Using Splunk to Assess and Implement Critical Security Control #3

splunk> .conf2017

Disclaimer

- During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward- looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Agenda

- Background of Critical Security Controls
- What is Critical Security Control #3
- Critical Security Control #3, sub-controls
- Risk Measure/Metrics
- Effectiveness Test
- Benchmark
- Splunk Supporting Data
- Splunk Searches
- Critical Security Control #3 Implementation Summary
- Q&A

splunk> .conf2017

Speakers

Why are you looking at the people on stage?

splunk> .conf2017

Speakers

Matt Gonter

- 18+ years in information technology, in the areas of security operations and architecture
- Former Navy, doing/managing intelligence collection and analysis
- SOC analyst, for a large software company, developing security processes and security content
- Splunk Professional Services Consultant, Concanon Security Director
- Master's Degree in Technology Management from Georgetown University

Matt Wade

- 18+ years in information security, in areas of offensive security, security operations/analysis, and security architecture
- Former Army, intelligence collection and analysis, cellular interdiction, cellular forensics, and media forensics
- Former DOD Contractor, doing and teaching some stuff
- Former Federal employee, Endpoint Exploitation Analyst, in the United States Army's Cyber Force
- Splunk Professional Services Consultant, Concanon Principal Security Consultant

splunk> .conf2017

Critical Security Control #3

What it is, what it was, what it shall be

splunk> .conf2017

Full Disclosure

- Splunk can detect or validate that a control is in place. We are not threat hunting.
- The scope of this discussion will surround Windows Servers with Universal Forwarders installed on them. It does not extend to Laptops/Desktops or mobile devices.
- We are not detecting for Malicious Software activity. We are detecting for a shift in configurations.
- Critical Security Control #1 and #2 are complete

Critical Security Controls = Assurance

Assurance != Compliance

Background

- 2008 Office of Secretary of Defense ask NSA for help in prioritizing security controls.
- Allowed public disclosure due to the inability to protect the nation if critical infrastructure was not protected.
- US State Department 2009 Validation and Adoption.
- 2011 United Kingdom Adoption and Participation.
- Maintained by the Center for Internet Security CIS since 2015.

Key Insight:
- Controls were only a priority when it could be shown to stop or mitigate a known attack.
- Publish by a consortium of volunteer Cyber Security Professionals from all over the globe.

Tom Donahue - CIA

"First fix the known bads"

What is Critical Security Control #3

Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Establish, implement, and actively manage (track, report on, correct) the security configuration *of laptops, servers, and workstations, using a rigorous configuration management and change control process, in order to prevent attackers from exploiting vulnerable services and settings.*

Prevent attackers from exploiting services and settings that allow easy access through networks and browsers: ***build a secure image*** *that is used for all new systems deployed to the enterprise,* ***host these standard images on secure storage*** *servers, regularly validate and update these configurations, and track system images in a configuration management system.*

As delivered by manufacturers and resellers, the default configurations for operating systems and applications are normally geared to ease-of-deployment and ease-of-use, not security. ***Basic controls, open services and ports, default accounts or passwords, older (vulnerable) protocols, pre-installation of unneeded software****; all can be exploitable in their default state.*

Sub-controls of Critical Security Control #3

splunk> .conf2017

Critical Security Control #3

- 1: **Establish standard secure configurations of your operating systems and software applications.** Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. These images should be validated and **refreshed on a regular basis** to update their security configuration in light of recent vulnerabilities and attack vectors.

- 2: **Follow strict configuration management**, building a **secure image** that is used to build all new systems that are deployed in the enterprise. **Any existing system that becomes compromised should be re-imaged** with the secure build. Regular updates or exceptions to this image should be integrated into the organization's change management processes. Images should be created for workstations, servers, and other system types used by the organization.

Critical Security Control #3

- 3: **Store the master images on securely configured servers**, validated with **integrity checking tools** capable of continuous inspection, and change management to ensure that only authorized changes to the images are possible. Alternatively, these master images can be **stored in offline machines, air-gapped** from the production network, with images copied via secure media to move them between the image storage servers and the production network.

- 4: Perform **all remote administration** of servers, workstation, network devices, and similar equipment **over secure channels**. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

Critical Security Control #3

- 5: **Use file integrity checking tools to ensure that critical system files** (including sensitive system and application executables, libraries, and configurations) **have not been altered**.
  The reporting system should:
  -Have the ability to account for routine and expected changes
  -Highlight and alert on unusual or unexpected alterations
  -Show the history of configuration changes over time
  -Identify who made the change (including the original logged-in account in the event of a user ID switch, such as with the su or sudo command).

  These **integrity checks should identify suspicious system alterations** such as:
  -Owner and permissions changes to files or directories
  -The use of alternate data streams which could be used to hide malicious activities
  -The introduction of extra files into key system areas (which could indicate malicious payloads left by attackers or additional files inappropriately added during batch distribution processes)

Critical Security Control #3

- 6: Implement and test an **automated configuration monitoring system** that verifies all remotely testable secure configuration elements, and alerts when unauthorized changes occur. This includes detecting new listening ports, new administrative users, changes to group and local policy objects (where applicable), and new services running on a system. Whenever possible use tools compliant with the **Security Content Automation Protocol (SCAP)** in order to streamline reporting and integration.

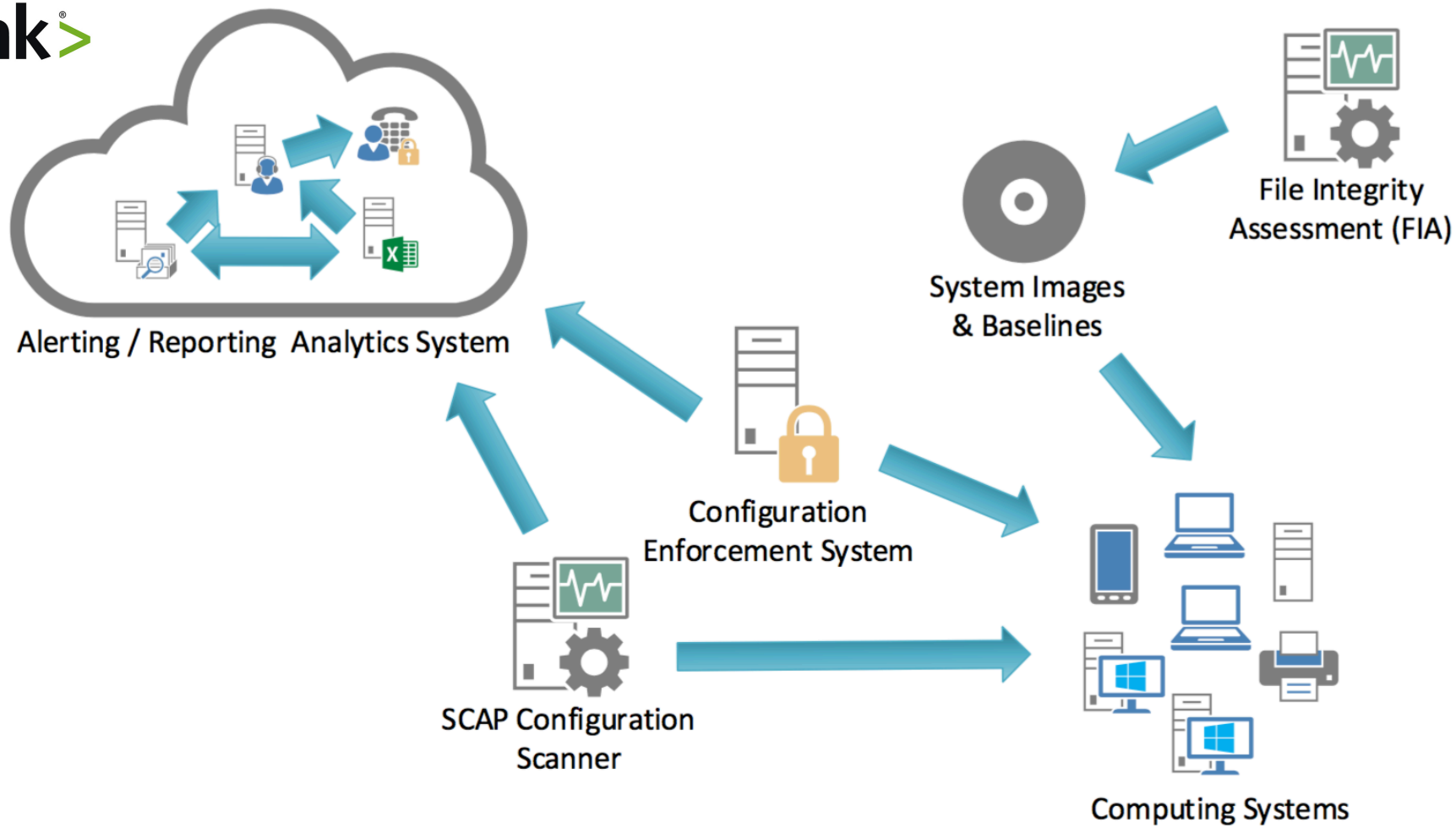
  https://nvd.nist.gov/scap/validated-tools

- 7: **Deploy system configuration management tools**, such as Active Directory Group Policy Objects for Microsoft Windows systems or Puppet for UNIX systems that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals. They should be **capable of triggering redeployment of configuration settings** on a scheduled, manual, or event-driven basis.

