	WinEventLog:Security	WinEventLog:Security	Administrator	Credential Manager credentials were read. Subject: Security ID: S-1-5-21-2020954294-3820947412-549806118-500 Account Name: Administrator Account Domain: ACCOUNTING1 Logon ID: 0x2E37B55 Read Operation: Enumerate Credentials This event occurs when a user performs a read operation on stored credentials in Credential Manager.
>	6/21/23 2:46:29.000 AM	ACCOUNTING1	WinEventLog:Security	WinEventLog:Security	Administrator	Credential Manager credentials were read. Subject: Security ID: S-1-5-21-2020954294-3820947412-549806118-500 Account Name: Administrator Account Domain: ACCOUNTING1 Logon ID: 0x2E37B55 Read Operation: Enumerate Credentials This event occurs when a user performs a read operation on stored credentials in Credential Manager.
>	6/21/23 2:46:29.000 AM	ACCOUNTING1	WinEventLog:Security	WinEventLog:Security	Administrator	Credential Manager credentials were read. Subject: Security ID: S-1-5-21-2020954294-3820947412-549806118-500 Account Name: Administrator Account Domain: ACCOUNTING1 Logon ID: 0x2E37B55 Read Operation: Enumerate Credentials This event occurs when a user performs a read operation on stored credentials in Credential Manager.
>	6/21/23 2:46:29.000 AM	ACCOUNTING1	WinEventLog:Security	WinEventLog:Security	user	Credential Manager credentials were read. Subject: Security ID: S-1-5-21-2020954294-3820947412-549806118-1004 Account Name: user Account Domain: ACCOUNTING1 Logon ID: 0x20527 Read Operation: Enumerate Credentials This event occurs when a user performs a read operation on stored credentials in Credential Manager.
>	6/21/23 2:46:29.000 AM	ACCOUNTING1	WinEventLog:Security	WinEventLog:Security	user	Credential Manager credentials were read. Subject: Security ID: S-1-5-21-2020954294-3820947412-549806118-1004 Account Name: user Account Domain: ACCOUNTING1 Logon ID: 0x20527 Read Operation: Enumerate Credentials This event occurs when a user performs a read operation on stored credentials in Credential Manager.
>	6/21/23 2:46:29.000 AM	ACCOUNTING1	WinEventLog:Security	WinEventLog:Security	user	Credential Manager credentials were read. Subject: Security ID: S-1-5-21-2020954294-3820947412-549806118-1004 Account Name: user Account Domain: ACCOUNTING1 Logon ID: 0x20527 Read Operation: Enumerate Credentials This event occurs when a user performs a read operation on stored credentials in Credential Manager.

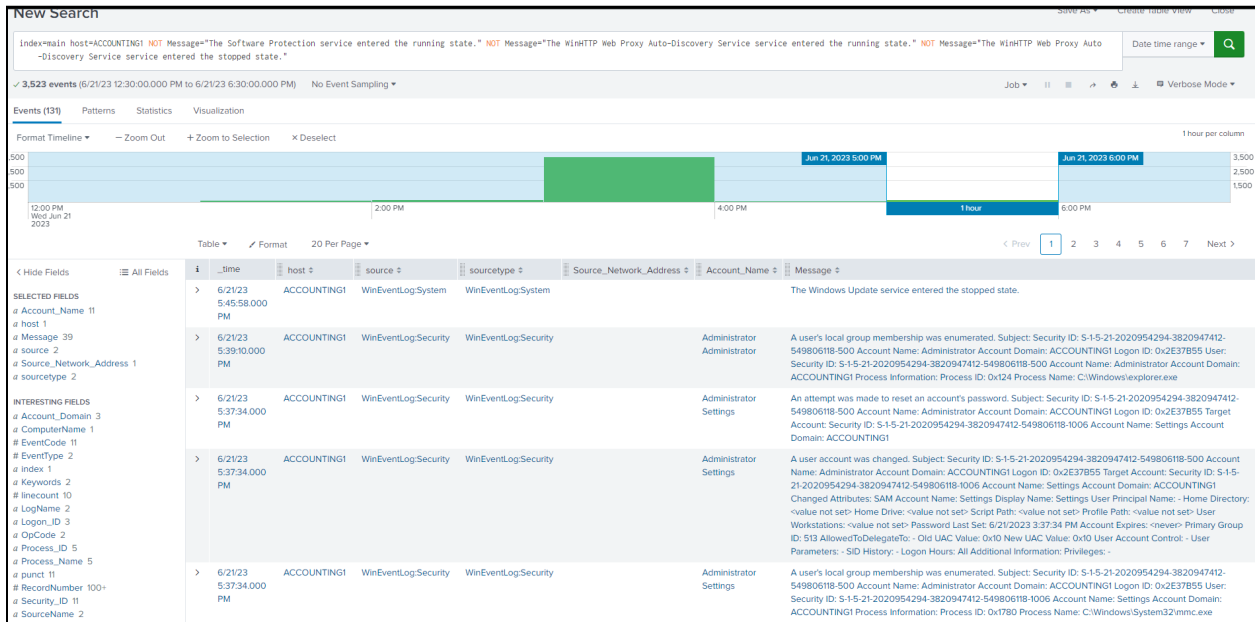
Login and changes to SYSTEM privilege (02:56)



