Splunk Like Your Life Depends on it

Katie Brown
Senior Solutions Engineer | Splunk

splunk> .conf19

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans 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 may differ materially. 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, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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 functionalities described or to include any such feature or functionality in a future release.

- Soluti
- Custom
- Manage
- SOC Ar
- Blue T
- GOT, v

Agenda

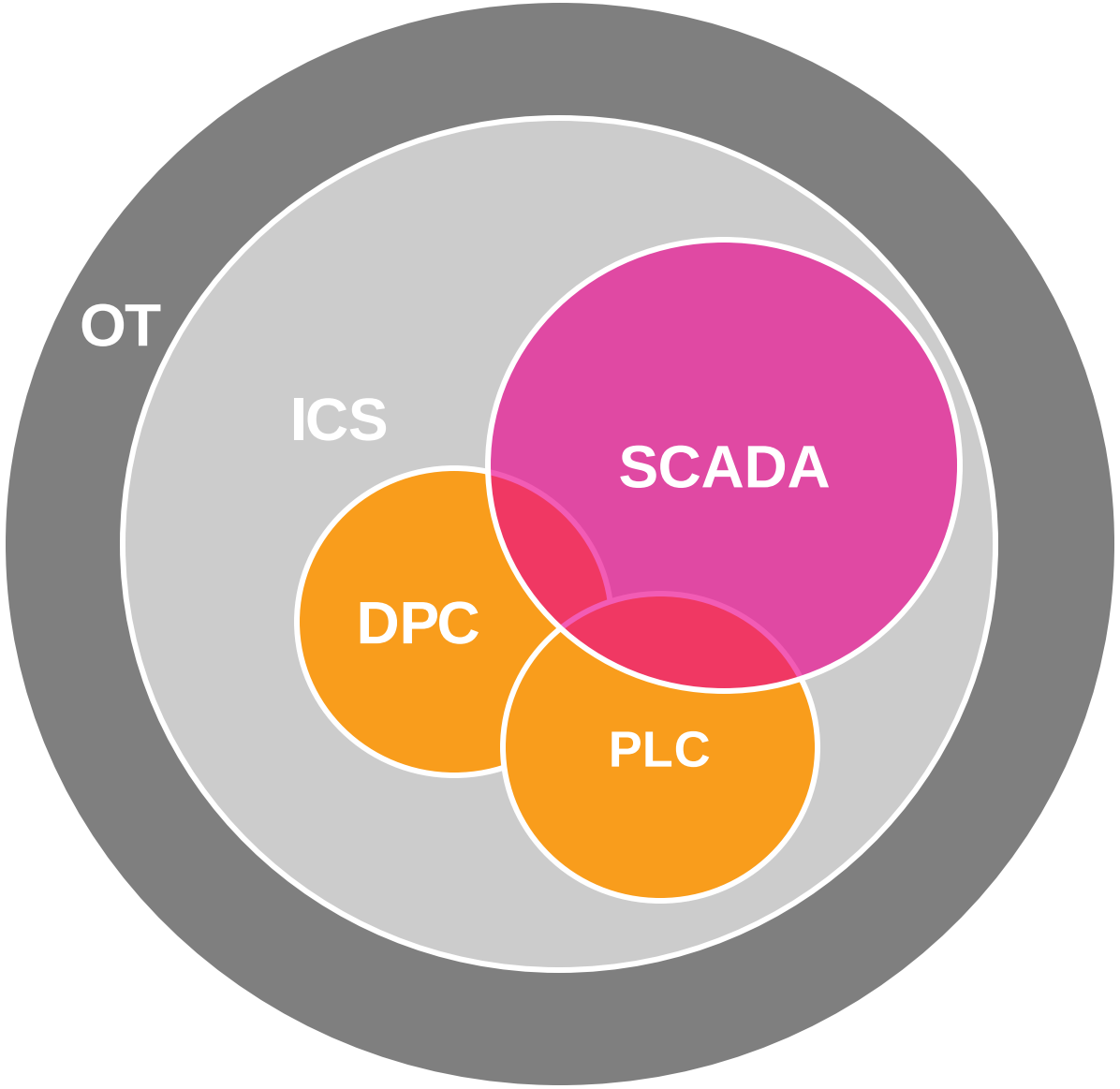
Or so I hope…

1. OT Terminology
2. Security in the ICS Realm
3. A look into ICS specific malware
4. Malware commonalities
5. Detecting with Splunk
6. Customer success story

OT > ICS > SCADA

Let's get our terminology straight!

- OT – management of industrial operations vs administrative
- ICS – systems used to monitor/control processes



It's natural to think in traditional terms:

a hacker sitting at a computer keyboard trying to worm his way into a web server

If it's so important …why isn't everyone doing it?