Risk Measure/Metrics and Tests

splunk> .conf2017

Entity Relationship Diagram



Metrics

Measure	Metrics
What is the percentage of business systems that are not currently configured with a security configuration that matches the organization's approved configuration standard (by business unit)?	Lower: Less than 1% Moderate: 1%-4% Higher: 5%-10%
What is the percentage of business systems whose security configuration is not enforced by the organization's technical configuration management applications (by business unit)?	Lower: Less than 1% Moderate: 1%-4% Higher: 5%-10%
What is the percentage of business systems that are not up to date with the latest available operating system software security patches (by business unit)?	Lower: Less than 1% Moderate: 1%-4 Higher: 5%-10

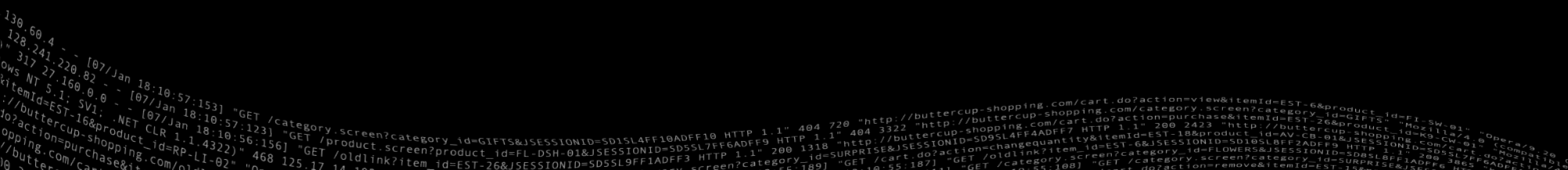
Metrics

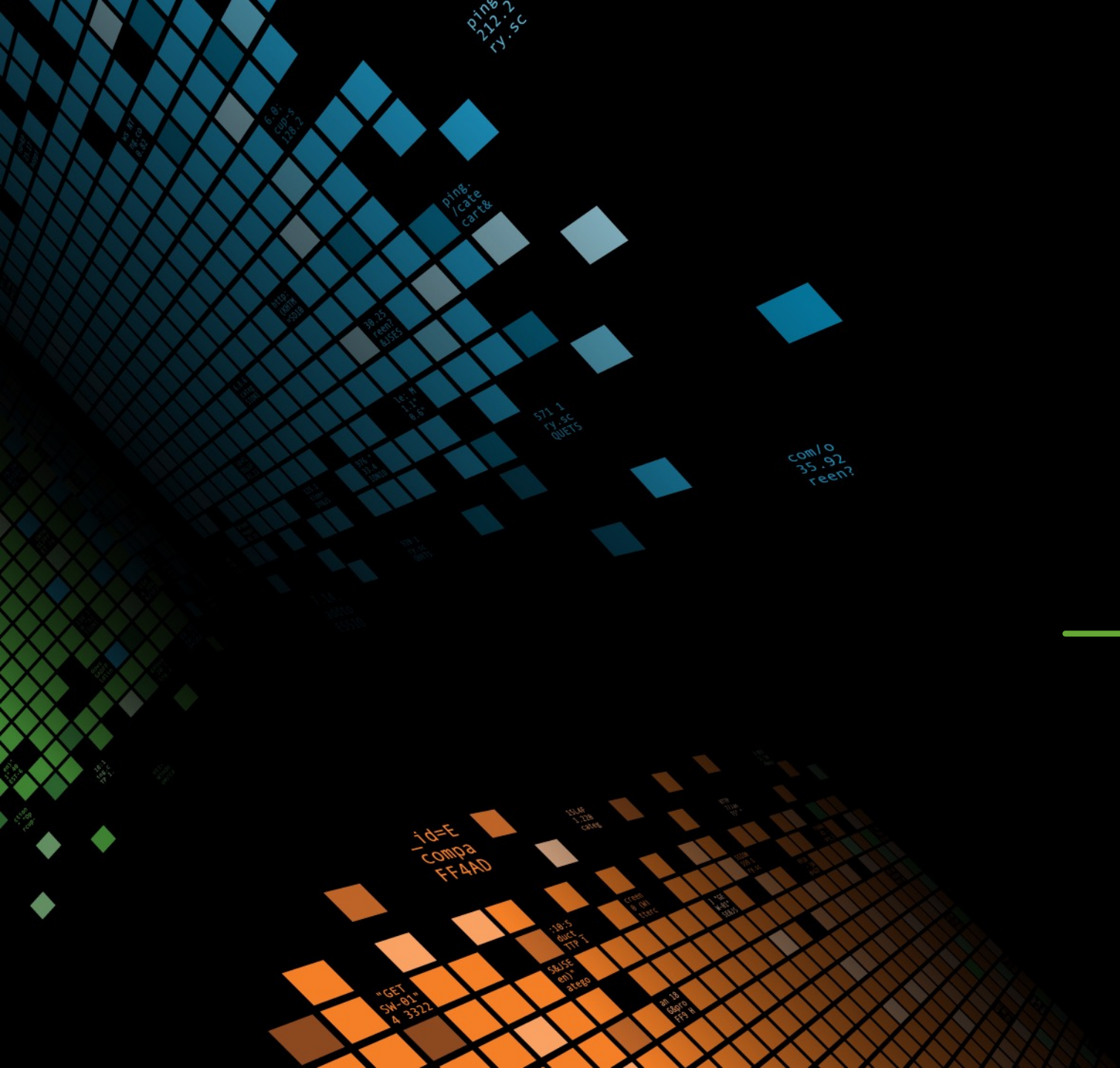
Measure	Metrics
What is the percentage of business systems that are not up to date with the latest available business software application security patches (by business unit)?	Lower: Less than 1% Moderate: 1%-4% Higher: 5%-10%
How many unauthorized configuration changes have been recently blocked by the organization's configuration management system (by business unit)?	Lower: Less than 1% Moderate: 1%-4% Higher: 5%-10%
How long does it take to reverse unauthorized changes on systems (time in minutes - by business unit)?	Lower: 60 Minutes Moderate: 1 Day Higher: 1 Week
How long does it take to detect configuration changes to a system (time in minutes - by business unit)?	Lower: 60 Minutes Moderate: 1 Day Higher: 1 Week

splunk> .conf2017

Effectiveness Test

- Use a benign system on 10 segments with unofficial configurations. Make changes:
  - Local Security Policy
  - Permissions
  - Install Application enabling unauthorized port
  - Delete logs
- Determine expected change information and validate against alerts for accuracy.
- Did the software execute successfully? Was anyone alerted to it?





Benchmarks

CIS Benchmarks

- Community Driven Configuration Guidelines

Level 1

- Practical and Prudent
- Clear Security Benefit
- Doesn't break as much

Level 2

- Security is Paramount
- Defense in Depth
- Most likely is going to break something.