Credentials were read and special privileges were assigned SYSTEM (11:30 - 12:30 CT) (?)



User account was changed (5:34 CT) (?)



>	6/22/23 9:25:43.000 AM	ACCOUNTING1	WinEventLog\Security	WinEventLog\Security	ACCOUNTING1\$	Credential Manager credentials were read. Subject: Security ID: S-1-5-18 Account Name: ACCOUNTING1\$ Account Domain: WORKGROUP Logon ID: 0x3E7 Read Operation: Enumerate Credentials This event occurs when a user performs a read operation on stored credentials in Credential Manager.
>	6/22/23 9:25:43.000 AM	ACCOUNTING1	WinEventLog\Security	WinEventLog\Security	Administrator	Credential Manager credentials were read. Subject: Security ID: S-1-5-21-2020954294-3820947412-549806118-500 Account Name: Administrator Account Domain: ACCOUNTING1 Logon ID: 0x2E37B55 Read Operation: Enumerate Credentials This event occurs when a user performs a read operation on stored credentials in Credential Manager.
>	6/22/23 9:25:43.000 AM	ACCOUNTING1	WinEventLog\Security	WinEventLog\Security	Administrator	Credential Manager credentials were read. Subject: Security ID: S-1-5-21-2020954294-3820947412-549806118-500 Account Name: Administrator Account Domain: ACCOUNTING1 Logon ID: 0x2E37B55 Read Operation: Enumerate Credentials This event occurs when a user performs a read operation on stored credentials in Credential Manager.
>	6/22/23 9:25:43.000 AM	ACCOUNTING1	WinEventLog\Security	WinEventLog\Security	Administrator	Credential Manager credentials were read. Subject: Security ID: S-1-5-21-2020954294-3820947412-549806118-500 Account Name: Administrator Account Domain: ACCOUNTING1 Logon ID: 0x2E37B55 Read Operation: Enumerate Credentials This event occurs when a user performs a read operation on stored credentials in Credential Manager.
>	6/22/23 9:25:43.000 AM	ACCOUNTING1	WinEventLog\Security	WinEventLog\Security	user	Credential Manager credentials were read. Subject: Security ID: S-1-5-21-2020954294-3820947412-549806118-1004 Account Name: user Account Domain: ACCOUNTING1 Logon ID: 0x20527 Read Operation: Enumerate Credentials This event occurs when a user performs a read operation on stored credentials in Credential Manager.
>	6/22/23 9:25:43.000 AM	ACCOUNTING1	WinEventLog\Security	WinEventLog\Security	user	Credential Manager credentials were read. Subject: Security ID: S-1-5-21-2020954294-3820947412-549806118-1004 Account Name: user Account Domain: ACCOUNTING1 Logon ID: 0x20527 Read Operation: Enumerate Credentials This event occurs when a user performs a read operation on stored credentials in Credential Manager.
>	6/22/23 9:25:43.000 AM	ACCOUNTING1	WinEventLog\Security	WinEventLog\Security	user	Credential Manager credentials were read. Subject: Security ID: S-1-5-21-2020954294-3820947412-549806118-1004 Account Name: user Account Domain: ACCOUNTING1 Logon ID: 0x20527 Read Operation: Enumerate Credentials This event occurs when a user performs a read operation on stored credentials in Credential Manager.
>	6/22/23 9:25:43.000 AM	ACCOUNTING1	WinEventLog\Security	WinEventLog\Security	Administrator	Credential Manager credentials were read. Subject: Security ID: S-1-5-21-2020954294-3820947412-549806118-500 Account Name: Administrator Account Domain: ACCOUNTING1 Logon ID: 0x2E37B55 Read Operation: Enumerate Credentials This event occurs when a user performs a read operation on stored credentials in Credential Manager.
>	6/22/23 9:25:43.000 AM	ACCOUNTING1	WinEventLog\Security	WinEventLog\Security	Administrator	Credential Manager credentials were read. Subject: Security ID: S-1-5-21-2020954294-3820947412-549806118-500 Account Name: Administrator Account Domain: ACCOUNTING1 Logon ID: 0x2E37B55 Read Operation: Enumerate Credentials This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Other users

