Pour Oil, Not Sand, into your Security Operations Center

René Agüero | Sr. Manager, Security Specialist

Forward-Looking Statements

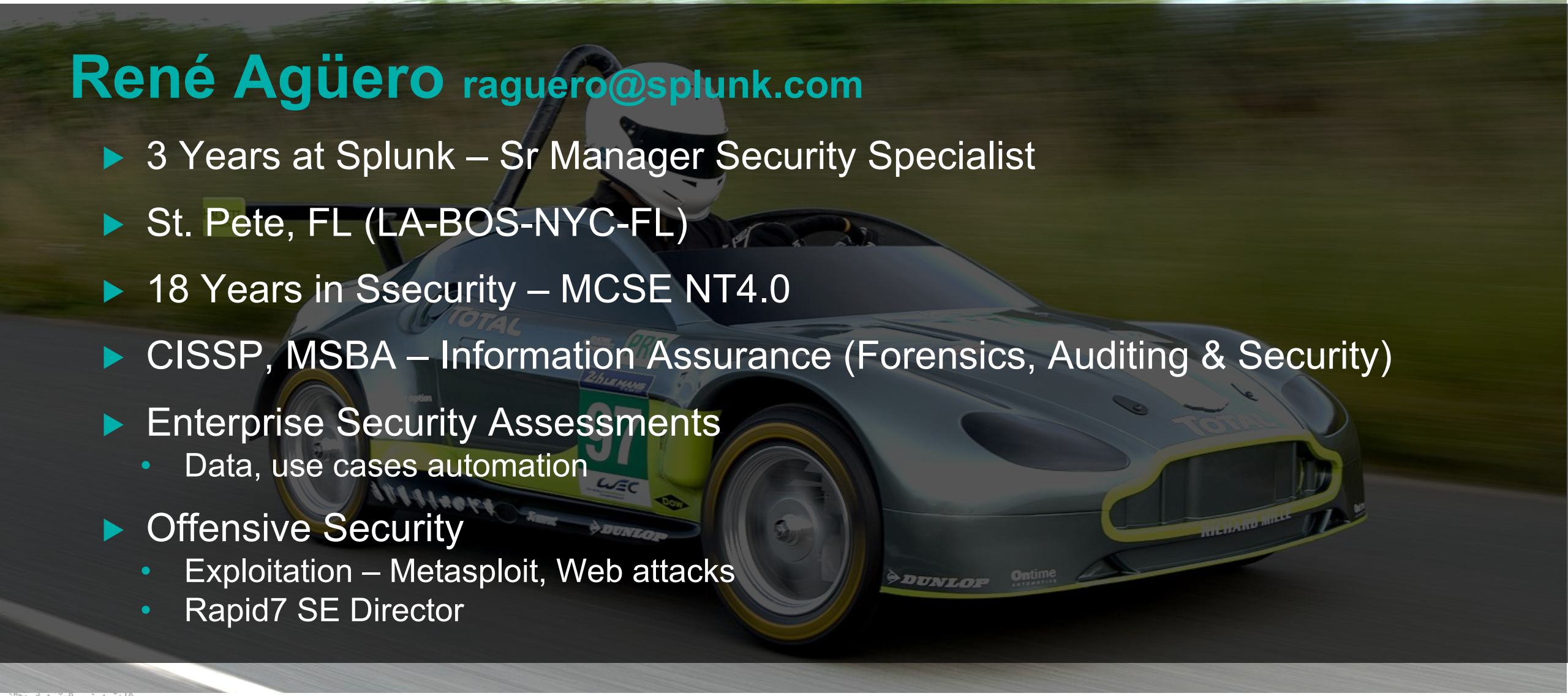
During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results 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

$whoami

$whoami

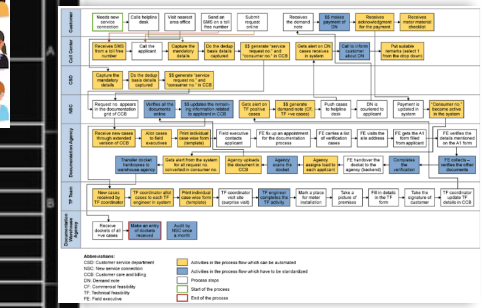


René Agüero raguero@splunk.com

- 3 Years at Splunk – Sr Manager Security Specialist
- St. Pete, FL (LA-BOS-NYC-FL)
- 18 Years in Ssecurity – MCSE NT4.0
- CISSP, MSBA – Information Assurance (Forensics, Auditing & Security)
- Enterprise Security Assessments
  - Data, use cases automation
- Offensive Security
  - Exploitation – Metasploit, Web attacks
  - Rapid7 SE Director

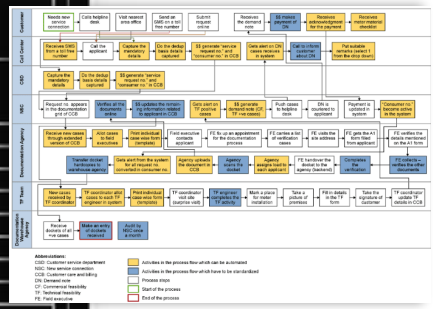
Lots of Data Points

- ~ 60 ES Benchmarks completed
- Security Operations
- Data ingested
- Workflows
- Automation
- Operationalization



Type:	MS S54
Engine Orientation:	Longitudinal
Displacement:	3246cc
Compression ratio:	11.5 : 1
Valve configuration:	Double Overhead valves
Valves per cylinder:	4
Valvetrain Operation:	VANOS
Induction:	NA
Bore x stroke:	87 mm bore / 91 mm stroke
Fuel system:	Bosch (4 hole plate) fuel injectors
Fuel type:	Premium fuel recommended, not required
Fire Order:	1-5-3-6-2-4
Camshaft drive:	2x double-roller chain
Engine Mass (kg / lbs):	217 kg / 478lbs
Maximum Engine Speed:	8000 RPM
Materials	
Block:	Cast iron
Pistons:	Graphite coated cast aluminum
Intake manifold:	Composite
Exhaust System:	Stainless Steel
Crankshaft:	Forged Steel
Camshaft:	
Connecting rod:	

splunk> .conf18



Type:	MS B54
Engine Orientation:	Longitudinal
Displacement:	3246cc
Compression ratio:	11.5 : 1
Valve configuration:	Double Overhead valves
Valves per cylinder:	4
Valvetrain Operation:	VANOS
Induction:	NA
Bore x stroke:	87 mm bore / 91 mm stroke
Fuel system:	Bosch (4 hole plate) fuel injectors
Fuel type:	Premium fuel recommended, not required
Fire Order:	1-5-3-6-2-4
Camshaft drive:	2x double-roller chain
Engine Mass (kg / lbs):	217 kg / 478lbs
Maximum Engine Speed:	8000 RPM
Materials	
Block:	Cast iron
Pistons:	Graphite coated cast aluminum
Intake manifold:	Composite
Exhaust System:	Stainless Steel
Crankshaft:	Forged Steel

splunk> .conf18

RIGHT

All Data is not Created Equally

- Collecting FW data
  - All FW data
- Collecting endpoint data
  - Standard AV
  - Advanced endpoint
  - All endpoints
- DNS data
  - All DNS data
- Proxy data
  - Domain, sub domain and folders
- Email data
  - To, From, Subject, Filename, File hash, Body

All Data is not Created Equally

- Collecting FW data
  - All FW data
- Collecting endpoint data
  - Standard AV
  - Advanced endpoint
  - All endpoints
- DNS data
  - All DNS data
- Proxy data
  - Domain, sub domain and folders
- Email data
  - To, From, Subject, Filename, File hash, Body