- Lab:
  - Windows 2012 R2 Domain Controller
  - Windows 2012 R2 Server (Applied L1 Member Server GPO)
  - Splunk Instance

Security Settings

Account Policies/ Password Policy

Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	60 days
Minimum password age	1 days
Minimum password length	14 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Account Policies/ Account Lockout Policy

Policy	Setting
Account lockout duration	15 minutes
Account lockout threshold	10 invalid logon attempts
Reset account lockout counter after	15 minutes

Local Policies/ User Rights Assignment

Policy	Setting
Access Credential Manager as a trusted caller	
Access this computer from the network	BUILTIN\Administrators, NT AUTHORITY\Authenticated Users
Act as part of the operating system	
Adjust memory quotas for a process	BUILTIN\Administrators, NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\NETWORK SERVICE
Allow log on locally	BUILTIN\Administrators
Allow log on through Terminal Services	BUILTIN\Administrators, BUILTIN\Remote Desktop Users
Back up files and directories	BUILTIN\Administrators
Change the system time	BUILTIN\Administrators, NT AUTHORITY\LOCAL SERVICE
Change the time zone	BUILTIN\Administrators, NT AUTHORITY\LOCAL SERVICE
Create a pagefile	BUILTIN\Administrators
Create a token object	
Create global objects	BUILTIN\Administrators, NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\SERVICE

Security Settings

Account Policies/ Password Policy

Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	60 days
Minimum password age	1 days
Minimum password length	14 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Account Policies/ Account Lockout Policy

Policy	Setting
Account lockout duration	15 minutes
Account lockout threshold	10 invalid logon attempts
Reset account lockout counter after	15 minutes

Local Policies/ User Rights Assignment

Policy	Setting
Access Credential Manager as a trusted caller	
Access this computer from the network	BUILTIN\Administrators, NT AUTHORITY\Authentica
Act as part of the operating system	
Adjust memory quotas for a process	BUILTIN\Administrators, NT AUTHORITY\LOCAL SE AUTHORITY\NETWORK SERVICE
Allow log on locally	BUILTIN\Administrators
Allow log on through Terminal Services	BUILTIN\Administrators, BUILTIN\Remote Desktop U
Back up files and directories	BUILTIN\Administrators
Change the system time	BUILTIN\Administrators, NT AUTHORITY\LOCAL SE
Change the time zone	BUILTIN\Administrators, NT AUTHORITY\LOCAL SE
Create a pagefile	BUILTIN\Administrators
Create a token object	
Create global objects	BUILTIN\Administrators, NT AUTHORITY\LOCAL SE AUTHORITY\NETWORK SERVICE, NT AUTHORIT

```
Account Policies
----------------
    GPO: Default Domain Policy
        Policy:             MaximumPasswordAge
        Computer Setting:   42
    GPO: Default Domain Policy
        Policy:             LockoutBadCount
        Computer Setting:   N/A
    GPO: 2012_L1_COMPUTER
        Policy:             LockoutDuration
        Computer Setting:   15
    GPO: Default Domain Policy
        Policy:             MinimumPasswordAge
        Computer Setting:   1
    GPO: 2012_L1_COMPUTER
        Policy:             MaximumPasswordAge
        Computer Setting:   60
    GPO: 2012_L1_COMPUTER
        Policy:             MinimumPasswordAge
        Computer Setting:   1
    GPO: Default Domain Policy
        Policy:             MinimumPasswordLength
        Computer Setting:   7
    GPO: 2012_L1_COMPUTER
        Policy:             ResetLockoutCount
        Computer Setting:   15
    GPO: Default Domain Policy
        Policy:             PasswordHistorySize
        Computer Setting:   24
    GPO: 2012_L1_COMPUTER
        Policy:             LockoutBadCount
        Computer Setting:   10
    GPO: 2012_L1_COMPUTER
        Policy:             PasswordHistorySize
        Computer Setting:   24
    GPO: 2012_L1_COMPUTER
        Policy:             MinimumPasswordLength
        Computer Setting:   14
```

Splunk Supporting Data

splunk> .conf2017

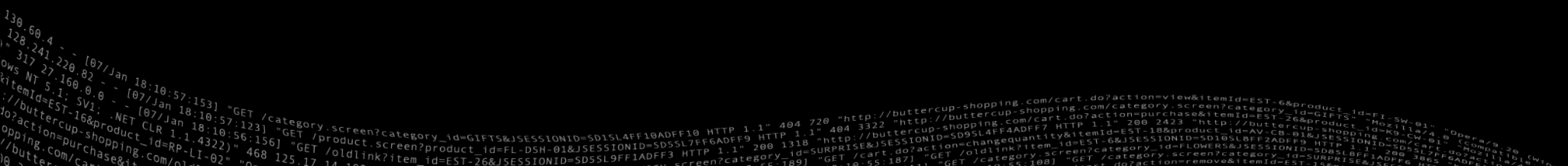
Splunk Supporting Data
(Configuration Management Tools)

Configuration Management

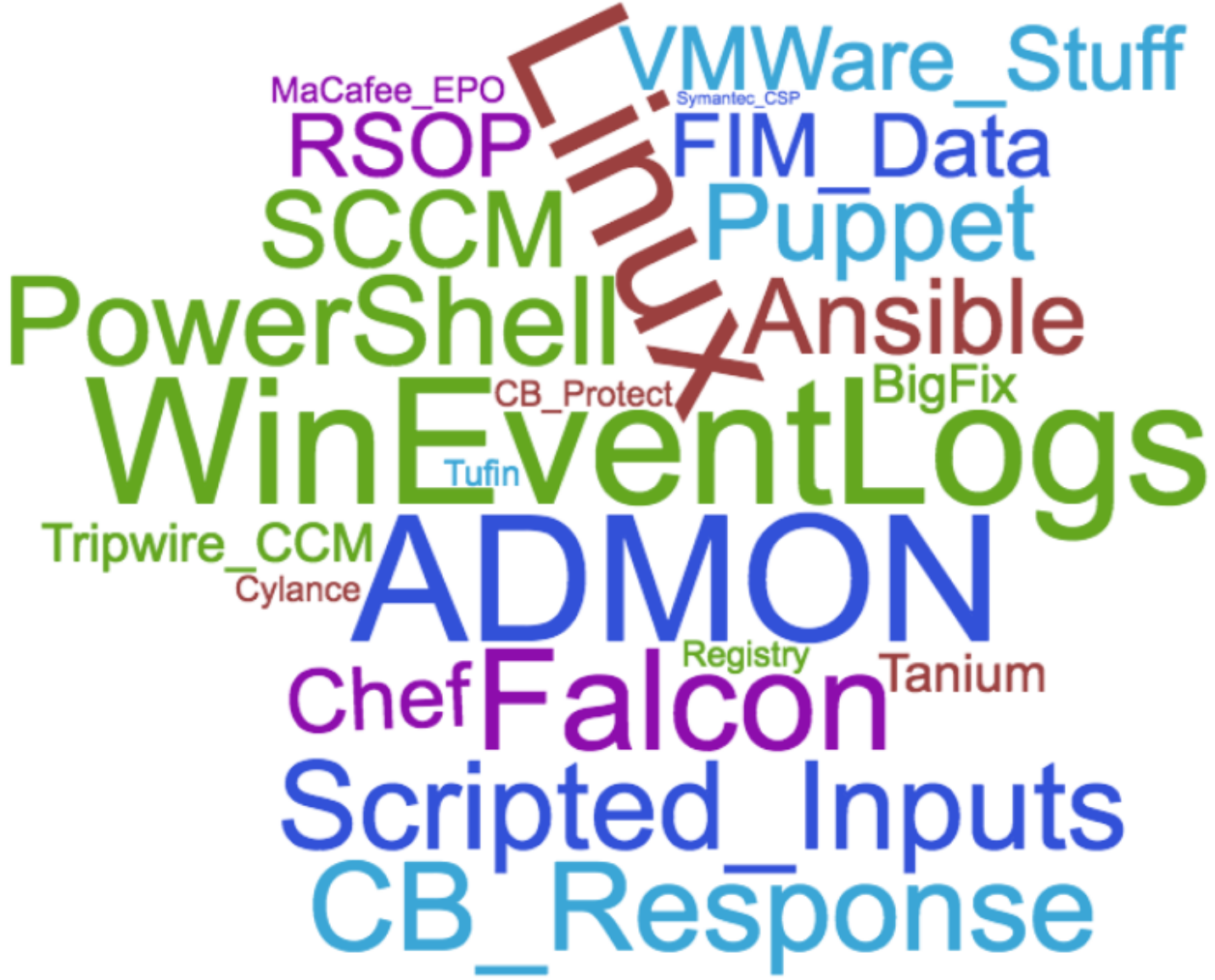
- **Active Directory**
- PowerShell
- SCCM
- Puppet
- Chef
- Ansible

