Pull Up Your SOCs | v. 2.0

A Splunk Primer on Building Your Security Operations

Dimitri McKay | Staff Security Architect | Splunk

CONF19

image compliments of harperandjane on ets

If I said I have the expressed *written* permission of Marvel Entertainment, Fox and Disney…

If I said I have the expressed *written* permission of Marvel Entertainment, Fox and Disney…

I'd be lying.

If I said I have the expressed *written* permission of Marvel Entertainment, Fox and Disney…

I'd be lying. :)

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.

Dimitri McKay | Staff Security Architect | Splunk | CISSP | CCSK | LOLZ

- 22 years of net/system security experience.
- Former pen-tester, corporate security slacker for a search engine and plus sized hand model.
- Enjoys making poor decisions, breaking things and disappointing my parents.
- Current role on the Global Security Specialist team focuses on security strategy for the fortune 50, evangelism and asking dumb questions.
- Currently interested in machine learning for home automation products, which will eventually become self aware and enslave humanity.
- If you read this far, you get 10 cool points. ☺

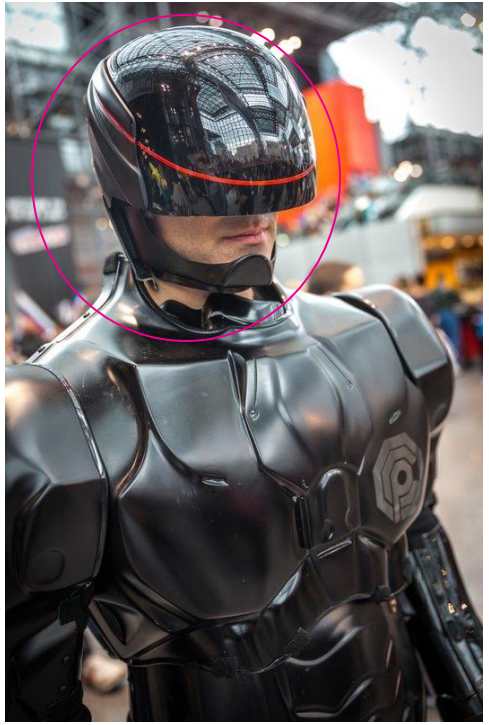
@dimitrimckay

HOW MUCH OF A FAN?

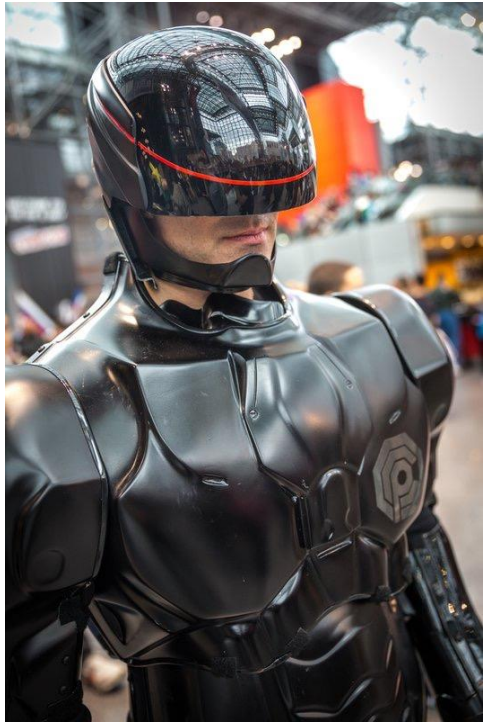
HOW MUCH OF A FAN?

HOW M
OF A F

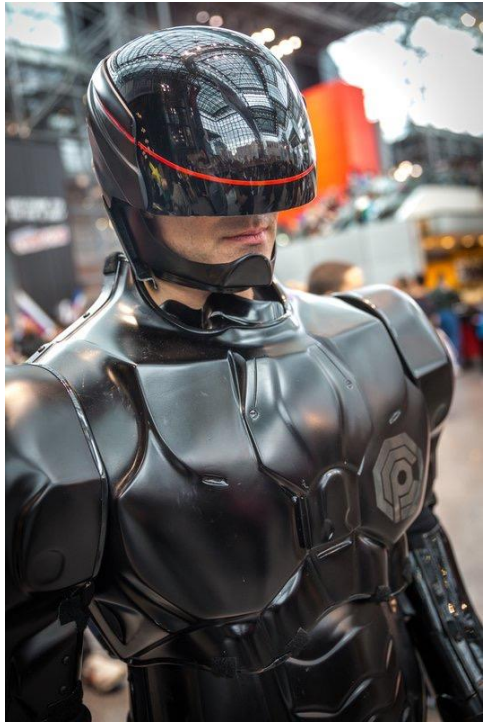
HOW M
OF A F



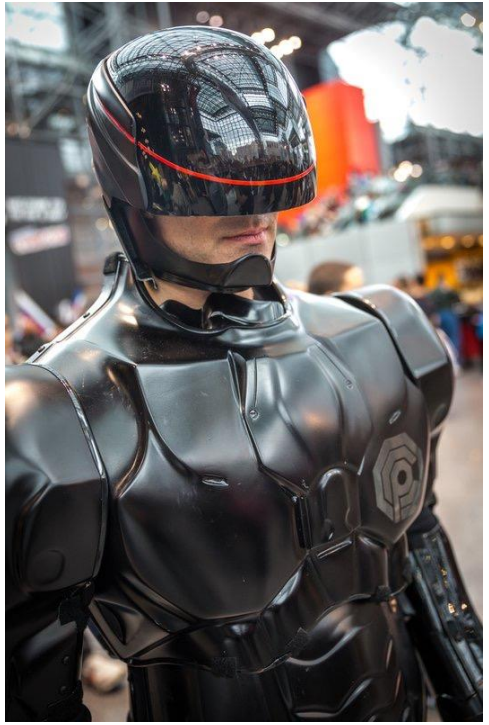
HOW M
OF A F



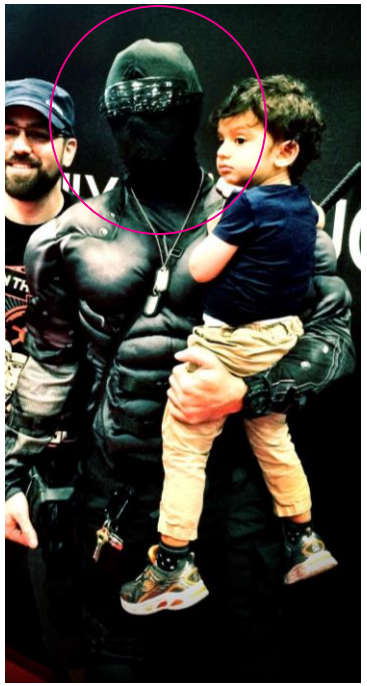
HOW M
OF A F

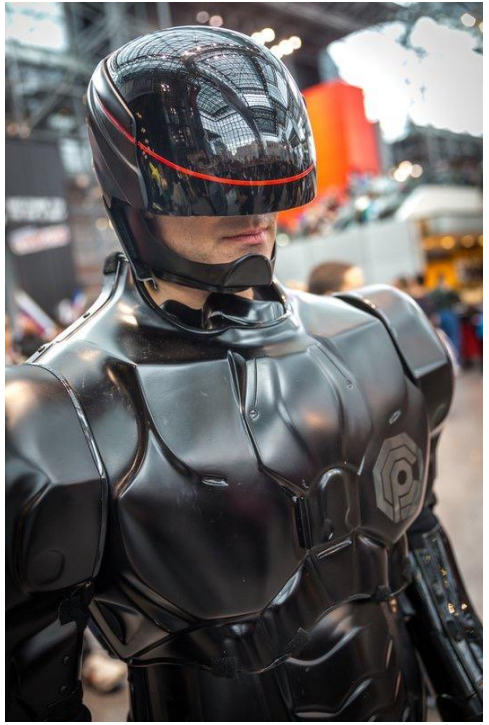


HOW M
OF A F



HOW M
OF A F





I'M **THAT** MUCH OF A FAN

splunk> .conf19

Worst. Cosplay. Ever.

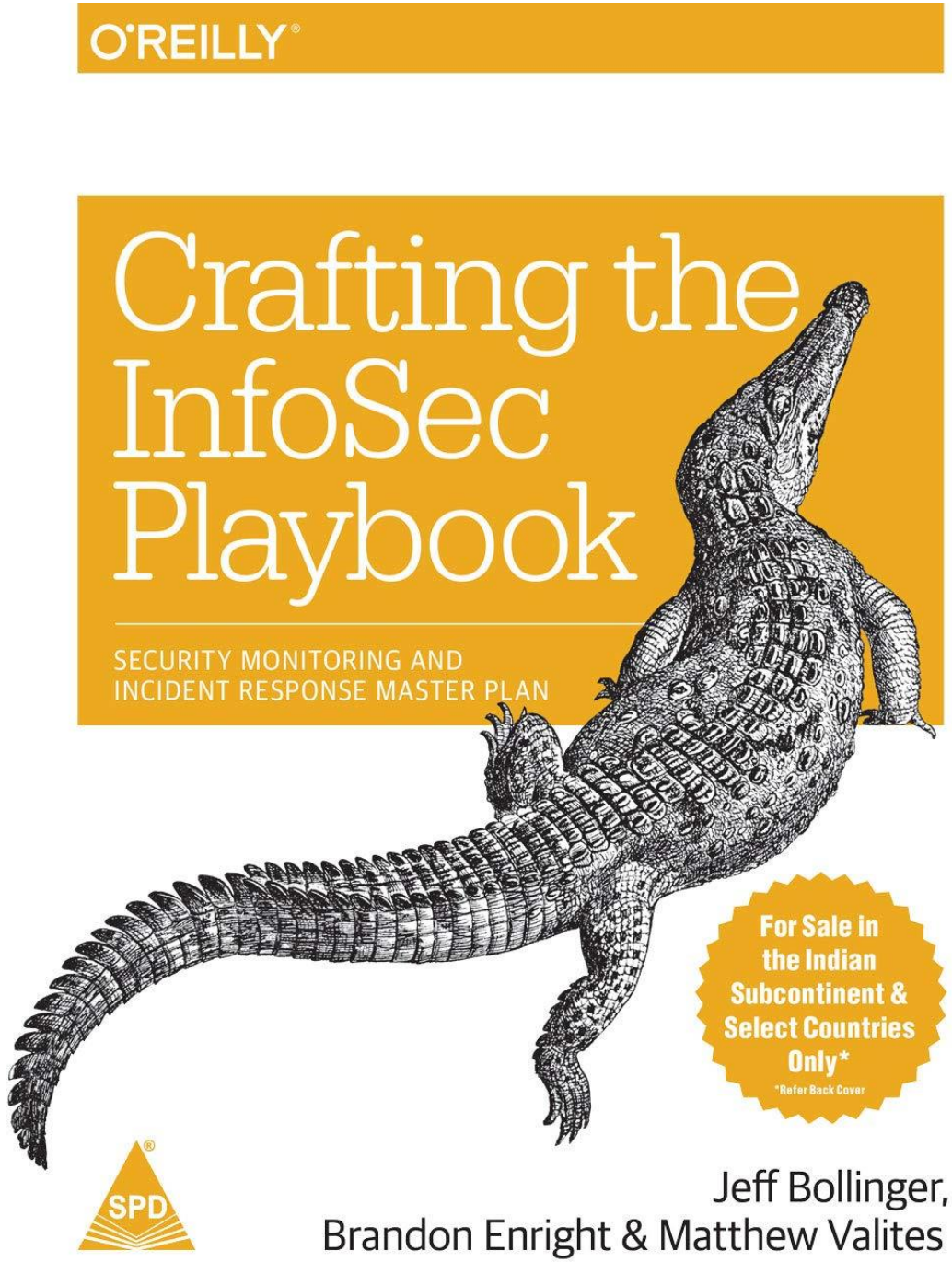
CREDIT WHERE CREDIT IS DUE

splunk> .conf19

CREDIT WHERE CREDIT IS DUE

splunk> .conf19

CREDIT WHERE CREDIT IS DUE



FULLY BALANCED SOC

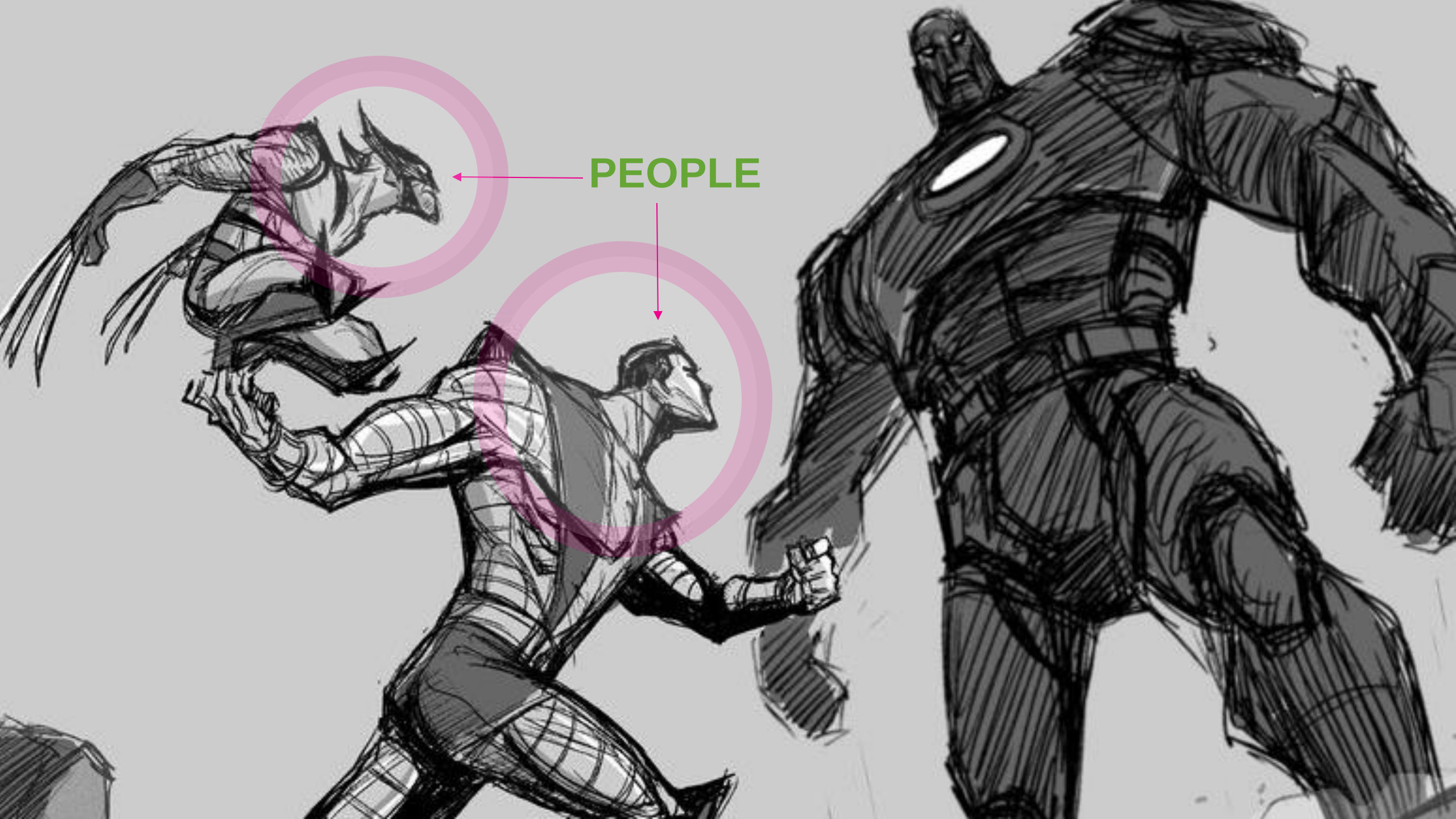
Image compliments of Disney


SNAP

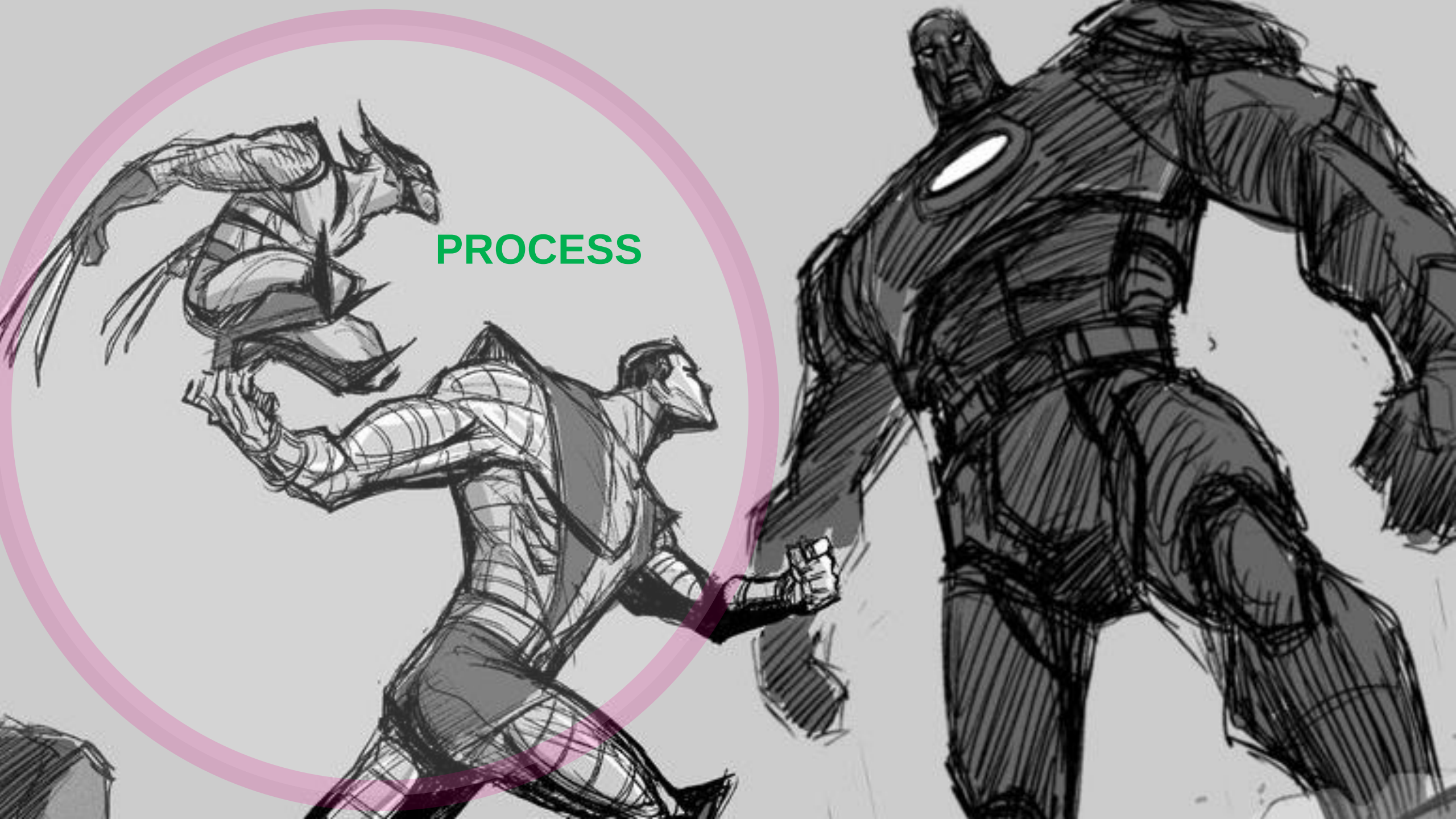
WHAT DO I KNOW?