All Data is not Created Equally

- Collecting FW data
  - All FW data
- Collecting endpoint data
  - Standard AV
  - Advanced endpoint
  - All endpoints
- DNS data
  - All DNS data
- Proxy data
  - Domain, sub domain and folders
- Email data
  - To, From, Subject, Filename, File hash, Body

All Data is not Created Equally

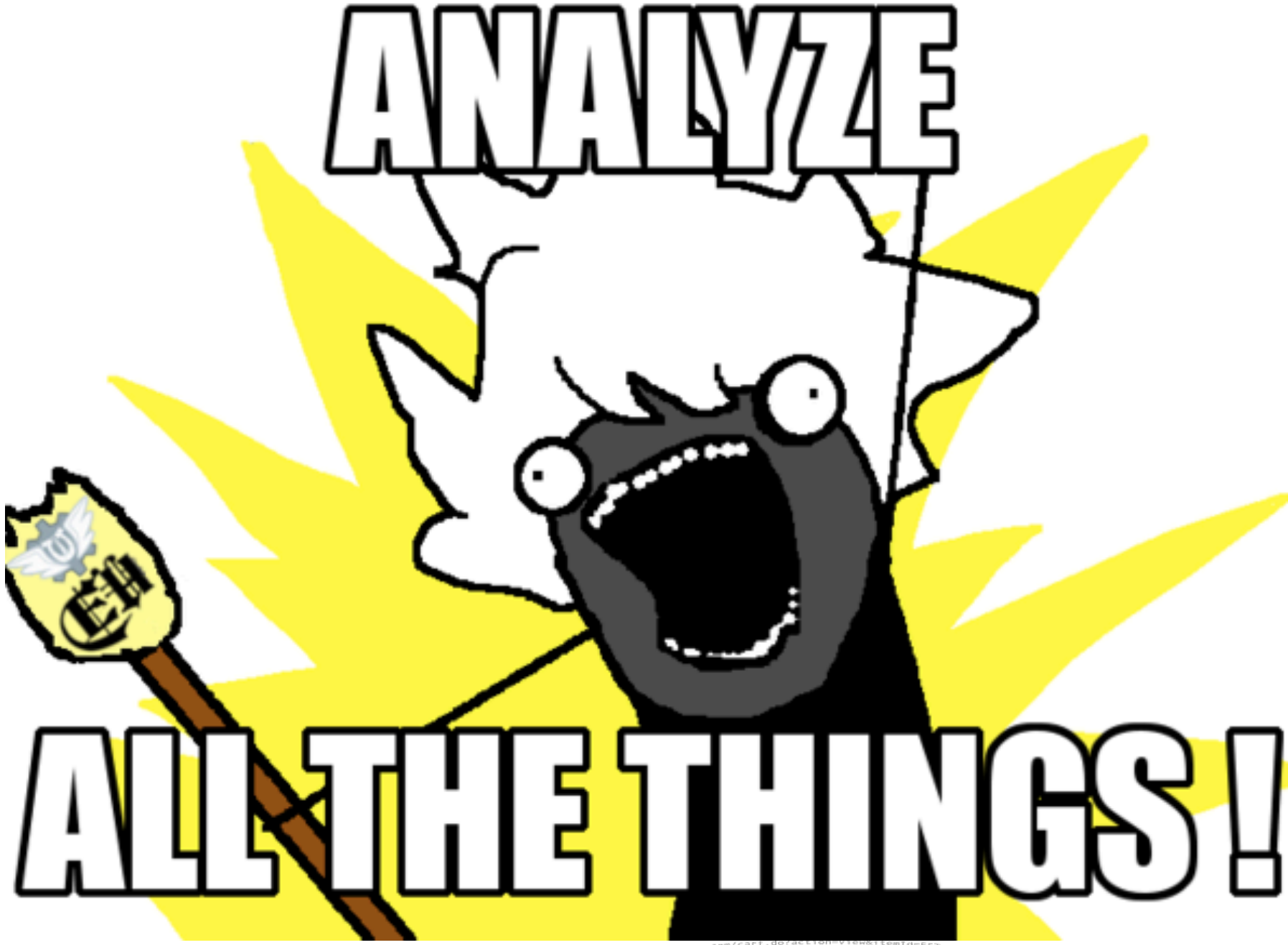
- Collecting FW data
  - All FW data
- Collecting endpoint data
  - Standard AV
  - Advanced endpoint
  - All endpoints
- DNS data
  - All DNS data
- Proxy data
  - Domain, sub domain and folders
- Email data
  - To, From, Subject, Filename, File hash, Body

All Data is not Created Equally

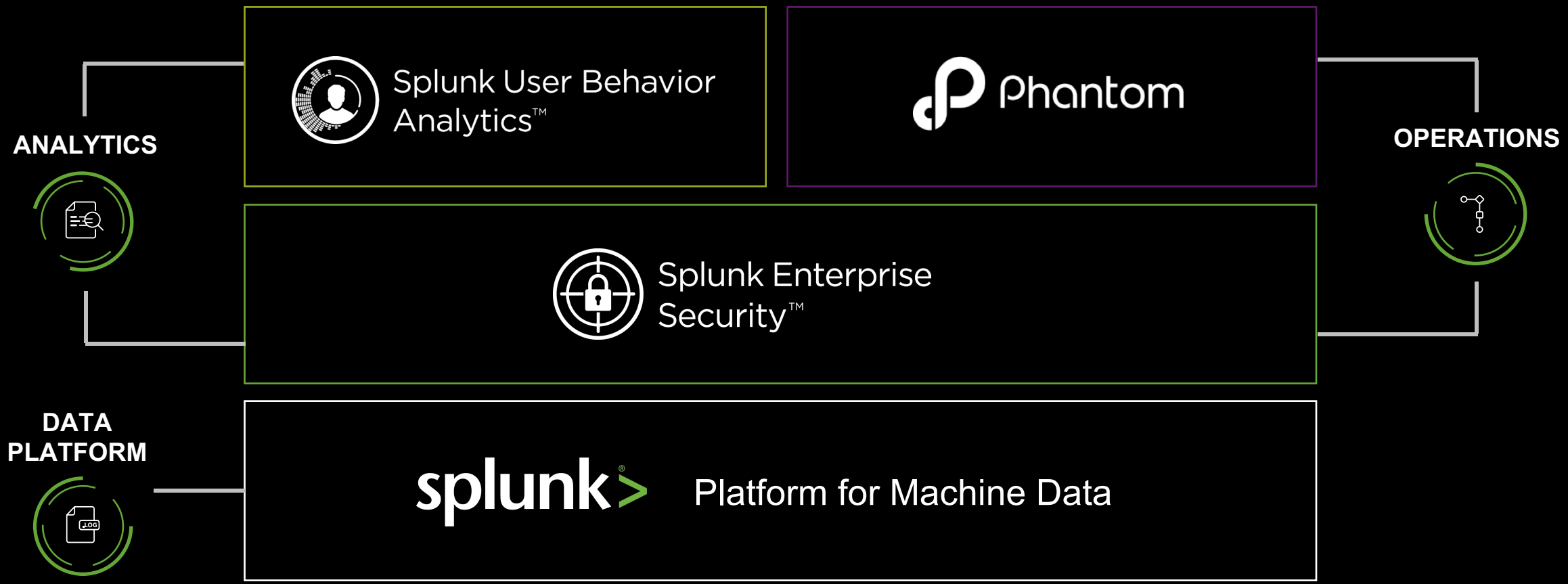
- Collecting FW data
  - All FW data
- Collecting endpoint data
  - Standard AV
  - Advanced endpoint
  - All endpoints
- DNS data
  - All DNS data
- Proxy data
  - Domain, sub domain and folders
- Email data
  - To, From, Subject, Filename, File hash, Body

All Data is not Created Equally

- Collecting FW data
  - All FW data
- Collecting endpoint data
  - Standard AV
  - Advanced endpoint
  - All endpoints
- DNS data
  - All DNS data
- Proxy data
  - Domain, sub domain and folders
- Email data
  - To, From, Subject, Filename, File hash, Body



Splunk Security Portfolio



splunk> .conf18

Journey

All selected (6)

Security Use Case

All

Category

All

Data Sources

All

Recommended

All

- [x] All
- [ ] Account Compromise (1 matches)
- [ ] Anti-Virus (24 matches)
- [ ] Any Host Logs (10 matches)
- [ ] Audit Trail (70 matches)
- [ ] Authentication (54 matches)
- [ ] Backup (4 matches)
- [ ] CRM Logs (7 matches)
- [ ] Configuration Management (2 matches)
- [ ] DHCP (1 matches)
- [ ] DNS (18 matches)
- [ ] Electronic Medical Record System (1
- [ ] Endpoint Detection and Response (104 matches)
- [ ] Host-based IDS (7 matches)
- [ ] IDS or IPS (11 matches)
- [ ] Malware Detonation (2 matches)

Stage 1: Collection

You have the data onboard, what do you do first?