Data Sources

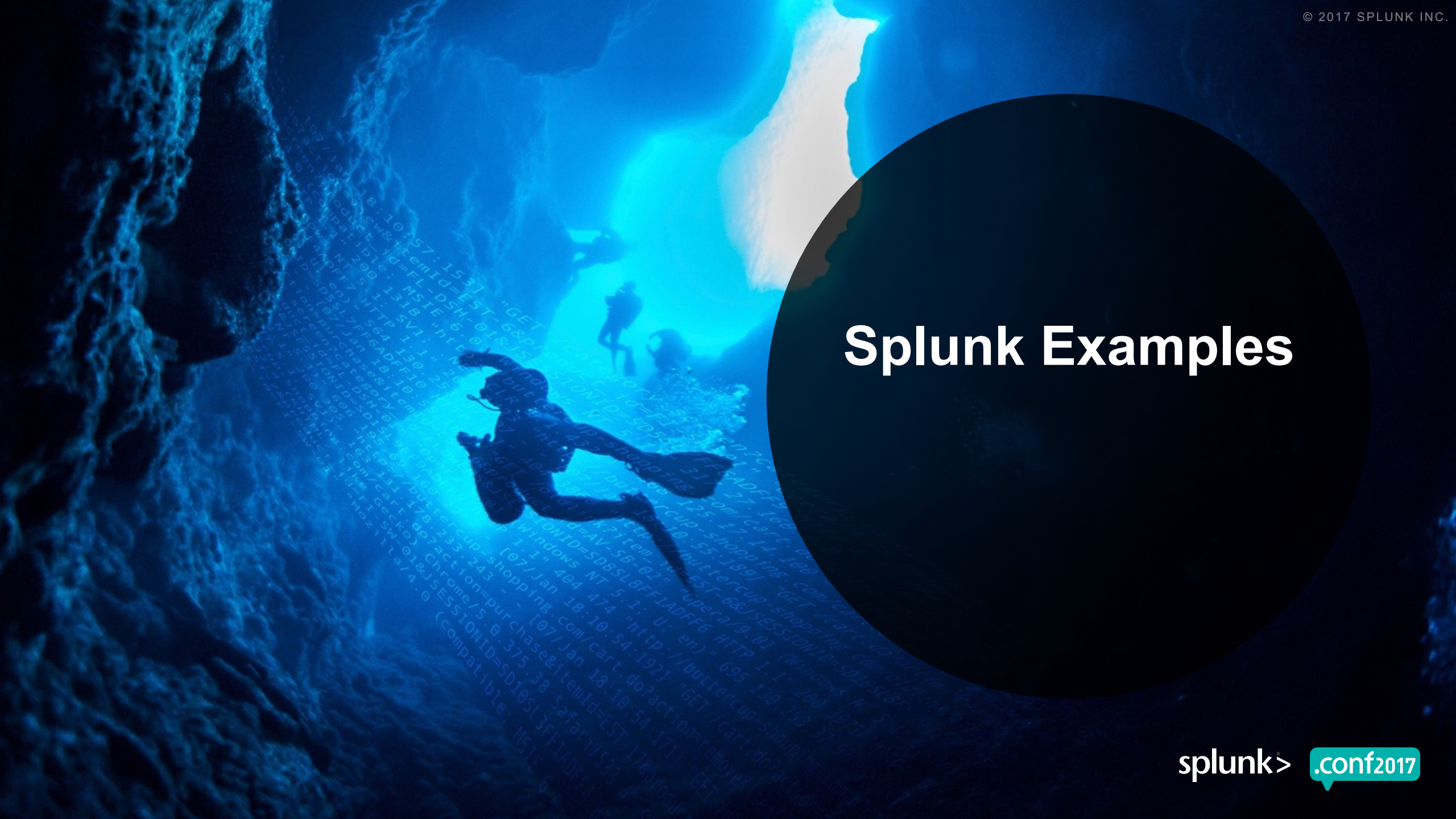
- Configuration Lookup
- Windows Event Logs
- ADMON
- Registry Data



splunk> .conf2017



splunk> .conf2017



Splunk Examples

splunk> .conf2017

Example 1

Change to Secure Configuration (Local & Domain)

Splunk Example 1

Change to Secure Configuration (Local & Domain)

- For Microsoft Active Directory, there's a ***LOT*** AND this isn't even the half of it

Event ID Range	Description
4000–4007	Group Policy start events: These informational events appear in the event log when an instance of Group Policy processing begins.
4016–4299	Component start events: These informational events appear in the event log when a component of Group Policy processing begins the task described in the event.
5000–5299	Component success events: These informational events appear in the event log when a component of Group Policy processing successfully completes the task described in the event.
5300–5999	Informative events: These informational events appear in the event log during the entire instance of Group Policy processing and provide additional information about the current instance.
6000–6007	Group Policy warning events: These warning events appear in the event log when an instance of Group Policy processing completes with errors.
6017–6299	Component warning events: These warning events appear in the event log when a component of Group Policy processing completes the task described in the event with errors.
6300–6999	Informative warning events: These warning events appear in the event log to provide additional information about possible error conditions with the action described in the event.
7000–7007	Group Policy error events: These error events appear in the event log when the instance of Group Policy processing does not complete.
7017–7299	Component error events: These error events appear in the event log when a component of Group Policy processing does not complete the task described in the event.
7300–7999	Informative error events: These error events appear in the event log to provide additional information about the error condition with the action described in the event.
8000–8007	Group Policy success events: These informational events appear in the event log when the instance of Group Policy completes successfully.

EventCode=4719

System audit policy was changed

```
index=wineventlog sourcetype=wineventlog:security (EventCode=4719) | stats values(Keywords) AS desc by _time, Account_Name, Account_Domain, Category,
    Subcategory, Changes | sort -_time | rename _time AS Time, Account_Name AS "Account That Did This", Account_Domain AS "Domain", desc AS Description |
    eval Time=strftime(Time, "%F %T")
```

✓ 712 events (before 9/25/17 1:44:30.000 PM) No Event Sampling Job Smart Mode

Events | Patterns | Statistics (712) | Visualization

100 Per Page Format Preview < Prev 1 2 3 4 5 6 7 8 Next >

Time	Account That Did This	Domain	Category	Subcategory	Changes	Description
2017-09-25 07:46:57	DC01$	CONCANON	Account Logon	Credential Validation	Success Added, Failure added	Audit Success
2017-09-25 07:46:57	DC01$	CONCANON	Account Logon	Credential Validation	Success removed, Failure removed	Audit Success
2017-09-25 07:46:57	DC01$	CONCANON	Account Logon	Kerberos Authentication Service	Success Added, Failure added	Audit Success
2017-09-25 07:46:57	DC01$	CONCANON	Account Logon	Kerberos Authentication Service	Success removed, Failure removed	Audit Success
2017-09-25 07:46:57	DC01$	CONCANON	Account Logon	Kerberos Service Ticket Operations	Success Added, Failure added	Audit Success
2017-09-25 07:46:57	DC01$	CONCANON	Account Logon	Kerberos Service Ticket Operations	Success removed, Failure removed	Audit Success
2017-09-25 07:46:57	DC01$	CONCANON	Account Logon	Other Account Logon Events	Success Added, Failure added	Audit Success
2017-09-25 07:46:57	DC01$	CONCANON	Account Logon	Other Account Logon Events	Success removed, Failure removed	Audit Success
2017-09-25 07:46:57	DC01$	CONCANON	DS Access	Detailed Directory Service Replication	Success Added, Failure added	Audit Success
2017-09-25 07:46:57	DC01$	CONCANON	DS Access	Detailed Directory Service Replication	Success removed, Failure removed	Audit Success
2017-09-25 07:46:57	DC01$	CONCANON	DS Access	Directory Service Replication	Success Added, Failure added	Audit Success
2017-09-25 07:46:57	DC01$	CONCANON	DS Access	Directory Service Replication	Success removed, Failure removed	Audit Success
2017-09-25 07:46:57	DC01$	CONCANON	Detailed Tracking	DPAPI Activity	Success Added, Failure added	Audit Success

splunk> .conf2017

EventCode=4739

Domain Policy was changed

https://answers.splunk.com/answers/400618/how-to-troubleshoot-why-we-are-seeing-unexpected-c.html

