From Risk to Intelligence – How Real-Time Visibility and Automation Using Splunk Helps Rationalize and Mitigate ICS Threats

Sebastien Tricaud, stricaud@splunk.com
Principal Solutions Architect

Chris Duffey, cduffey@splunk.com
Senior IoT Practitioner

October 2018 | Version 0.0.7

Forward-Looking Statements

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 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.

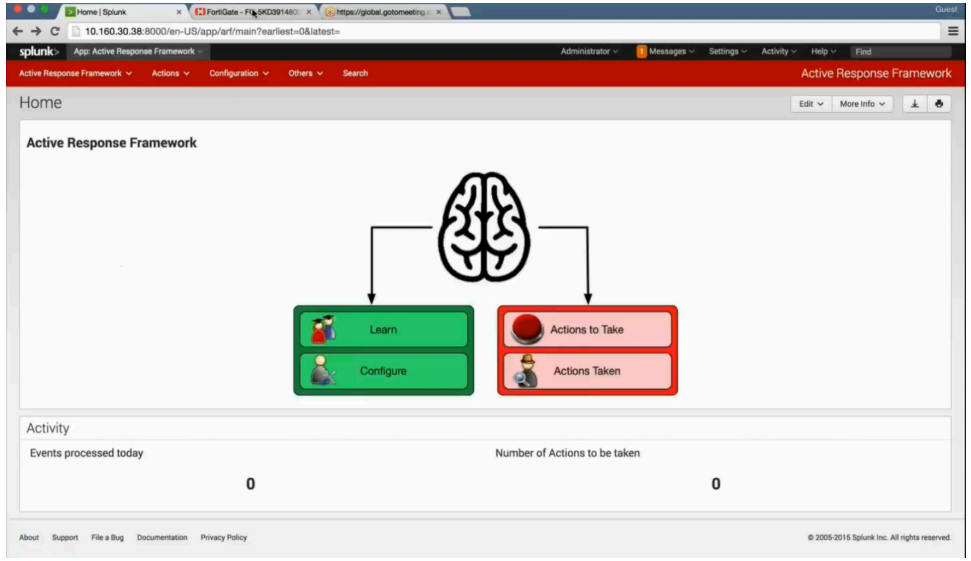
splunk> .conf18

About Me

Sebastien Tricaud / Principal Solutions Architect @splunk

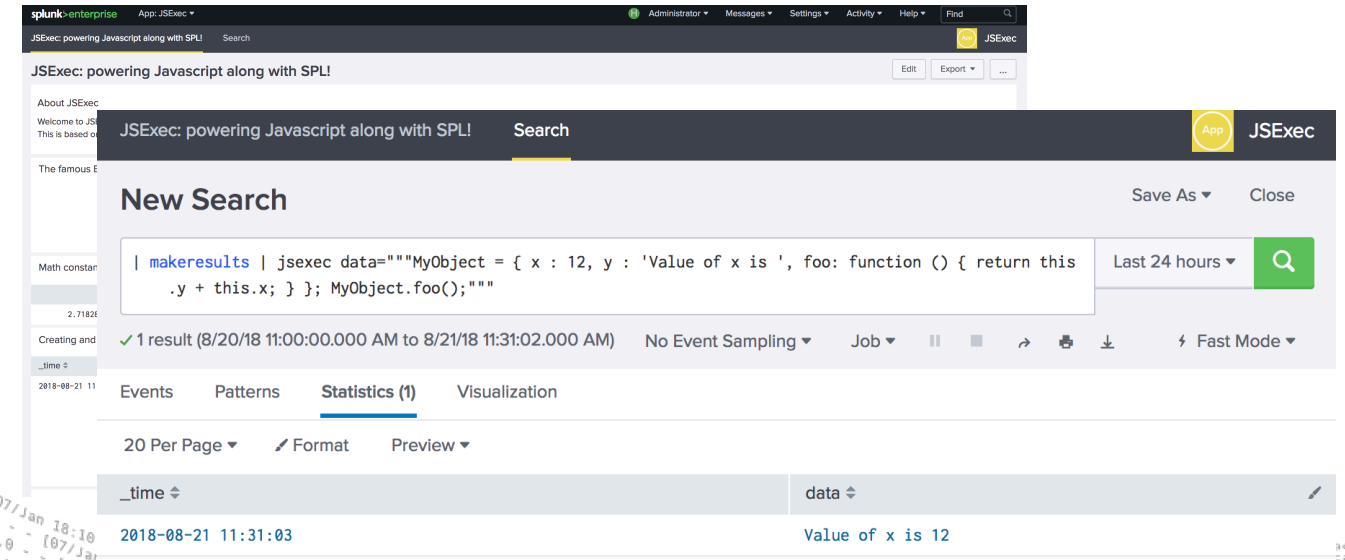
- At Splunk for almost 6 years!
- Worked on a S2S Protocol to proxy data between forwarders and indexers
- Wrote the first Adaptive Response Prototype
- Wrote a way to write Javascript along with SPL
- Former Maintainer of Linux PAM, the Linux Authentication Layer
- Major Contributor of the first SIEM, Prelude IDS back in 1998
- Honeynet Project Board Member

My Fun Lab




```
[stricaud:~] $ s2s-send 127.0.0.1 9997 sourcetype lol _raw "$(cat rotflcopter.txt)"
[stricaud:~] $
```

i	Time	Event
>	8/21/18 11:54:19.000 AM	ROTFL:ROTFL:ROTFL:ROTFL _^___ L __/ [] \ LOL===__ \ L _____] I I --------/ Collapse host = localhost source = /var/log/system.log sourcetype = lol




```
[stricaud:~] $ faup -o json www.bbc.co.uk
{
        "scheme": "",
        "credential": "",
        "subdomain": "www",
        "domain": "bbc.co.uk",
        "domain_without_tld": "bbc",
        "host": "www.bbc.co.uk",
        "tld": "co.uk",
        "port": "",
        "resource_path": "",
        "query_string": "",
        "fragment": "",
        "url_type": "mozilla_tld"
}
```