Access to In-scope Resources

Visibility into who is accessing in-scope resources is key to your GDPR efforts. Splunk allows easy analysis of that information.

Recommended

Searches Included

Web Proxy

Access to In-Scope Unencrypted Resources

Unencrypted communications leaves you vulnerable to a data breach -- when users access PII data, ensure that all connections are encrypted.

Recommended

Searches Included

Web Proxy

Authentication Against a New Domain Controller

A common indicator for lateral movement is when a user starts logging into new domain controllers.

Recommended

Searches Included

Basic Malware Outbreak

Looks for the same malware occurring on multiple systems in a

Basic Scanr

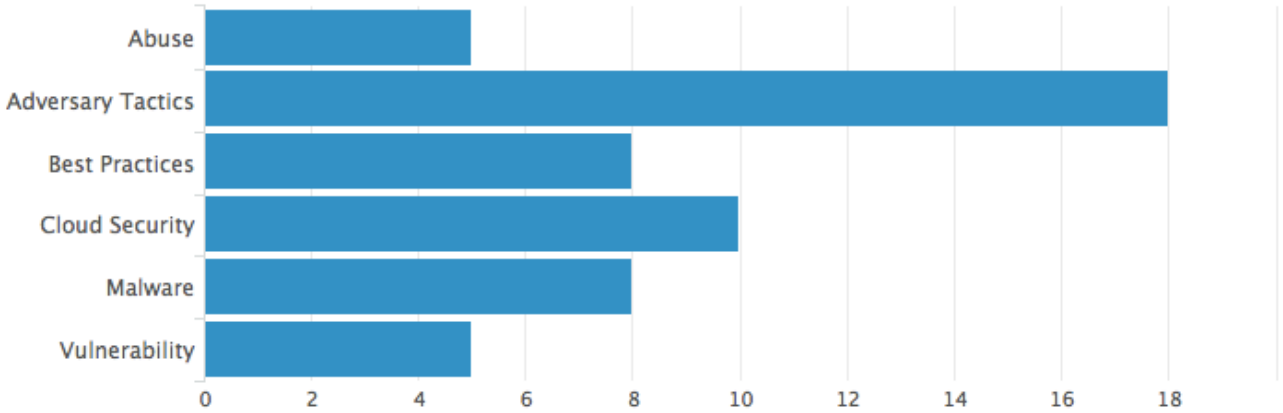
Looks for hosts that reach out to more than 500 hosts, or more

The anonymity of TOR makes it
perfect place to hide C&C,

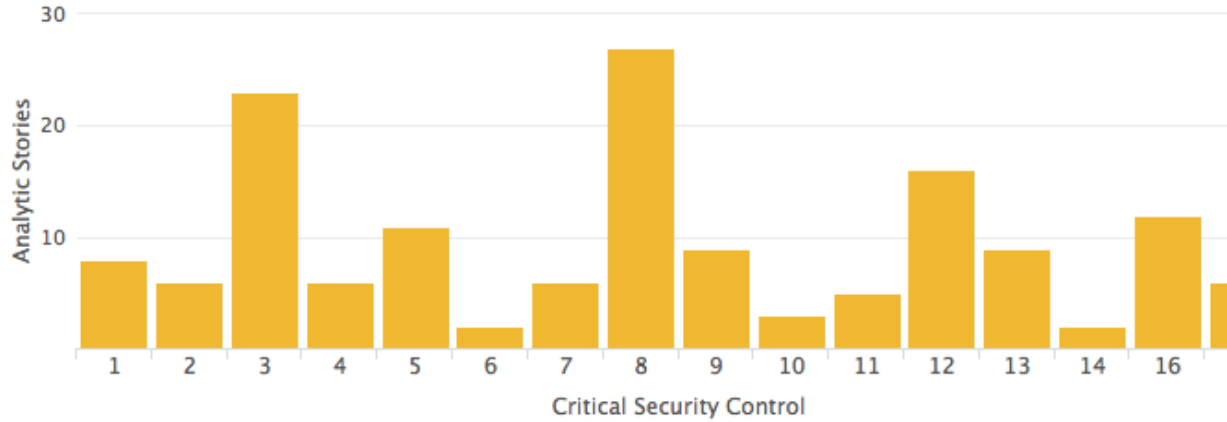
i	Example Content	Demo Data	Live Data	Accelerated Data
>	AWS APIs Called More Often Than Usual Per User	✓	!	N/A
>	AWS Cloud Provisioning Activity from Unusual Country	✓	!	N/A
>	AWS Cloud Provisioning Activity from Unusual IP	✓	!	N/A
>	AWS Instance Created by Unusual User	✓	!	N/A
>	AWS Instance Modified by Unusual User	✓	!	N/A
>	AWS New API Call Per Peer Group	✓	!	N/A
>	AWS New API Call Per User	✓	!	N/A
>	AWS Unusual Amount of Modifications to ACLs	✓	!	N/A
>	Access to In-Scope Unencrypted Resources	✓	!	N/A
>	Access to In-scope Resources	✓	!	N/A
>	Activity from Expired User Identity - on Category	✓	✓	N/A
>	Authentication Against a New Domain Controller	✓	✓	N/A
>	Basic Brute Force Detection	✓	✓	N/A
>	Basic Dynamic DNS Detection	✓	!	✓
>	Basic Malware Outbreak	✓	✓	N/A
>	Basic Scanning	✓	✓	N/A
>	Basic TOR Traffic Detection	✓	✓	N/A

splunk> .conf18

Story Categories



Analytic Stories by CIS Critical Security Control



1h

Kill Chain Phases

Category: All

Kill Chain Phases: All

ATT&CK Tactic: All

Data Models: All

CIS Critical Security Controls: All

splunk> .conf18

Analytic Story Detail

Export ...

Select an Analytic Story

Suspicious Windows Regi... Hide Filters

Category: Adversary Tactics **Version:** 1.0 **Created:** 2018-05-31 **Modified:** 2018-08-07

Suspicious Windows Registry Activities

Run Analytics

Description:

Monitor and detect registry changes initiated from remote locations, which can be a sign that an attacker has infiltrated your system.

Narrative:

Attackers are developing increasingly sophisticated techniques for hijacking target servers, while evading detection. One such technique that has become progressively more common is registry modification.

The registry is a key component of the Windows operating system. It has a hierarchical database called "registry" that contains settings, options, and values for executables. Once the threat actor gains access to a machine, they can use reg.exe to modify their account to obtain administrator-level privileges, maintain persistence, and move laterally within the environment.

The searches in this story are designed to help you detect behaviors associated with manipulation of the Windows registry.