1. Lack of visibility
2. Reliance on insecure communication processes & outdated protocols
3. Slow/delayed/NO patch management
4. Limited OT security products

A look at ICS malware…

splunk> turn data into doing™

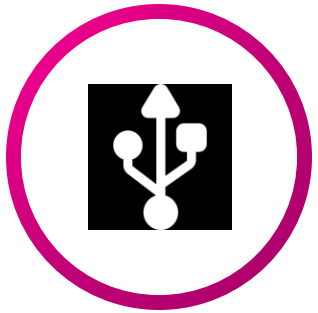
ICS SPECIFIC MALWARE

A look at past incidents

- STUXNET
- BLACK ENERGY
- INDUSTROYER
- HAVEX
- TRISIS

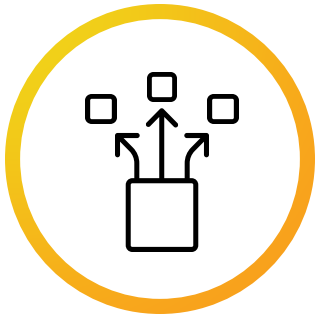
Malware Commonalities

Removable Media

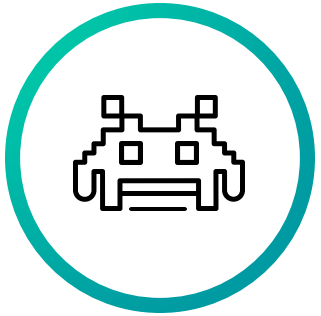


Password Spraying

C2

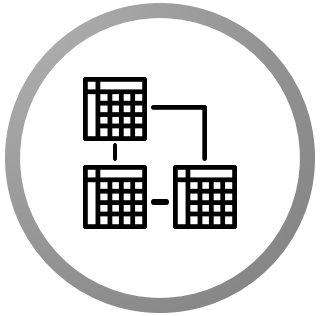


Process start Anomalies



Firmware Changes

Lateral movement



Detection Capabilities with Splunk

splunk> turn data into doing™

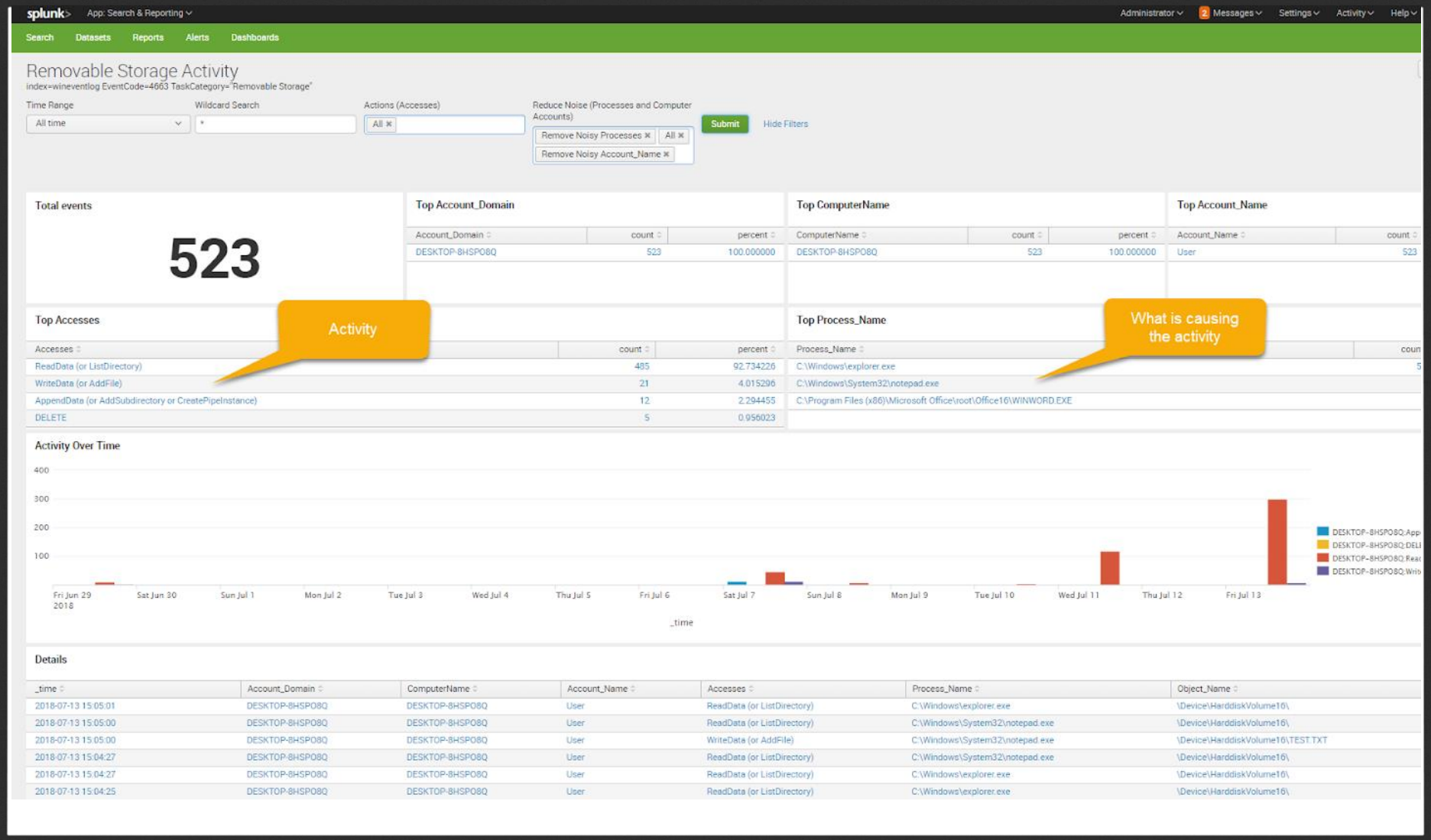
Detection with Splunk: Removable Media

1) Configure your audit policy

2) ….Splunk it!


```
index=wineventlog EventCode=2003 USBSTOR
```

```
index=wineventlog EventCode=2102 USBSTOR
```



Detection with Splunk: Password Spraying

- index=win_sec EventCode=4625 AND NOT [|inputlookup DomainControllers.csv]
- | bin _time span=1d
- | stats values(user) dc(user) AS num_users count span=1d BY dest _time
- | search count>15 AND num_users>1

Detection with Splunk: C2 Activity

- sourcetype=bluecoat_proxy
- | streamstats current=f last(_time) as next_time by dest
- | eval gap = next_time - _time
- | stats count avg(gap) as avg_gap, var(gap) as var_gap by dest src
- | search avg_gap<50 count>500
- | sort avg_gap

New Search

Save As | New Table | Close

```