✓ 13 events (before 9/25/17 1:52:50.000 PM) No Event Sampling

Job Smart Mode

Events Patterns Statistics (13) Visualization

100 Per Page Format Preview

_time	Account_Name	Account_Domain	Change_Type	Domain_Name	Domain_ID	Min_Password_Age	Max_Password_Age	Force_Logoff	Lockout_Threshold	Lock
2017-09-22 01:20:34	WORKSTATION01$	CONCANON	Password Policy modified	WORKSTATION01	WORKSTATION01\				粉	
2017-09-21 23:40:56	WORKSTATION01$	CONCANON	Password Policy modified	WORKSTATION01	WORKSTATION01\				粉	
2017-09-21 04:48:11	WORKSTATION01$	CONCANON	Password Policy modified	WORKSTATION01	WORKSTATION01\				粉	
2017-09-21 02:54:10	WORKSTATION01$	CONCANON	Password Policy modified	WORKSTATION01	WORKSTATION01\				粉	
2017-09-21 01:19:08	WORKSTATION01$	CONCANON	Password Policy modified	WORKSTATION01	WORKSTATION01\				粉	
2017-09-20 21:34:42	WORKSTATION01$	CONCANON	Lockout Policy modified	WORKSTATION01	WORKSTATION01\			-	0	
2017-09-20 21:34:42	WORKSTATION01$	CONCANON	Logoff Policy modified	WORKSTATION01	WORKSTATION01\			-	-	-
2017-09-20 21:34:42	WORKSTATION01$	CONCANON	Password Policy modified	WORKSTATION01	WORKSTATION01\				粉	
2017-09-20 01:32:14	WORKSTATION01$	CONCANON	Lockout Policy modified	WORKSTATION01	WORKSTATION01\			-	0	

EventCode=5136

A directory service object was modified

Computer Name	Type	Correlation ID	Account Name	Domain	Distinguished Name
dc01.concanon.local	Active Directory Domain Services	{015FF569-AC6F-4B3A-9AEF-591CD9A2772D}	Administrator	CONCANON	CN={79B100C1-3817-44B9-AE85-E78C62E4F227}CN=POLICIES,CN=SYSTEM,DC=CONCANON,DC=LOCAL
dc01.concanon.local	Active Directory Domain Services	{0764526B-FDEC-450F-B9FD-E4837A6856A4}	Administrator	CONCANON	CN={6AC1786C-016F-11D2-945F-00C04FB984F9}CN=POLICIES,CN=SYSTEM,DC=CONCANON,DC=LOCAL
dc01.concanon.local	Active Directory Domain Services	{0E56D930-5CC3-45B3-8BF4-39ACF4CB8A10}	Administrator	CONCANON	CN=ipsecNegotiationPolicy{d4f37a2b-03c1-4f5e-a66f-fba8c08fa071}CN=IP Security,CN=System,DC=CONCANON,DC=LOCAL
dc01.concanon.local	Active Directory Domain Services	{0F717B98-53E5-4293-A813-A8ED753D45A4}	Administrator	CONCANON	CN=WORKSTATION01,OU=CIS_2012_Servers,DC=concanon,DC=local
dc01.concanon.local	Active Directory	{0FB6838F-B85E-4BE4-9896-6EBCE1966AAE}	Administrator	CONCANON	CN={79B100C1-3817-44B9-AE85-

Computer Name	Type	Correlation ID	Account Name	Domain	Distinguished Name
dc01.concanon.local	Active Directory Domain Services	{508429FD-BA94-4024-A90C-70B931BBDCED}	adm_mgonter	CONCANON	CN={79B100C1-3817-44B9-AE85-E78C62E4F227}CN=POLICIES,CN=SYSTEM,DC=CONCANON,DC=LOCAL
dc01.concanon.local	Active Directory Domain Services	{5A0BB737-9FFE-448F-9AEC-FCBB26312CDF}	adm_mgonter	CONCANON	CN={79B100C1-3817-44B9-AE85-E78C62E4F227}CN=POLICIES,CN=SYSTEM,DC=CONCANON,DC=LOCAL
dc01.concanon.local	Active Directory Domain Services	{5C408158-53E8-4D5A-A167-9656F39F0A8D}	adm_mgonter	CONCANON	CN={79B100C1-3817-44B9-AE85-E78C62E4F227}CN=POLICIES,CN=SYSTEM,DC=CONCANON,DC=LOCAL
dc01.concanon.local	Active Directory Domain Services	{75525166-D878-478D-B92E-6CF56B1C71E6}	adm_mgonter	CONCANON	CN={79B100C1-3817-44B9-AE85-E78C62E4F227}CN=POLICIES,CN=SYSTEM,DC=CONCANON,DC=LOCAL
dc01.concanon.local	Active Directory Domain Services	{82268966-1580-4842-9812-873A99548D65}	adm_mgonter	CONCANON	CN={79B100C1-3817-44B9-AE85-E78C62E4F227}CN=POLICIES,CN=SYSTEM,DC=CONCANON,DC=LOCAL
dc01.concanon.local	Active Directory Domain Services	{DBA0DBDA-A468-4FCE-9D3A-C609694B62C5}	adm_mgonter	CONCANON	CN={79B100C1-3817-44B9-AE85-E78C62E4F227}CN=POLICIES,CN=SYSTEM,DC=CONCANON,DC=LOCAL
dc01.concanon.local	Active Directory Domain Services	{E75EC9B9-5D2E-4C48-B89D-62F12F851C4A}	adm_mgonter	CONCANON	CN={79B100C1-3817-44B9-AE85-E78C62E4F227}CN=POLICIES,CN=SYSTEM,DC=CONCANON,DC=LOCAL
dc01.concanon.local	Active Directory Domain Services	{EC0634AD-8243-4E91-9998-ED4B46E003AE}	adm_mgonter	CONCANON	CN=CIS_L1_MS,OU=CIS_2012_Servers,DC=concanon,DC=local

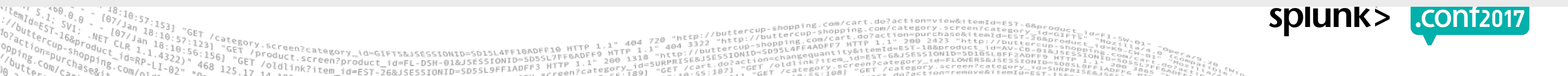
EventCode=5137,5138,5139,5141

A directory service object was created, undeleted, moved, deleted

Events | Patterns | Statistics (10) | Visualization

100 Per Page | Format | Preview

Computer Name	Type	Correlation ID	Account Name	Domain	Distinguished Name
dc01.concanon.local	Active Directory Domain Services	{0E56D930-5CC3-45B3-8BF4-39ACF4CB8A10}	Administrator	CONCANON	CN=ipsecNegotiationPolicy{d4f37a2b-03c1-4f5e-a66f-fba8c08fa071}CN=IP Security,CN=System,DC=CONCANON,DC=LOCAL
dc01.concanon.local	Active Directory Domain Services	{1D2694FF-0446-405B-9C04-2DE7633FAADA}	Administrator	CONCANON	CN=ipsecFilter{effd9d32-aeaf-4ec4-bd7d-29bd3b3d3de5}CN=IP Security,CN=System,DC=CONCANON,DC=LOCAL
dc01.concanon.local	Active Directory Domain Services	{55C3725F-DC22-49FE-9201-AF8D5853F0DF}	Administrator	CONCANON	CN=ipsecPolicy{4ee58776-1a17-4e76-9c36-ae7ea71ce148}CN=IP Security,CN=System,DC=CONCANON,DC=LOCAL
dc01.concanon.local	Active Directory Domain Services	{95B43E8F-C506-49E2-9662-AA4241527360}	Administrator	CONCANON	CN=ipsecNFA{7fa3ee30-9058-493d-917f-d22683df8102}CN=IP Security,CN=System,DC=CONCANON,DC=LOCAL
dc01.concanon.local	Active Directory Domain Services	{EECE8A8A-AAF3-4A08-B0E8-D7360443ABBC}	Administrator	CONCANON	CN=ipsecISAKMPPolicy{e2fc898b-c797-4d63-ad34-68f56389dccf}CN=IP Security,CN=System,DC=CONCANON,DC=LOCAL
dc01.concanon.local	Information	{0E56D930-5CC3-45B3-8BF4-39ACF4CB8A10}	Administrator	CONCANON	CN=ipsecNegotiationPolicy{d4f37a2b-03c1-4f5e-a66f-fba8c08fa071}CN=IP Security,CN=System,DC=CONCANON,DC=LOCAL
dc01.concanon.local	Information	{1D2694FF-0446-405B-9C04-2DE7633FAADA}	Administrator	CONCANON	CN=ipsecFilter{effd9d32-aeaf-4ec4-bd7d-29bd3b3d3de5}CN=IP Security,CN=System,DC=CONCANON,DC=LOCAL
dc01.concanon.local	Information	{55C3725F-DC22-49FE-9201-AF8D5853F0DF}	Administrator	CONCANON	CN=ipsecPolicy{4ee58776-1a17-4e76-9c36-ae7ea71ce148}CN=IP Security,CN=System,DC=CONCANON,DC=LOCAL
dc01.concanon.local	Information	{95B43E8F-C506-49E2-9662-AA4241527360}	Administrator	CONCANON	CN=ipsecNFA{7fa3ee30-9058-493d-917f-d22683df8102}CN=IP Security,CN=System,DC=CONCANON,DC=LOCAL
dc01.concanon.local	Information	{EECE8A8A-AAF3-4A08-B0E8-D7360443ABBC}	Administrator	CONCANON	CN=ipsecISAKMPPolicy{e2fc898b-c797-4d63-ad34-68f56389dccf}CN=IP Security,CN=System,DC=CONCANON,DC=LOCAL