ATT&CK: Modify Registry, Local Port Monitor, Application Shimming, Lateral Movement, Authentication Package, Registry Run Keys / Start Folder, AppInit DLLs, Privilege Escalation, Defense Evasion, Accessibility Features, Change Default File Association, Persistence

Kill Chain Phases: Actions on Objectives

CIS Controls: CIS 5, CIS 3, CIS 8

Data Model: Application_State, Authentication, Change_Analysis, Risk

Technologies: Carbon Black Response, CrowdStrike Falcon, Linux, Microsoft Windows, Splunk Enterprise Security, Sysmon, Tanium, Ziften, macOS

References: https://redcanary.com/blog/windows-registry-attacks-threat-detection/
https://attack.mitre.org/wiki/Technique/T1112

splunk> .conf18

Analytic Story Searches

Detection

ESCU - Disabling Remote User Account Control

Configure in ES

Description
The search looks for modifications to registry keys that control the enforcement of Windows User Account Control (UAC).

Explain It Like I'm 5
This search checks to see if the registry key SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy was modified. This registry key can be used to disable remote User Account Control. The search returns the count, the first time activity was seen, last time activity was seen, the registry path that was modified, the host where the modification took place and the user that performed the modification.

Search

```
| tstats `summariesonly` count min(_time) as firstTime max(_time) as lastTime FROM datamodel
    =Change_Analysis.All_Changes where All_Changes.object_category=registry AND All_Changes
    .object_path="*Windows\\CurrentVersion\\Policies\\System\\LocalAccountTokenFilterPolicy" by
    All_Changes.dest, All_Changes.command, All_Changes.user, All_Changes.object, All_Changes
    .object_path | `ctime(lastTime)` | `ctime(firstTime)` | `drop_dm_object_name("All_Changes")`
```

All time

ATT&CK
Defense Evasion | Modify Registry

Kill Chain Phases
Actions on Objectives

CIS Controls
CIS 8

Data Models
Change_Analysis

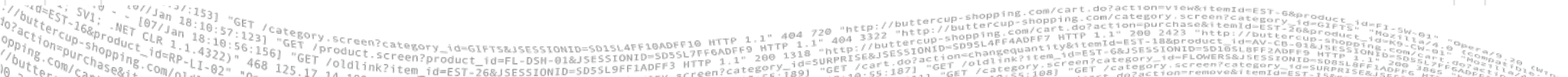
Technologies
Carbon Black Response | CrowdStrike Falcon | Sysmon