1 sourcetype=bluecoat_proxy
2 | streamstats current=f last(_time) as next_time by dest
3 | eval gap = next_time - _time
4 | stats count, avg(gap) as avg_gap, var(gap) as var_gap by dest src
5 | search avg_gap<50 count>500
6 | sort avg_gap
```

All time

✓ 84,089 events (before 2/7/17 4:20:58.000 AM) No Event Sampling

Job | Verbose Mode

Events (84,089) | Statistics (11) | Visualization

20 Per Page | Format | Preview

dest	src	count	avg_gap	var_gap
www.yourfavoritzshop.cn	10.1.21.153	4133	14.298331	208.84926
www.yourfavoritzshop.cn	10.19.240.12	1288	14.564880	204.165111
www.yourfavoritzshop.cn	10.44.13.33	527	16.204934	231.007352
mail.google.com	10.13.223.31	546	16.355311	223.572605
bpmsupplychain.acmetech.com	173.69.12.16	2716	31.786372	988.204162
i.cdn.turner.com	10.9.131.94	2641	32.725379	1111.904471
freezegame.dynadnssvc.net	157.235.78.193	2450	35.257248	1309.615169
boostifun.cellmania.com	10.180.6.76	1001	36.350000	1245.673173
boostifun.cellmania.com	10.180.6.74	558	37.849462	1370.681068
media.cnbc.com	10.52.1.6	2052	42.111165	1778.760319
office.microsoft.com	10.44.13.222	1833	47.120633	2034.290737

Detection with Splunk: Process Start Anomalies

New Search

Save As Close

```
sourcetype=xmlwineventlog:microsoft-windows-sysmon/operational EventCode=1
| eval cmdlen = len (CommandLine)
| eventstats avg(cmdlen) as avg, stdev(cmdlen) as stdev by host
| stats max(cmdlen) as maxlen, values(avg) as avgperhost, values(stdev) as stdevperhost by host, CommandLine
```