Other users



Add someone else to this PC



Settings
Local account



accounting
Administrator - Local account



general-user
Administrator - Local account



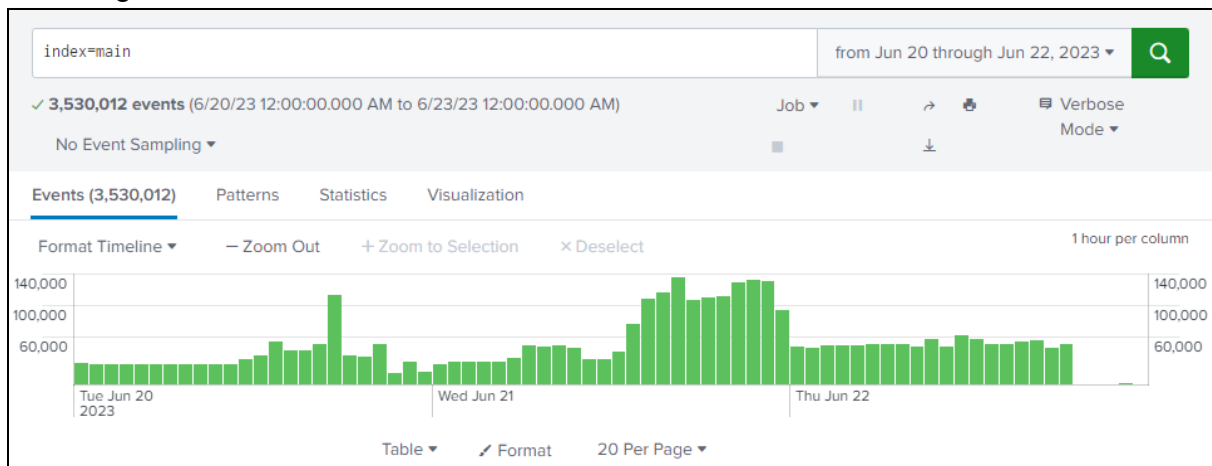
user
Local account

Change account type

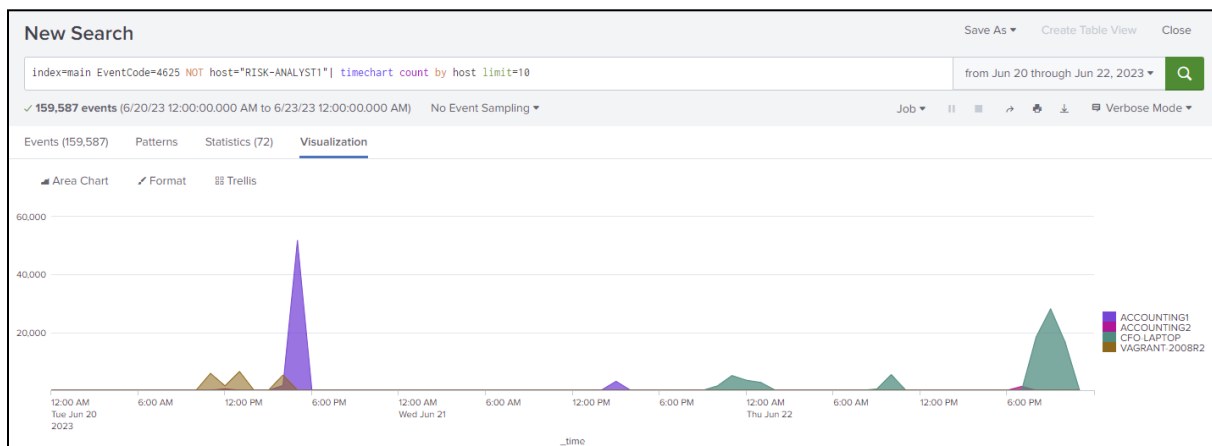
Remove

Analysis

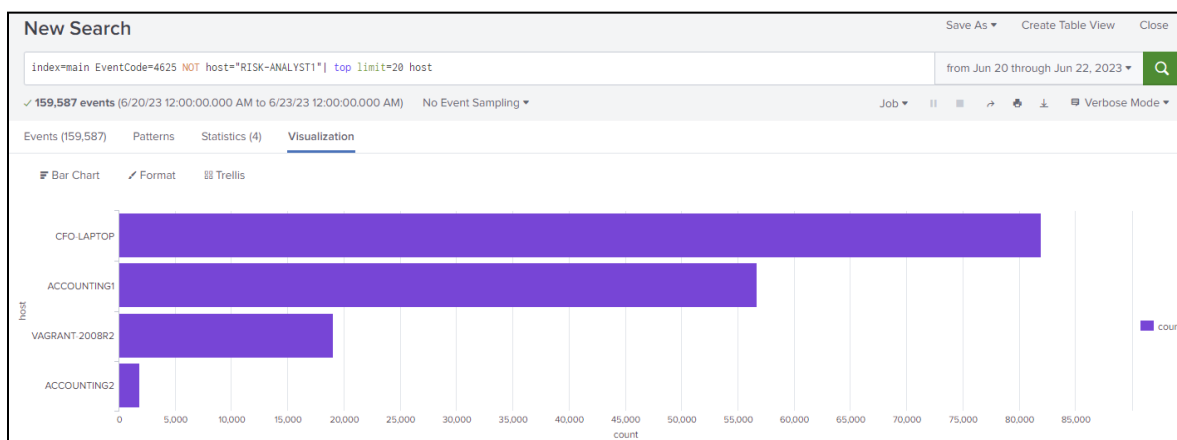
All the logs from June 20 - June 22



Visual Representation of the brute force attack on Accounting1, Accounting2, Metasploitable3, and CFO



Bar graph on the same the brute force attack on Accounting1, Accounting2, Metasploitable3, and CFO



Description

On June 20, 2023, there were several notable activities recorded in the system logs. At 16:58 - 17:38 CT, the server Accounting1 (IP: 10.0.0.126) experienced a concerning number of failed login attempts, reaching a total of 53,460. At 17:21:31, an account managed to successfully log in. Similarly, Accounting2 (IP: 10.0.0.197) encountered 493 failed attempts from 12:52 to 13:00, at 12:52:16, the first successful login occurred. Another server named Vagrant/Metasploitable3 (IP: 10.0.0.82) faced 19,080 failed attempts between 11:50 and 16:10, with the first successful login taking place at 16:08:55.

Moving to June 22, 2023, the CFO server (IP: 10.0.0.206) encountered 81,972 failed login attempts from 09:56 to 23:59. There have been no successful logins recorded.

These events indicate a high level of suspicious activity, with numerous failed login attempts on various servers. It is crucial to investigate the source and nature of these attempts to ensure the security of the systems and prevent any unauthorized access.

Summary

20 June 2023

- Accounting1 (10.0.0.126)
 - 16:58 - 17:38 CT → 53,460 failed attempts
 - 17:21:31 → first successful login
- Accounting2 (10.0.0.197)
 - 12:52 - 13:00 → 493 failed attempts
 - 12:52:16 → first Successful login
- VAGRANT/Metasploitable3 (10.0.0.82)
 - 11:50 - 16:10 → 19,080 failed attempts