Asset at Risk
Endpoint

Confidence
medium

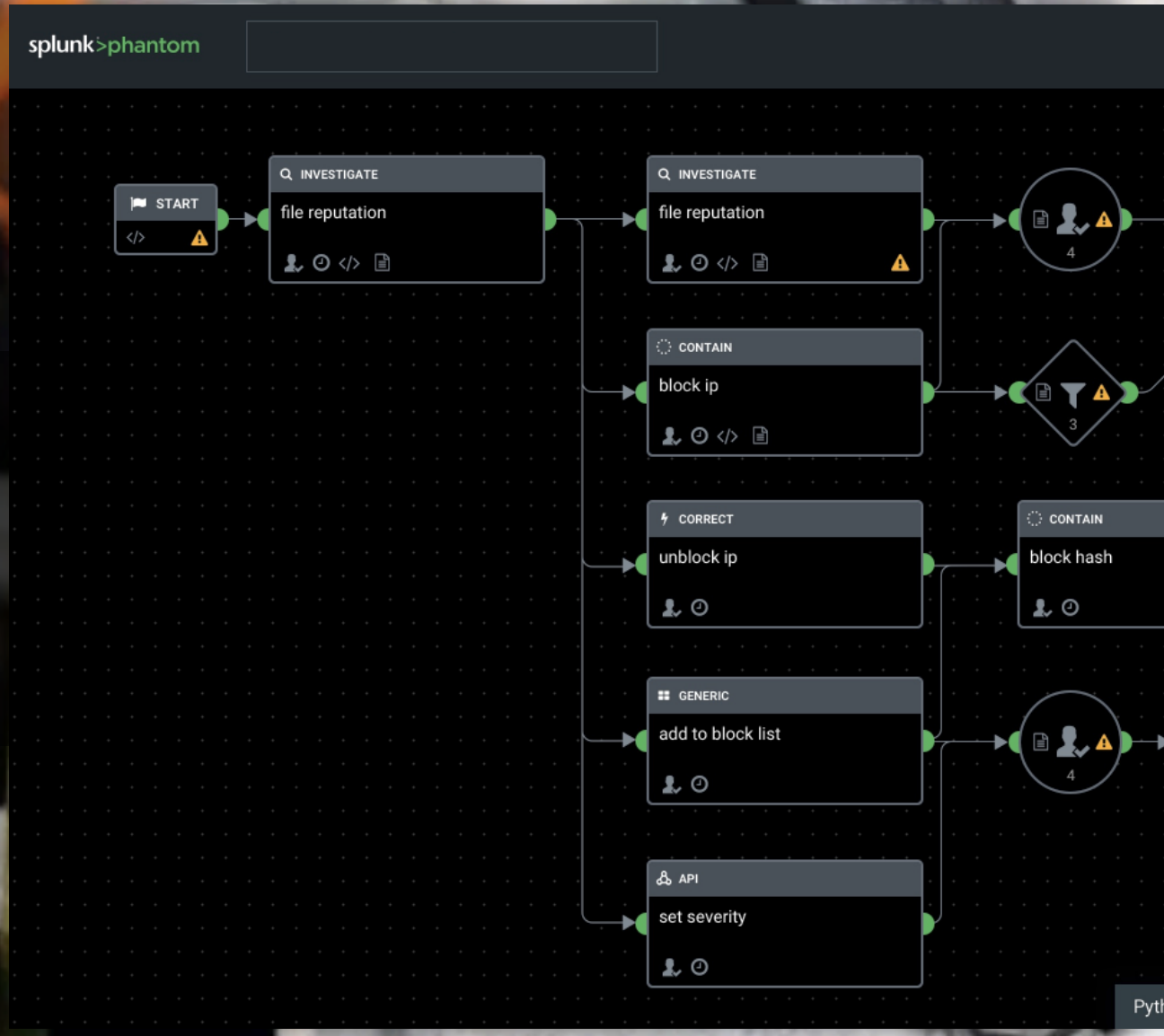
Creation Date
2017-10-12

Modification Date
2017-10-10

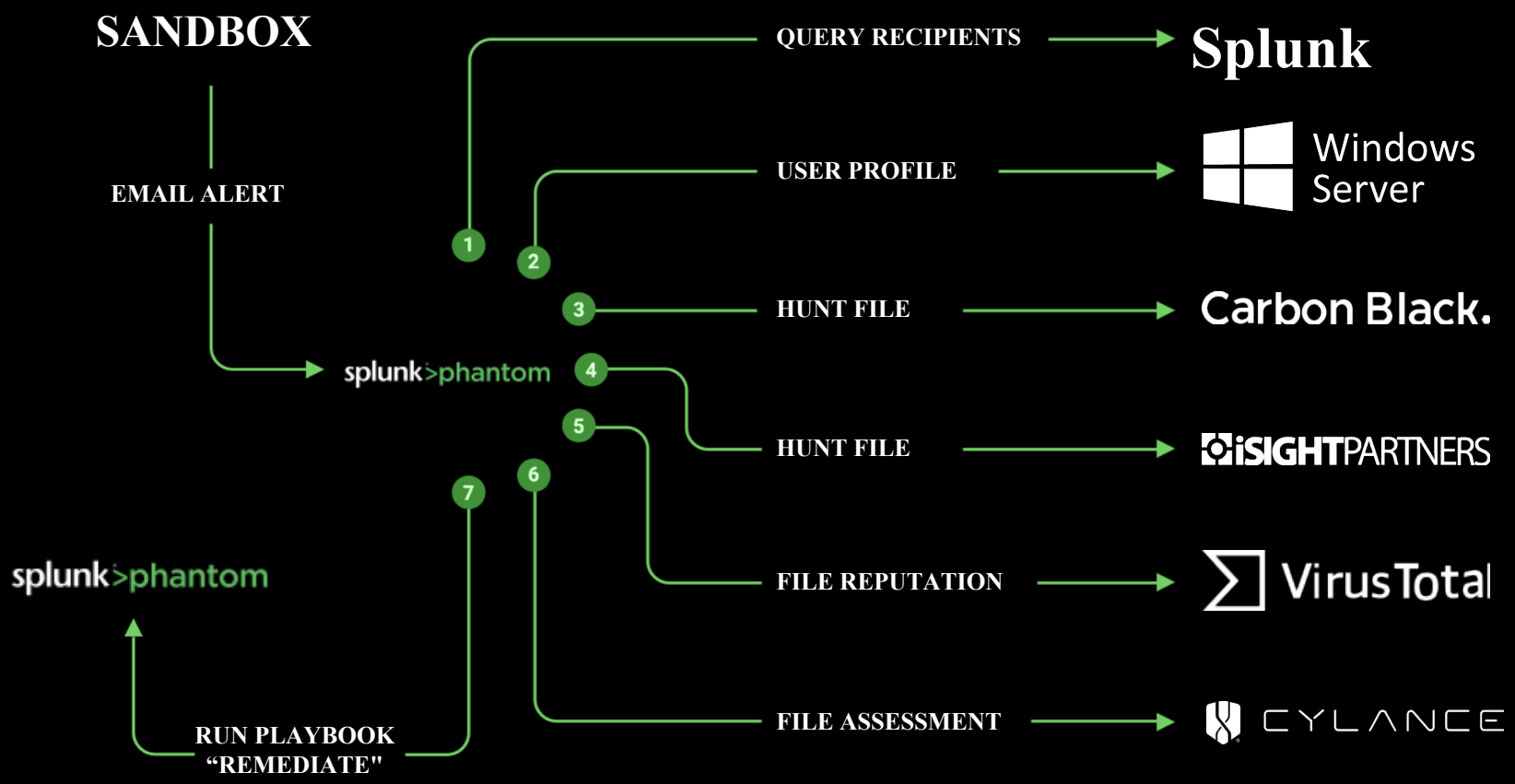


splunk> .conf18

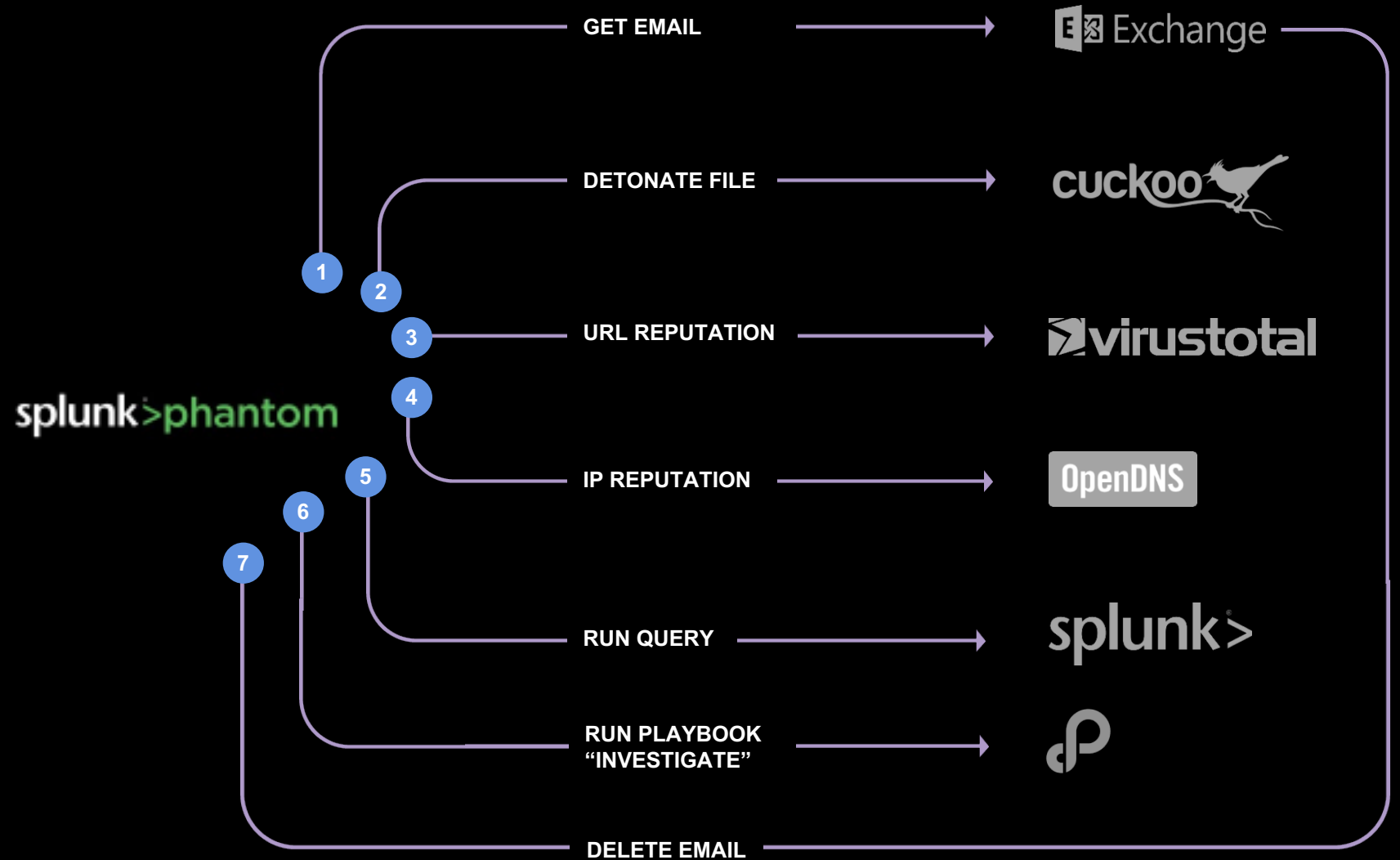
LET'S AUTOMATE!