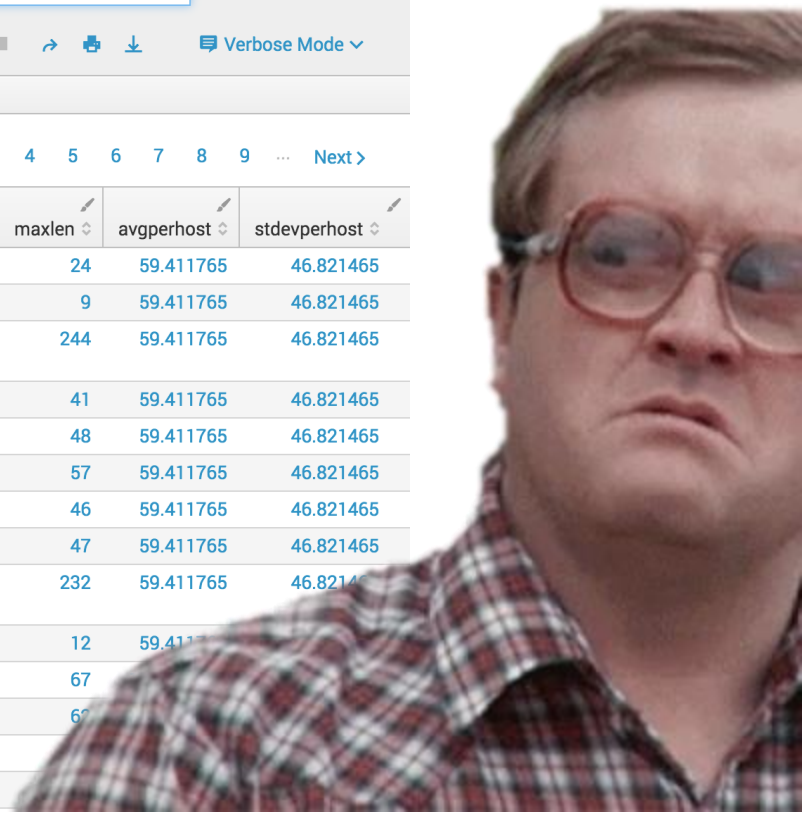
All time

379 events (before 12/11/16 12:39:10.000 AM) No Event Sampling Job Verbose Mode

Events (379) Patterns Statistics (227) Visualization

20 Per Page Format Preview Prev 1 2 3 4 5 6 7 8 9 ... Next

host	CommandLine	maxlen	avgperhost	stdevperhost
we1149srv	"LogonUI.exe" /flags:0x0	24	59.411765	46.821465
we1149srv	"dwm.exe"	9	59.411765	46.821465
we1149srv	%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16	244	59.411765	46.821465
we1149srv	C:\Windows\system32\sc.exe start wuauserv	41	59.411765	46.821465
we1149srv	C:\Windows\system32\wbem\wmiprvse.exe -Embedding	48	59.411765	46.821465
we1149srv	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	57	59.411765	46.821465
we1149srv	\??\C:\Windows\system32\conhost.exe 0xffffffff	46	59.411765	46.821465
we1149srv	\SystemRoot\System32\smss.exe 00000000 00000050	47	59.411765	46.821465
we1149srv	c:\windows\system32\inetsrv\w3wp.exe -ap "DefaultAppPool" -v "v4.0" -l "webengine4.dll" -a \\.\pipe\iisipm45a13fae-8ca5-408b-a9e4-631fc0631086 -h "C:\inetpub\temp\apppools\DefaultAppPool\DefaultAppPool.config" -w "" -m 0 -t 20 -ta 0	232	59.411765	46.821
we1149srv	winlogon.exe	12	59.41	
we8105desk	"C:\Program Files (x86)\Acronis\TrueImageHome\TrueImageMonitor.exe"	67		
we8105desk	"C:\Program Files (x86)\Common Files\Acronis\CDP\afcdpsrv.exe"	6		
we8105desk	"C:\Program Files (x86)\Common Files\Acronis\Infrastructure\mms_mini.exe"			
we8105desk	"C:\Program Files (x86)\Common Files\Acronis\Schedule2\schedhlp.exe"			



New Search

Save As Close

```
sourcetype=xmlwineventlog:microsoft-windows-sysmon/operational EventCode=1
| eval cmdlen = len (CommandLine)
| eventstats avg(cmdlen) as avg, stdev(cmdlen) as stdev by host
| stats max(cmdlen) as maxlen, values(avg) as avgperhost, values(stdev) as stdevperhost by host, CommandLine
| eval threshold = 4 * ( stdevperhost + avgperhost )
| where maxlen > threshold
```