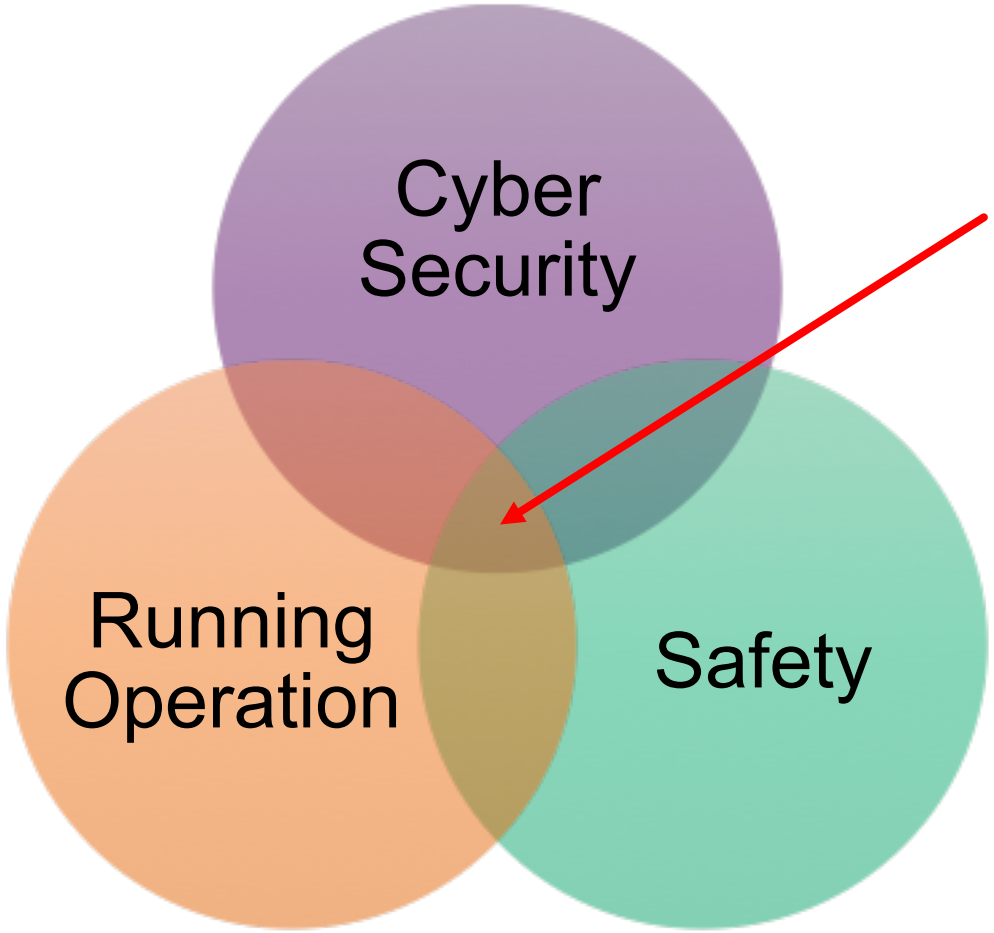
splunk> .conf18

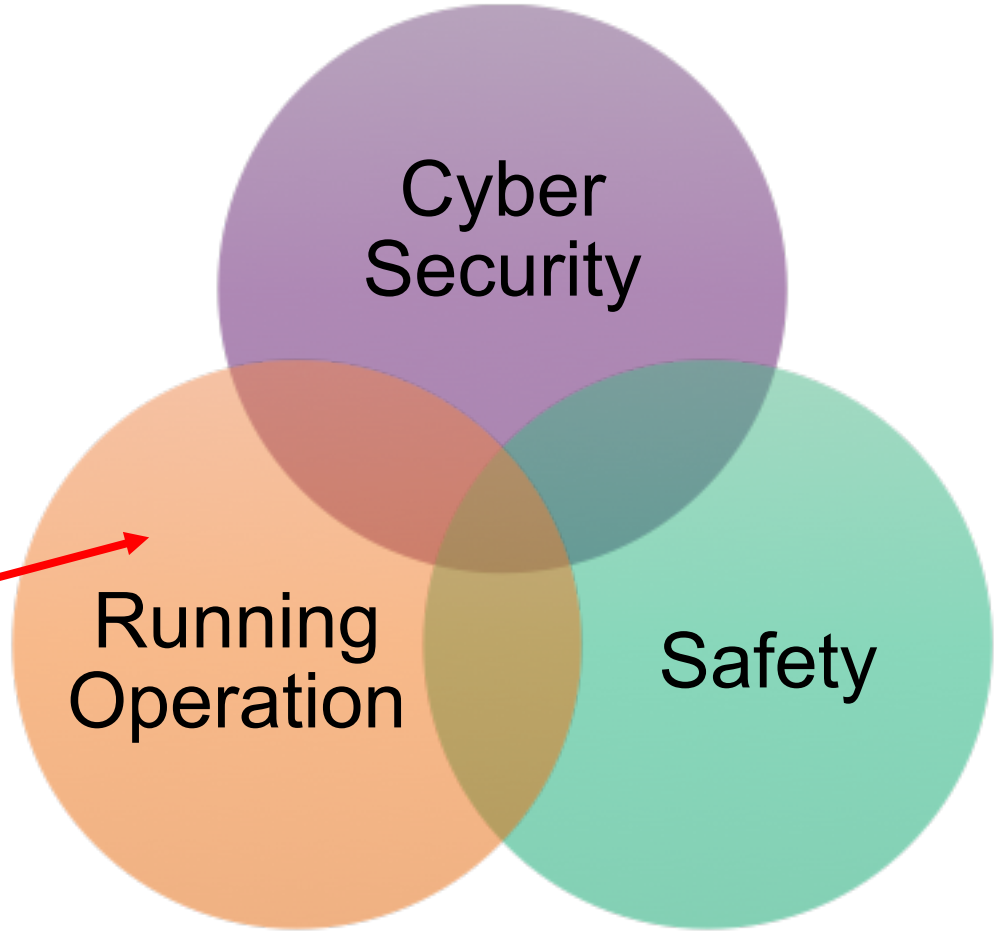
About Me

Chris Duffey / Senior IoT Practitioner @splunk

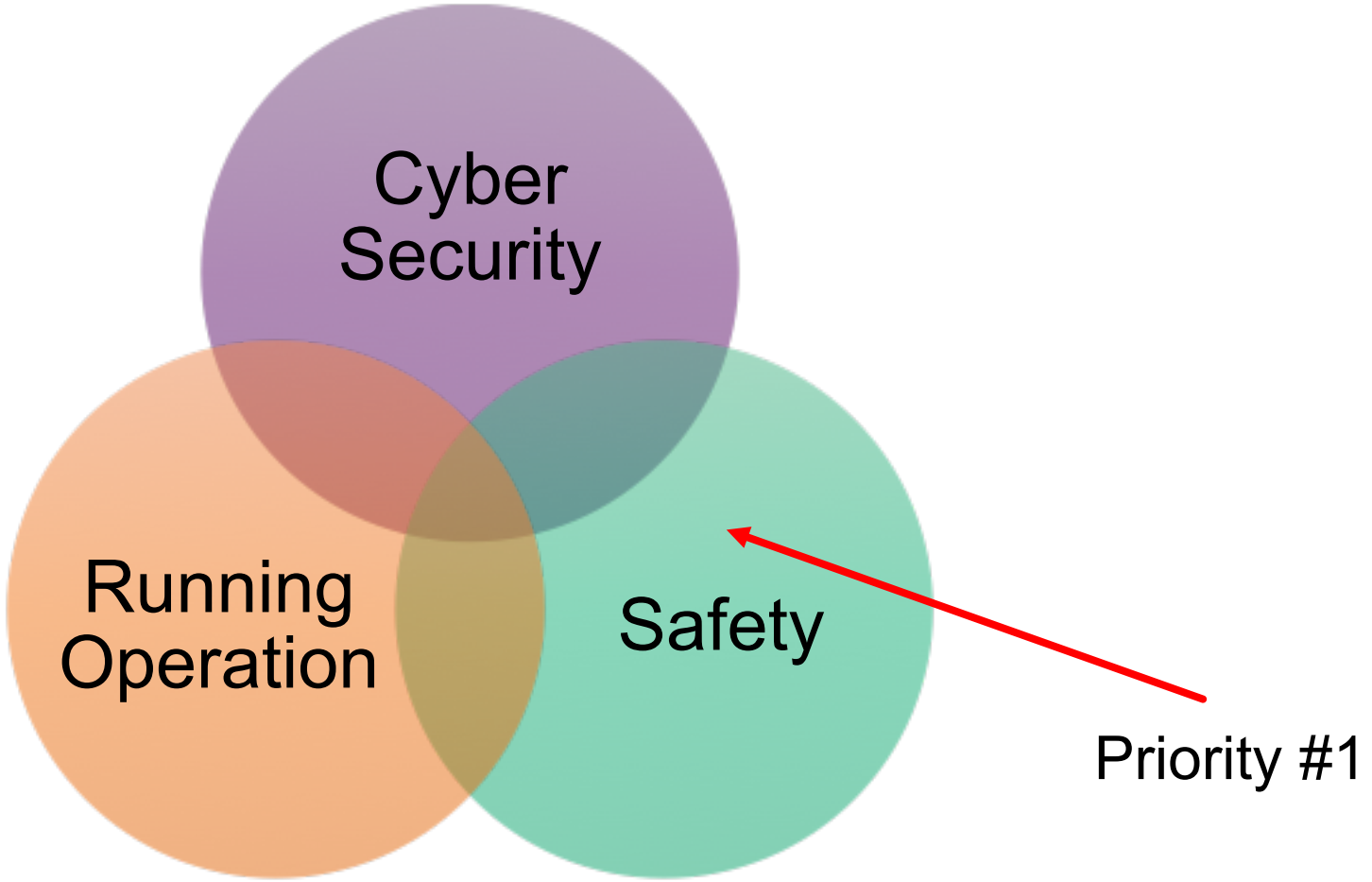
- 10+ years experience in SCADA
- Worked at major oil & gas pipeline company with over 50k+ of pipeline across the US
- Worked as a SCADA Developer before transitioning to Infrastructure & Cyber Security role
- Deployed Splunk on pipeline system for:
  - ICS Monitoring
  - ICS Cyber Security
- Focused Splunk deployments in OT environments as consultant

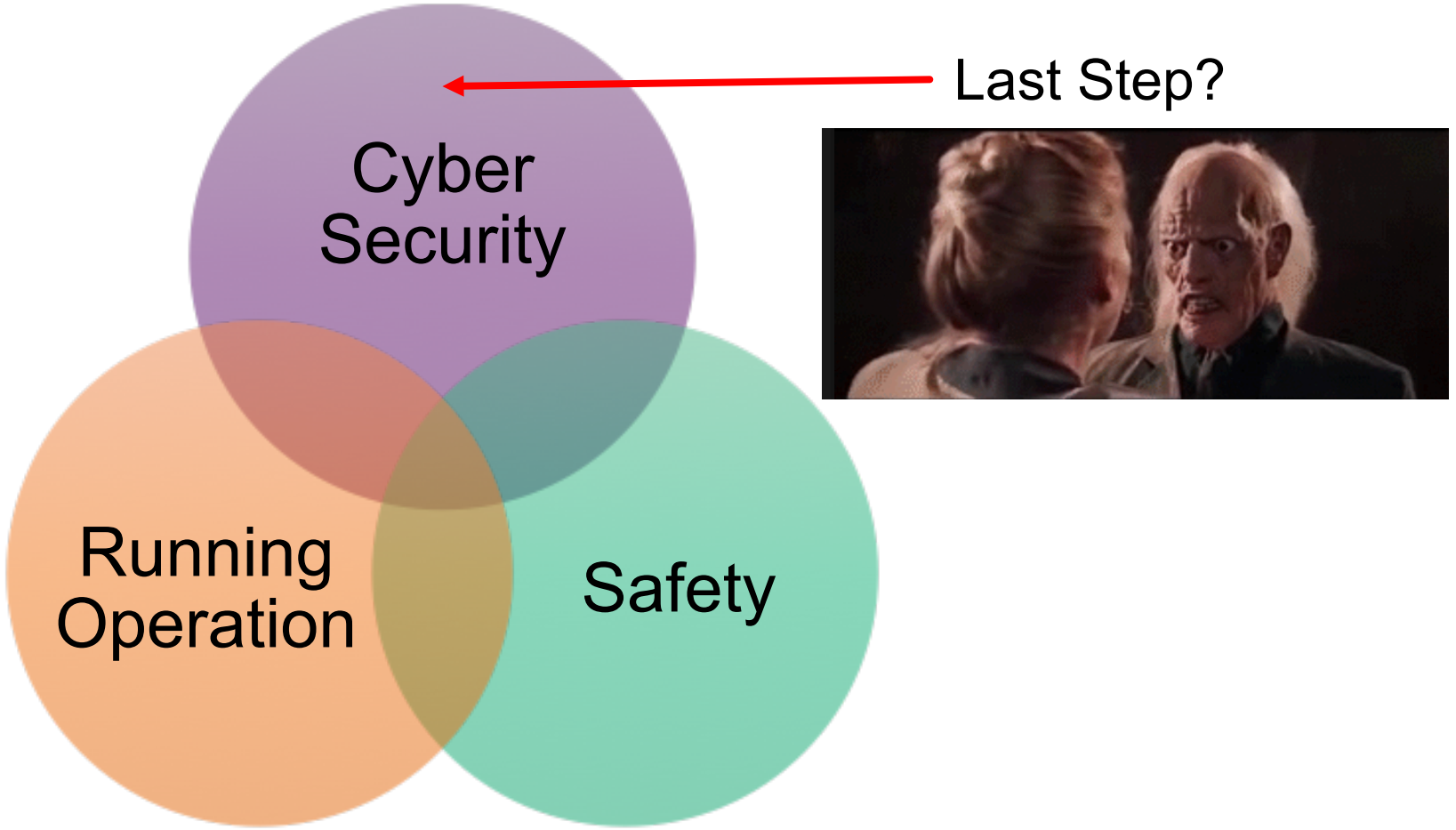
Introduction





Where anyone starts





OT Cyber Security

- Challenges
  - Low visibility
  - Lifecycles of system 15+ years
  - No pro-active measures (safety first)
  - Limited OT Cyber Security products
  - Vendor approval
  - Patching slow to deploy
  - No scanning of equipment

OT Cybersecurity

- OT and IT Convergence
  - Increased connectivity and need to share
  - Cloud computing
  - Common hardware/software packages (e.g. Windows, TCPIP)
  - USB ports everywhere
  - Offshore reliance
  - Direct internet access to PLCs
  - Complexity increasing
  - Lack of workforce
  - OT vs IT mentality