Email Use Case

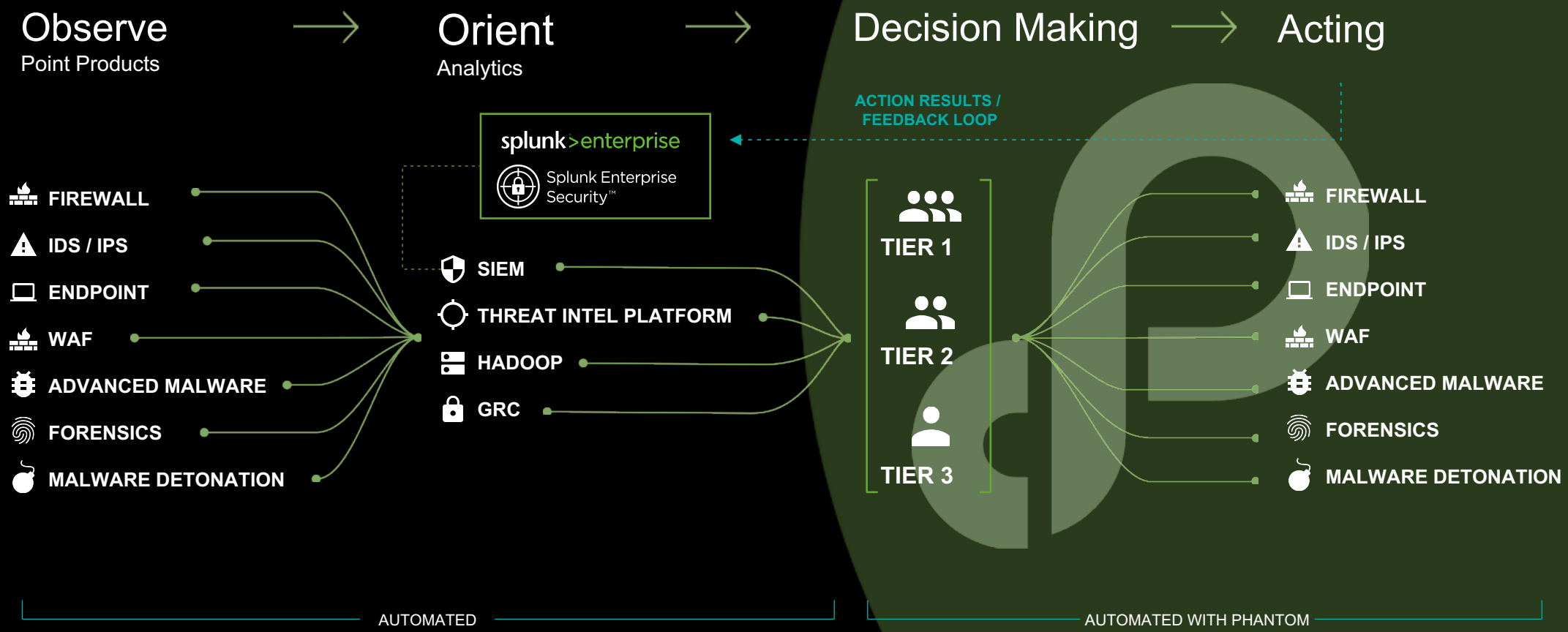


Phishing Use Case



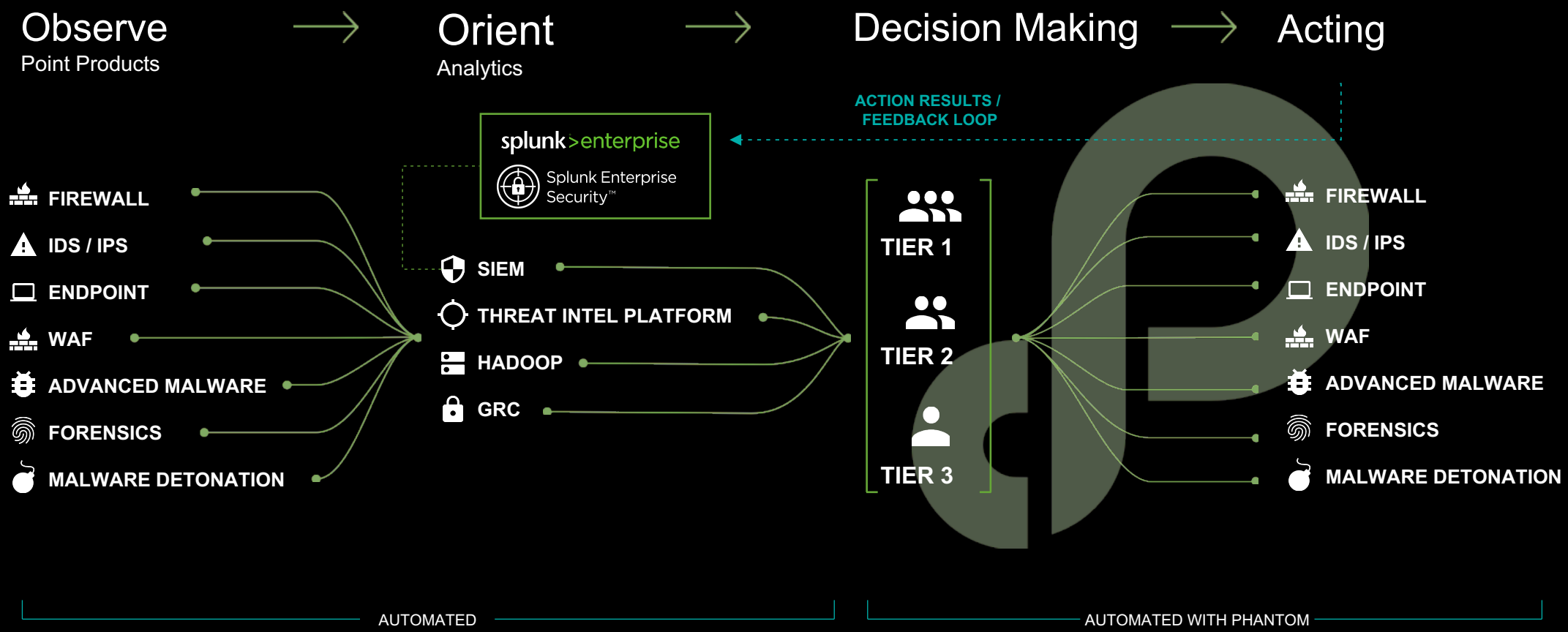
SOAR for Security Operations

Faster execution through the loop yields better security



SOAR for Security Operations

Faster execution through the loop yields better security



splunk> .conf18

Frameworks

Help you prioritize

CIS 20

Center for Internet Security Critical Security Controls for Effective Cyber Defense

ATT&CK

MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) model

Diamond

"Diamond Model of Intrusion Analysis," Center for Cyber Threat Intelligence and Threat Research

splunk> .conf18

Splunk Security Specialists

We're here to help make you a big winner

splunk> .conf18

Splunk Security Specialists

We're here to help make you a big winner

splunk> .conf18

Splunk Security Specialists

We're here to help

Workshops

- Lunch and Learn
  - Splunk Enterprise for Security SPL
- Investigating with Splunk
  - Splunk Enterprise and SA Investigator
- ES Hands on
  - Enterprise Security walk through with Notable Events and workflow investigations

Splunk Security Specialists

We're here to help

Workshops

- Lunch and Learn
  - Splunk Enterprise for Security SPL
- Investigating with Splunk
  - Splunk Enterprise and SA Investigator
- ES Hands on
  - Enterprise Security walk through with Notable Events and workflow investigations

Splunk Security Specialists

We're here to help

Workshops

- Lunch and Learn
  - Splunk Enterprise for Security SPL
- Investigating with Splunk
  - Splunk Enterprise and SA Investigator
- ES Hands on
  - Enterprise Security walk through with Notable Events and workflow investigations