splunk> .conf2017

EventCode=6144

Security policy in the group policy objects has been applied successfully

Events | Patterns | Statistics (21) | Visualization

100 Per Page | Format | Preview

Latest Time	Computer Name	Policy	GUID
2017-09-25 23:47:20	dc01.concanon.local	Default Domain Controllers Policy Default Domain Policy	31B2F340-016D-11D2-945F-00C04FB984F9 6AC1786C-016F-11D2-945F-00C04fB984F9
2017-09-25 11:16:05	workstation01.concanon.local	2012_L1_COMPUTER Default Domain Policy	31B2F340-016D-11D2-945F-00C04FB984F9 79B100C1-3817-44B9-AE85-E78C62E4F227
2017-09-25 07:46:57	dc01.concanon.local	Default Domain Controllers Policy Default Domain Policy	31B2F340-016D-11D2-945F-00C04FB984F9 6AC1786C-016F-11D2-945F-00C04fB984F9
2017-09-24 18:26:59	workstation01.concanon.local	2012_L1_COMPUTER Default Domain Policy	31B2F340-016D-11D2-945F-00C04FB984F9 79B100C1-3817-44B9-AE85-E78C62E4F227
2017-09-24 15:41:33	dc01.concanon.local	Default Domain Controllers Policy Default Domain Policy	31B2F340-016D-11D2-945F-00C04FB984F9 6AC1786C-016F-11D2-945F-00C04fB984F9
2017-09-24 02:02:53	workstation01.concanon.local	2012_L1_COMPUTER Default Domain Policy	31B2F340-016D-11D2-945F-00C04FB984F9 79B100C1-3817-44B9-AE85-E78C62E4F227
2017-09-23 23:36:09	dc01.concanon.local	Default Domain Controllers Policy Default Domain Policy	31B2F340-016D-11D2-945F-00C04FB984F9 6AC1786C-016F-11D2-945F-00C04fB984F9
2017-09-23 09:58:46	workstation01.concanon.local	2012_L1_COMPUTER Default Domain Policy	31B2F340-016D-11D2-945F-00C04FB984F9 79B100C1-3817-44B9-AE85-E78C62E4F227
2017-09-23 07:35:46	dc01.concanon.local	Default Domain Controllers Policy Default Domain Policy	31B2F340-016D-11D2-945F-00C04FB984F9 6AC1786C-016F-11D2-945F-00C04fB984F9
2017-09-22 17:39:40	workstation01.concanon.local	2012_L1_COMPUTER Default Domain Policy	31B2F340-016D-11D2-945F-00C04FB984F9 79B100C1-3817-44B9-AE85-E78C62E4F227
2017-09-22 15:30:22	dc01.concanon.local	Default Domain Controllers Policy	31B2F340-016D-11D2-945F-00C04FB984F9

splunk> .conf2017

source=ActiveDirectory

Events (2) | Patterns | Statistics (2) | Visualization

100 Per Page | Format | Preview

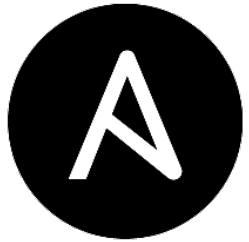
Latest Time	SAM Account Name	Changed	Created	Object GUID	Member Of
2017-09-26 00:07:20	CIS_L1_MS	00:07.20 AM, Tue 09/26/2017	09:32.38 PM, Sun 09/10/2017	4acc7336-7305-47b5-8564-70f423a0a9f6	CN=WORKSTATION01,OU=CIS_2012_Servers
2017-09-25 23:56:38	CIS_L1_MS	11:56.38 PM, Mon 09/25/2017	09:32.38 PM, Sun 09/10/2017	4acc7336-7305-47b5-8564-70f423a0a9f6	

splunk> .conf2017

Splunk Example 1

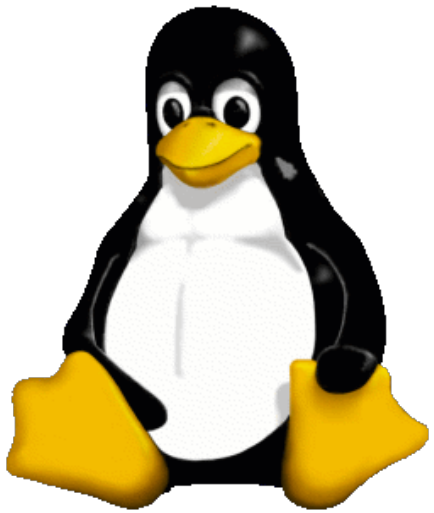
Change to Secure Configuration (Local & Domain)

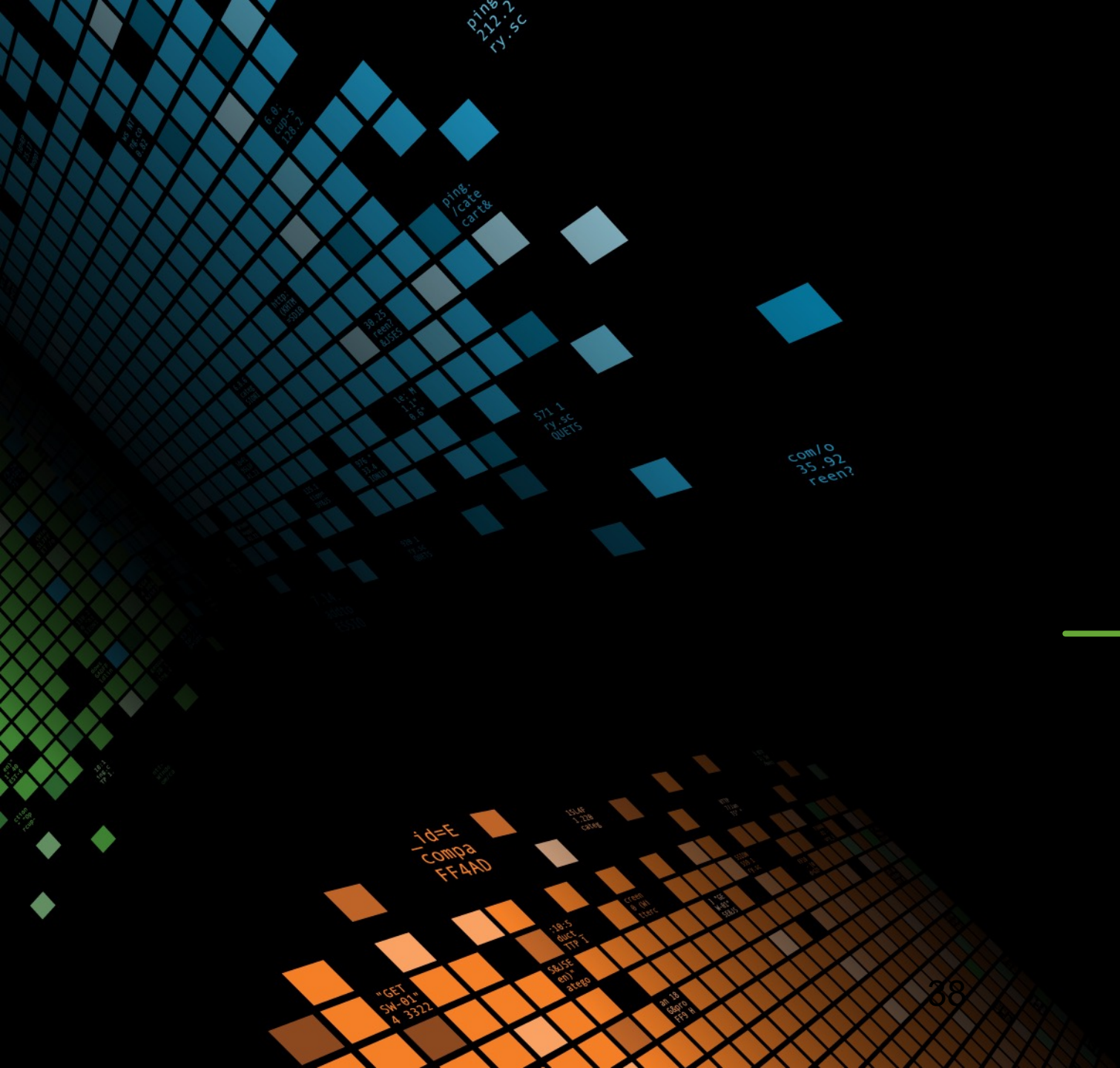
- Down the Rabbit hole we go.