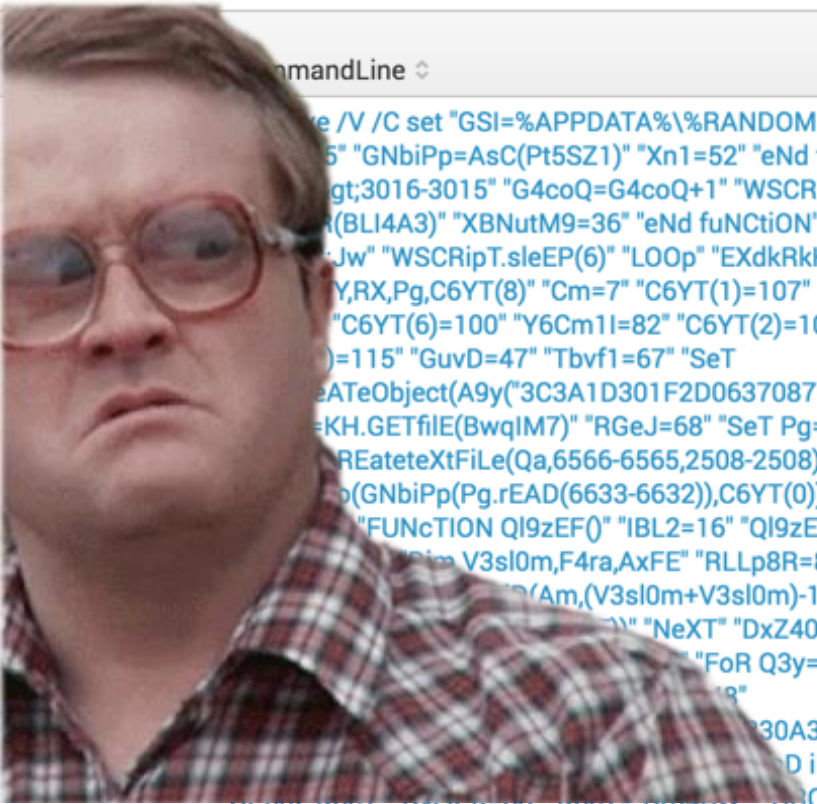
All time

✓ 379 events (before 12/11/16 12:40:57.000 AM) No Event Sampling

Job Verbose Mode

Events (379) Patterns Statistics (1) Visualization

20 Per Page Format Preview



mandLine	maxlen	avgperhost	stdevperhost	threshold
e /V /C set "GSI=%APPDATA%\%RANDOM%.vbs" && (for %i in ("DIm RWRL" "FuNCtioN GNbiPp(Pt5SZ1)" 5" "GNbiPp=AsC(Pt5SZ1)" "Xn1=52" "eNd fuNCtiON" "SUb OjrYyD9()" "J0Nepq=56" "Dim UJv,G4coQ" "LT=23" "dO WHiLE gt;3016-3015" "G4coQ=G4coQ+1" "WSCRiPt.sLEeP(11)" "LoOP" "UsZK0=85" "ENd suB" "fuNctIon J7(BLI4A3)" "K5AU=29" (BLI4A3)" "XBNutM9=36" "eNd fuNCtiON" "SUb MA(QrG)" "WXCzRz=9" "Dim Jw" "Qt7=34" "Jw=TIMeR+QrG" "Do WhiLE Jw" "WSCRipT.sleEP(6)" "LOOp" "EXdkRkH=78" "enD sUB" "fUnCTion M1p67jL(BwqIM7,Qa)" "Yi=80" "dIM Y,RX,Pg,C6YT(8)" "Cm=7" "C6YT(1)=107" "Rzf=58" "C6YT(5)=115" "BSKoW=10" "C6YT(4)=56" "Cwd6=35" "C6YT(7)=110" "C6YT(6)=100" "Y6Cm1I=82" "C6YT(2)=103" "JH3F2i=74" "C6YT(8)=119" "JRvsG2s=76" "C6YT(3)=53" "Yh=31")=115" "GuvD=47" "Tbvf1=67" "SeT eATeObject(A9y("3C3A1D301F2D063708772930033C3C201C2D0A34203B053C0C2D", "Yo"))" "V2JR=73" "Set KH.GETfilE(BwqIM7)" "RGeJ=68" "SeT Pg=ChnFY.opEnASTExTstReAM(6806-6805,7273-7273)" "CtxOk=82" "seT REateteXtFiLe(Qa,6566-6565,2508-2508)" "XPL9af=76" "Do uNtil Pg.aTEnDOfStReam" "RX.wRitE (GNbiPp(Pg.rEAD(6633-6632)),C6YT(0)))" "LooP" "IQz=49" "RX.cloSe" "CBR1gC7=51" "Pg.cLOSE" "PmG=64" "eNd "FUNcTION Ql9zEF()" "IBL2=16" "Ql9zEF=secoND(Time)" "MUTkPNJ=41" "End FUNcTiOn" "FUnCtion A9y(Am,T1GCbB)" V3sl0m,F4ra,AxFE" "RLLp8R=89" "For V3sl0m=1 To (lEn(Am)/2)" "F4ra=(J7((8270-8232)) & (Am,(V3sl0m+V3sl0m)-1,2)))" "AxFE=(GNbiPp(mID(T1GCbB,((V3sl0m MOd Len(T1GCbB))+1),1)))")" "NeXT" "DxZ40=89" "enD fUNction" "Sub AylniN()" "N6nzb=92" "DIm GWJCk,Q3y,GKasG0" "FoR Q3y=1 To GWJCk" "GKasG0=GKasG0+1" "neXt" "B1jq2Hk=63" "If GKasG0=GWJCk 30A3B0C503D31230C3700593135344D201B53772C39173D475E2826","QcOi4XA"))" D iF" "XyUP=64" "eND SuB" "sUB GKfD3aY(FaddNPJ)" "SDU0BLq=57" "DiM Olc7=82" "sET	4490	101.498361	266.247475	1470.98334