Splunk Security Specialists

We're here to help

Workshops

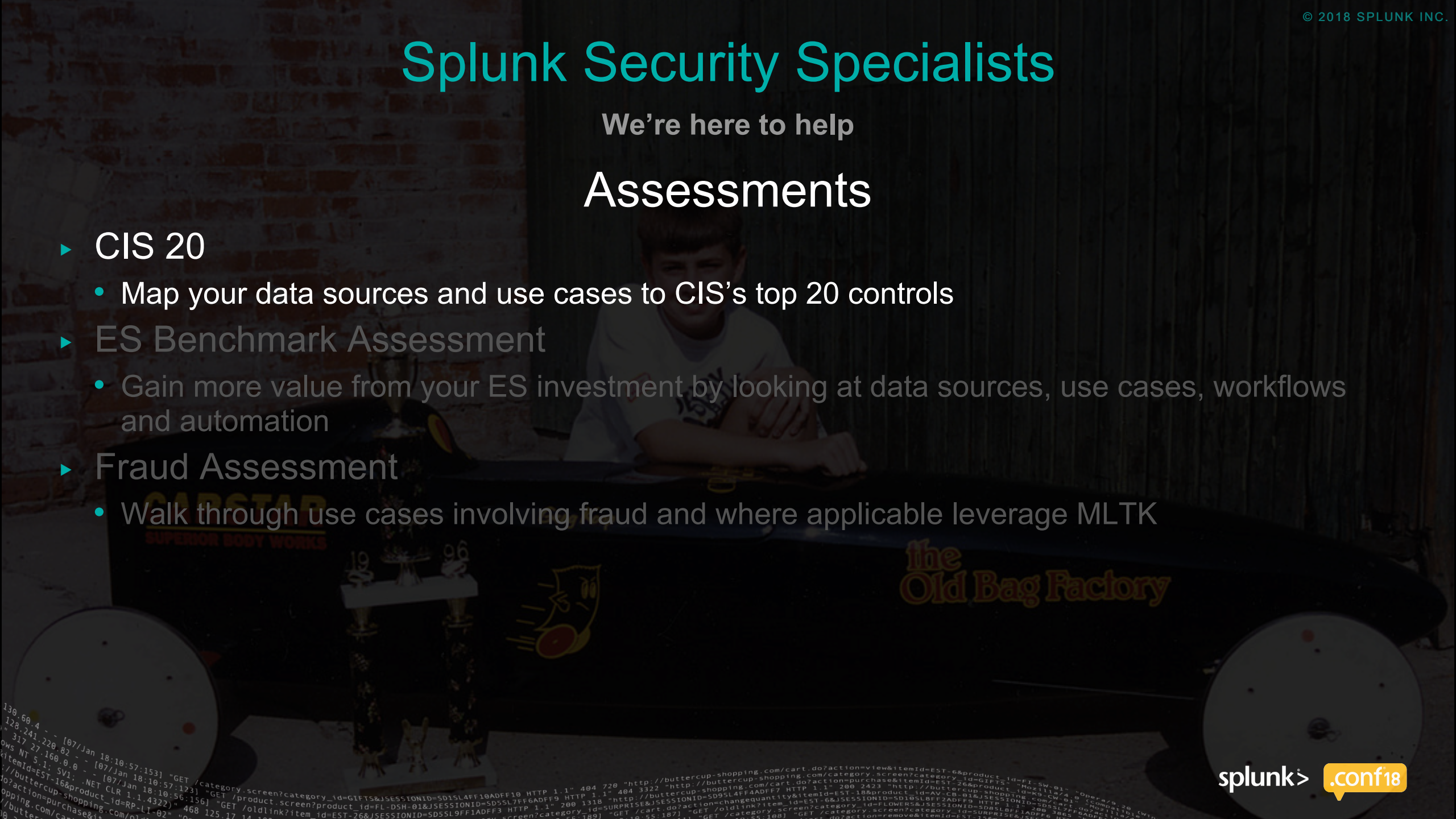
- Lunch and Learn
  - Splunk Enterprise for Security SPL
- Investigating with Splunk
  - Splunk Enterprise and SA Investigator
- ES Hands on
  - Enterprise Security walk through with Notable Events and workflow investigations

Splunk Security Specialists

We're here to help

Assessments

- CIS 20
  - Map your data sources and use cases to CIS's top 20 controls
- ES Benchmark Assessment
  - Gain more value from your ES investment by looking at data sources, use cases, workflows and automation
- Fraud Assessment
  - Walk through use cases involving fraud and where applicable leverage MLTK



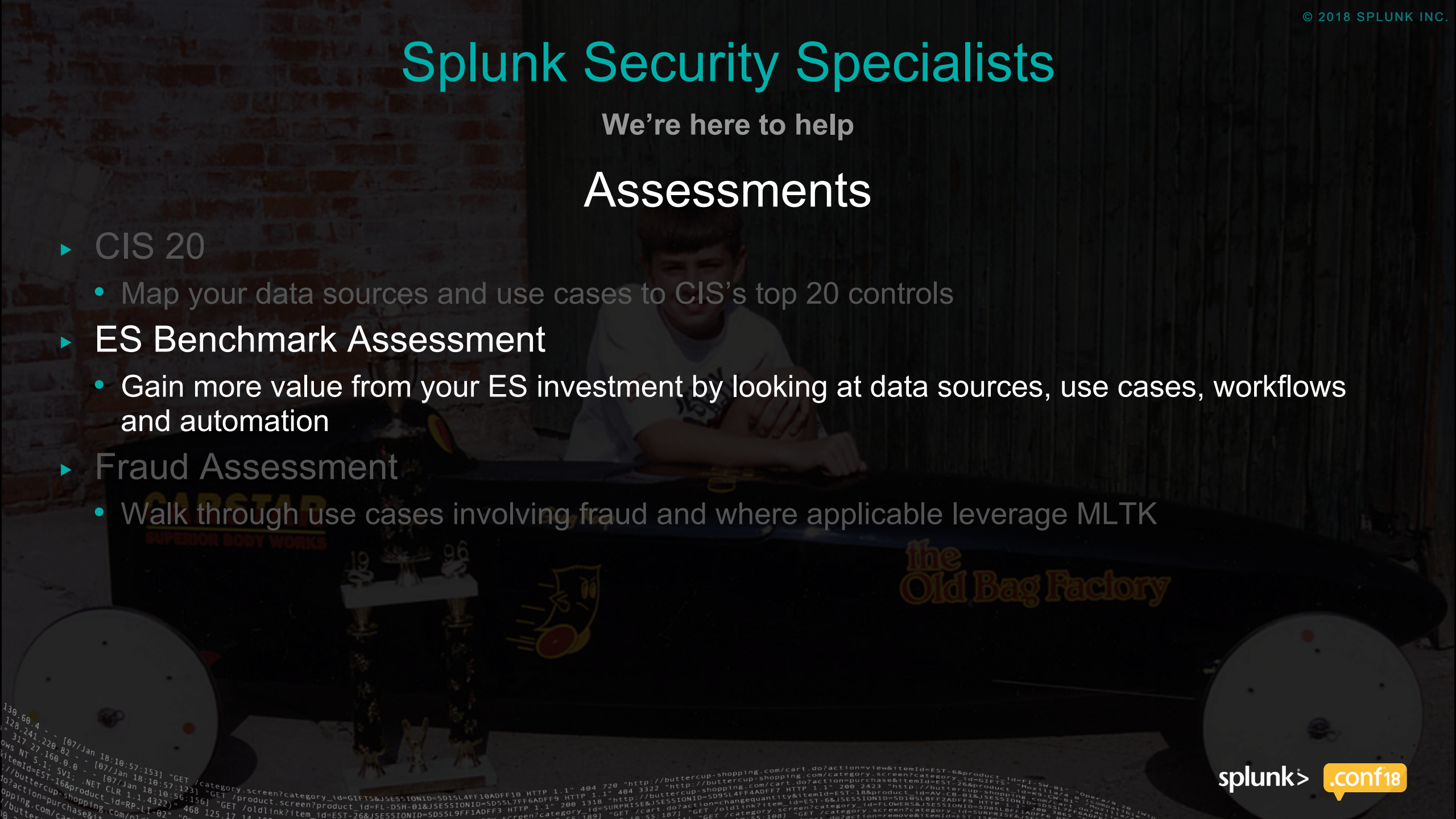
splunk> .conf18

Splunk Security Specialists

We're here to help

Assessments

- CIS 20
  - Map your data sources and use cases to CIS's top 20 controls
- ES Benchmark Assessment
  - Gain more value from your ES investment by looking at data sources, use cases, workflows and automation
- Fraud Assessment
  - Walk through use cases involving fraud and where applicable leverage MLTK