ANSIBLE

NMAP





Example 2

New Port on Server

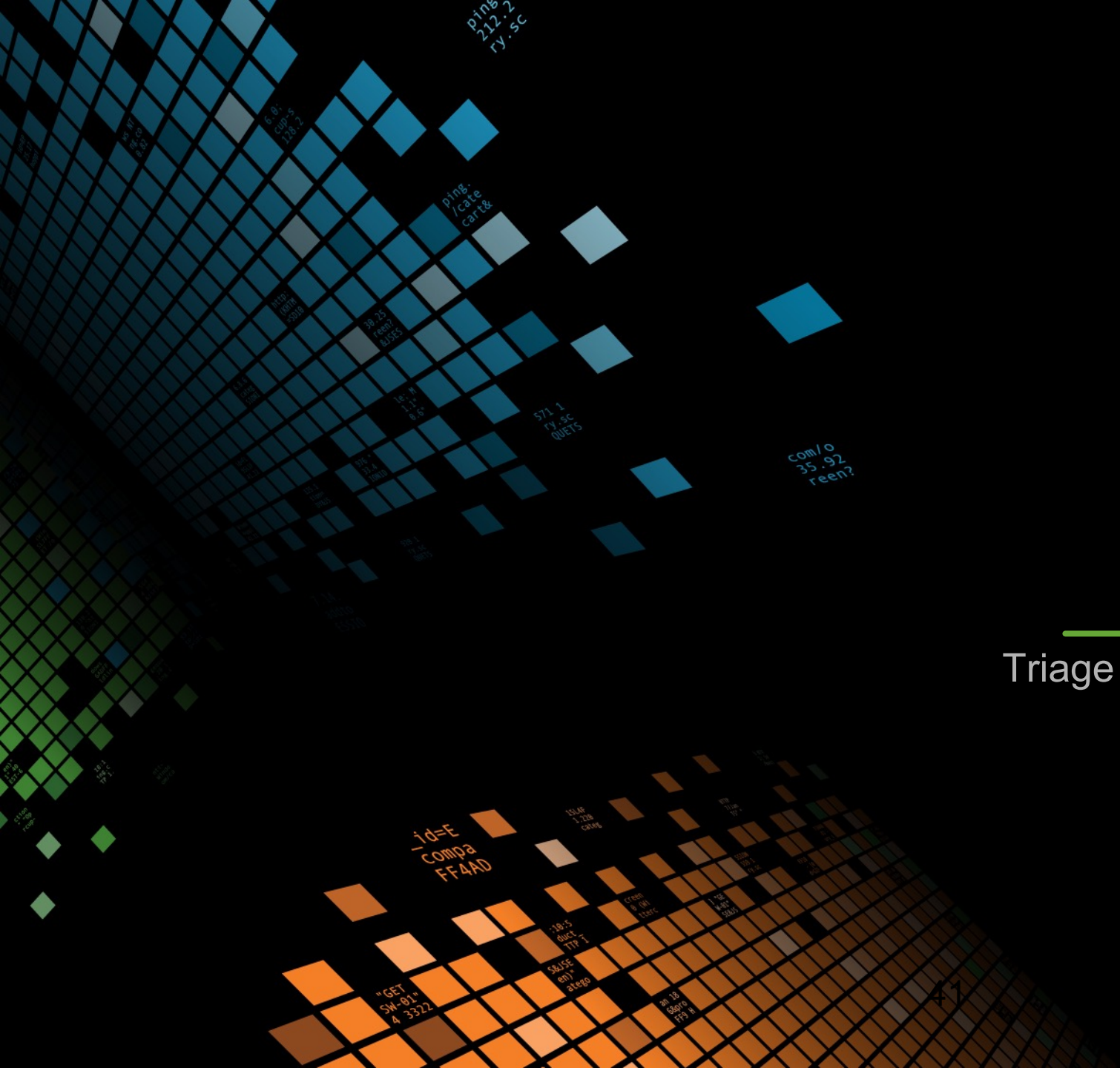
Splunk Example 2

- Detect for New Ports that are in continual use.
- Indicative of a new application or service running on the server.
- Does not detect Malicious Software. Detects for undocumented use of new ports on servers.
- Requirements
  - Inputs:
    - [monitor://C:\System32\LogFiles\Firewall]
  - Need to Track Ports that are typically used per host
  - Need a baseline to compare against.

Splunk Example 2

- Create Baseline
  - index=windows sourcetype="WinEventLog:firewall" NOT (src_ip=127.0.0.1 OR dest_port="-")
    | stats count min(_time) as baseTime max(_time) as lastTime by dest_port host
    | where count> 10
    | inputlookup append=true listeningports_tracker
    | eval dest=if(isnull(dest), host, dest)
    | fields – host
    | dedup dest_port
    | outputlookup listeningports_tracker

- Correlation Search
  - index=windows sourcetype="WinEventLog:firewall" NOT (src_ip=127.0.0.1 OR dest_port="-")
    | stats count max(_time) as lastTime values(dest) as dest by dest_port host
    | lookup listeningports_tracker.csv dest as host dest_port
    | eval dest=if(isnull(dest), host, dest)
    | where isnull(baseTime) AND isnotnull(dest_port)



Example 3

Triage Security Settings of Host in Incident

Splunk Example

- Displays local security policy of host to standardized security benchmarks

- Requirements
  - Scripted Inputs:
    - gpresult /USER concanon\adm_mgonter /R /Z /SCOPE Computer

      - /USER [domain\]user Specifics the User Context
      - /R Display RSoP data
      - /Z Super Verbose (Can be substituted for /V)
      - /SCOPE [USER | COMPUTER] Specifies the user or computer settings to display.

- XML Version of the GPResults.
- Regular Version.

- Why LINE_BREAKING is so important here.

```
        </q4:Policy>
        <q4:Policy>
          <GPO xmlns="http://www.microsoft.com/GroupPolicy/Settings/Base">
            <Identifier
xmlns="http://www.microsoft.com/GroupPolicy/Types">{79B100C1-3817-44B9-AE85-E78C62E4F227}<
/Identifier>
            <Domain
xmlns="http://www.microsoft.com/GroupPolicy/Types">concanon.local</Domain>
          </GPO>
          <Precedence
xmlns="http://www.microsoft.com/GroupPolicy/Settings/Base">1</Precedence>
          <q4:Name>Hardened UNC Paths</q4:Name>
          <q4:State>Enabled</q4:State>
          <q4:Explain>This policy setting configures secure access to UNC paths.

If you enable this policy, Windows only allows access to the specified UNC paths after
fulfilling additional security requirements.
</q4:Explain>
          <q4:Supported>At least Windows Vista</q4:Supported>
          <q4:Category>Network/Network Provider</q4:Category>
          <q4:Text>
            <q4:Name>Specify hardened network paths.
In the name field, type a fully-qualified UNC path for each network resource.
To secure all access to a share with a particular name, regardless of the server name,
specify a server name of '*' (asterisk). For example, "\\*\NETLOGON".
To secure all access to all shares hosted on a server, the share name portion of the UNC
path may be omitted. For example, "\\SERVER".

In the value field, specify one or more of the following options, separated by commas:
    'RequireMutualAuthentication=1': Mutual authentication between the client and server
is required to ensure the client connects to the correct server.
    'RequireIntegrity=1': Communication between the client and server must employ an
integrity mechanism to prevent data tampering.
    'RequirePrivacy=1': Communication between the client and the server must be encrypted
to prevent third parties from observing sensitive data.</q4:Name>
          </q4:Text>
          <q4:ListBox>
            <q4:Name>Hardened UNC Paths:</q4:Name>
            <q4:State>Enabled</q4:State>
            <q4:ExplicitValue>true</q4:ExplicitValue>
            <q4:Additive>true</q4:Additive>
            <q4:Value>
```

- XML Version of the GPResults.
- Regular Version.