Image courtesy of sensacine.com

WHAT IS A SOC?

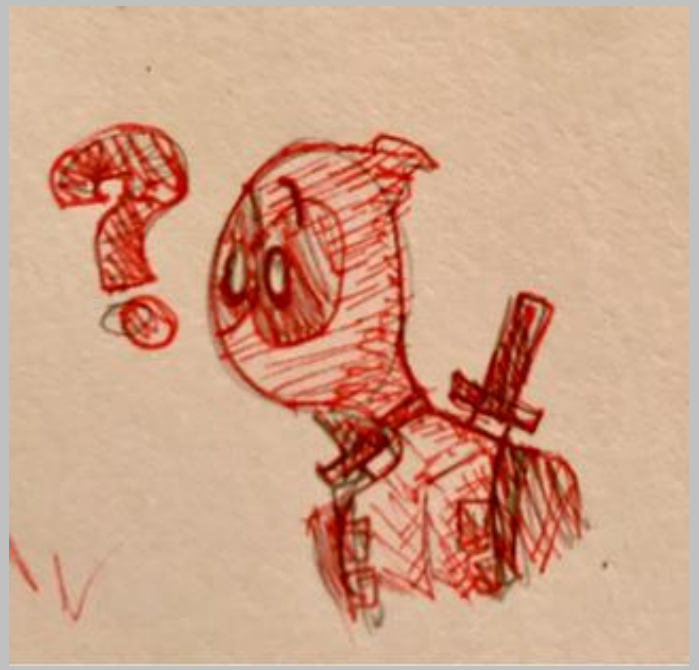

PEOPLE

PROCESS

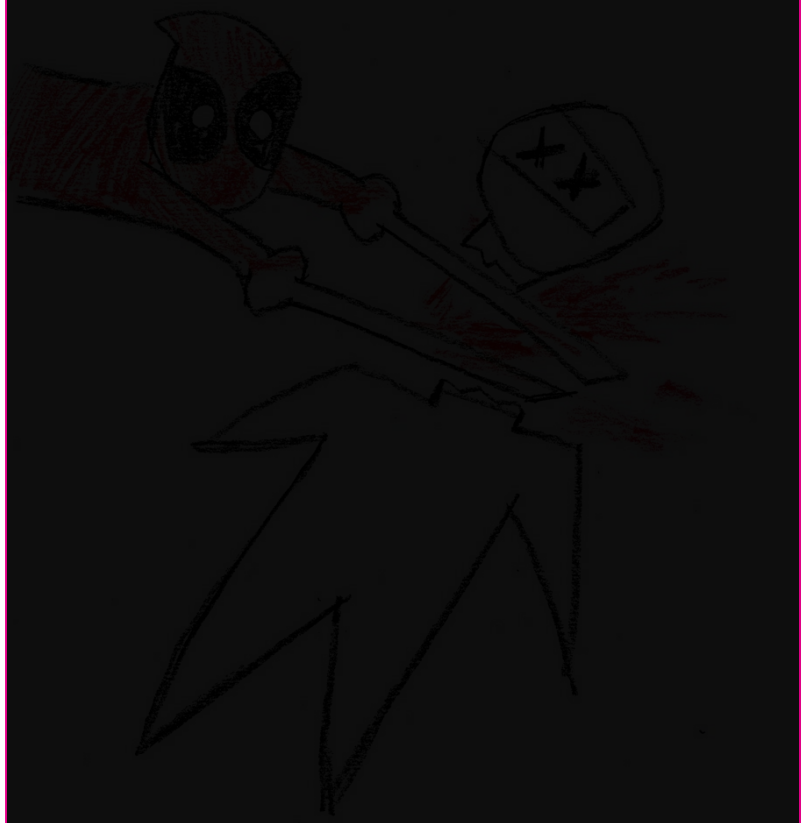



TECH

DETECT



RESPOND



DETECT

RESPOND

DETECT

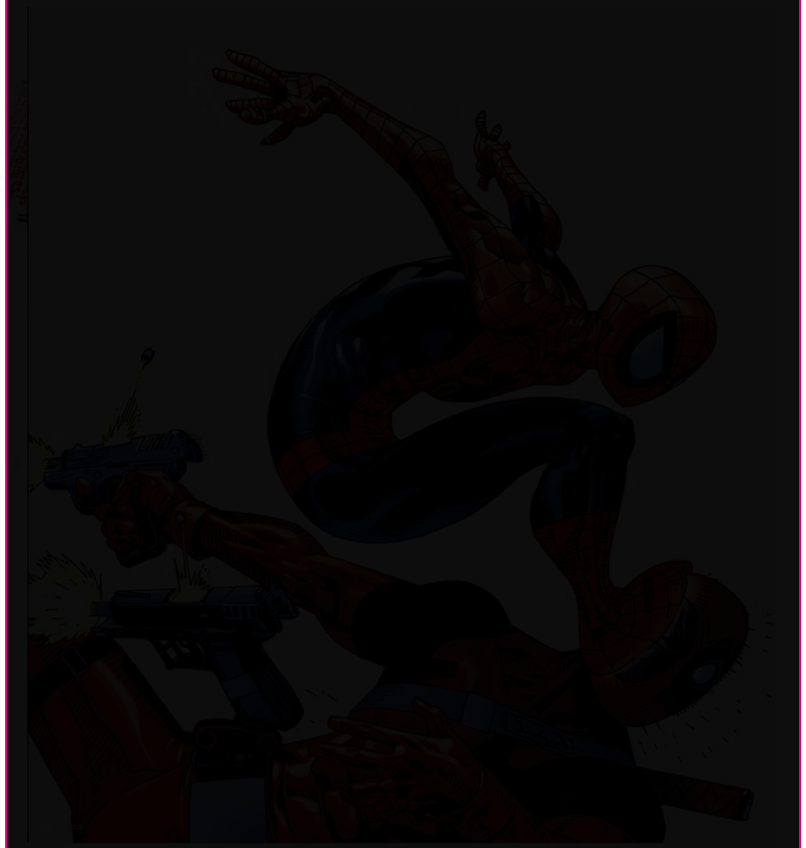
RESPOND

PREVENT

WHAT IS A SOC?

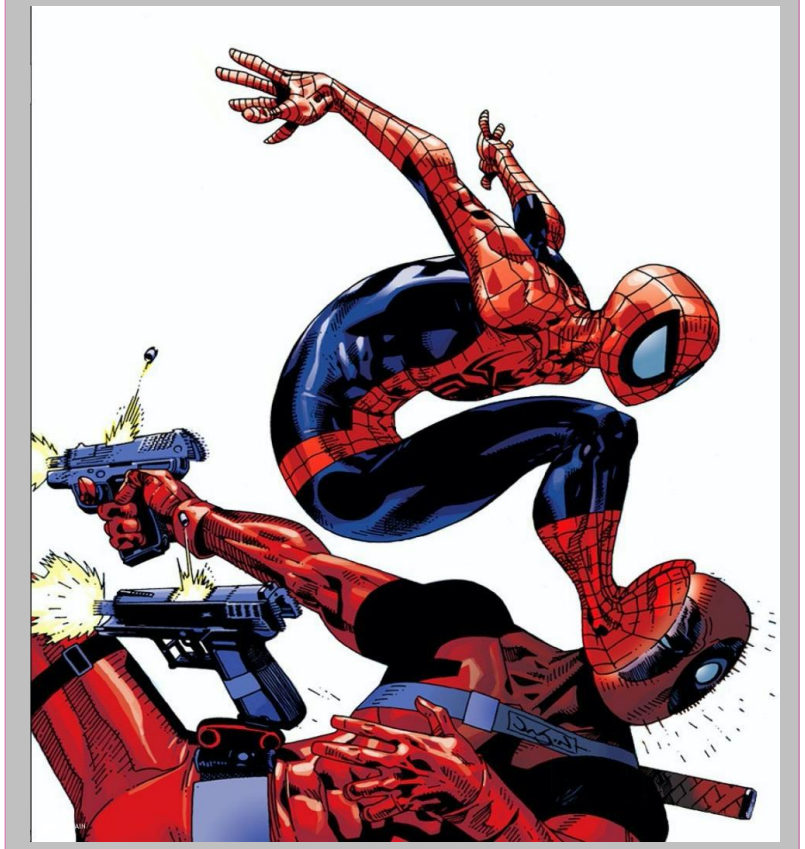
DETECT

RESPOND



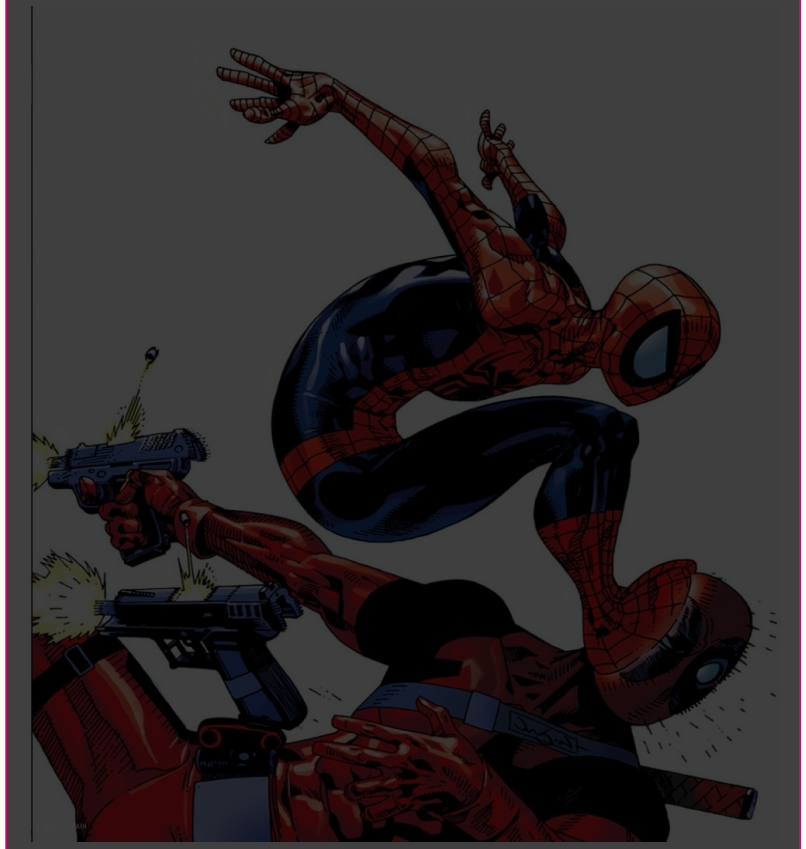
DETECT

RESPOND



DETECT

RESPOND



PREVENT

Program Maturity

Program Maturity

Phase 1

Program Maturity

Phase 1

Program Maturity

Phase 1

Program Maturity

Phase 2

Program Maturity

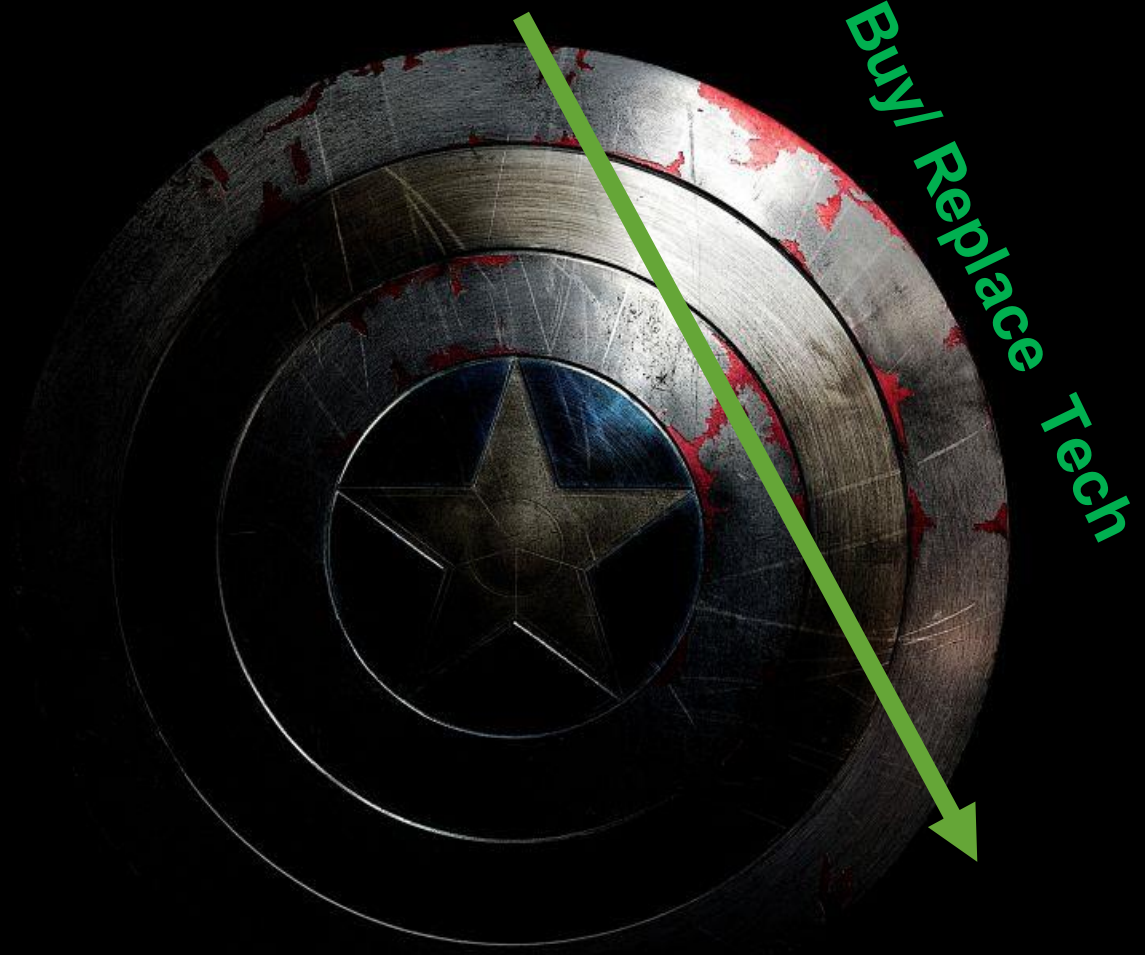
Phase 2

Program Maturity

Phase 2

Program Maturity

Phase 3



Program Maturity

Phase 3

Program Maturity

Phase 3

WHAT IS YOUR CHARTER?