 - 16:08:55 → first successful login

22 June 2023

- CFO (10.0.0.206)
 - 09:56 - 10:46 → 81,972 failed attempts


As of June 22, 2023 there have been no successful logins.

Detection Implementation

Implemented 20 JUN 23


Failed Windows Logon Attempts (Splunk Triggered Alert)

- EventCode of 4625 triggers in real time, when triggered is added to triggered alerts

Search	index=main EventCode=4625		
Alert type	Scheduled		Real-time
Expires	5	day(s) ▼	
Trigger Conditions			
Trigger alert when	Per-Result ▼		
Throttle ?	<input type="checkbox"/>		
Trigger Actions			
	+ Add Actions ▼		
When triggered	▼	 Add to Triggered Alerts	Remove
		Severity	Medium ▼



SSH Attempt - Failed Password (Splunk Triggered Alert)

- String “Failed password” triggers in real time, when triggered is added to triggered alerts

Search	index=main "Failed password"		
Alert type	Scheduled		Real-time
Expires	7	day(s) ▼	
Trigger Conditions			
Trigger alert when	Per-Result ▼		
Throttle ?	<input type="checkbox"/>		
Trigger Actions			
	+ Add Actions ▼		
When triggered	▼	 Add to Triggered Alerts	Remove



Windows Brute Force Attack (Splunk Triggered Alert)

- EventCode of 4625 triggers in real time, ten triggers in one minute launches alert
- Added to triggered alerts, email is also sent to admin with HIGH priority

Trigger alert when	Number of Results ▼	
	is greater than ▼	10
in	1	minute(s) ▼
Trigger	Once For each result	
Throttle ?	<input checked="" type="checkbox"/>	
Suppress results containing field value	index=main EventCode=4625	
Suppress triggering for	5	minute(s) ▼
Trigger Actions		
	+ Add Actions ▼	
When triggered	▼  Add to Triggered Alerts Remove	
	Severity	Critical ▼
	>  Send email Remove	

SSH Brute Force Attack (Splunk Triggered Alert)

- String “Failed password” triggers in real time, ten triggers in one minute launches alert
- Added to triggered alerts, email is also sent to admin with HIGH priority.