Detection with Splunk: Lateral Movement

SMB

- | search (dest_port=139 OR dest_port=445)
- bucket _time span=1d
- | stats dc(dest_ip) as count by src_ip, _time
- | eventstats max(_time) as maxtime | stats count as num_data_samples max(eval(if(_time >= relative_time(maxtime, "-1d@d"), 'count',null))) as "count" avg(eval(if(_time<relative_time(maxtime,"-1d@d"),'count',null))) as avg stdev(eval(if(_time<relative_time(maxtime,"-1d@d"),'count',null))) as stdev by "src_ip”
- | eval isOutlier=if(('count' < lowerBound OR 'count' > upperBound) AND num_data_samples >=7, 1, 0)

New Search

Save As ▾ Close

```
| inputlookup UC_smb_spike_detection
| search (dest_port=139 OR dest_port=445)
| bucket _time span=1d
| stats dc(dest_ip) as count by src_ip, _time | eventstats max(_time) as maxtime | stats count as num_data_samples max(eval(if(_time >= relative_time(maxtime, "-1d@d"), 'count',null))) as "count" avg(eval(if(_time
   <relative_time(maxtime,"-1d@d"),'count',null))) as avg stdev(eval(if(_time<relative_time(maxtime,"-1d@d"),'count',null))) as stdev by "src_ip" | eval lowerBound=(avg-stdev*2), upperBound=(avg+stdev*2) | eval
   isOutlier=if(('count' < lowerBound OR 'count' > upperBound) AND num_data_samples >=7, 1, 0) | table "src_ip", num_data_samples, "count",  avg, lowerBound, upperBound, isOutlier
```

All time ▾

✓ 4 results (1/1/70 12:00:00.000 AM to 8/12/19 1:09:29.000 AM) No Event Sampling ▾ Job ▾ Smart Mode ▾

Events Patterns **Statistics (4)** Visualization

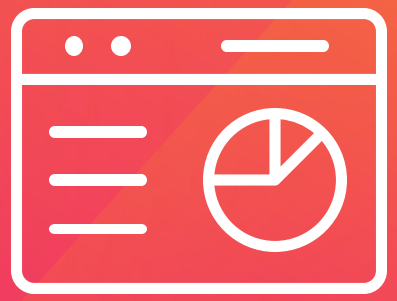
20 Per Page ▾ Format Preview ▾

src_ip	num_data_samples	count	avg	lowerBound	upperBound	isOutlier
10.83.84.205	5	9	5.75	-0.6531242374328485	12.153124237432849	0
10.83.84.244	9	9	6.875	-0.0066526254340137925	13.756652625434015	0
10.84.42.134	31	58	2.1724137931034484	0.855603196326808	3.4892243898800888	1
10.84.42.231	5	29	1.25	0.25	2.25	0

splunk> .conf19

btdubz, there's an APP for that

ICS Security Essentials App



splunk> turn data into doing™

Introduction

Export ▾ ...

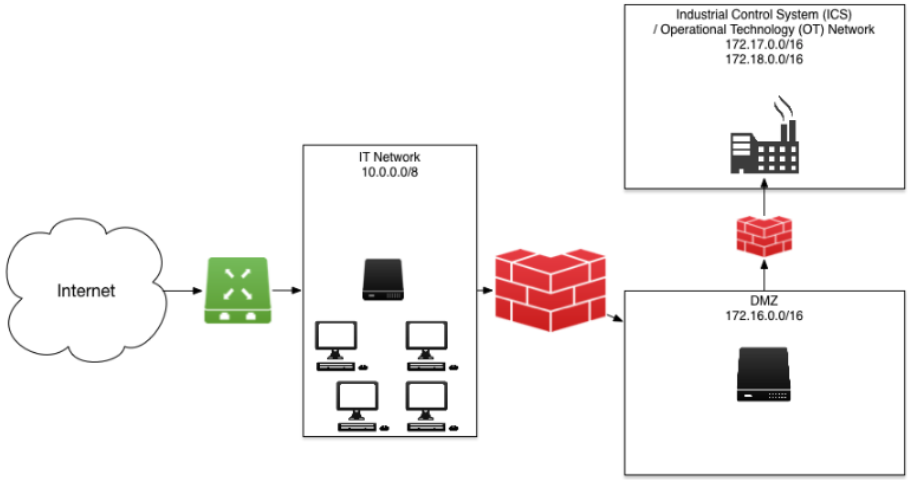
Introduction

Welcome to the Splunk Essentials for ICS Security and Compliance. This app provides **13** different use cases designed to help you gain a clearer understanding of the impact of security incidents on Industrial Control Systems (ICS) and how you can use Splunk to see and respond to real-world threats immediately.