Data Breaches
Law Enforcement Investigation
Human Resources investigation
Legal investigation
Kill Thanos
Compromised systems
Denial of Service
Credential compromise
Phishing
Vulnerability management
Reverse the snap
Lost device
Stolen device
Malware infection
Malware outbreak
Avenge Black Window
DoX
Cloud Partner compromise
External vulnerability notification
Nation State attacks
Fraudulent use of services
Supply chain compromise
Secure funding
Insurance mandate
Regulatory compliance
Growth
Boardroom conversation
Showcase SOC

Data Breaches
Law Enforcement Investigation
Human Resources investigation
Legal investigation

Kill Thanos
Compromised systems
Denial of Service
Credential compromise
Phishing
Vulnerability management

Reverse the snap
Lost device
Stolen device
Malware infection
Malware outbreak

Avenge Black Window
DoX
Cloud Partner compromise
External vulnerability notification
Nation State attacks
Fraudulent use of services
Supply chain compromise
Secure funding
Insurance mandate
Regulatory compliance
Growth
Boardroom conversation
Showcase SOC

People

HIRE SMART PEOPLE

HIRE SMART PEOPLE

SECURITY KNOWLEDGE
COMPUTER NETWORKING
APPLICATION LAYER PROTOCOLS
DATABASES AND QUERY LANGUAGES
UNIX
WINDOWS
BASIC PARSING
COMMAND LINE FAMILIARITY
SECURITY MONITORING TOOLS
CODING/SCRIPTING
REGULATORY COMPLIANCE
SECURITY CLEARANCE
COMMUNICATION
WRITING
CRITICAL THINKING
PENETRATION TESTING
VULNERABILITY SCANNING
CREATIVITY
CURIOSITY
INVESTIGATIONS
MOTIVATION
TROUBLESHOOTING

HIRE SMART PEOPLE

SECURITY KNOWLEDGE
COMPUTER NETWORKING
APPLICATION LAYER PROTOCOLS
DATABASES AND QUERY LANGUAGES
UNIX
WINDOWS
BASIC PARSING
COMMAND LINE FAMILIARITY
SECURITY MONITORING TOOLS
CODING/SCRIPTING
REGULATORY COMPLIANCE
SECURITY CLEARANCE
COMMUNICATION
WRITING
CRITICAL THINKING
PENETRATION TESTING
VULNERABILITY SCANNING
CREATIVITY
CURIOSITY
INVESTIGATIONS
MOTIVATION
TROUBLESHOOTING

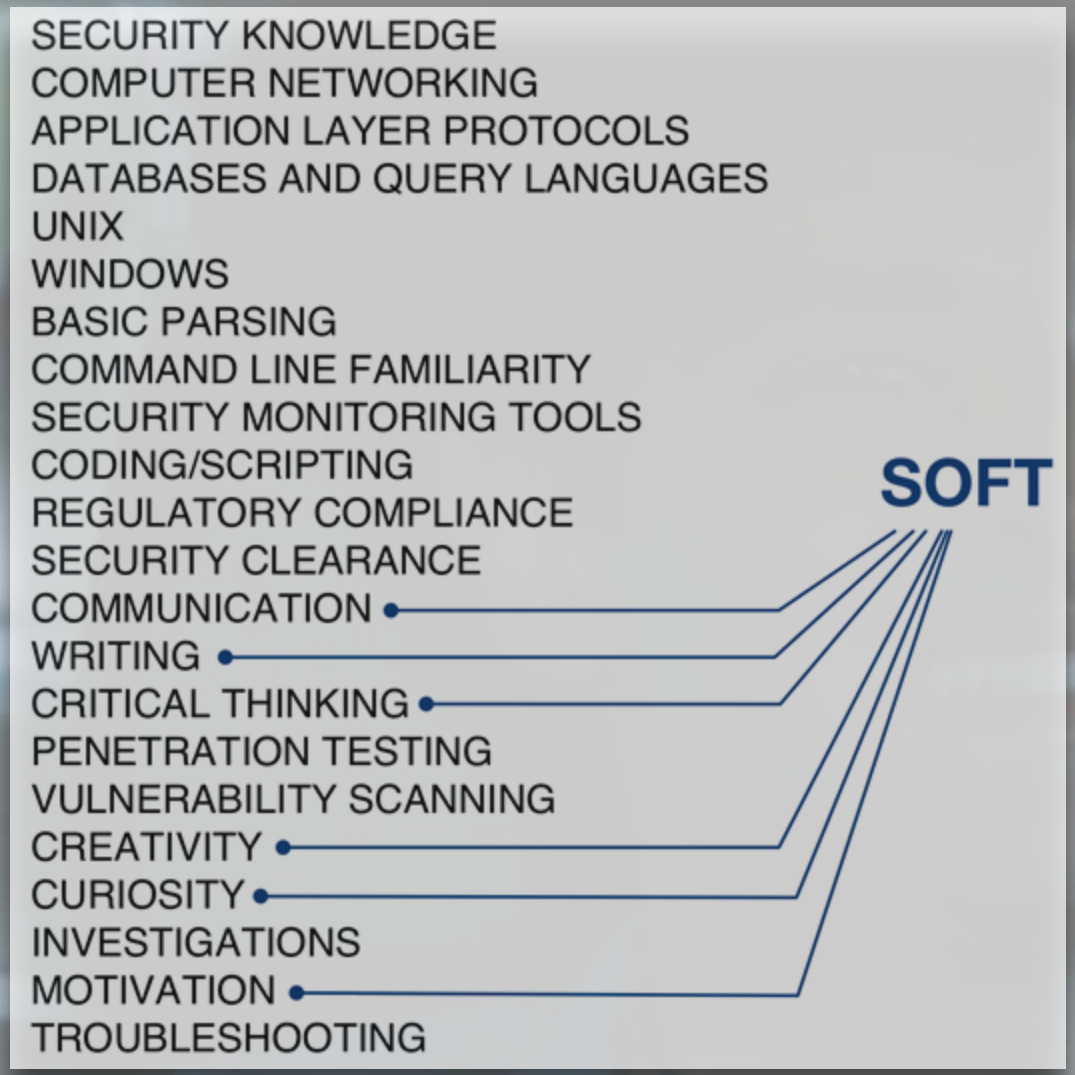
PEOPLE

HIRE SMART PEOPLE

splunk> .conf19

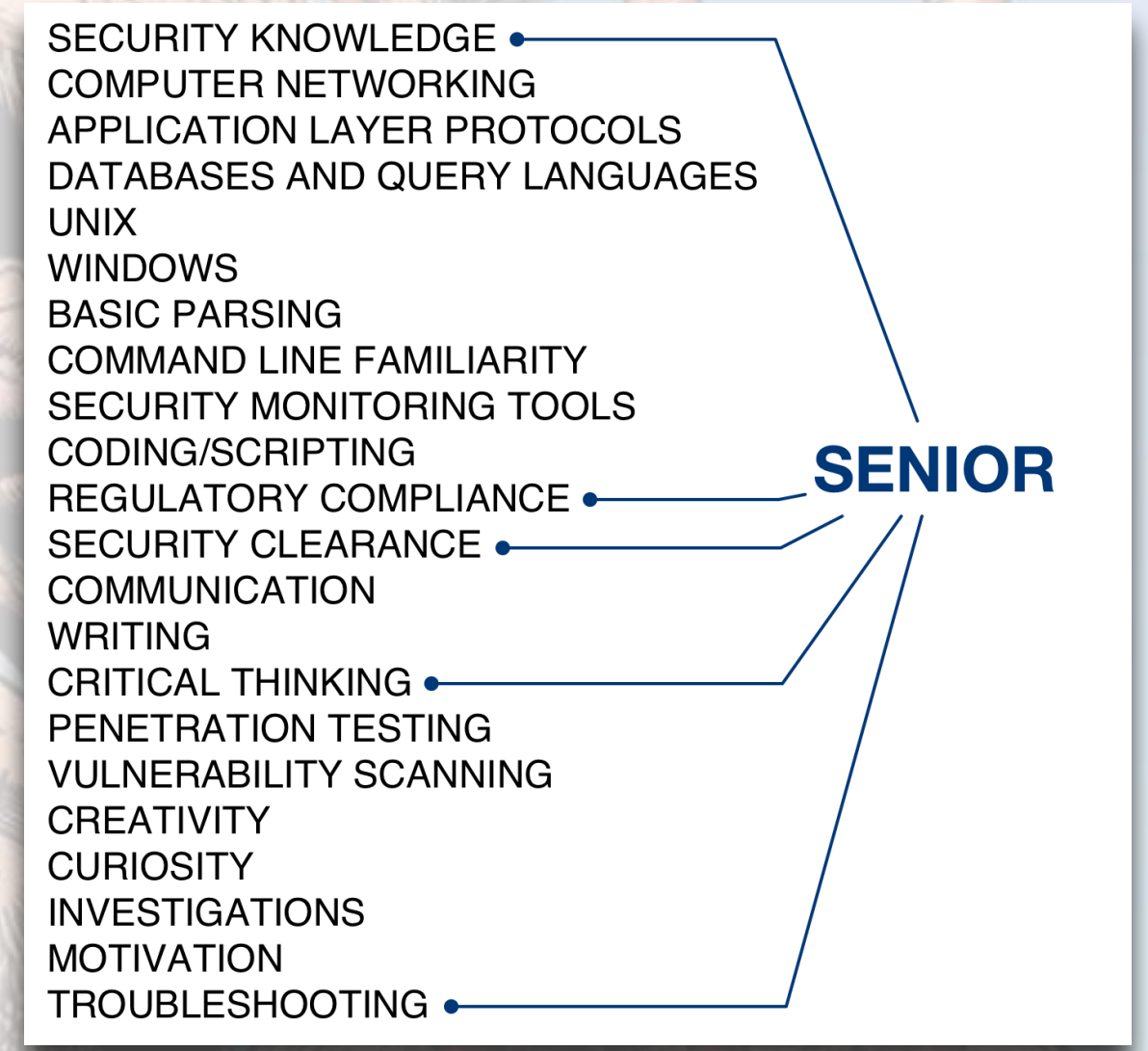
Image compliments of 20th Century Fox

HIRE SMART PEOPLE



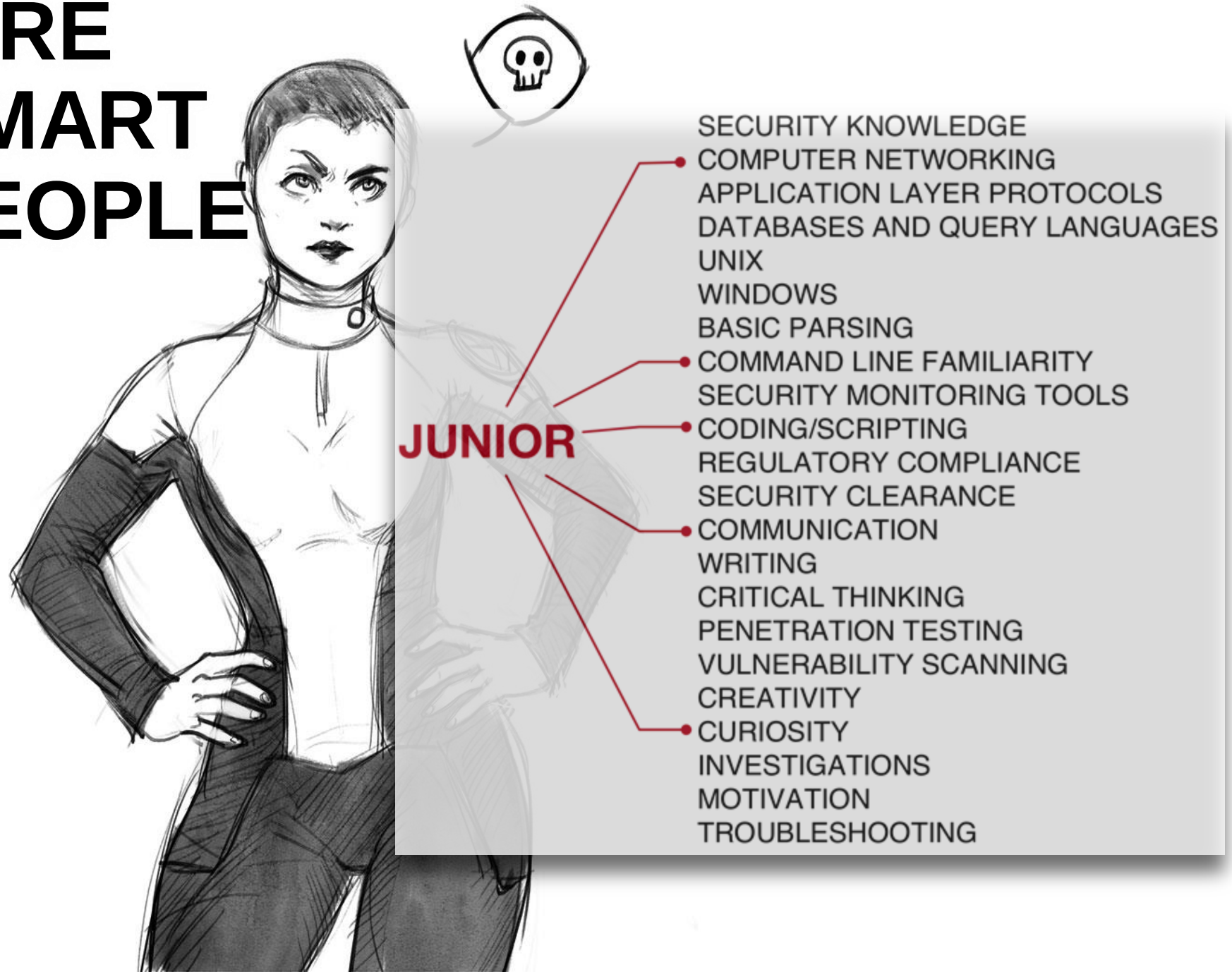
HIRE SMART PEOPLE

HIRE SMART PEOPLE



HIRE SMART PEOPLE

HIRE SMART PEOPLE



JUNIOR

- SECURITY KNOWLEDGE
- COMPUTER NETWORKING
- APPLICATION LAYER PROTOCOLS
- DATABASES AND QUERY LANGUAGES
- UNIX
- WINDOWS
- BASIC PARSING
- COMMAND LINE FAMILIARITY
- SECURITY MONITORING TOOLS
- CODING/SCRIPTING
- REGULATORY COMPLIANCE
- SECURITY CLEARANCE
- COMMUNICATION
- WRITING
- CRITICAL THINKING
- PENETRATION TESTING
- VULNERABILITY SCANNING
- CREATIVITY
- CURIOSITY
- INVESTIGATIONS
- MOTIVATION
- TROUBLESHOOTING

PEOPLE

HIRE SMART PEOPLE

splunk> .conf19

Image compliments of 20th Century Fox

HIRE SMART PEOPLE

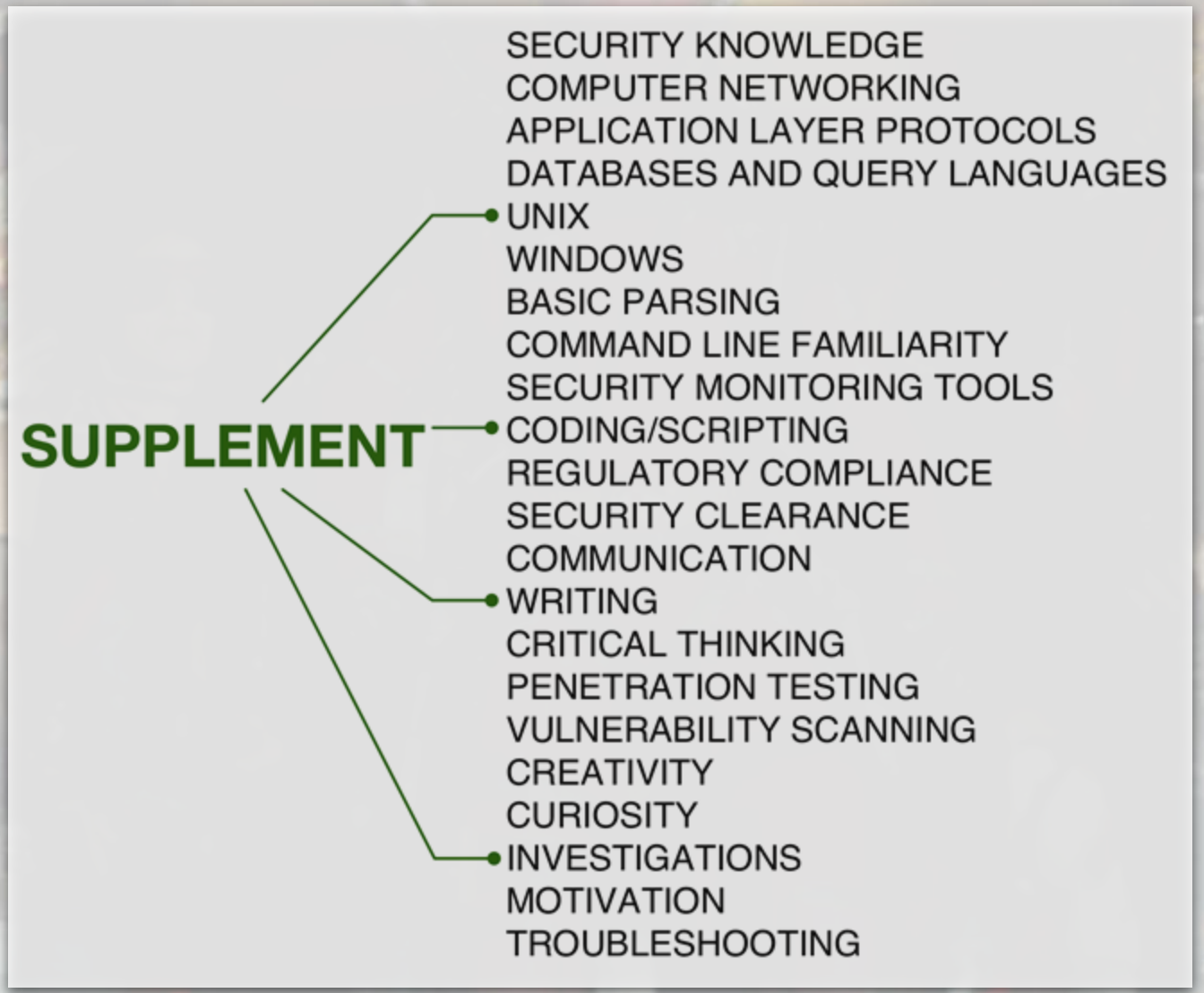


Image compliments of 20th Century Fox

PEOPLE

But… security people are hard to find…

PEOPLE

HIRE SMART PEOPLE

HIRE SMART PEOPLE

…and train them

Photo Compliments of https://www.deviantart.com/artofbarbs

PEOPLE

HIRE SMART PEOPLE

…and train them

TRAINEE

Photo Compliments of https://www.deviantart.com/artofbarbs

PEOPLE

JOURNEY STAGE 1

- SEC401: Security Essentials Bootcamp Style

  FOR610 for malware analysis.