ICS Threats Landscape

Increasing Sophistication

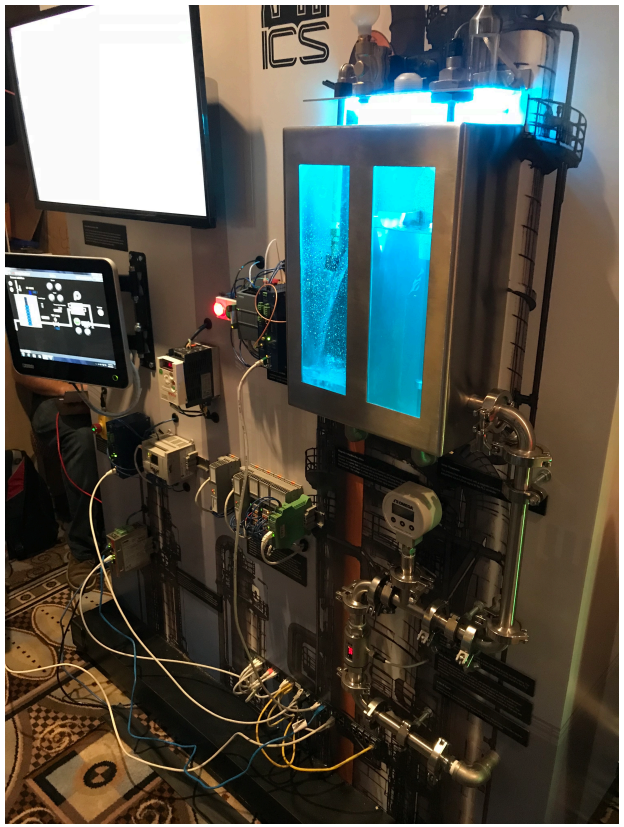
splunk> .conf18

- **ICSMA-18-240-01** : **Qualcomm Life Capsule**
  This advisory includes mitigations for a code weakness vulnerability in the Qualcomm Life Capsule Datacaptor Terminal Server software.
  08/28/2018 - 10:20
- **ICSA-18-240-01** : **Schneider Electric Modicon M221**
  This advisory includes mitigation recommendations for information management errors, and permissions, privileges, and access controls vulnerabilities in Schneider Electric's Modicon 221 programmable logic controller.
  08/28/2018 - 10:15
- **ICSA-18-240-02** : **Schneider Electric Modicon M221**
  This advisory includes mitigation recommendations for an improper check for unusual or exceptional conditions vulnerability in Schneider Electric's Modicon M221 programmable logic controller.
  08/28/2018 - 10:10
- **ICSA-18-240-03** : **Schneider Electric PowerLogic PM5560**
  This advisory includes mitigation recommendations for a cross-site scripting vulnerability in Schneider Electric's PowerLogic PM5560 power management system.
  08/28/2018 - 10:05
- **ICSA-18-240-04** : **ABB eSOMS**
  This advisory includes mitigation recommendations for an improper authentication vulnerability in ABB's eSOMS.
  08/28/2018 - 10:00
- **ICSMA-18-235-01** : **BD Alaris Plus**
  This medical device advisory includes mitigation recommendations for an improper authentication vulnerability in specific versions of BD's Alaris Plus medical syringe pumps.
  08/23/2018 - 10:00
- **ICSMA-18-233-01** : **Philips IntelliVue Information Center iX**
  This medical device advisory includes mitigation recommendations for a resource exhaustion vulnerability in Philips' IntelliVue Information Center iX real-time central monitoring system.
  08/21/2018 - 10:05
- **ICSA-18-233-01** : **Yokogawa iDefine, STARDOM, ASTPLANNER, and TriFellows**
  This advisory includes mitigation recommendations for stack-based buffer overflow vulnerabilities in Yokogawa's iDefine, STARDOM, ASTPLANNER, and TriFellows products.
  08/21/2018 - 10:00
- **ICSMA-18-228-01** : **Philips PageWriter TC10, TC20, TC30, TC50, and TC70 Cardiographs**
  This medical device advisory includes mitigation recommendations for improper input validation and use of hard-coded credentials vulnerabilities in Philips' PageWriter Cardiographs.
  08/16/2018 - 10:10
- **ICSA-18-228-01** : **Emerson DeltaV DCS Workstations**
  This advisory includes mitigation recommendations for uncontrolled search path element, relative path traversal, improper privilege management, and stack-based buffer overflow vulnerabilities in Emerson's Delta V workstations.
  08/16/2018 - 10:05

Alert (TA17-293A)

Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors

Independent cybersecurity researchers found nearly double the number of vulnerabilities in SCADA systems in the first six months of 2018 as they did in H1 of 2017, according to a new report by Japanese multinational Trend Micro, amid rising concerns about infrastructure security.



Incidents

- STUXNET
  - Target and focused on specific equipment and very specialized
- Dragonfly/HAVEX
  - Primarily espionage and utilized OPC to map out environment
- BLACKENERGY
  - Exploited specific HMI interfaces
  - Allowed groups to see graphical representations of the systems
  - Pivoted from IT to OT
  - ~225k customers left without power for 6 hours
    - Some sites lost automated control for up to a year
  - Malware combined with direct interaction

Incidents

- CRASHOVERRIDE aka, Industroyer
  - Ukrainian Power Grid
  - Adversaries showed knowledge of how electric grids function
  - Malware Framework targeting electric grids
    - Not unique to vendor or system
    - Modular
  - Focused on disruption and destruction not espionage

How to understand ICS Security

When honeypots get in the mix!

splunk> .conf18

Why Honeypots?

”A **Honeypot** is a system **designed** to act as a decoy **to lure cybercriminals** to understand tactics and motives involved in computer and network attacks”

- Believe a paper or believe data?
- Useful content == gathered from data
- Lots of details, papers, challenges, code, information on the Honeynet Project webpage: http://www.honeynet.org

Example, Gas Station Honeypot

- The GasPot Experiment: Unexamined Perils in UsingGas-Tank-Monitoring Systems
- By Kyle Wilhoit and Stephen Hilt
- Talk given at BlackHat in 2015
- https://documents.trendmicro.com/assets/wp/wp_the_gaspot_experiment.pdf

> ”
> An **explosion rattled the sleepy town of Bayamon**, Puerto Rico, in the wee hours of 23 October 2009 [1]. The fire blazed for three days, burning down houses and causing thick black clouds of gasoline-fueled smoke and forcing residents to flee their homes. The culprit behind the catastrophe? Investigators said it was **a glitch in the facility's computerized monitoring system**. A storage tank was getting refilled with gasoline from a fuel ship docked along the San Juan harbor. Since the tank's meter malfunctioned, the petrol kept overflowing **until it met an ignition source**. The burning district became the aftermath. ”

Nmap already provides a Guardian AST scanner!

```
$ nmap --script atg-info -p 10001 <host>
  10001/tcp open   Guardian AST reset
  | atg-info:
  | I20100
  | SEP 19, 2015  5:33 PM
  |
  |     Fuel Company
  |     12 Fake St
  |     Anytown, USA 12345
  |
  |
  | IN-TANK INVENTORY
  |
  | TANK PRODUCT          VOLUME TC VOLUME   ULLAGE  HEIGHT  WATER  TEMP
  |    1  UNLEADED          5135          0     6647   42.71   0.00 72.01
  |    2  UNLEADED          5135          0     6647   42.70   0.00 71.55
  |    3  PREMIUM UNLEADED  5135          0     5350   19.27   0.00 72.52
  |_
```

Conpot, the ICS Honeypot

- Available at: https://github.com/mushorg/conpot
- Written by Lukas Rist in 2013
- Works with a templating system
- Creates /var/log/conpot/conpot.log
- Simulates Siemens S7-200 PLC, Guardian AST tank monitor

Gas Tank Monitor Honeypots

- Only tied to a given class of devices
- Need to create QUICKLY a honeypot to simulate a given environment
- No time to write/debug code

splunk> .conf18

Siemens S7-200 Communication

Interfaces

- Profinet / Industrial Ethernet
- Industrial Wireless LAN
- Profibus
- AS-Interface
- WAN
- Multi-Point Interface (MPI)
- Point-to-Point Interface (PPI)
- KNX/EIB (KONNEX)

Services

- FTP
- Email
- SNMP
- OPC
- Profinet IO
- Profinet CBA
- S7
- PG/OP

Bridging PLCs with IDS

- Hard/Dangerous/Prohibited to install a sensor on a PLC
- Probing a PLC can cause it to malfunction
  - And not necessary right now, but in a random amount of time…
- Want to take the risk?