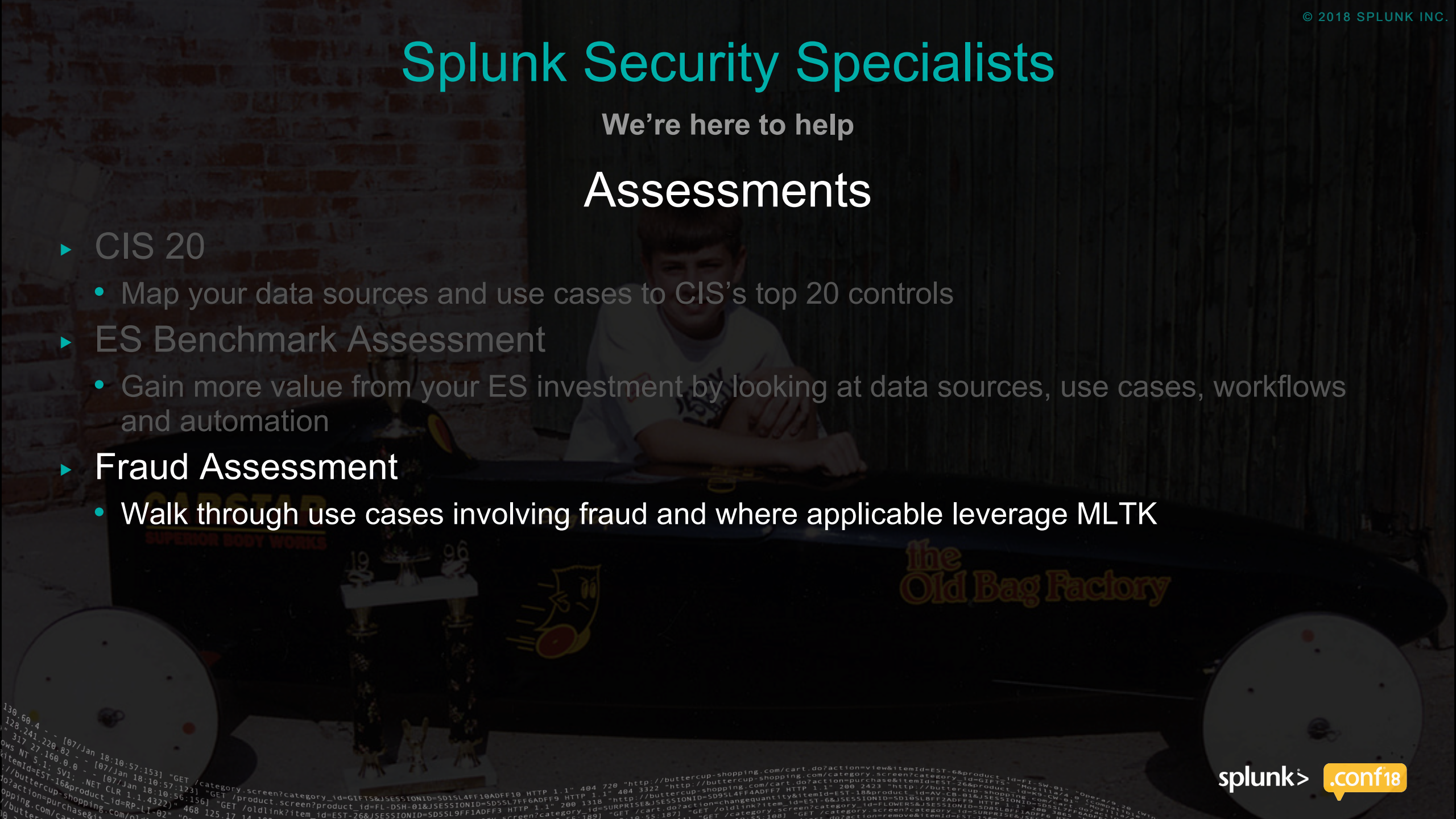


Splunk Security Specialists

We're here to help

Assessments

- CIS 20
  - Map your data sources and use cases to CIS's top 20 controls
- ES Benchmark Assessment
  - Gain more value from your ES investment by looking at data sources, use cases, workflows and automation
- Fraud Assessment
  - Walk through use cases involving fraud and where applicable leverage MLTK



splunk> .conf18

Splunk Security Specialists

We're here to help

Assessments

- CIS 20
  - Map your data sources and use cases to CIS's top 20 controls
- ES Benchmark Assessment
  - Gain more value from your ES investment by looking at data sources, use cases, workflows and automation
- Fraud Assessment
  - Walk through use cases involving fraud and where applicable leverage MLTK

Splunk Recommendations

(note: can be accelerated with PS)

Short Term (3 Months)

- ✓ Review existing ES rules to look for output codes in Windows events to suppress
- ✓ Install ES Content Update (ESCU) and evaluate high value use cases to enable
- ✓ Install Security Essentials and evaluate use cases
- ✓ Get data from FW in renewables flowing into Splunk
- ✓ Install ES Health Check app

3mo

Splunk Recommendations

(note: can be accelerated with PS)

Short Term (3 Months)

- ✓ Review existing ES rules to look for output codes in Windows events to suppress
- ✓ Install ES Content Update (ESCU) and evaluate high value use cases to enable
- ✓ Install Security Essentials and evaluate use cases
- ✓ Get data from FW in renewables flowing into Splunk
- ✓ Install ES Health Check app

3mo

Mid Term (6 Months)

- ✓ Add assets and identities data to be able to to effectively use the investigator workbench
- ✓ Ingest data from all Domain Controllers
- ✓ Ingest data for DNS
- ✓ Have team go through Splunk Fundamentals 2 and advanced search and reporting
- ✓ Add vuln scanner IPs to whitelist

6mo

Splunk Recommendations

(note: can be accelerated with PS)

Short Term (3 Months)

- ✓ Review existing ES rules to look for output codes in Windows events to suppress
- ✓ Install ES Content Update (ESCU) and evaluate high value use cases to enable
- ✓ Install Security Essentials and evaluate use cases
- ✓ Get data from FW in renewables flowing into Splunk
- ✓ Install ES Health Check app

3mo

Mid Term (6 Months)

- ✓ Add assets and identities data to be able to to effectively use the investigator workbench
- ✓ Ingest data from all Domain Controllers
- ✓ Ingest data for DNS
- ✓ Have team go through Splunk Fundamentals 2 and advanced search and reporting
- ✓ Add vuln scanner IPs to whitelist

6mo

Long Term (9 Months)

- ✓ Create glass tables based on KPIs
- ✓ Begin using the machine learning toolkit capabilities for data driven anomaly detection
- ✓ Evolve hunting technique and processes
- ✓ Enable user access to broader internal community

9mo

Splunk Recommendations

(note: can be accelerated with PS)

Short Term (3 Months)

- ✓ Review existing ES rules to look for output codes in Windows events to suppress
- ✓ Install ES Content Update (ESCU) and evaluate high value use cases to enable
- ✓ Install Security Essentials and evaluate use cases
- ✓ Get data from FW in renewables flowing into Splunk
- ✓ Install ES Health Check app

3mo

Mid Term (6 Months)

- ✓ Add assets and identities data to be able to to effectively use the investigator workbench
- ✓ Ingest data from all Domain Controllers
- ✓ Ingest data for DNS
- ✓ Have team go through Splunk Fundamentals 2 and advanced search and reporting
- ✓ Add vuln scanner IPs to whitelist

6mo

Long Term (9 Months)

- ✓ Create glass tables based on KPIs
- ✓ Begin using the machine learning toolkit capabilities for data driven anomaly detection
- ✓ Evolve hunting technique and processes
- ✓ Enable user access to broader internal community

9mo

Strategic

- ✓ Develop “Board-ready” reports and dashboards to demonstrate bottom-line contribution of security
- ✓ Create value across organization using existing data
  - ✓ IT Ops, Fraud Detection, Insider Threat
  - ✓ Business Operations Center

S


VIPER

Thank You

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