Trigger Conditions		
Trigger alert when	Number of Results ▼	
	is greater than ▼	10
in	1	minute(s) ▼
Trigger	Once For each result	
Throttle ?	<input checked="" type="checkbox"/>	
Suppress results containing field value	index=main "Failed Password"	
Suppress triggering for	5	minute(s) ▼
Trigger Actions		
	+ Add Actions ▼	
When triggered	▼  Add to Triggered Alerts Remove	
	Severity	Critical ▼
	>  Send email Remove	

Metasploit Signature Identified (Splunk Triggered Alert)

- Entry with either port 4444 (default msf port), user agent containing the string “Metasploit”, or user agent containing the string “Mozilla/4.0 (compatible; MSIE 6.1; Windows NT)” triggers in real time.
- Added to triggered alerts, email is also sent to admin with HIGH priority.

Search	index=main port=4444 OR user_agent="*Metasploit*" OR user_agent="*Mozilla/4.0 (compatible; MSIE 6.1; Windows NT)*"	
Alert type	Scheduled	Real-time
Expires	5	day(s) ▼
Trigger Conditions		
Trigger alert when	Per-Result ▼	
Throttle ?	<input type="checkbox"/>	
Trigger Actions		
	+ Add Actions ▼	
When triggered	▼ Add to Triggered Alerts Remove	
	Severity	Critical ▼
	> Send email Remove	

Implemented 21 JUN 23


Windows User Created (Splunk Triggered Alert)

- EventCode 4720 indicating a windows user was created triggers in real time, when triggered is added to triggered alerts

Search	index=main EventCode=4720	
Alert type	Scheduled	Real-time
Expires	7	day(s) ▼
Trigger Conditions		
Trigger alert when	Per-Result ▼	
Throttle ?	<input type="checkbox"/>	
Trigger Actions		
	+ Add Actions ▼	
When triggered	▼ Add to Triggered Alerts Remove	
	Severity	Medium ▼


Windows Logon Successful (Splunk Triggered Alert)

- EventCode 4624 indicating a successful windows logon triggers in real time, when triggered is added to triggered alerts

Search	index=main EventCode=4624	
Alert type	<div>Scheduled</div> <div>Real-time</div>	
Expires	7	day(s) ▼
Trigger Conditions		
Trigger alert when	Per-Result ▼	
Throttle ?	<input type="checkbox"/>	
Trigger Actions		
	<div>+ Add Actions ▼</div>	
When triggered	<div>▼  Add to Triggered Alerts Remove</div> <div>Severity <div>Medium ▼</div></div>	


Linux User Created (Splunk Triggered Alert)

- Strings “COMMAND=/usr/sbin/useradd” OR “COMMAND=/usr/sbin/adduser” indicate new linux user created, triggers in real time, when triggered is added to triggered alerts

Search	index=main "COMMAND=/usr/sbin/useradd" OR "COMMAND=/usr/sbin/adduser"	
Alert type	<div>Scheduled</div> <div>Real-time</div>	
Expires	7	day(s) ▼
Trigger Conditions		
Trigger alert when	Per-Result ▼	
Throttle ?	<input type="checkbox"/>	
Trigger Actions		
	<div>+ Add Actions ▼</div>	
When triggered	<div>▼  Add to Triggered Alerts Remove</div> <div>Severity <div>Medium ▼</div></div>	

SSH Login Successful (Splunk Triggered Alert)

- Strings “sshd” “Accepted” and “for” identifies a successful SSH login, triggers in real time, when triggered is added to triggered alerts

Search	index=main "sshd" "Accepted" "for"		
Alert type	<div>ScheduledReal-time</div>		
Expires	7	day(s) ▼	
Trigger Conditions			
Trigger alert when	Per-Result ▼		
Throttle ?	<input type="checkbox"/>		
Trigger Actions			
	<div>+ Add Actions ▼</div>		
When triggered	▼	 Add to Triggered Alerts	Remove
		Severity	Medium ▼