  FOR578: Cyber Threat Intelligence

  MGT517: Managing Security Operations: Detection, Response, and Intelligence
- SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling
- MGT414: SANS Training Program for CISSP® Certification

  FOR572: Advanced Network Forensics and Analysis

  SEC511: Continuous Monitoring and Security Operations

  SEC555: SIEM with Tactical Analytics

HIRE SMART PEOPLE …and train them

JOURNEY STAGE 2

PEOPLE

SEC401: Security Essentials Bootcamp Style

FOR610 for malware analysis.

FOR578: Cyber Threat Intelligence

- MGT517: Managing Security Operations: Detection, Response, and Intelligence

SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling

MGT414: SANS Training Program for CISSP® Certification

FOR572: Advanced Network Forensics and Analysis

- SEC511: Continuous Monitoring and Security Operations

SEC555: SIEM with Tactical Analytics

HIRE SMART PEOPLE …and train them

JOURNEY STAGE 3

PEOPLE

SEC401: Security Essentials Bootcamp Style

- FOR610 for malware analysis.
- FOR578: Cyber Threat Intelligence

MGT517: Managing Security Operations: Detection, Response, and Intelligence

SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling

MGT414: SANS Training Program for CISSP® Certification

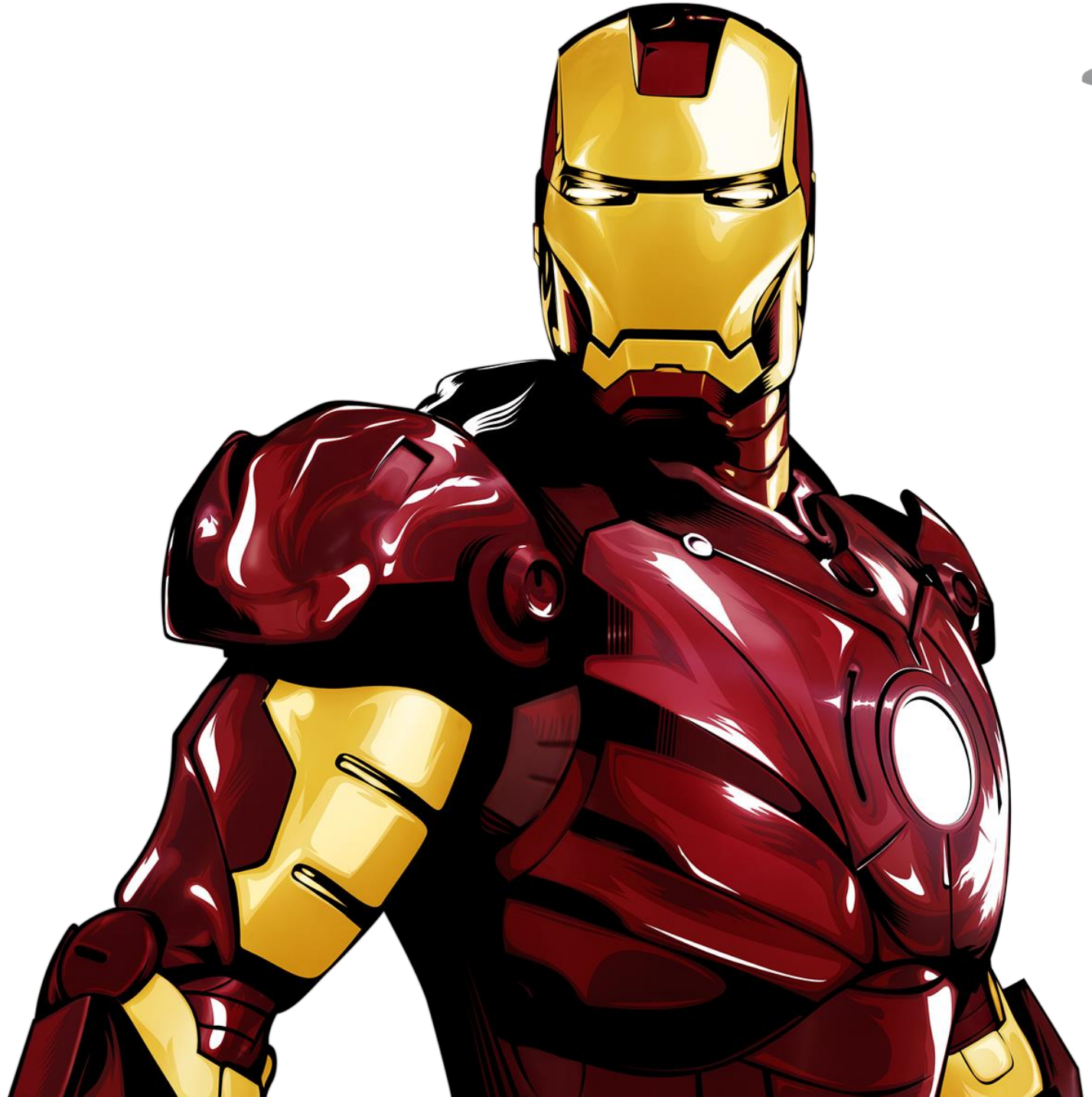
- FOR572: Advanced Network Forensics and Analysis