- Why LINE_BREAKING is so important here.

```
Account Policies
----------------
    GPO: Default Domain Policy
        Policy:             MaximumPasswordAge
        Computer Setting:   42
    GPO: Default Domain Policy
        Policy:             LockoutBadCount
        Computer Setting:   N/A
    GPO: 2012_L1_COMPUTER
        Policy:             LockoutDuration
        Computer Setting:   15
    GPO: Default Domain Policy
        Policy:             MinimumPasswordAge
        Computer Setting:   1
    GPO: 2012_L1_COMPUTER
        Policy:             MaximumPasswordAge
        Computer Setting:   60
    GPO: 2012_L1_COMPUTER
        Policy:             MinimumPasswordAge
        Computer Setting:   1
    GPO: Default Domain Policy
        Policy:             MinimumPasswordLength
        Computer Setting:   7
    GPO: 2012_L1_COMPUTER
        Policy:             ResetLockoutCount
        Computer Setting:   15
    GPO: Default Domain Policy
        Policy:             PasswordHistorySize
        Computer Setting:   24
    GPO: 2012_L1_COMPUTER
        Policy:             LockoutBadCount
        Computer Setting:   10
    GPO: 2012_L1_COMPUTER
        Policy:             PasswordHistorySize
        Computer Setting:   24
    GPO: 2012_L1_COMPUTER
        Policy:             MinimumPasswordLength
        Computer Setting:   14
```

Splunk Example 3

- LINE_BREAKER = (\s+)GPO\:
- LOTS OF EXTRACTS

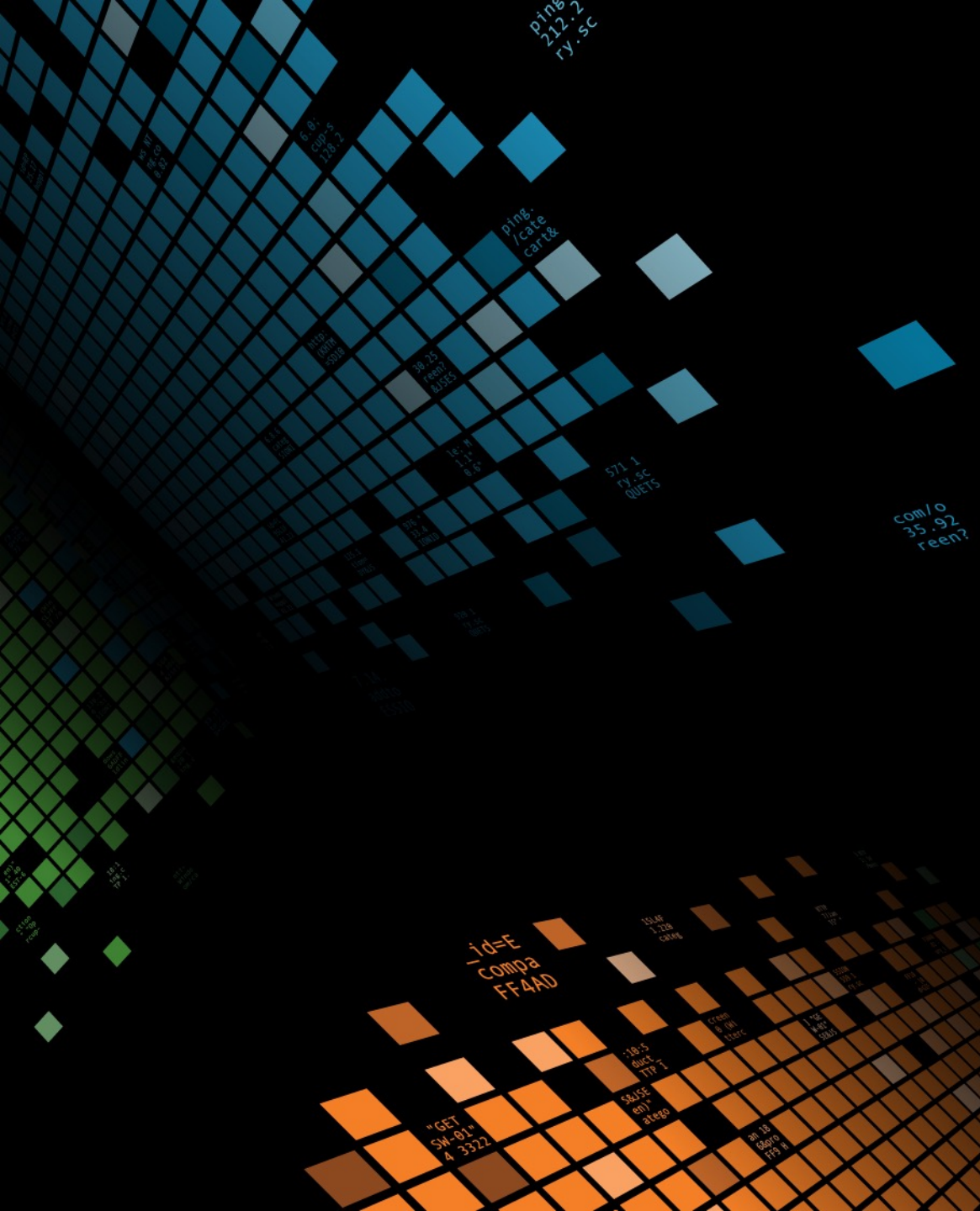
- Dashboard Search
  - index=main host="win-1743nenjft4" sourcetype=script:csc3
    | rex "GPO\:\s+(?<gpo>[^\r\n]+)" | rex "Policy:\s+(?<policy>[^\r\n]+)" | rex "ValueName\:\s+.+\\\(?<policy>\S+)" | rex "Computer\sSetting\:\s+(?<setting>[\r\n\S\s]+)" | rex field=setting max_match=0 "(?<setting>[^\r\n]+)"
    | mvexpand setting
    | search gpo=2012_L1_COMPUTER
    | stats count by setting host,gpo,policy
    | lookup host_base_config_lookup base_policy as policy host gpo
    | stats values(base_setting) as base_setting by gpo policy setting
    | eval compare=if(setting=base_setting, "1", "0")

Comparison Table

GPO For WIN-1743NENJFT4

gpo	policy	setting	base_setting	compare
2012_L1_COMPUTER	AuditAccountLogon	Success, Failure	Success, Failure	1
2012_L1_COMPUTER	AuditAccountManage	Success, Failure	Success, Failure	1
2012_L1_COMPUTER	AuditDSAccess	Success, Failure	Success, Failure	1
2012_L1_COMPUTER	AuditLogonEvents	Success, Failure	Success, Failure	1
2012_L1_COMPUTER	AuditObjectAccess	Success, Failure	Success, Failure	1
2012_L1_COMPUTER	AuditPolicyChange	Success, Failure	Success, Failure	1
2012_L1_COMPUTER	AuditPrivilegeUse	Success, Failure	Success, Failure	1
2012_L1_COMPUTER	AuditProcessTracking	Success, Failure	Success, Failure	1
2012_L1_COMPUTER	ClearTextPassword	Not Enabled	Not Enabled	1
2012_L1_COMPUTER	EnableAdminAccount	Not Enabled	Not Enabled	1
2012_L1_COMPUTER	EnableGuestAccount	Not Enabled	Not Enabled	1
2012_L1_COMPUTER	LSAAnonymousNameLookup	Not Enabled	Not Enabled	1
2012_L1_COMPUTER	PasswordComplexity	Not Enabled	Not Enabled	1

splunk> .conf2017



This is the end, my only friend, the end

splunk> .conf2017

Critical Security Control #3 Implementation Summary

- Example Requirements:
  - Baseline of Active Ports on a Server
  - Input that detects new ports being activated.
  - Windows Security Logs
  - Correlation Search
- Remediation
  - Determine cause of new port

Questions

Bueller? Bueller? Bueller?