ICS are often tasked with monitoring and managing highly sensitive processes associated with manufacturing and industrial environments. ICS technologies include systems, such as supervisory control and data acquisition (SCADA), distributed control systems (DCS), and programmable logic controllers (PLC). These devices constitute the operational technology (OT) network.

Unlike traditional IT networks that are designed to secure and exchange information, OT networks are primarily used for monitoring and controlling how physical devices perform in critical infrastructure. As these systems increasingly connect to IT networks to achieve process optimization and cost savings leveraging real time online data, they become targets for cybercriminals looking to cause havoc. In this app, we help you understand the common vulnerabilities in ICS devices, and demonstrate the ability to implement an ICS security use case using Splunk detection capabilities. Each use case can be implemented as a stand-alone or in conjunction with others. The use cases are mapped into six steps of ICS security maturity.

We provide a network diagram below to help you understand and visualize the use case concepts in an interconnected OT and IT environment.



Boundary Protection

Featuring 5 Examples!

When ICS and corporate IT networks are connected, cybercriminals will look patiently for flaws in architecture design and exploit them.

Access Control

Featuring 3 Examples!

Without a formalized review and validation of logs, unauthorized users, applications, and unauthorized events, hackers could operate

Monitoring

Featuring 3 Examples!

Lack of monitoring could allow unauthorized physical access to field equipment and locations. This increases the opportunity for cybercriminals

Step 5: Authorize Information System

Handle the authorization properly

Detect access during after-hours

Alerts suspicious login activities such as authentication during unusual hours.

Searches Included

Firewall | Syslog | Windows

Detect configuration changes in Routers/Switches

Network devices such as routers and switches on the ICS network serve as the first line of defense by permitting or denying communications between the ICS network and the corporate network. This search looks for changes in routing policies governing permitted communication.

Detect policy changes in the firewall

Properly configured firewalls can be used to protect control systems from unauthorized access, but rule sets need to be monitored and reviewed to provide continuous, adequate protection. This search looks for changes in the firewall configuration rulesets.

Searches Included

Detect successful access to OT network from IT network

Detect all connections initiated and allowed from the corporate IT network to the ICS network.

Searches Included

Firewall | Syslog

Detect successful user authentications to OT from IT network

Detect both successful and unsuccessful authentication attempts to the ICS network from systems or users in the corporate IT network.

Searches Included

Syslog

Detect unknown new device activity

Detect new equipment or device in the ICS network to understand its role and impact on the entire environment.

Searches Included

Network Traffic | Syslog | Firewall | Proxy | Windows

Step 6: Monitor Security Controls

It is all good, now you want to make sure you have proper alerts etc.

Detect File Transfers from OT to IT networks

Monitor all file transfers as well as the protocol used for transferring the file.

Searches Included

Monitor endpoints with outdated protection definitions

Sometimes endpoint protection may fail to update the signature files due to bandwidth limitations, and equipment or other system issues. This search identifies the

Monitor endpoints without protection software

Detect systems that don't have endpoint protection installed or running an unsupported version, as the connections of the systems to the ICS network creates attack

ICS Security Use Cases / Detect File Transfers from OT to IT networks

Export ...

Assistant: Simple Search

Description

Monitor all file transfers as well as the protocol used for transferring the file.

Learn how to use this page | View Demo Data

Use Case

Boundary Protection

Category

Monitor Security Control

Security Impact

Protocols such as FTP, HTTP and NFS are not secure by design. Files are stored unencrypted, allowing hackers to easily intercept and read the data as it traverses the network. Sensitive data belonging to both the OT and IT networks must only be accessible to users with appropriate access rights.

Alert Volume

Medium (?)