SEC511: Continuous Monitoring and Security Operations

- SEC555: SIEM with Tactical Analytics

HIRE SMART PEOPLE …and train them

PEOPLE



YOU


PEOPLE
YOUR TEAM


PEOPLE
BAD GUYS

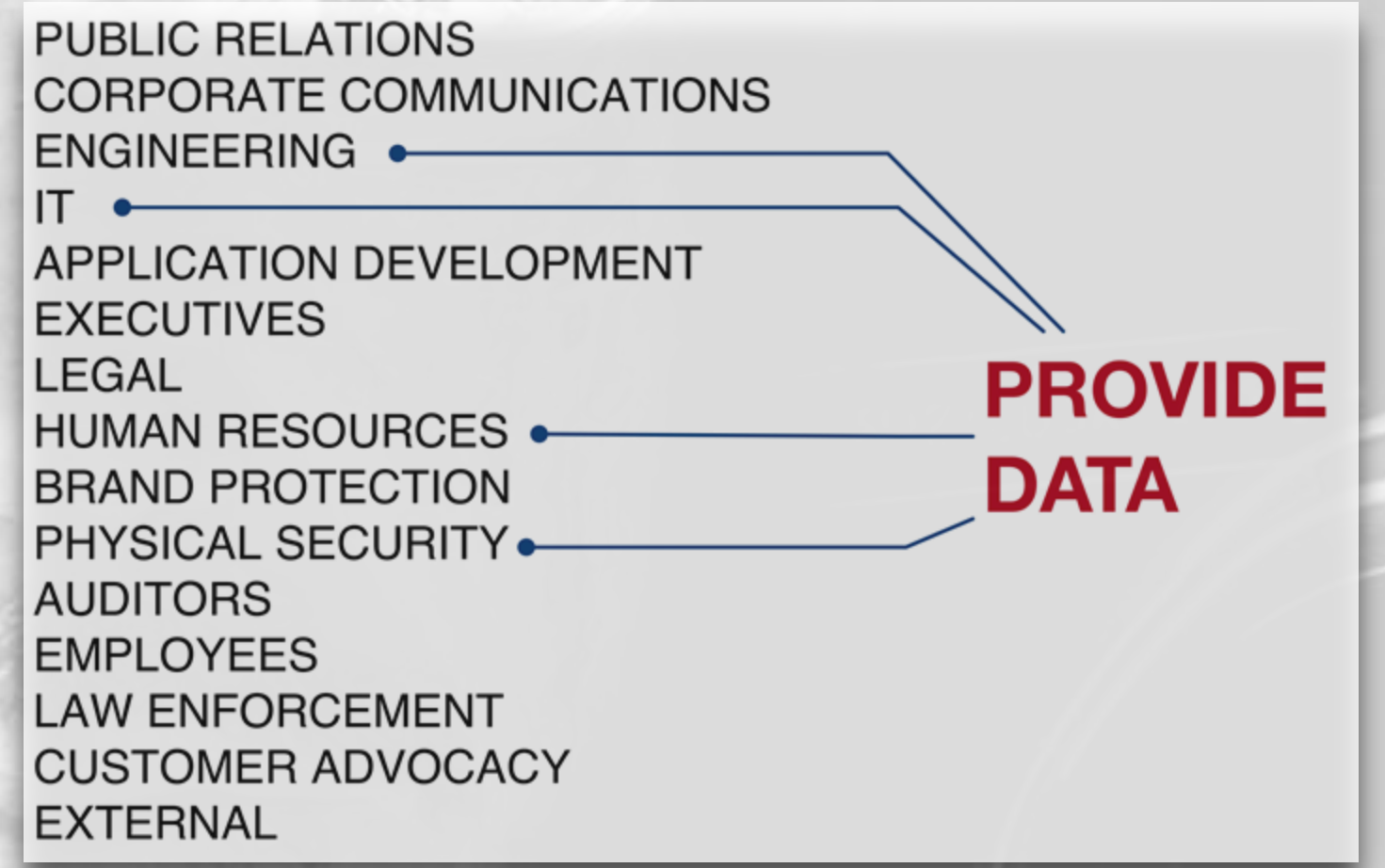

Deal With It
REAL BAD GUYS


PEOPLE
PARTNERS


PEOPLE
PARTNERS


PEOPLE
PARTNERS
rupshree.deviantart.com

PEOPLE

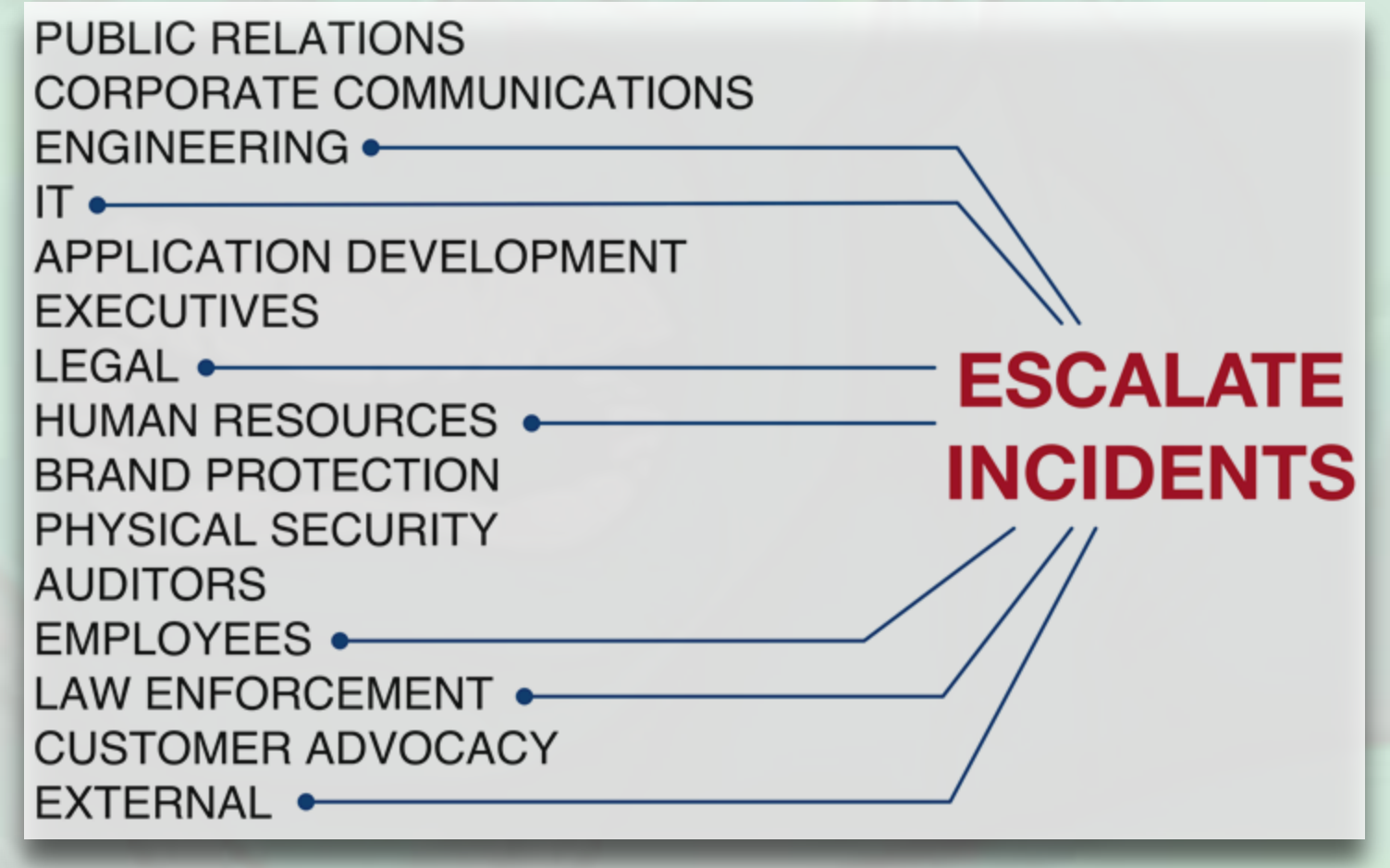


PARTNERS

PEOPLE

PARTNERS

PEOPLE



PARTNERS


INSTA/EXTREME_PHOTOSHOPER
PEOPLE
PARTNERS

PEOPLE

PARTNERS

PEOPLE

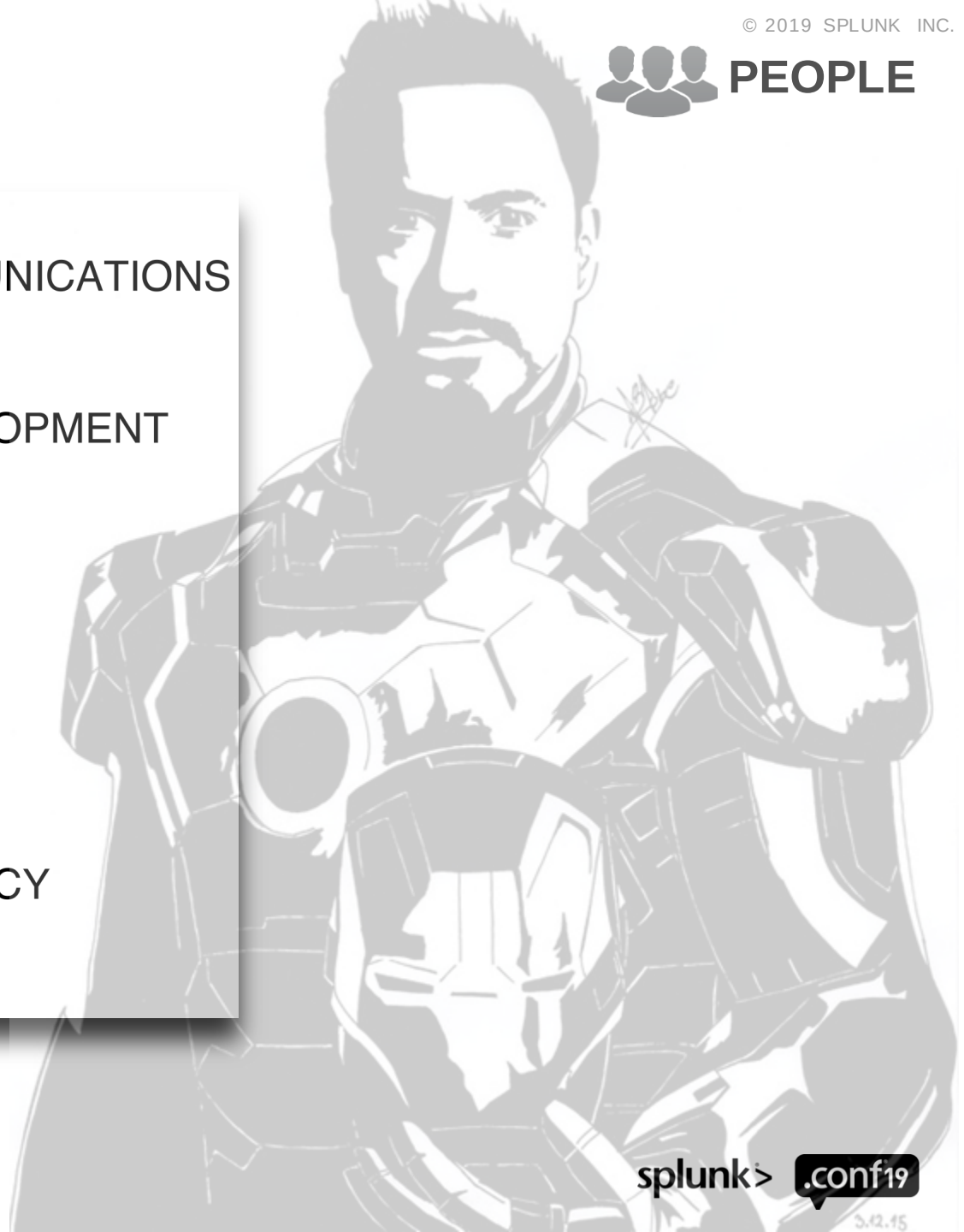
PARTNERS

splunk> .conf19

PEOPLE

FUNDING

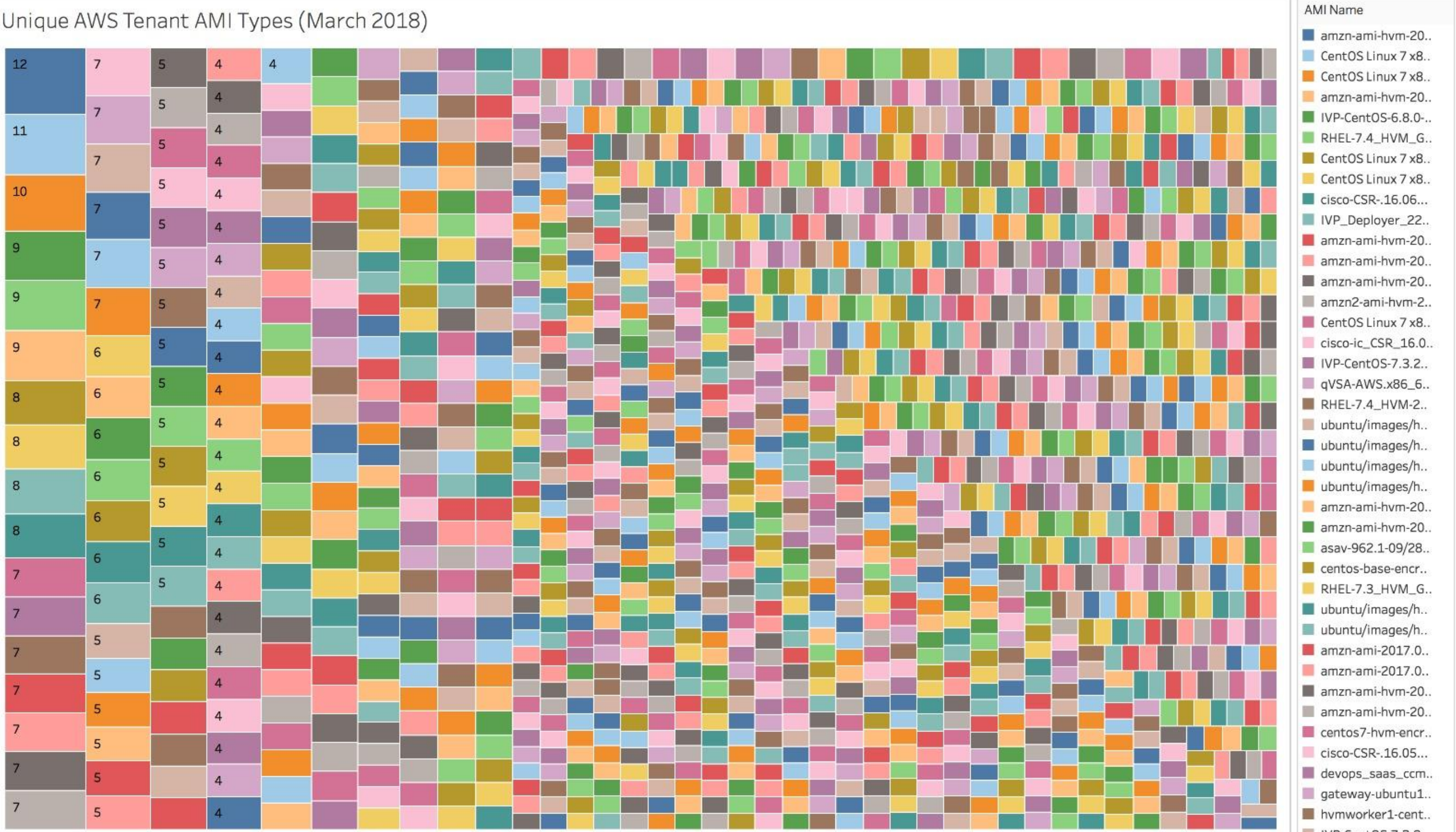
- PUBLIC RELATIONS
- CORPORATE COMMUNICATIONS
- ENGINEERING
- IT
- APPLICATION DEVELOPMENT
- EXECUTIVES
- LEGAL
- HUMAN RESOURCES
- BRAND PROTECTION
- PHYSICAL SECURITY
- AUDITORS
- EMPLOYEES
- LAW ENFORCEMENT
- CUSTOMER ADVOCACY
- EXTERNAL

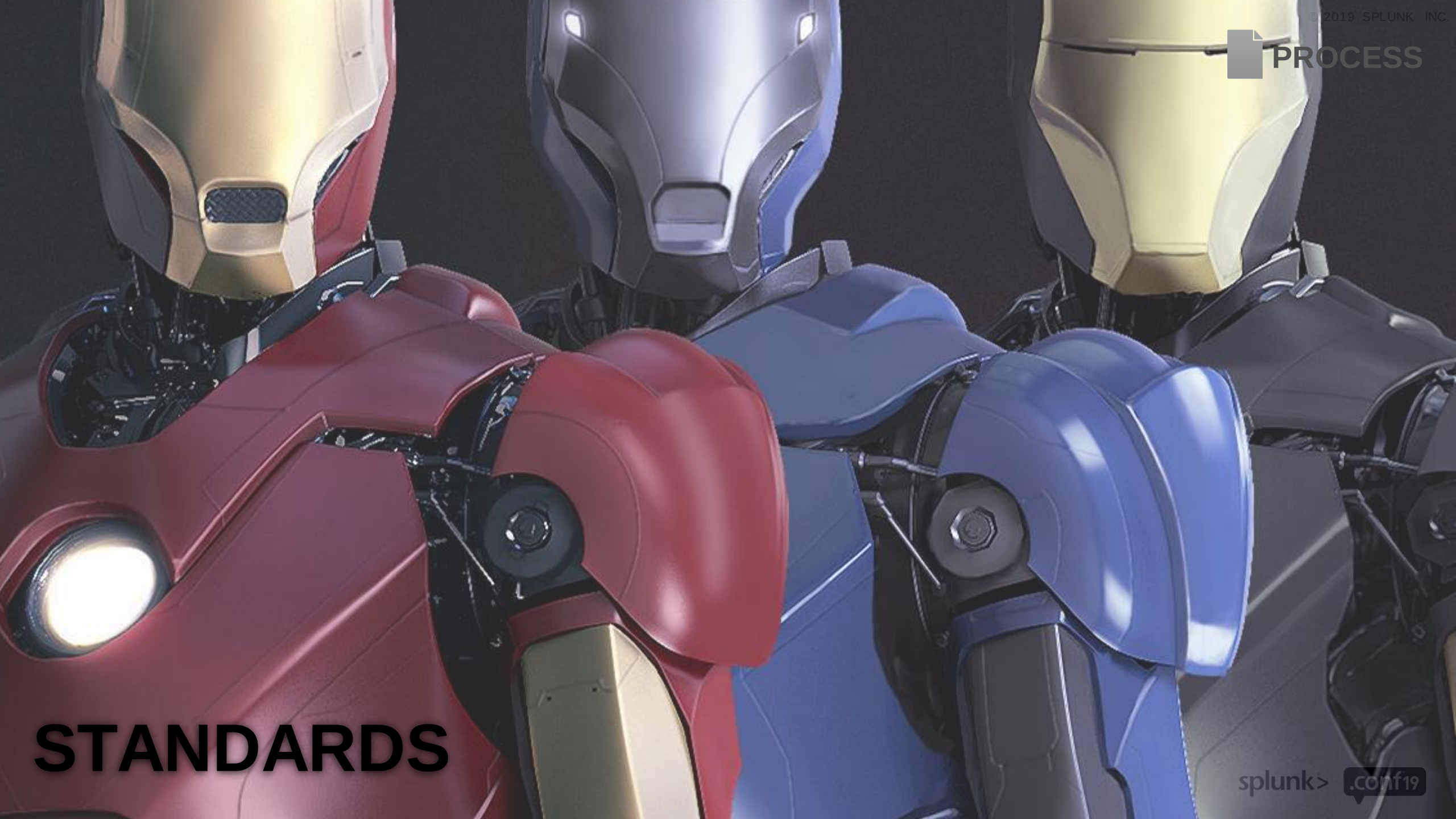


PARTNERS

PROCESS

Unique AWS Tenant AMI Types (March 2018)



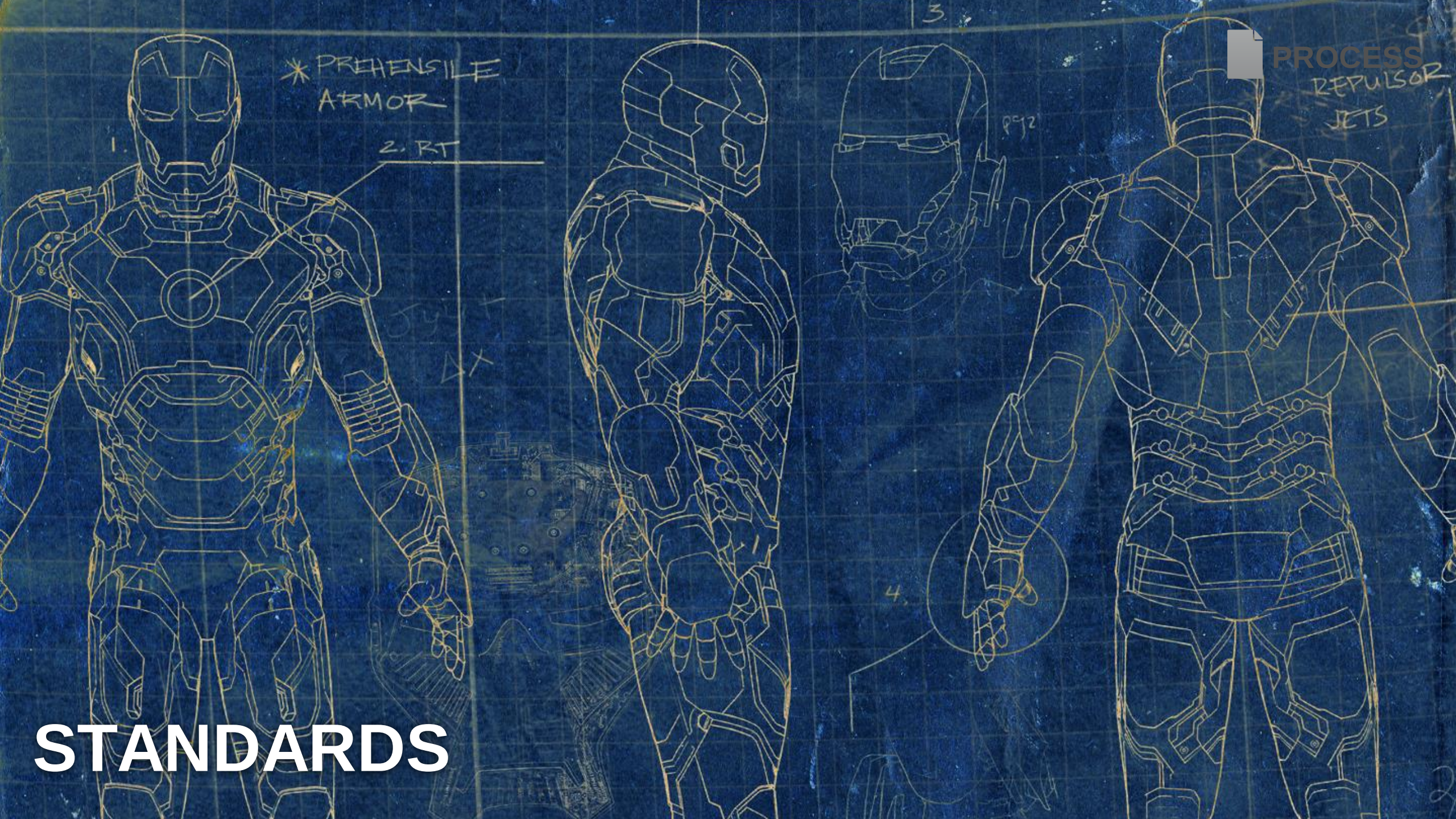


STANDARDS

PROCESS

HOST
NETWORK
ACCEPTABLE USE
PASSWORD/AUTHENTICATION
MINIMUM REQUIREMENTS

STANDARDS



STANDARDS

DEFINE YOUR STANDARDS

STANDARDS


PROCESS
STANDARDS
MARK I
MARK II
MARK III
MARK IV

PROCESS

EVOLVE OVER TIME

STANDARDS

PREPARE FOR THE INEVITABLE

PROCESS


CHARTER


ESCALATION PATHS


ENGAGEMENT PROCESS


RESPONSE TEMPLATES


PARTNER DIRECTORY


SERVICE LEVEL AGREEMENTS

INCIDENT RESPONSE HANDBOOK

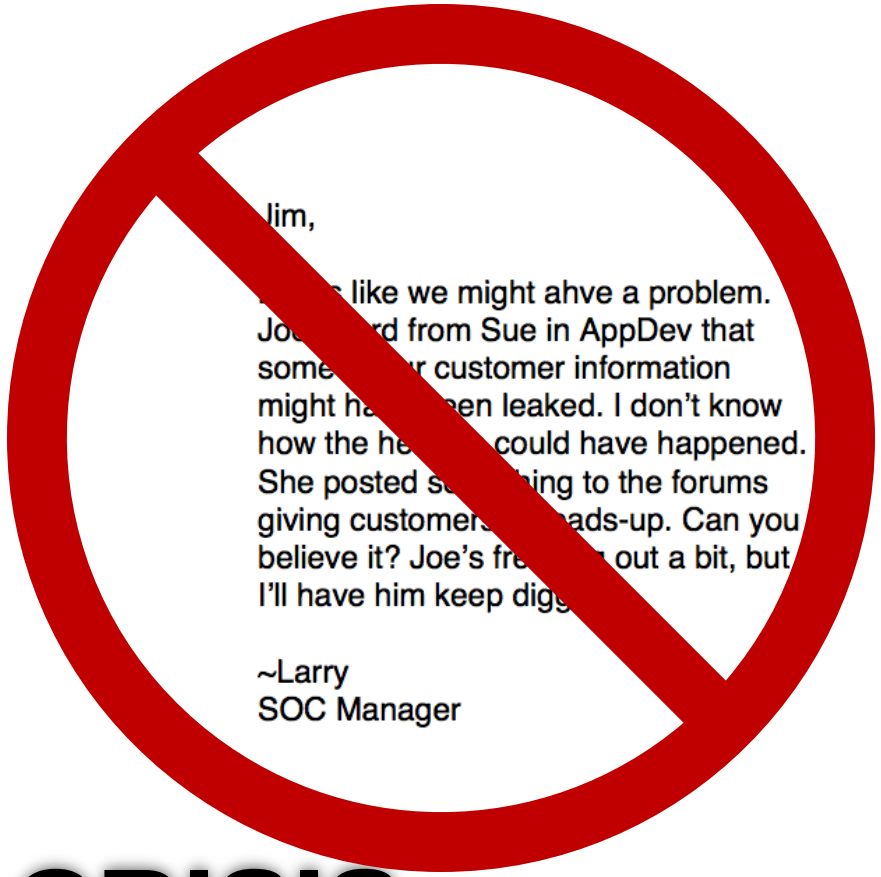
splunk> .conf19

CRISIS COMMS

Jim,

Looks like we might ahve a problem. Joe heard from Sue in AppDev that some of our customer information might have been leaked. I don't know how the hell this could have happened. She posted something to the forums giving customers a heads-up. Can you believe it? Joe's freaking out a bit, but I'll have him keep digging.

~Larry
SOC Manager



CRISIS COMMS

VS.

PROCESS

To whom it may concern,

Please find information about active incident INC00304 below.

SUMMARY

At 10:00 this morning, the SOC verified exposed customer data, as notified by an external entity. Unfortunately the SOC lacks forensic data from application servers in Splunk to investigate root cause. Investigators are working with App Dev to collect missing data.

After the incident, and prior to SOC engagement, a user from App Dev posted an unauthorized notice to the customer forums. Investigators are working to have the message removed.

Access to the suspected exposed data has been removed and the Crisis Communication process has been enacted.

The next update will be provided in 2 hours or as new evidence is revealed.

IMPACT

The incident has no known service impact. The SOC verified that customer data has been exposed publicly to the world, but the scope and type of data exposed is currently unknown.

CONTACTS

Joe - Lead Investigator
Sue - App Dev

ACTIONS TAKEN

- Opened incident case INC00304
- Applications servers taken offline
- Requested snapshot of historical app data
- Working with App Dev to removing unauthorized message on user forums
- Provided summary of incident to PR to draft public statement

OUTSTANDING ITEMS

- Collect Data
- Analyze data for signs of compromise
- Setup continuous feed of app data to Splunk

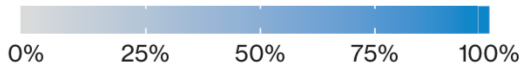
~Joe
Investigator

THREAT-BASED MONITORING PLAN

Image compliments of - on aminoapps.com

PROCESS

Patterns	Incidents									Breaches								
	Accommodation	Education	Financial	Healthcare	Information	Manufacturing	Professional	Public	Retail	Accommodation	Education	Financial	Healthcare	Information	Manufacturing	Professional	Public	Retail
Crimeware	21	19	49	154	57	284	248	5,988	26	5	2	8	14	3	8	9	9	4
Cyber-Espionage	1	12	9	24	4	82	41	120		1	12	8	9	2	22	14	77	
Denial of Service	2	151	336	1	580	74	104	703	85									
Everything Else	13	48	59	63	81	39	41	68	12	11	36	19	54	28	17	30	52	8
Lost and Stolen Assets	4	10	16	96	3	15	17	3,728	7	2	7	10	73	2		8	17	5
Miscellaneous Errors	2	16	22	181	34	3	30	1,774	11	1	15	20	172	27	2	27	50	9
Payment Card Skimmers	6		49	5		1		1	81	4		40	5				1	61
Privilege Misuse	7	7	21	138	5	22	28	10,311	11	5	3	11	128	2	8	17	51	8
Point of Sale	306		2	1	2		1		11	302		2	1	2		1		10
Web Applications	11	29	36	88	277	17	34	97	73	10	26	29	81	45	15	28	49	64
Actions																		
Environmental																		
Error	2	17	26	203	36	5	35	5,482	12	1	16	21	188	28	2	27	55	10
Hacking	324	210	400	139	880	150	201	925	176	316	46	50	121	62	47	66	159	77
Malware	326	35	70	185	70	359	296	6,121	71	307	14	24	27	8	24	25	90	45
Misuse	7	7	21	138	5	22	28	10,311	11	5	3	11	128	2	8	17	51	8
Physical	10	11	64	87	3	16	12	23	89	6	8	49	68	2		8	15	67
Social	14	46	63	105	69	314	257	171	10	10	41	25	56	15	18	28	96	7
Assets																		
Embedded					1	1		3										
Kiosk/terminal	6		50	6	1	2		1	82	4		38	5				1	62
Media	5	6	25	193	2	11	12	827	16	3	5	16	183	2	1	7	36	12
Network		1	8	3	4	2	2	1	1		1		1	1				
Person	15	45	62	104	69	314	258	172	9	11	41	24	55	15	18	28	97	6
Server	338	210	419	299	920	127	202	885	189	322	42	64	245	86	42	76	105	89
User Dev	306	28	42	115	30	336	290	3,851	22	302	20	19	52	4	16	29	98	13



Reference: the 2018 Verizon Data Breach Investigation Report


CHAMPIONS
THE SUPER ROLE-PLAYING GAME™

1. WHAT ARE YOU TRYING TO **PROTECT**?
2. WHAT ARE THE **THREATS**?
3. HOW DO YOU **DETECT** THEM?
4. HOW DO YOU **RESPOND**?

THE PLAYBOOK METHODOLOGY

playbook ˈplāˌbŏk (n)

A prescriptive collection of repeatable queries (reports) against security event data sources that lead to incident detection and response.

Stage 3: Expansion

You're ingesting advanced data sources and running better investigations.

AWS Cloud Provisioning Activity from Unusual Country

Looks for AWS Provisioning activities that occur from new IPs, using GeoIP to resolve the Country.

Recommended
Searches Included
Audit Trail

AWS Unusual Amount of Modifications to ACLs

Looks for a large number of Security Group ACL changes in a short period of time for a user.

Recommended
Searches Included
Endpoint Detection and Response
Windows Security

Concentration of Attacker Tools by Filename

It's uncommon to see attacker tools used in rapid succession on an endpoint. This search will identify tools by filename, and look for multiple executions. (MITRE CAR Reference)

Recommended
Searches Included
Endpoint Detection and Response
Windows Security

Detect Long DNS TXT Record Response

This search is used to detect attempts to use DNS tunneling, by calculating the length of responses to DNS TXT queries. Endpoints using DNS as a method of transmission for data exfiltration, command and control, or evasion of security controls can often be detected by noting unusually large volumes of DNS traffic.

Recommended
Try ES Content Update

Emails from Outside the Organization with Company Domains

Phishers will often try to send emails

Endpoint Detection and Response

First Time Accessing an Internal Git Repository

Find users who accessed a git repository for the first time.

Recommended
Searches Included
Source Code Respository

Abnormally High Number of Endpoint Changes By User

Endpoint Detection and Response

Anomalous New Process

Alerts when an anomalous number of hosts are detected with a new process

Try Splunk ES
Endpoint Detection and Response

AWS Instance Modified by Unusual User

Detects the first time a user modifies an existing instance.

Searches Included
Audit Trail

Host-based IDS

DNS

Windows Security

Journal Clearing

Searches Included
Endpoint Detection and Response
Windows Security

Detect Lateral Movement With WMI

This use case looks for WMI being used for lateral movement.

Searches Included
Endpoint Detection and Response
Windows Security

Detect Log Clearing With wevtutil

This use case looks for the wevutil process clearing the Windows Audit Logs

Searches Included
Endpoint Detection and Response
Windows Security

Detect Path Interception via creation of program.exe

The search is looking for the creation of file C:\program.exe. The

Try ES Content Update
Endpoint Detection and Response

Endpoint communicating with an excessive number of unique hosts

Endpoints attempting to communicate with an excessive number of unique hosts over a given time period may indicate malicious code.

Use Splunk PS
Network Communication

Endpoint communicating with an excessive number of unique ports

Endpoints communicating with an excessive number of unique destination ports could indicate malicious code probing for vulnerabilities. Certain server applications will arrange for communication on a high number port with the client such as ftp in passive mode and RPC on windows server.

Use Splunk PS
Network Communication

Endpoint communicating with external service identified on a threat list.

The endpoint has attempted (success or fail) to communicate with an external server identified on a threat list using any protocol. An attempted communication could indicate activity generated by malicious code.

Endpoint Multiple infections over short time

Multiple infections detected on the same endpoint in a short period of time could indicate the presence of an undetected loader malware component (apt).

Use Splunk PS

Excessive DNS Failures

Alerts when a host receives many DNS failures in a short span

Try Splunk ES
DNS

Excessive DNS Qu

Alerts when a host starts excessive DNS queries

Try Splunk ES
DNS

Find Unusually Long CLI Commands

Oftentimes we're able to detect malware by looking for unusually long command line strings.

Searches Included
Endpoint Detection and Response

High Number of Newly Seen Connections to Internal Hosts

Detect lateral movement by searching for hosts with an unusually high number of connections to hosts it has never connected to before, within a given time period.

Use Splunk PS

High Process Count

Alerts when host has a high number of processes. This may be due to an infection or a runaway process.

Try Splunk ES
Endpoint Detection and Response

POW!

BOOM

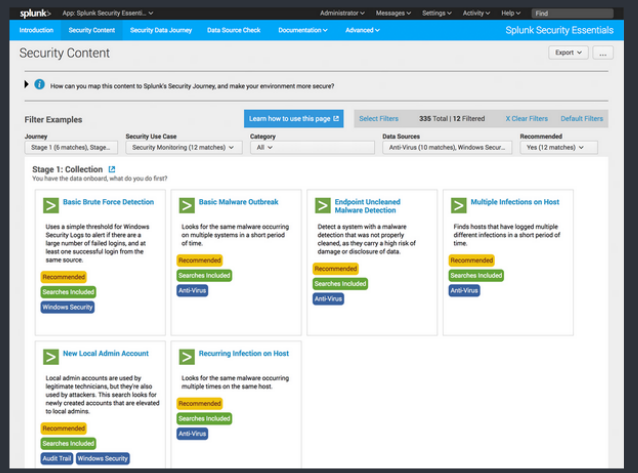
BANG

splunkbase™ Search App by keyword, technology... My Account Support & Services

Splunk Security Essentials

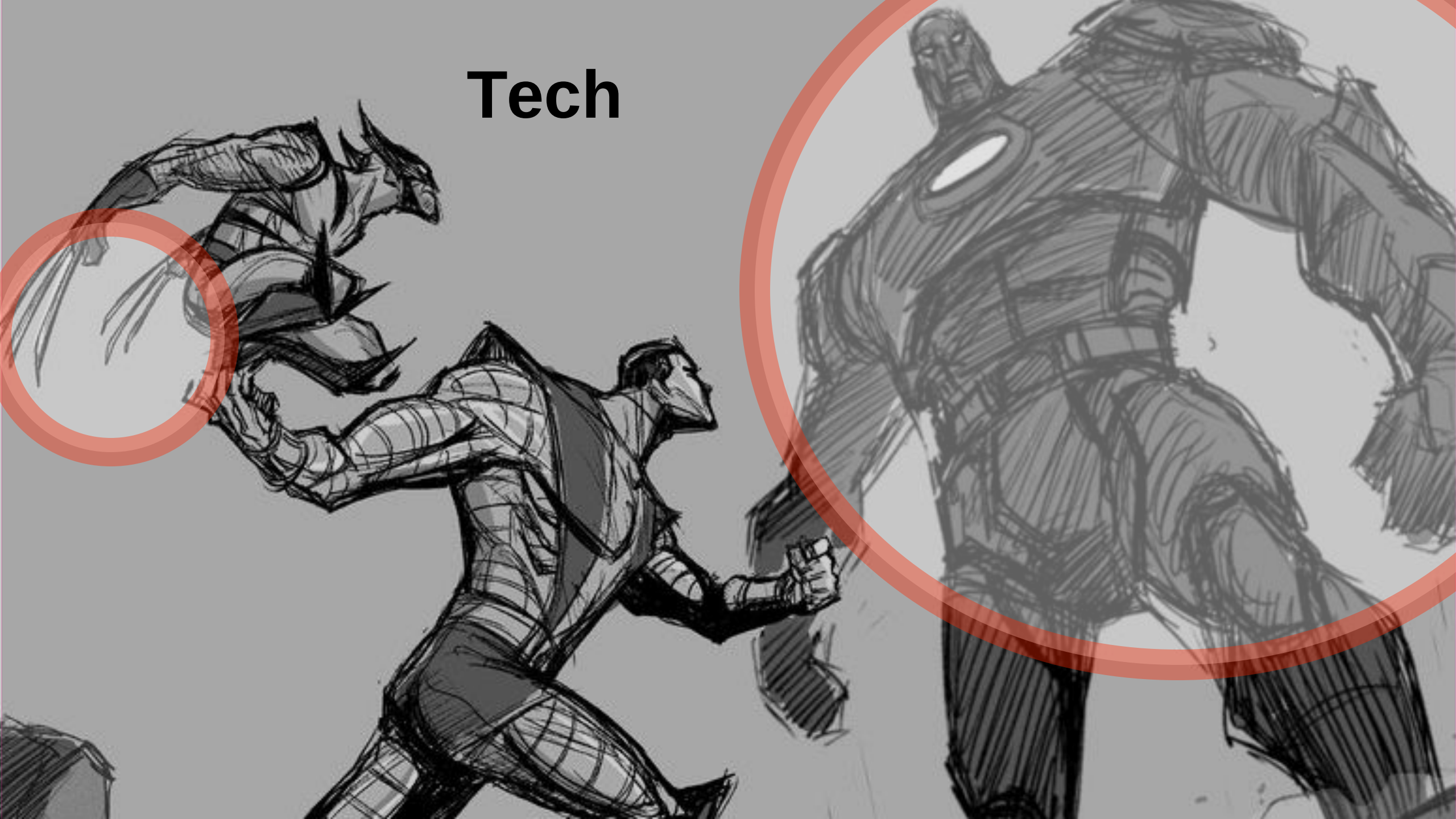
★★★★★ 22 ratings

Splunk Built

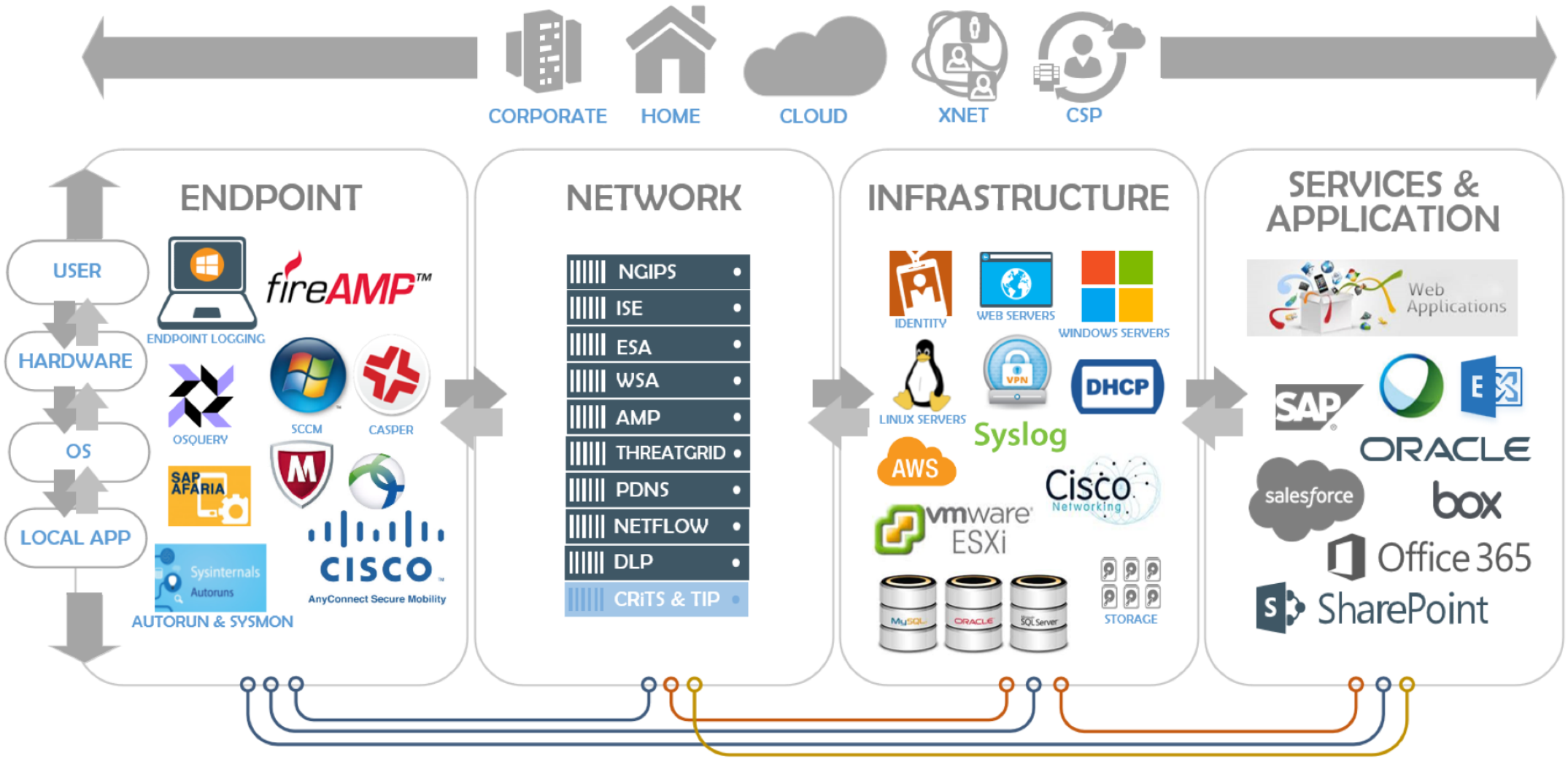


splunk> .conf19

Tech



UNDERSTAND YOUR ENVIRONMENT



Random University in the Midwest:

splunk> .conf19

Random University in the Midwest:

“We based our program on PCI.”

Random University in the Midwest:

“We based our program on PCI.”

“No. We don’t work well with IT.”

Random University in the Midwest:

"We based our program on PCI."

"No. We don't work well with IT."

"We don't segregate our network."

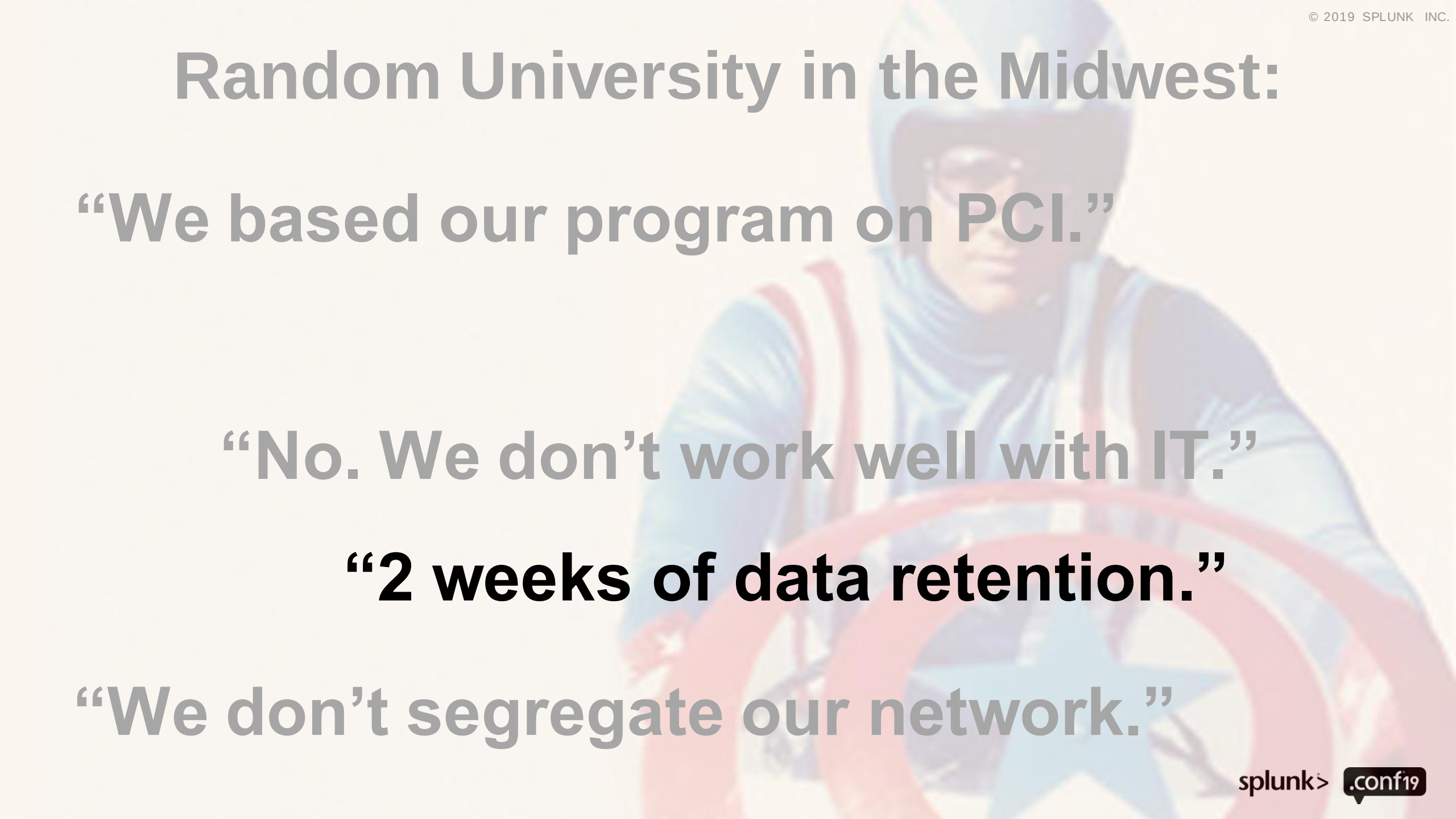
Random University in the Midwest:

"We based our program on PCI."

"No. We don't work well with IT."

"2 weeks of data retention."

"We don't segregate our network."



Random University in the Midwest:

"We based our program on PCI."

"No. Everything is important."

"No. We don't work well with IT."

"2 weeks of data retention."

"We don't segregate our network."

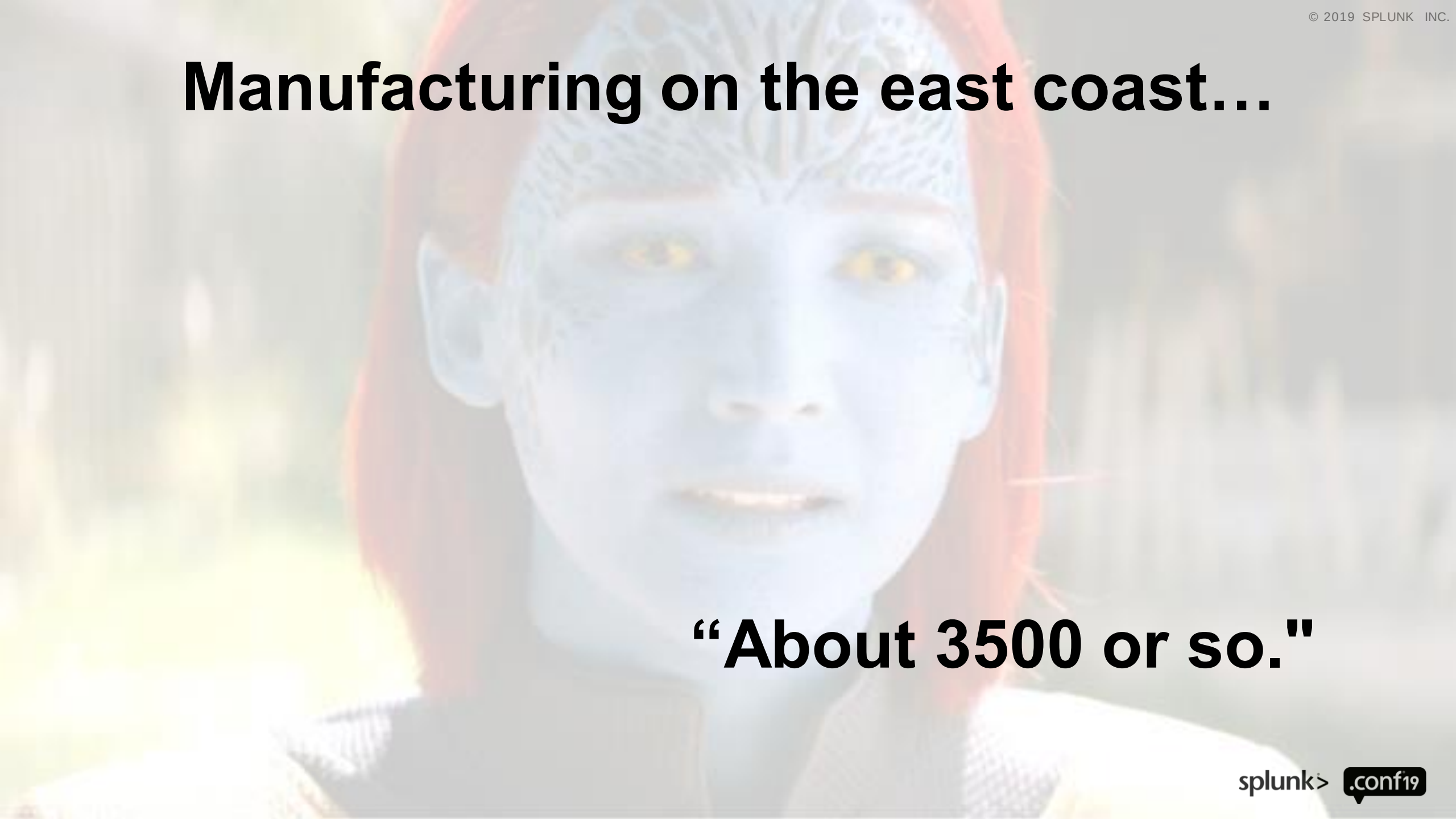

PENN

splunk> .conf19

splunk> .conf19

Manufacturing on the east coast…

Manufacturing on the east coast…



"About 3500 or so."

Manufacturing on the east coast…

“Four.”

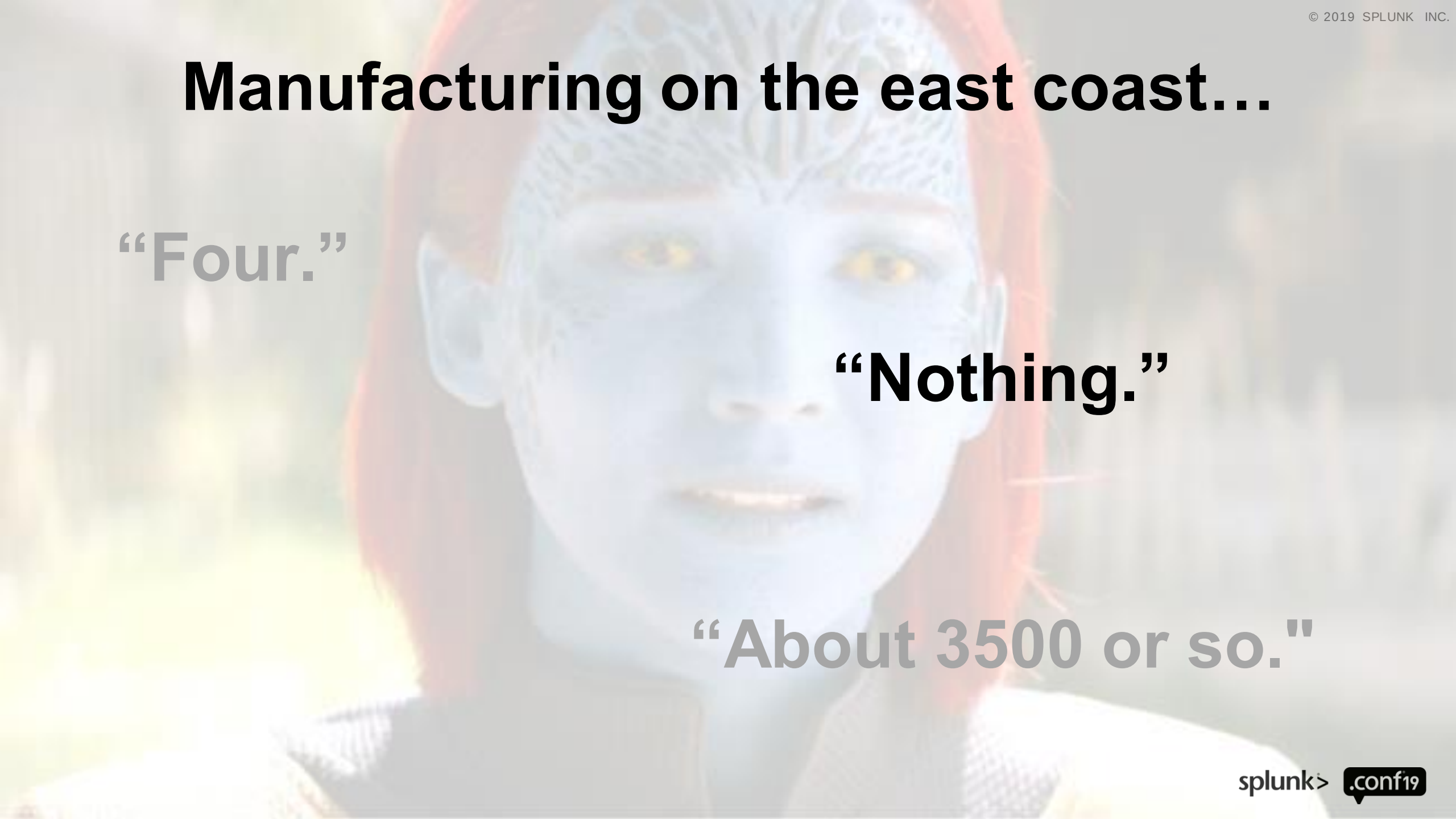
“About 3500 or so."

Manufacturing on the east coast…

"Four."

"Nothing."

"About 3500 or so."



Manufacturing on the east coast…

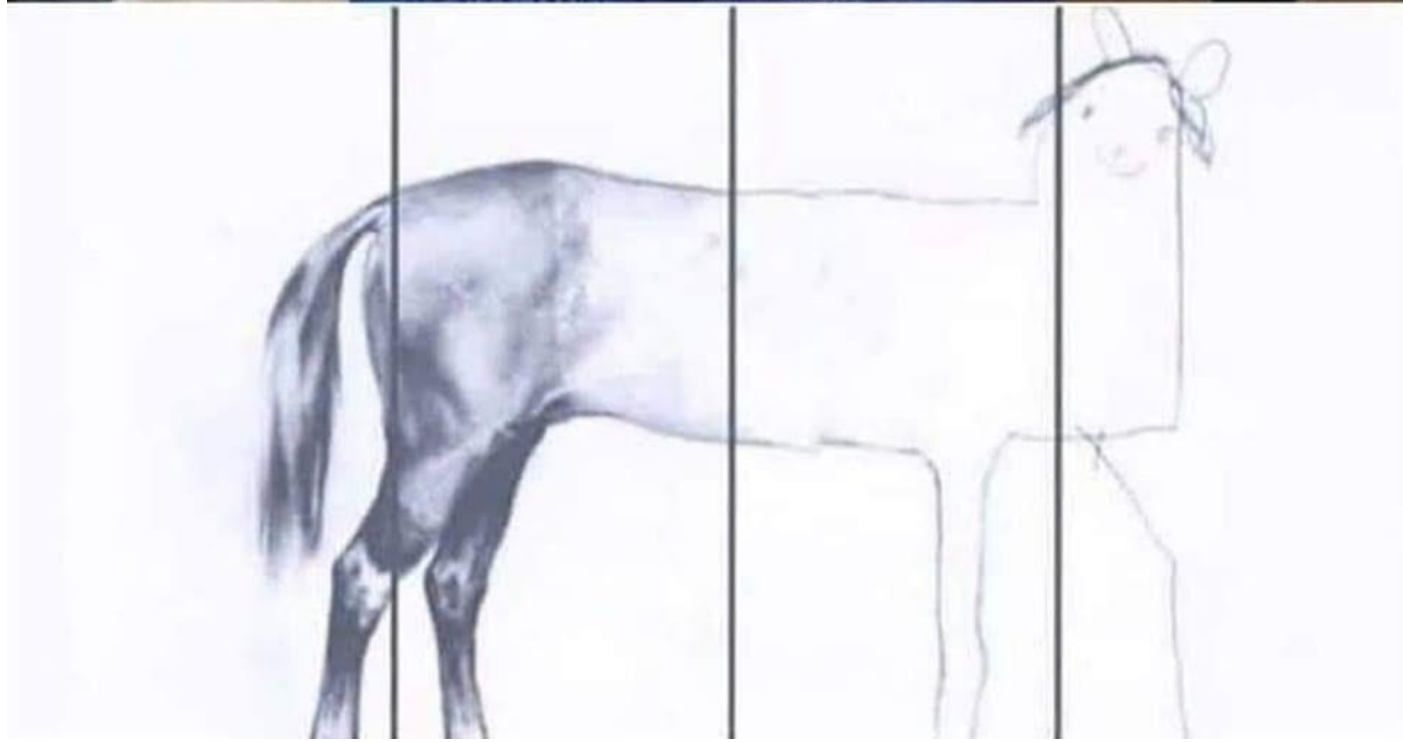
"Four."

"Nothing."

"We don't have time."

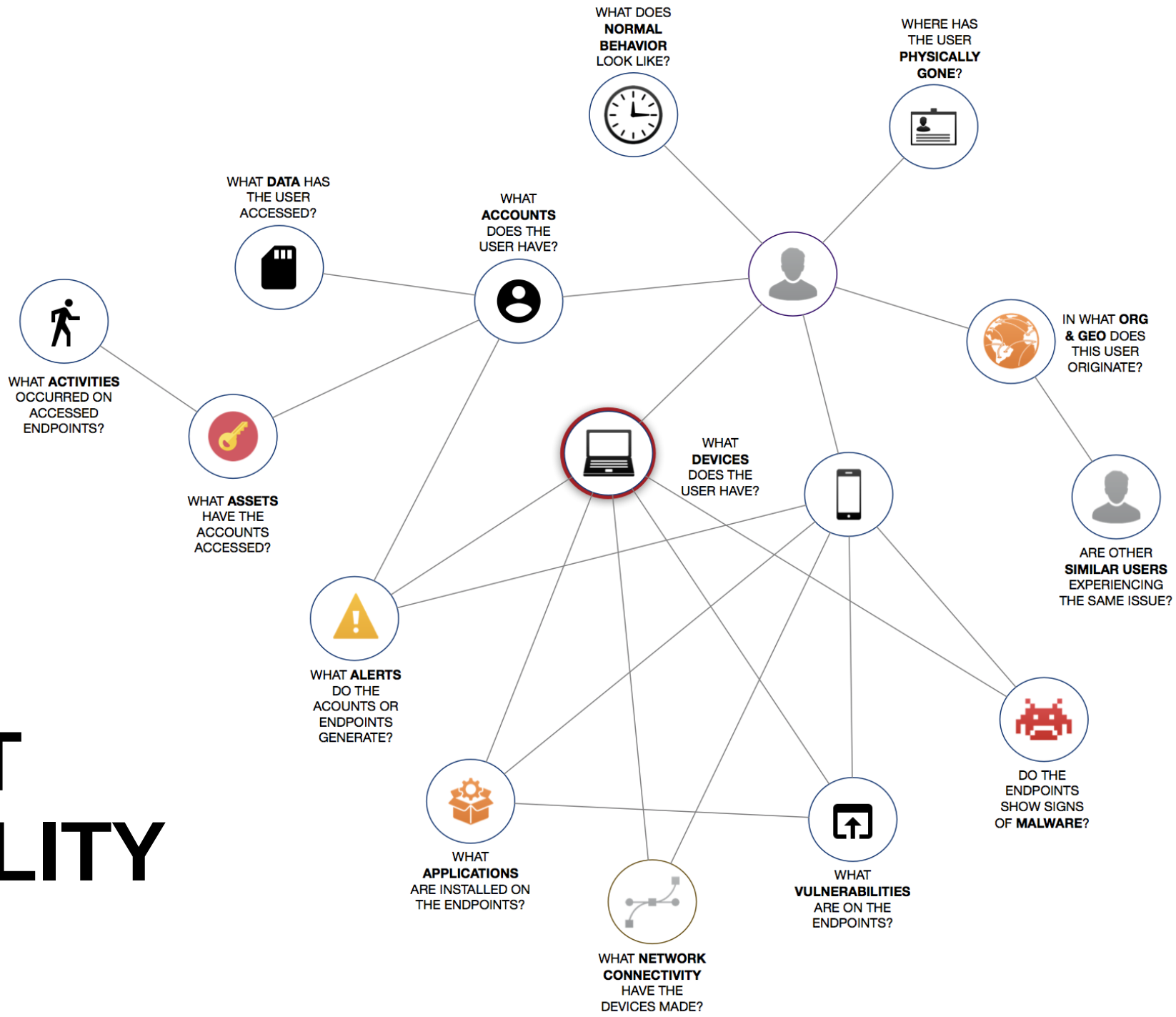
"About 3500 or so."

splunk> .conf19



TECH

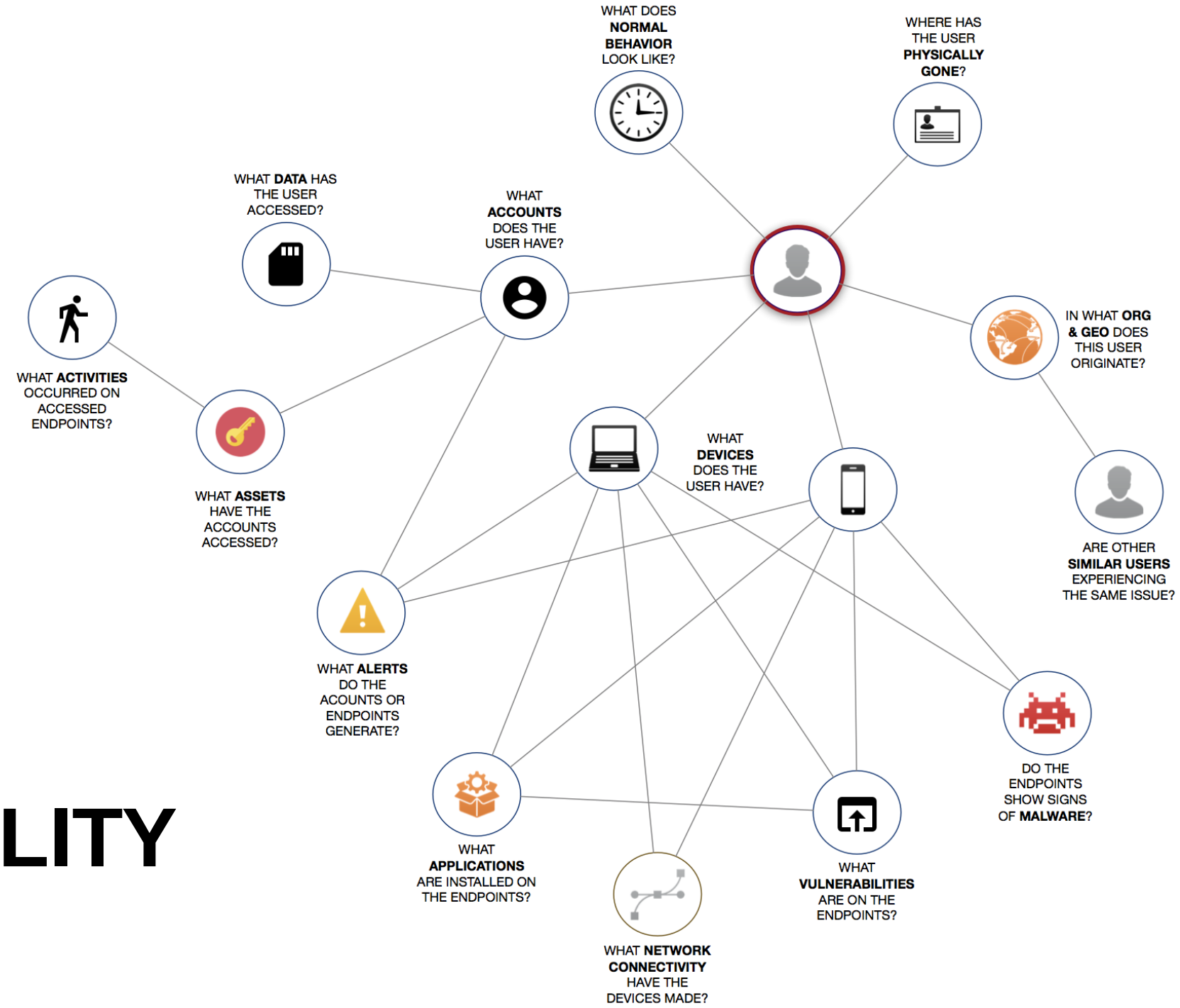
ASSET VISIBILITY



splunk> .conf19

TECH

USER VISIBILITY



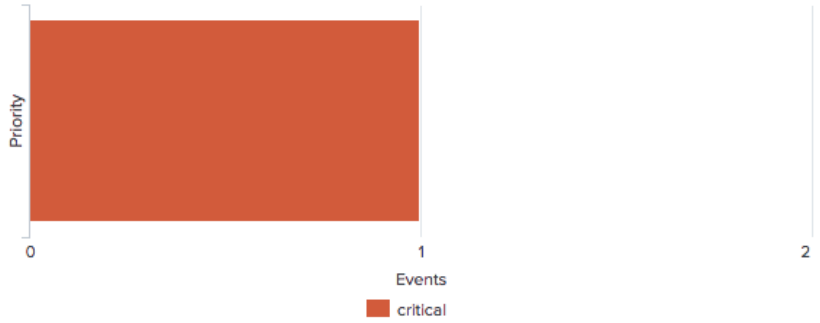
splunk> .conf19

Asset Center

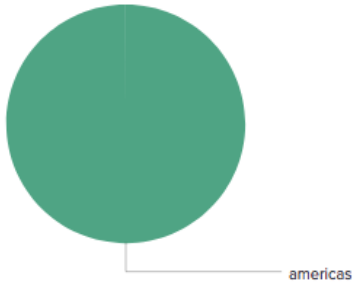
Export ▾ ...

Asset: *
Priority: All
Business Unit:
Category: All
Owner: Mark_Pittman
Submit Hide Filters

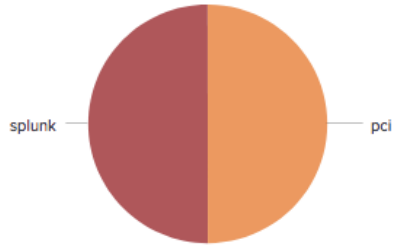
Assets By Priority



Assets By Business Unit



Assets By Category



Asset Information

ip	mac	nt_host	dns	owner	priority	lat	long	city	country	bunit	category	pci_domain	is_expected	should_timesync	should_update	requires_av
10.116.240.105				Mark_Pittman	critical	37.694452	-121.894461	San Francisco	USA	americas	pci splunk	trust	true	true	true	false

SYSTEM OF RECORD

splunk> .conf19

Asset Investigator

10.116.240.105 Search

10.116.240.105

bunit: **americas**
category: **pci, splunk**
ip: **10.116.240.105**
owner: **Mark_Pittman**
lat: **37.694452**
pci_domain: **trust**
should_timesync: **true**
country: **USA**
_time: **2018-05-25T05:16:28+0000**
is_expected: **true**
city: **San Francisco**
should_update: **true**
priority: **critical**
requires_av: **false**
long: **-121.894461**

UEBA Threats

May 24, 2018 8:15 PM - May 24, 2018 8:18 PM GMT-0700

Apps
ssl
tcp

Description
Remote account takeover followed by unusual activity and data exfiltration . Entity involved in a sequence of events constituting a threat: it was first involved in unusual login activity and unusual internal activity, followed by an unusual data transfer to external destination.This threat should be investigated for possible user compromise followed by data exfiltration.

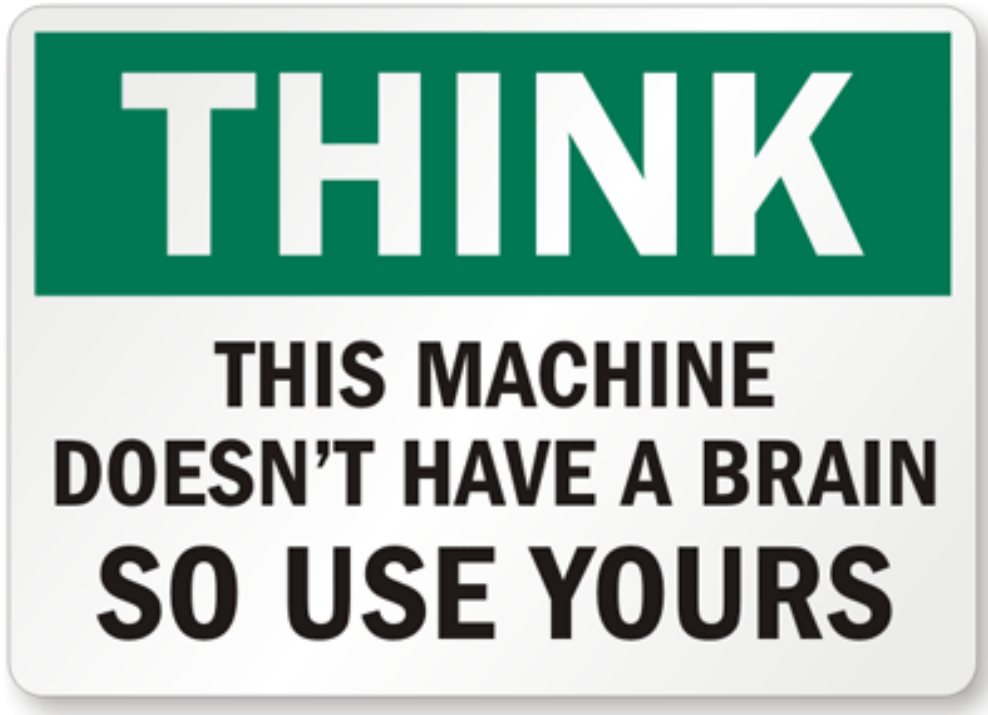
Detection Time

Devices
1.94.32.234
10.1.1.26
+11 more

Domains

AI / ML

Image courtesy of ClipartXtras



Machine Learning is a technology, which enhances people and process, it does not replace them.

Image courtesy of ClipartXtras

Image courtesy of ClipartXtras

Aww…

Sorry buddy.

TECH

SOAR

Image compliments of movieplayer.net

TECH

SECURITY **O**RCHESTRATION and **A**UTOMATED **R**ESPONSE

SECURITY **O**PERATIONS, **A**NALYTICS, AND **R**EPORTING

SOAR

splunk> .conf19

Image compliments of movieplayer.net

TECH

Automation

- Automate repetitive tasks to force multiply team efforts.
- Execute automated actions in seconds versus hours.
- Pre-fetch intelligence to support decision making.

Orchestration

Coordinate complex workflows across your SOC.

SOAR

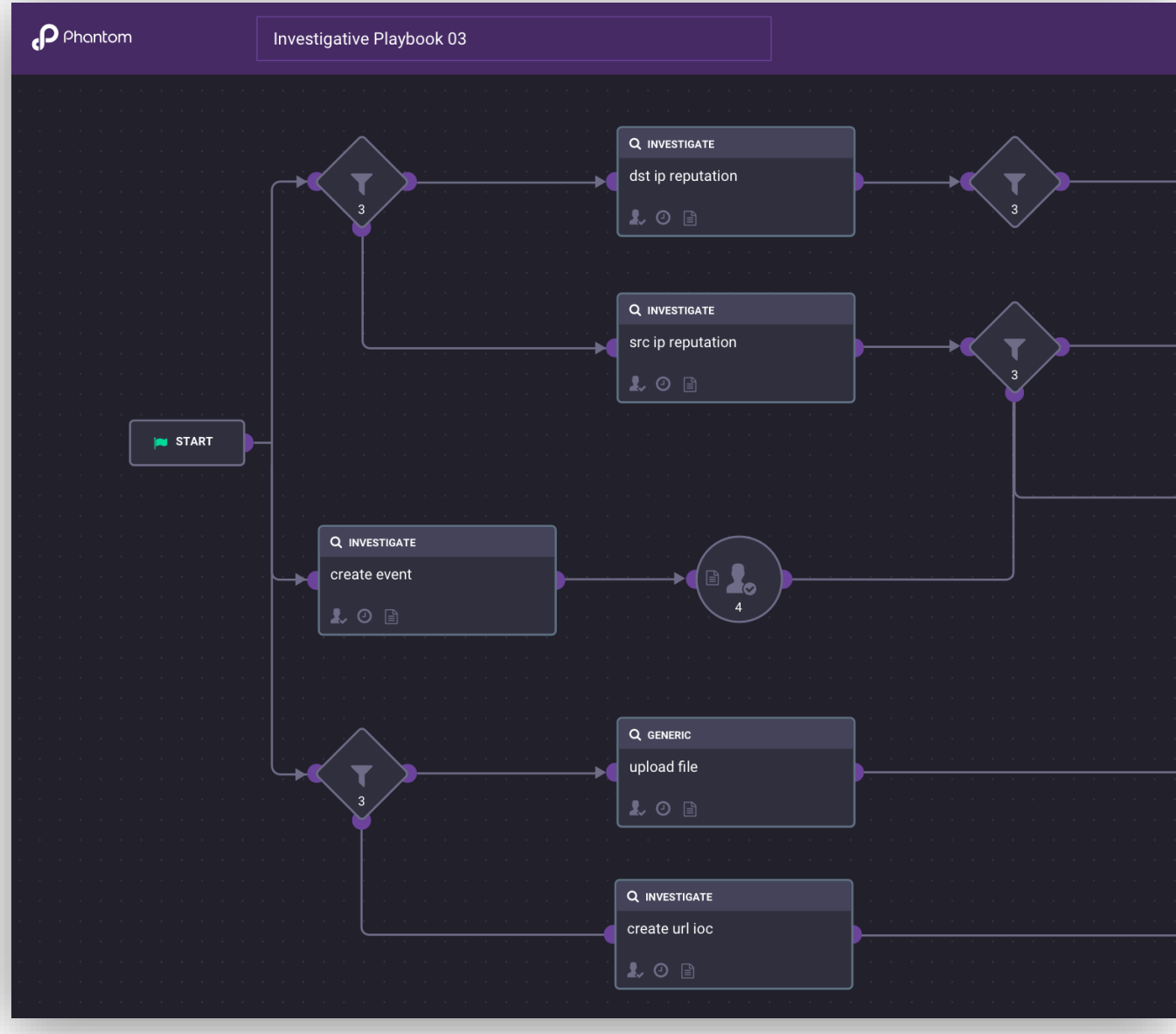


Image compliments of wooser on pinterest

SHOWING OPERATIONAL VALUE

Time to detect
Time to contain
Time to eat lunch
Time to close
Time to analyze by play/analyst
Detection efficacy by play/analyst
Operational availability
Incidents by category
Incidents according to HR
Incidents by source country, group, exec, environment…
Incidents involving prior exceptions
Incidents involving sensitive data
Incidents by policy violation
Number of tickets closed by analyst
Repeat infections
Repeat offenders
Vulnerability posture across incidents
Trending detections
Hot Threats
Operational improvement via automation
Quantity of data consumed
Unused data
Detections by threat intel category/source

SHOWING OPERATIONAL VALUE

Time to detect
Time to contain
~~*Time to eat lunch*~~
~~*Time to close*~~
Time to analyze by play/analyst
Detection efficacy by play/analyst
Operational availability
Incidents by category
~~*Incidents according to HR*~~
Incidents by source country, group, exec, environment…
Incidents involving prior exceptions
Incidents involving sensitive data
Incidents by policy violation
~~*Number of tickets closed by analyst*~~
Repeat infections
~~*Repeat offenders*~~
Vulnerability posture across incidents
Trending detections
Hot Threats
Operational improvement via automation
Quantity of data consumed
Unused data
Detections by threat intel category/source

SHOWING STRATEGIC VALUE

Outstanding Audit Events
Project status (on time | within budget) or not
Compliance status over time
Number of events collected
Critical application vulnerabilities
Patch status over time
Cost savings via automation
Cost of paper towels used in mens room
CAPEX vs. OPEX costs when migrating to cloud
Internal security training status
SLA's not being met
Corporate phishing tests
Fantasy Football Winner
Analyst accuracy
Number/type of externally reported issues
Number of Firewall Blocks
Cost of Incidents
Number of handicap spots in the parking lot

SHOWING STRATEGIC VALUE

Outstanding Audit Events
Project status (on time | within budget) or not
Compliance status over time
~~*Number of events collected*~~
Critical application vulnerabilities
Patch status over time
Cost savings via automation
~~*Cost of paper towels used in mens room*~~
CAPEX vs. OPEX costs when migrating to cloud
Internal security training status
SLA's not being met
Corporate phishing tests
~~*Fantasy Football Winner*~~
Analyst accuracy
Number/type of externally reported issues
~~*Number of Firewall Blocks*~~
Cost of Incidents
~~*Number of handicap spots in the parking lot*~~

SHOWING SECURITY COMMUNITY VALUE

Industry Participation
Publications
Bake Sales
Conference hosting
Executive Briefings
Threat Data Contribution
Foosball Championships
Showcase SOC
Release open source tools

SHOWING SECURITY COMMUNITY VALUE

Industry Participation
Publications
~~*Bake Sales*~~
Conference hosting
Executive Briefings
Threat Data Contribution
~~*Foosball Championships*~~
Showcase SOC
Release open source tools

FULLY BALANCED SOC

Image compliments of Disney

Thank You!

PEOPLE

Matthew Valites
Fox + Disney + Marvel Studios
Ryan Reynolds
Mom
Robert Downey, Jr.

A BIG THANKS