- Network IDS to the rescue

Here comes Suricata

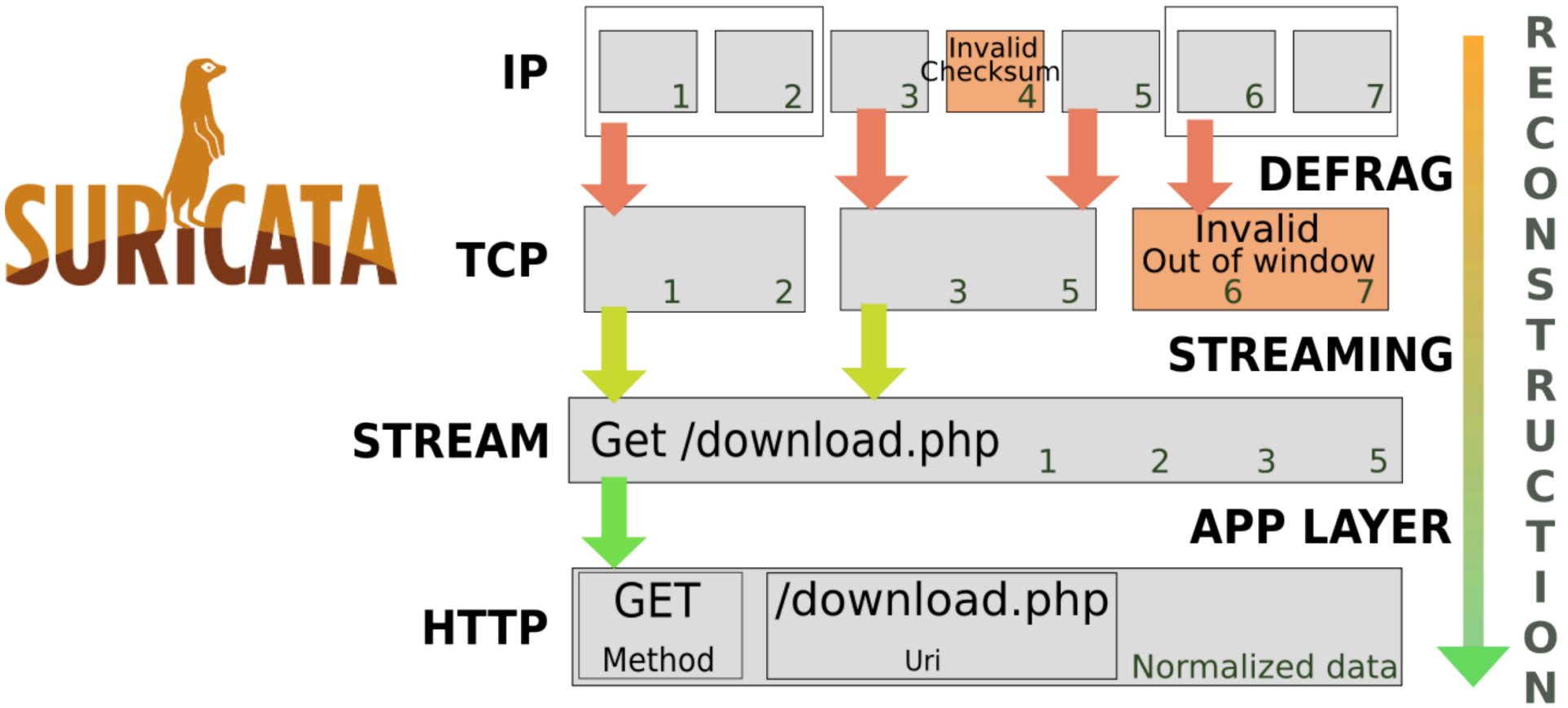


Image courtesy of Eric Leblond

Changing Suricata to transform it into a honeypot

Alerting when this signature matches

```
alert http any any -> any any (msg:"HTTP
    download";
content:"GET"; http_method;
content:"/download.php"; http_uri; sid:7891011)
```

Replying a fake web page content when this signature matches

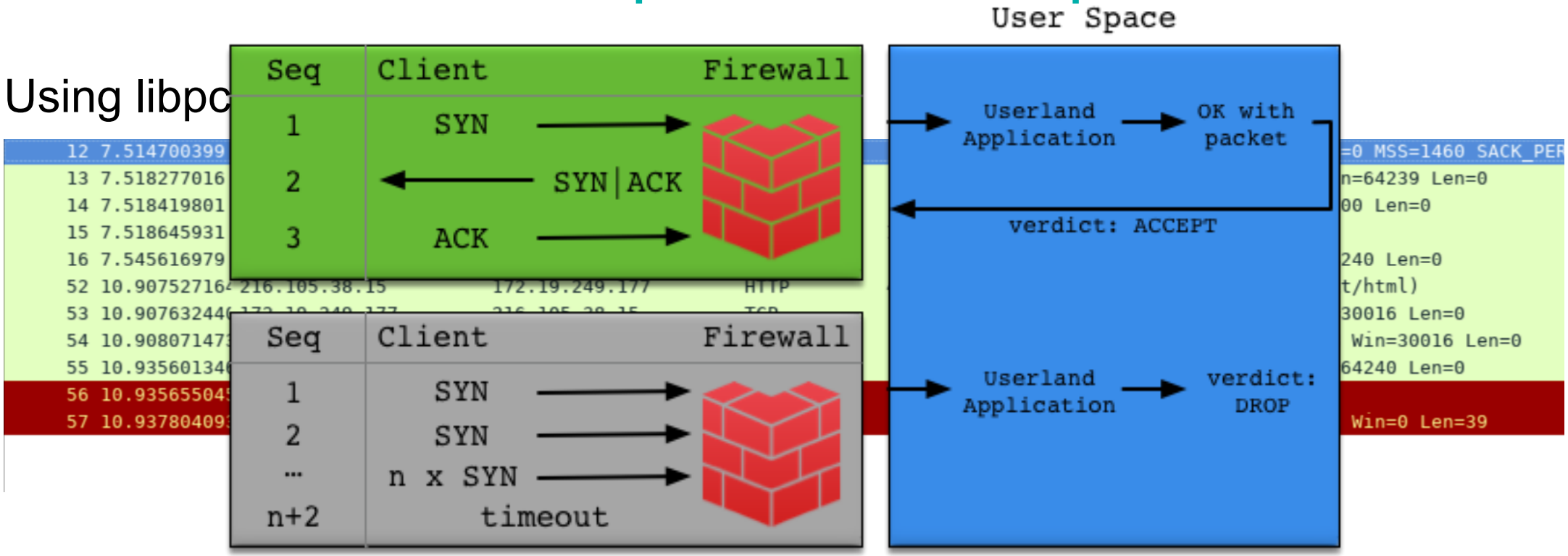
```
response http any any -> any any (msg:"HTTP
    download";
content:"GET"; http_method;
content:"/download.php"; http_uri; sid:7891011)
```

Strategy to send a response

- Packet matches a signature
- Fetch the SID (Signature ID)
- Open the file (prefix)/lib/suricata/response/sid
- Send raw packet(s) from the opened sid
- Log it, with the flow-id from Suricata to understand sessions

How to Capture and Respond?

Using libpc



Nope, Using Netfilter Queue, to intercept!

Suricata Apps Protocols Decoding

- HTTP
- SSL
- TLS
- SMB
- DCERPC
- SMTP
- FTP
- SSH
- DNS
- Modbus
- ENIP/CIP
- DNP3
- NFS
- NTP
- TFTP
- NFS
- Kerberos
- IKEv2
- DHCP
- …

Suricata and Modbus

```
# Note: Modbus probe parser is minimalist due to the poor significant field
# Only Modbus message length (greater than Modbus header length)
# And Protocol ID (equal to 0) are checked in probing parser
# It is important to enable detection port and define Modbus port
# to avoid false positive
modbus:
  # How many unreplied Modbus requests are considered a flood.
  # If the limit is reached, app-layer-event:modbus.flooded; will match.
  #request-flood: 500

  enabled: yes
```

Starting from Scratch

Capture any Modbus Event

1

```
alert modbus any any -> any 502 (msg:"Modbus Traffic Detected"; flow:to_server; sid:999042; rev:1;)
```

2

```
# suricata -D -c /etc/suricata/suricata.yaml -s simple-modbus.rules -i eth0
```

3

```
# tail -f /var/log/suricata/fast.log
08/30/2018-20:00:22.156169  [**] [1:999042:1] Modbus Traffic Detected [**]
[Classification: (null)] [Priority: 3] {TCP} 4.14.104.185:62330 ->
37.187.73.159:502
```

Capture

```
>>> from pymodbus.client.sync import ModbusTcpClient
>>> client = ModbusTcpClient("myserver")
>>> client.write_coil(1, True)
```

```
# tshark -f 'tcp port 502' -i eth0
```

```
1 0.000000000 4.14.104.185 → 37.187.73.159 Modbus/TCP 78    Query: Trans:     2; Unit:   0, Func:   5: Write Single Coil
2 0.000496081 37.187.73.159 → 4.14.104.185 Modbus/TCP 78 Response: Trans:     2; Unit:   0, Func:   5: Write Single Coil
3 0.154409928 4.14.104.185 → 37.187.73.159 TCP 66 38055 → 502 [ACK] Seq=13 Ack=13 Win=4117 Len=0 TSval=950735067 TSecr=2243137934
```

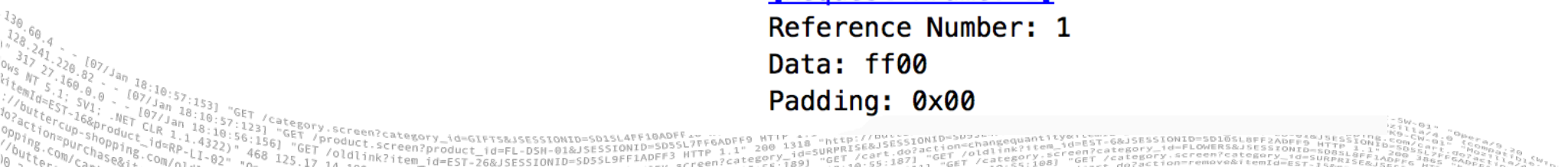
Exchange

Request

```
▼ Modbus/TCP
    Transaction Identifier: 5
    Protocol Identifier: 0
    Length: 6
    Unit Identifier: 0
▼ Modbus
    Function Code: Write Single Coil (5)
    Reference Number: 1
    Data: ff00
    Padding: 0x00
```

Response

```
▼ Modbus/TCP
    Transaction Identifier: 5
    Protocol Identifier: 0
    Length: 6
    Unit Identifier: 0
▼ Modbus
    Function Code: Write Single Coil (5)
    [Request Frame: 1]
    Reference Number: 1
    Data: ff00
    Padding: 0x00
```

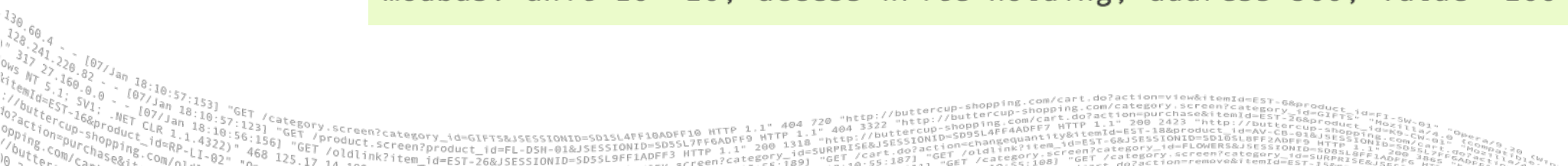


Adding options to Suricata rules to go fine grain

```
alert modbus any any -> any 502 (msg:"Modbus Traffic Detected";
modbus: unit 42, function 4, subfunction 4; flow:to_server;
sid:999042; rev:1;)
```

Read more:
https://suricata.readthedocs.io/en/latest/rules/modbus-keyword.html

```
modbus: unit 10
modbus: unit 10, function 21
modbus: unit 10, function 4, subfunction 4
modbus: unit 10, function assigned
modbus: unit 10, function !reserved
modbus: unit 10, access read
modbus: unit 10, access write coils
modbus: unit >10, access read discretes, address <100
modbus: unit 10<>20, access write holding, address 500, value >200
```



splunk> .conf18

Results

- During the month of July-August 2018:
  - 525 connections established
  - From 3 different IP addresses
    - The most active from ”**Kudelski Security Innovation**”, a Security Research Team
    - Another from **burger.census.shodan.io** ; a security Scanner

- People ARE scanning actively for Modbus (and other ICS-related protocols ;))

Benefits

- Suricata allows you to understand your security posture
- Ability to create custom protocols decoder in Rust, lots of examples!
- Your network security is tailored for your environment
- There are so many devices it is important to emulate them rapidly

Splunk Essentials for ICS Security and Compliance

All of it, in just one App!

splunk> .conf18

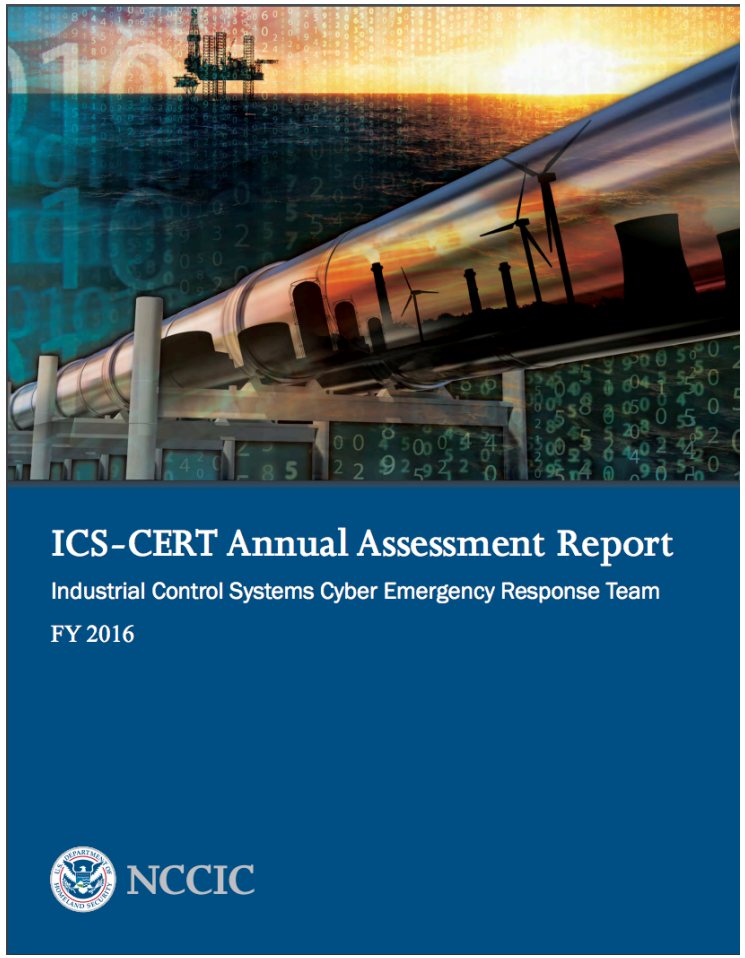
NIST 800-82 Methodology

- Step 1: Categorize Information System
- Step 2: Select Security Controls
- Step 3: Implement Security Controls
- Step 4: Assess Security Controls
- Step 5: Authorize Information System
- Step 6: Monitor Security Controls

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf

ICS US CERT

Top Threats



TOP 30 IDENTIFIED WEAKNESSES IN FY 2016			
NIST 800-53 Weakness Categories	**Instances**	**Percentage**	**Order**
Boundary Protection	94	13.4%	1
Least Functionality	42	6.0%	2
Identification and Authentication (Organizational Users)	36	5.1%	3
Physical Access Control	28	4.0%	4
Audit Review, Analysis, and Reporting	26	3.7%	5
Authenticator Management	24	3.4%	6
Least Privilege	20	2.9%	7
Allocation of Resources	19	2.7%	8
Account Management	17	2.4%	9
Remote Access	16	2.3%	10
Security Awareness Training	16	2.3%	11
System Security Plan	15	2.1%	12
Flaw Remediation	15	2.1%	13
Information System Monitoring	15	2.1%	14
Security Impact Analysis	14	2.0%	15
Transmission Confidentiality and Integrity	13	1.9%	16
Baseline Configuration	12	1.7%	17
Contingency Plan	12	1.7%	18
Information System Backup	12	1.7%	19
Security Engineering Principles	12	1.7%	20
Information System Component Inventory	11	1.6%	21
Media Use	11	1.6%	22
Role-Based Security Training	10	1.4%	23
Configuration Change Control	10	1.4%	24
System Interconnections	9	1.3%	25
Configuration Settings	9	1.3%	26
Publicly Accessible Content	8	1.1%	27
Audit Events	8	1.1%	28
Incident Response Plan	8	1.1%	29
Protection of Information at Rest	8	1.1%	30
Total Discoveries Identified for Top 30 Weaknesses	550		
Total Discoveries Identified in FY2016	700		

https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/FY2016_Industrial_Control_Systems_Assessment_Summary_Report_S508C.pdf

splunk>enterprise App: Splunk Essentials for ICS Security and Compliance ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Introduction | ICS Security Use Cases ▾ | ICS Security Maturity | Data Source Check | Documentation ▾ | Advanced ▾

Introduction

Export ▾ ...

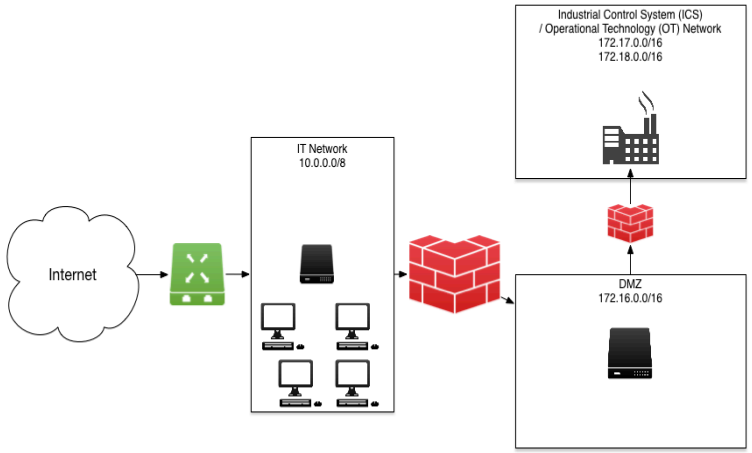
Introduction

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.



We strongly discourage the use of this App on production data.

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. The ICS must be protected against malicious cyberattacks as well as non-malicious

Access Control

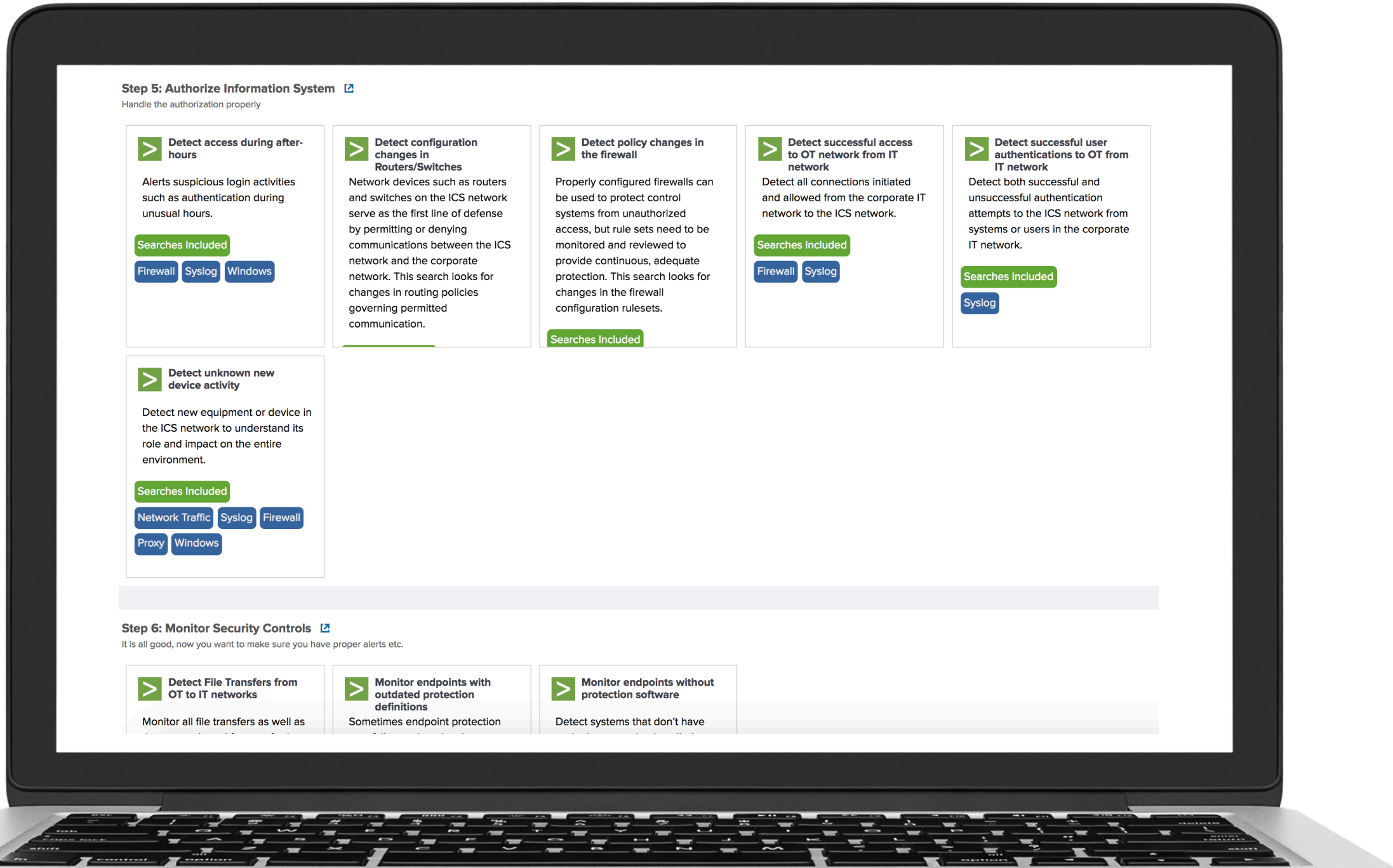
Featuring 3 Examples!
Without a formalized review and validation of logs, unauthorized users, applications, and unauthorized events, hackers could operate within the ICS network undetected.

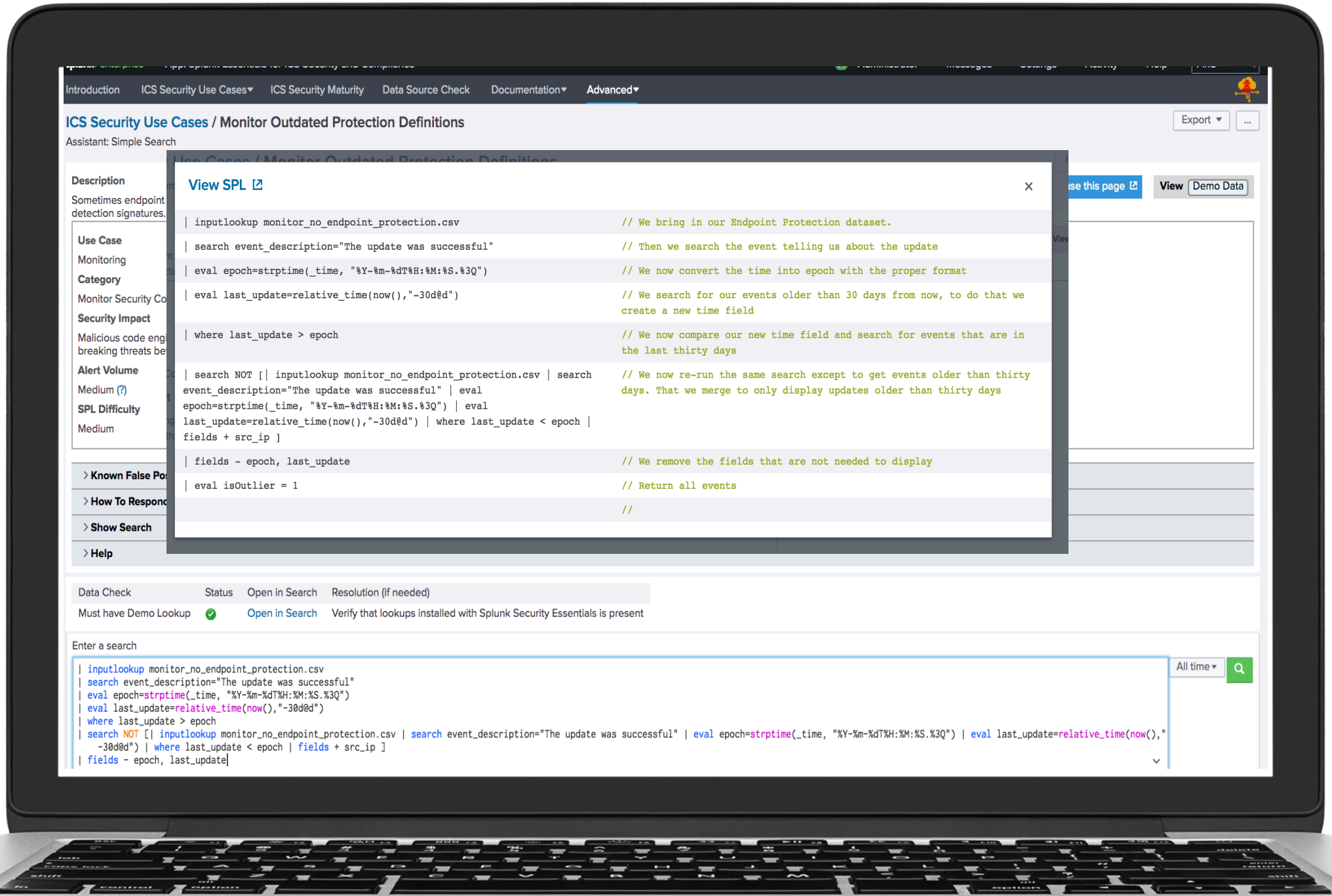
Monitoring

Featuring 3 Examples!
Lack of monitoring could allow unauthorized physical access to field equipment and locations. This increases the opportunity for cybercriminals to access the ICS network and maliciously modify,

Change Management

Featuring 2 Examples!
Integrating new information systems into existing industrial control processes require organizations to create additional communication and information exchange paths, mostly unverified ad-hock solutions. This





Conclusion

Key Takeaways

Splunk Enables Securing your Industrial Assets

1. Passive Monitoring Works!
2. Splunk core feature of indexing any type of Data is a strong benefit for OT Security
3. Splunk Essentials for ICS Security helps you to get started and gain in maturity (Available on: https://splunkbase.splunk.com/app/4150/)

Thank You

Don't forget to rate this session in the .conf18 mobile app