SPL Difficulty

Easy

Stage 6

Data Sources

Firewall

> Known False Positives

> How To Respond

> Show Search

> Help

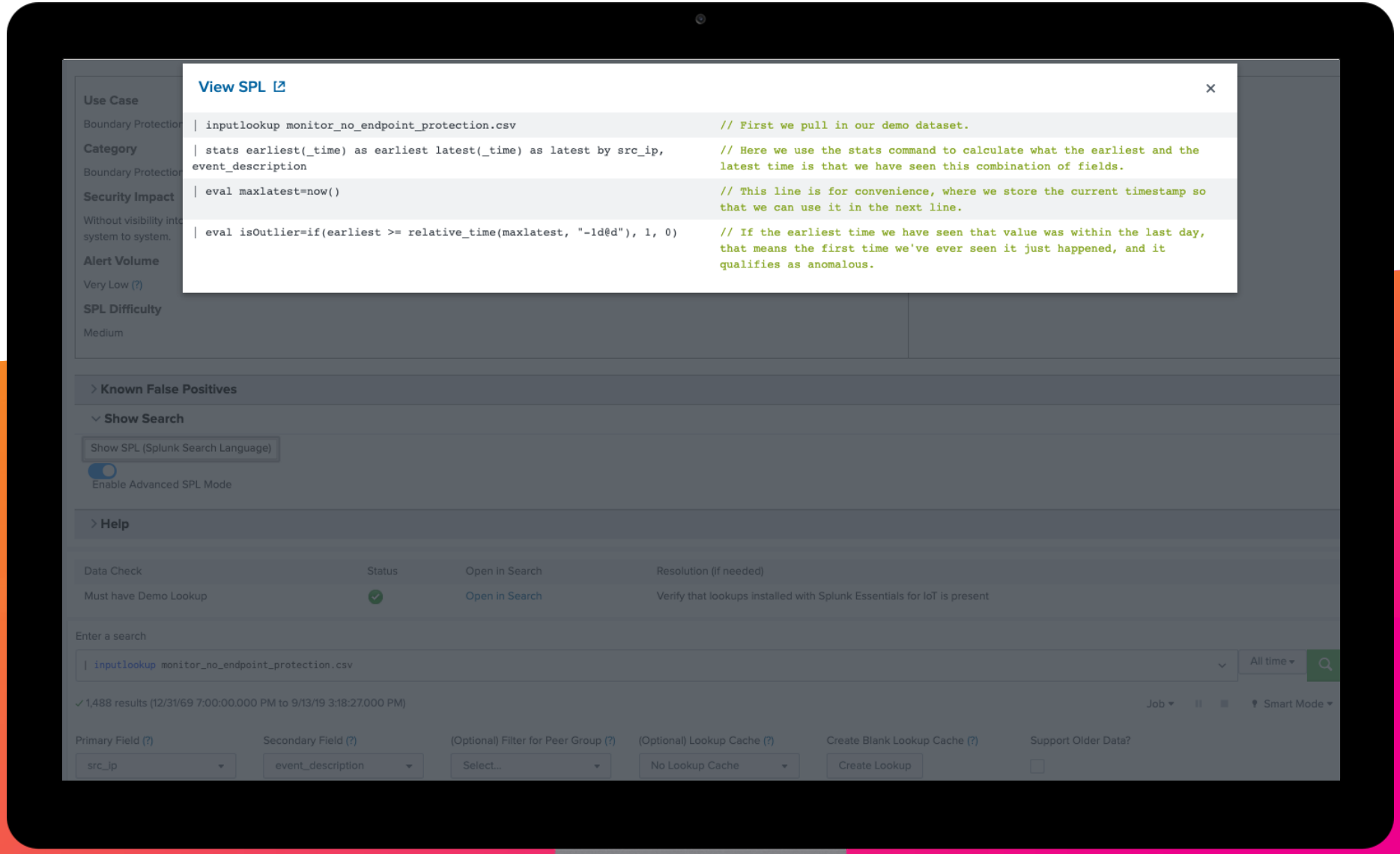
Data Check	Status	Open in Search	Resolution (if needed)
Must have Demo Lookup	✓	Open in Search	Verify that lookups installed with Splunk Security Essentials is present

Enter a search

```
| inputlookup dmz_to_ics.csv
| eval dest_net_type=if(cidrmatch("10.0.0.0/8", dest_ip) OR cidrmatch("172.16.0.0/16", dest_ip), "IT", "OT")
| eval src_net_type=if(cidrmatch("10.0.0.0/8", src_ip) OR cidrmatch("172.16.0.0/16", src_ip), "IT", "OT")
| search src_net_type=OT AND dest_net_type=IT AND file_name="*"
```

All time

splunk> .conf19



Customer Success Story

Splunk at an Energy Company

splunk> turn data into doing™

Energy Company

Supporting SCADA Systems to Secure Pipeline

"We discovered that we could accomplish the same tasks as four different applications with a single instance of Splunk Enterprise. The TCO of Splunk is approximately 400 percent less. We are very pleased with our investment and the capabilities of Splunk software."

company's supervisor of SCADA infrastructure and cybersecurity

- **1 solution instead of 4+**
- **Improved visibility, reliability**
- **Cut security investigation time from 12 hours to 1**
- **TCO reduced by 400%**

splunk> .conf19

Key Takeaways

1. Importance of OT Security
2. Common ICS malware TTPs
3. How to Detect with Splunk Enterprise
4. ….btw we have an app for that!
   - https://splunkbase.splunk.com/app/4150/
5. People use Splunk and stuff….

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION