Pull Up Your SOCs!

A Splunk Primer on Building Your Security Operations

Matthew Valites & Dimitri McKay

CONF18

image compliments of harperandjane on etsy

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> listen to your data

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

splunk> .conf18

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

I'd be lying.

splunk> .conf18

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

I'd be lying. :)

splunk> .conf18


@matthewvalites
@dimitrimckay


@matthewvalites
@dimitrimckay

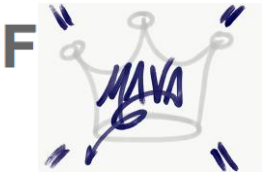
Dimitri McKay | Staff Security Architect | Splunk | CISSP | CCSK | LOLZ

@dimitrimckay

- 21 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. ☺

THE EVOLUTION OF

@matthewvalites



LINUX ADMIN

2002

POSTMASTER

2006

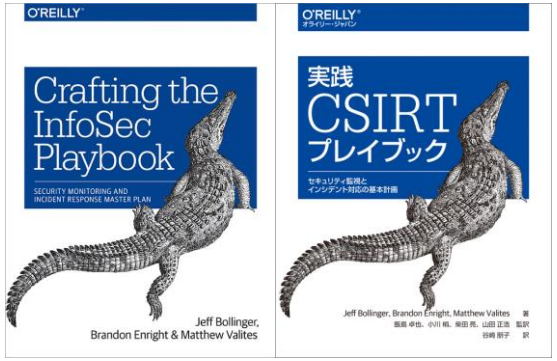
2000

2004

2008

CSIRT INVESTIGATOR

cisco



2010

2012

2014

INFOSEC PLAYBOOK O'REILLY PUBLICATION

2016

CSIRT INVESTIGATIONS MANAGER

cisco

splunk>

SECURITY SPECIALIST

2018

.conf18
splunk>
BOSS
of the SOC

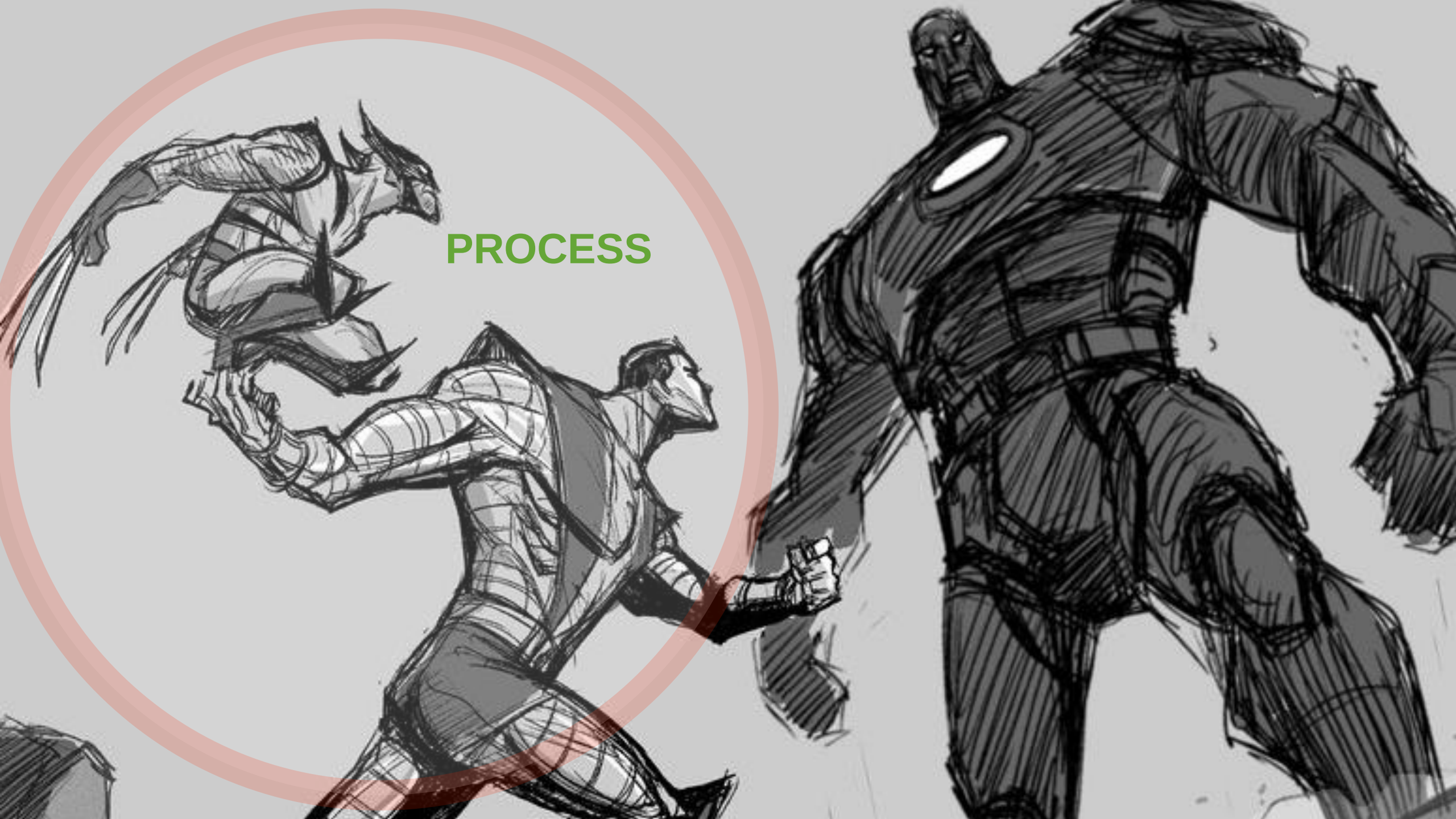
Image courtesy of sensacine.com

WHAT IS A SOC?

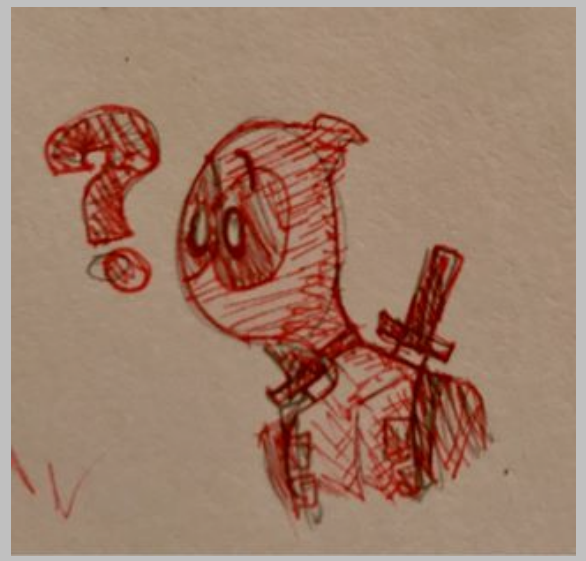

PEOPLE


TECH

PROCESS



DETECT



RESPOND

WHAT IS A SOC?

DETECT

RESPOND

WHAT IS A SOC?

DETECT

RESPOND

PREVENT

WHAT IS A SOC?

WHAT IS YOUR CHARTER?

Data Breaches
Law Enforcement Investigation
Human Resources investigation
Legal investigation
Revenge
Compromised systems
Denial of Service
Credential compromise
Phishing
Vulnerability management
Avenge parents murder
Lost device
Stolen device
Malware infection
Malware outbreak
Romance
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

+25 cool points?

Data Breaches
Law Enforcement Investigation
Human Resources investigation
Legal investigation
Revenge
Compromised systems
Denial of Service
Credential compromise
Phishing
Vulnerability management
Avenge parents murder
Lost device
Stolen device
Malware infection
Malware outbreak
Romance
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

WHAT IS YOUR CHARTER?

image credit compliments of shutterstock.com

WHAT DO WE KNOW?

Photo compliments of https://www.deviantart.com/endock-cepl0k

SOC Maturity

Image compliments of http://marvelcinematicuniverse.wikia.com/wiki/Captain_America%27s_Shield

Buy Tech

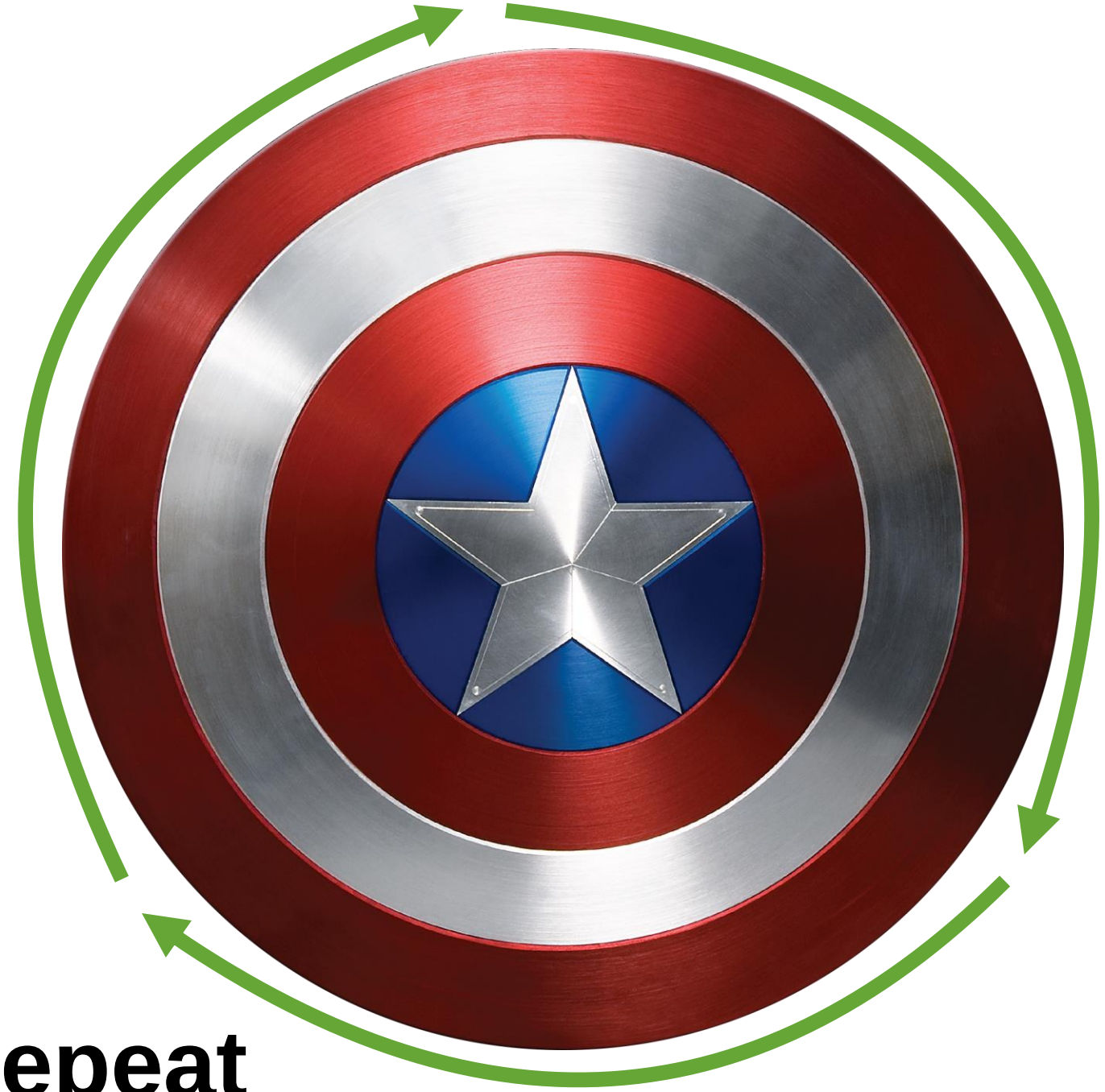
Image compliments of http://marvelcinematicuniverse.wikia.com/wiki/Captain_America%27s_Shield

Hire People

Image compliments of http://marvelcinematicuniverse.wikia.com/wiki/Captain_America%27s_Shield

Add Process

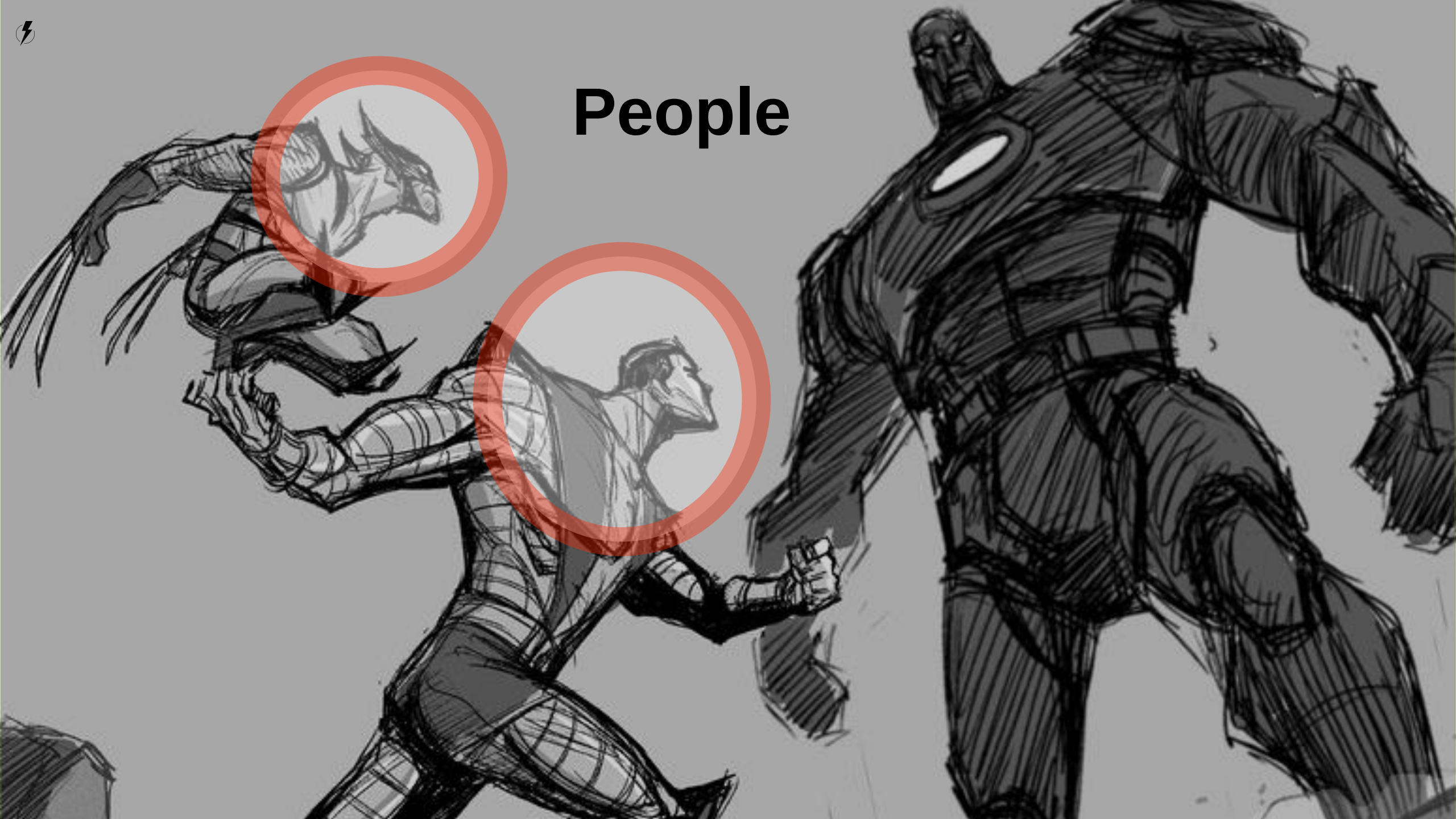
Image compliments of http://marvelcinematicuniverse.wikia.com/wiki/Captain_America%27s_Shield



Rinse & Repeat

Image compliments of http://marvelcinematicuniverse.wikia.com/wiki/Captain_America%27s_Shield

People




PEOPLE
HIRE
SMART
PEOPLE
image compliments of voydkessler on deviantart

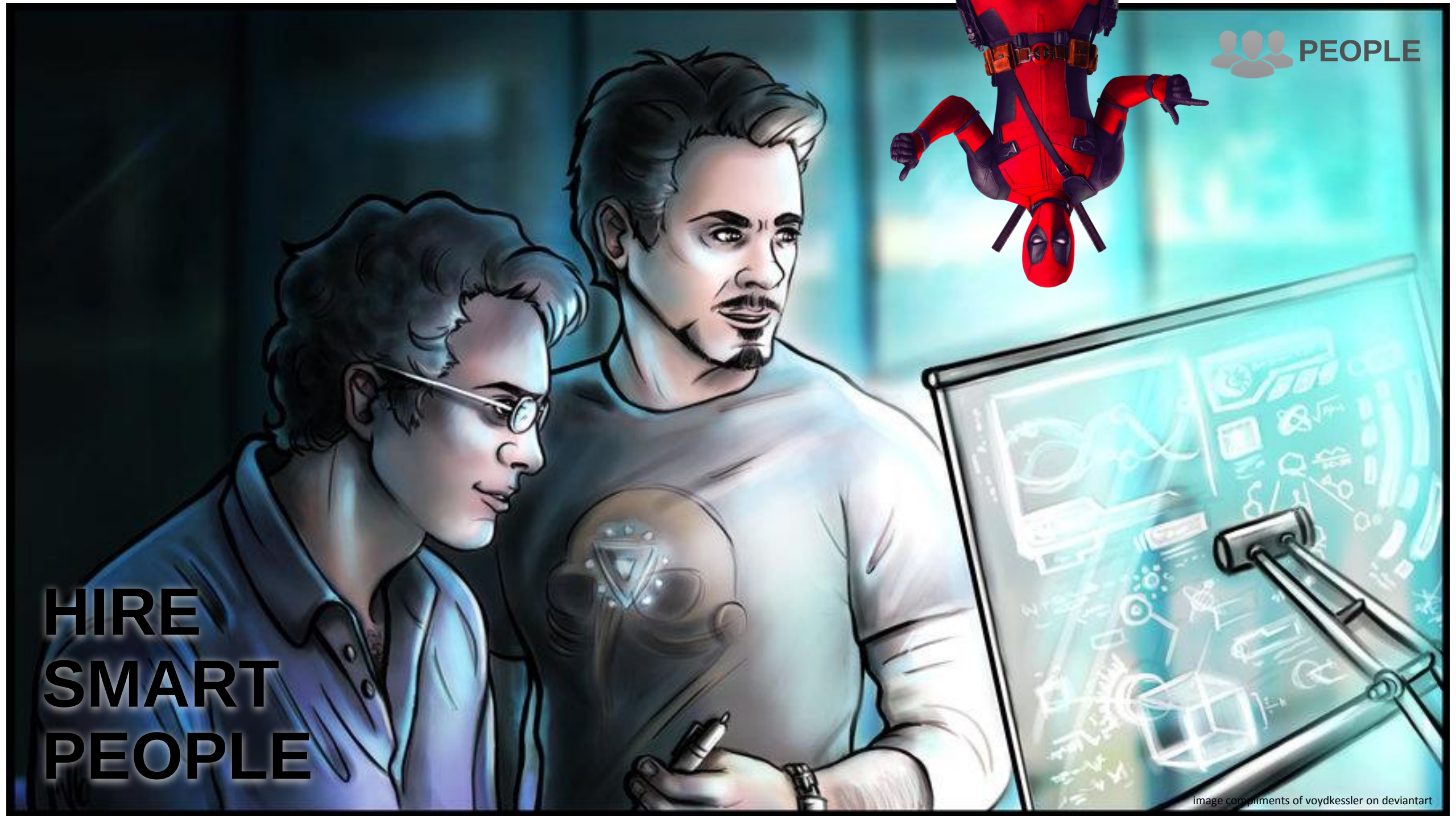


image compliments of voydkessler on deviantart

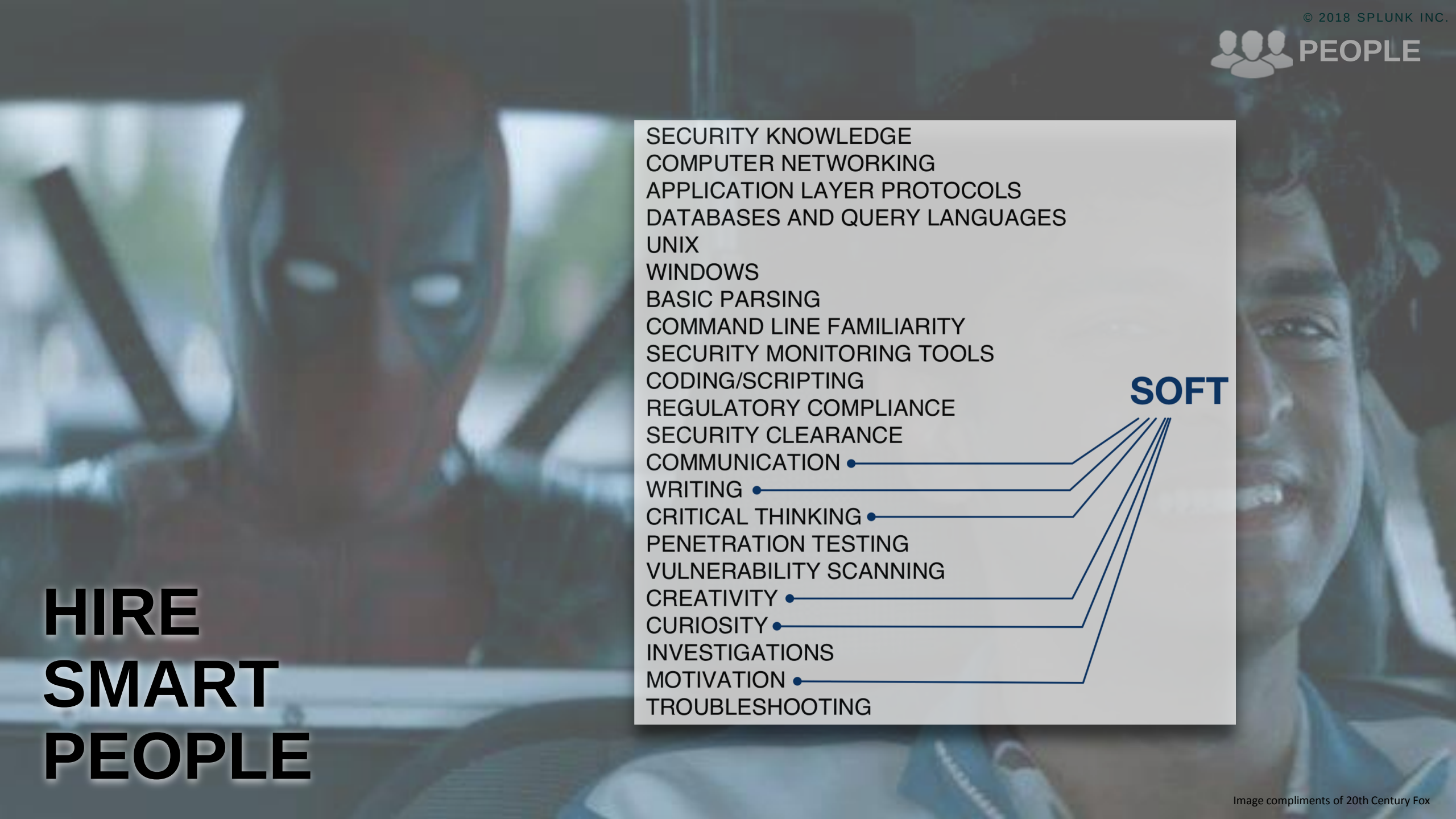
SECURITY KNOWLEDGE
COMPUTER NETWORKING
APPLICATION LAYER PROTOCOLS
DATABASES AND QUERY LANGUAGES
UNIX
WINDOWS
BASIC PARSING
COMMAND LINE FAMILIARITY
SECURITY MONITORING TOOLS
CODING/SCRIPTING
REGULATORY COMPLIANCE
SECURITY CLEARANCE
COMMUNICATION
WRITING
CRITICAL THINKING
PENETRATION TESTING
VULNERABILITY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

HIRE SMART PEOPLE

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

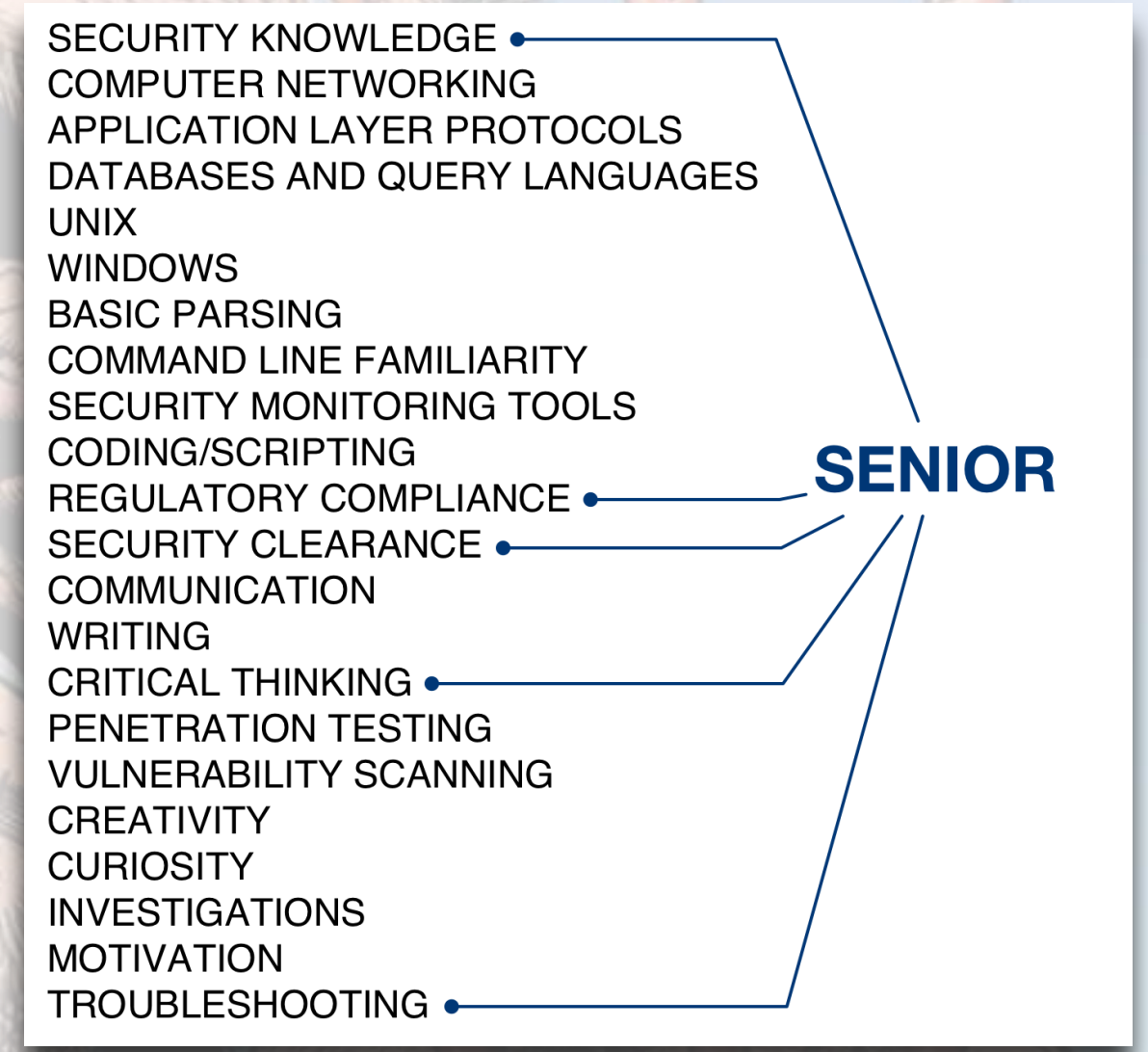
PEOPLE



HIRE SMART PEOPLE

Image compliments of 20th Century Fox

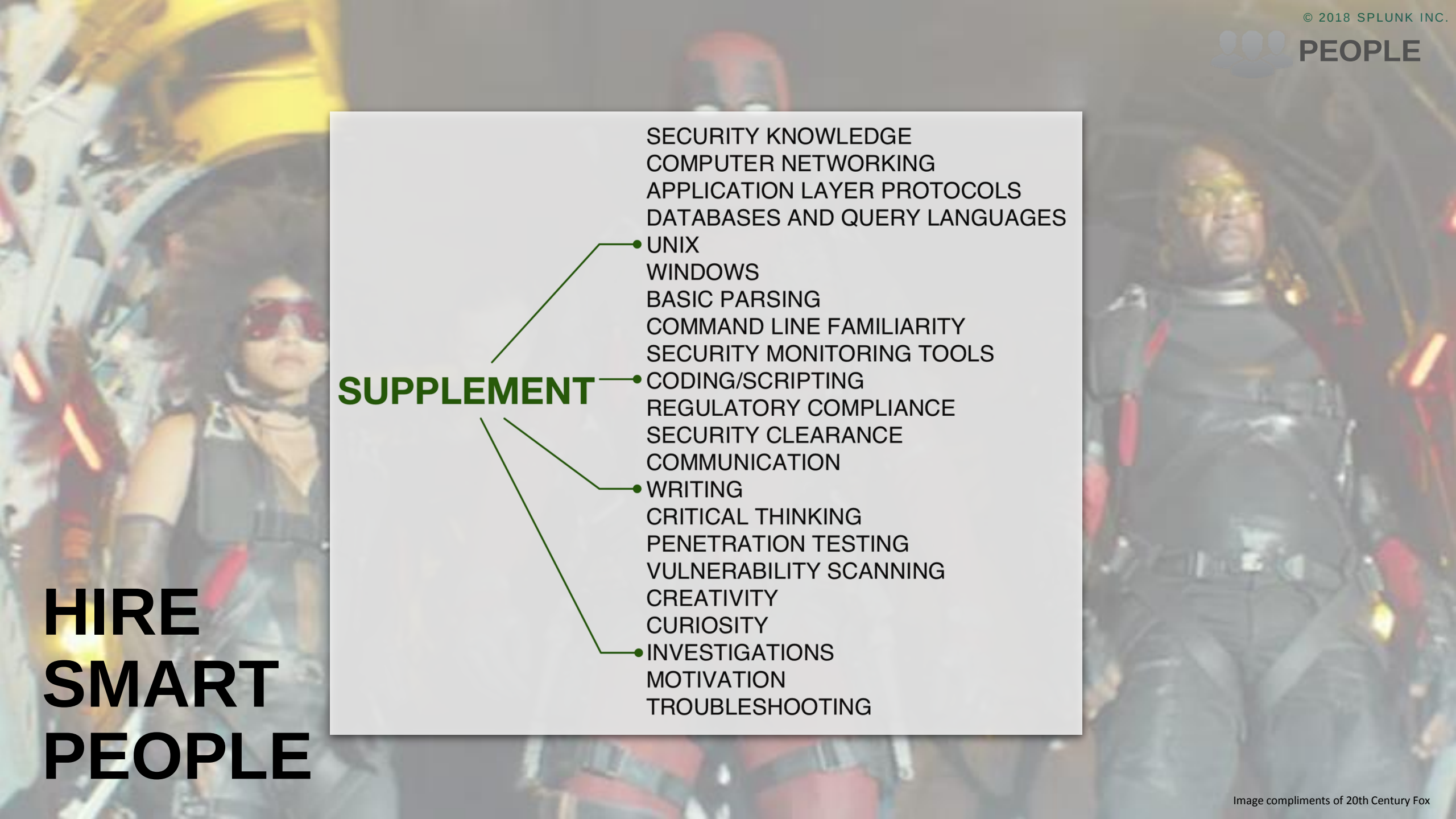
HIRE SMART PEOPLE



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



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

TRAINEE

HIRE SMART PEOPLE …and train them

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

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

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

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

PARTNERS

PEOPLE

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

PARTNERS

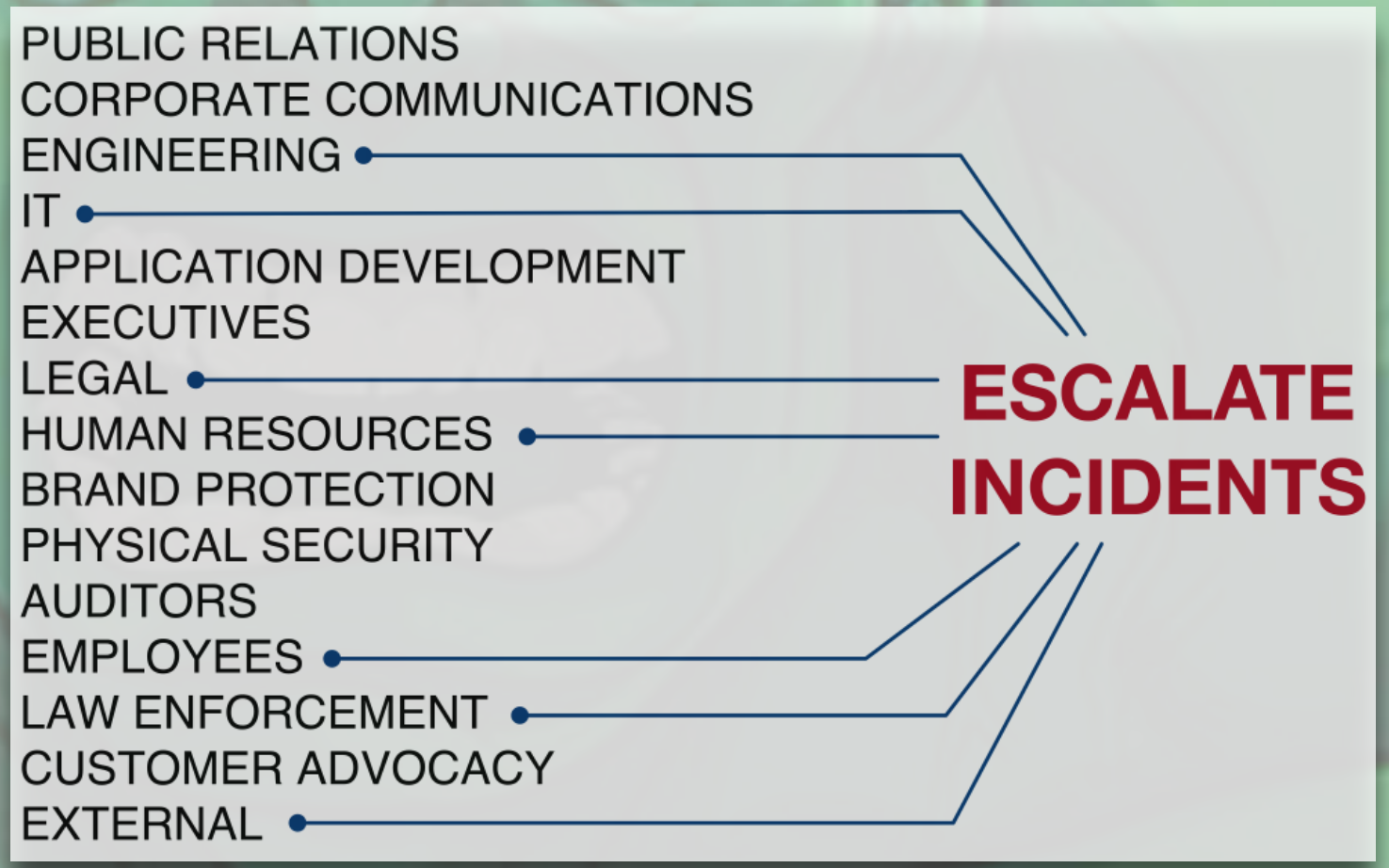
PEOPLE

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

PROVIDE DATA

PARTNERS

PEOPLE



PARTNERS

PARTNERS

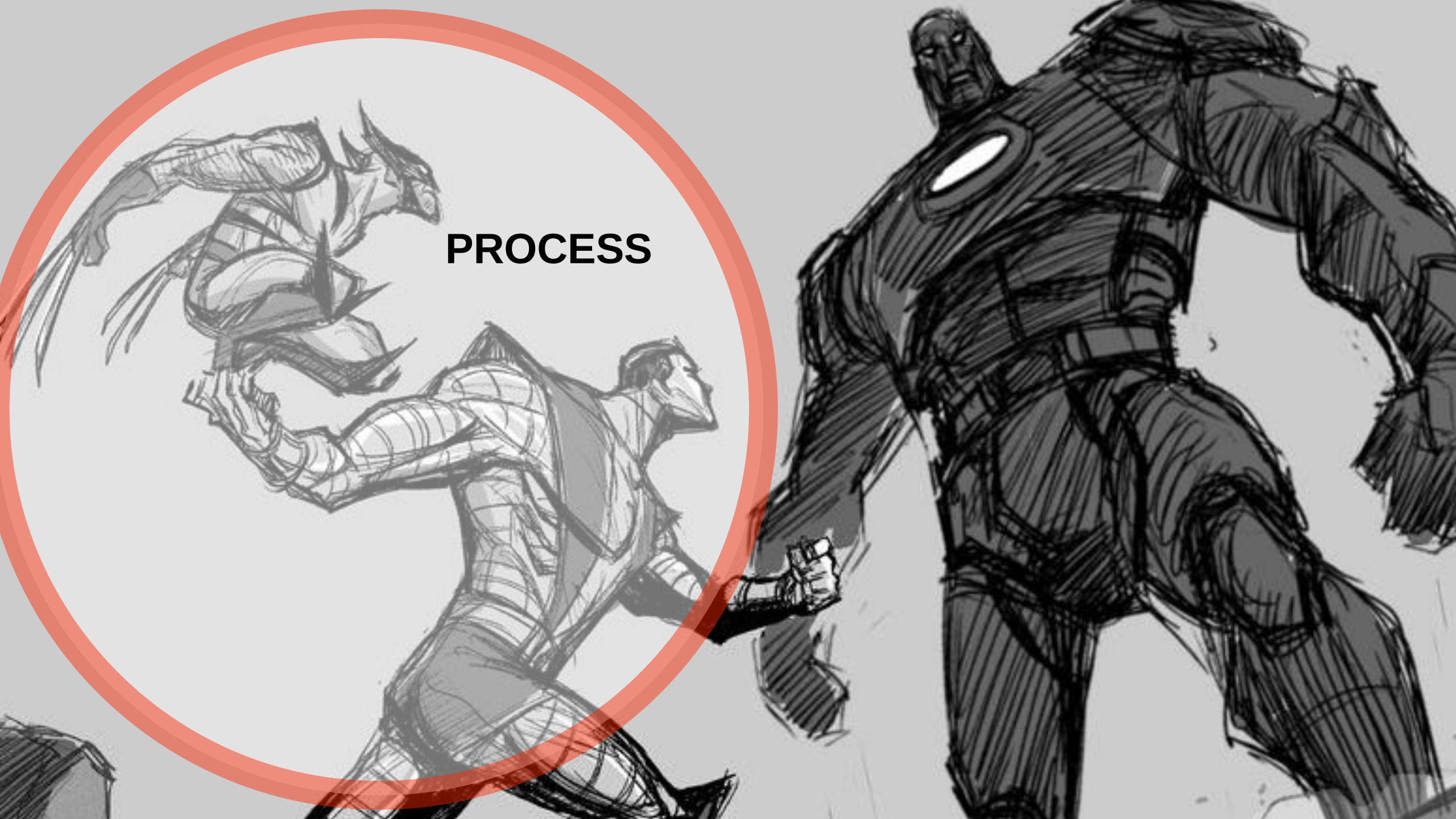
PEOPLE

FUNDING

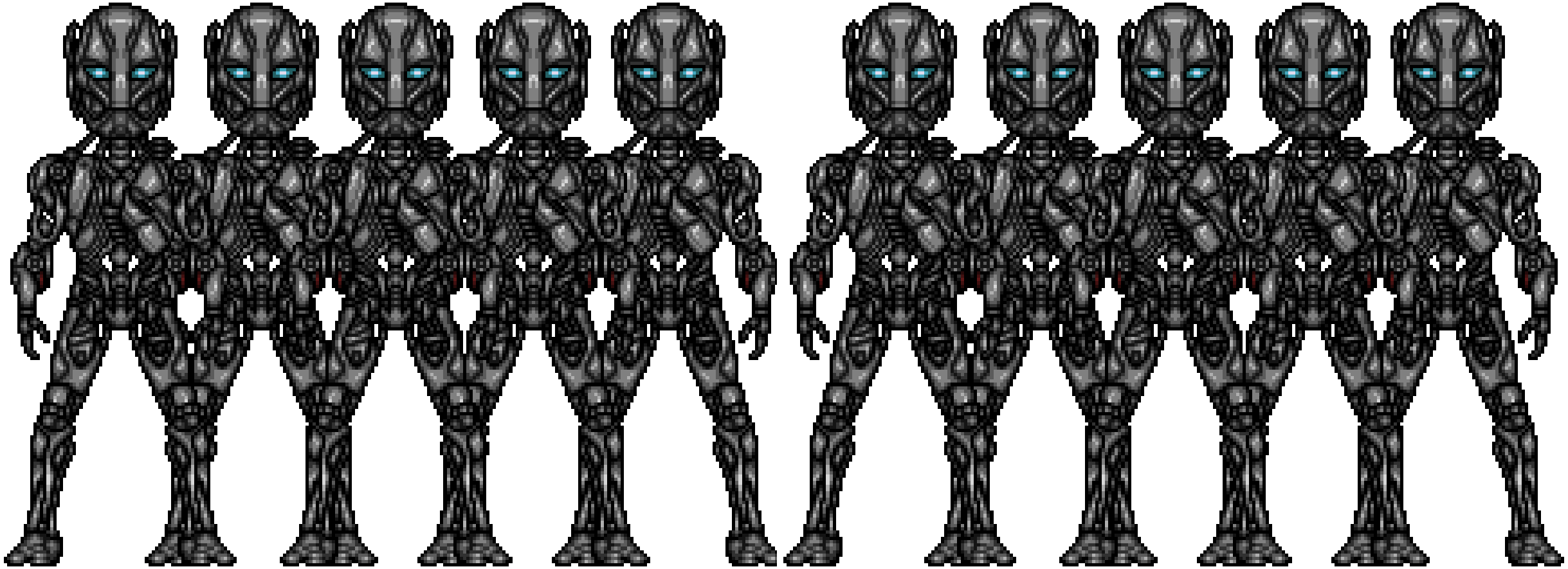
- PUBLIC RELATIONS
- CORPORATE COMMUNICATIONS
- ENGINEERING
- IT
- APPLICATION DEVELOPMENT
- EXECUTIVES
- LEGAL
- HUMAN RESOURCES
- BRAND PROTECTION
- PHYSICAL SECURITY
- AUDITORS
- EMPLOYEES
- LAW ENFORCEMENT
- CUSTOMER ADVOCACY
- EXTERNAL

PARTNERS

PROCESS

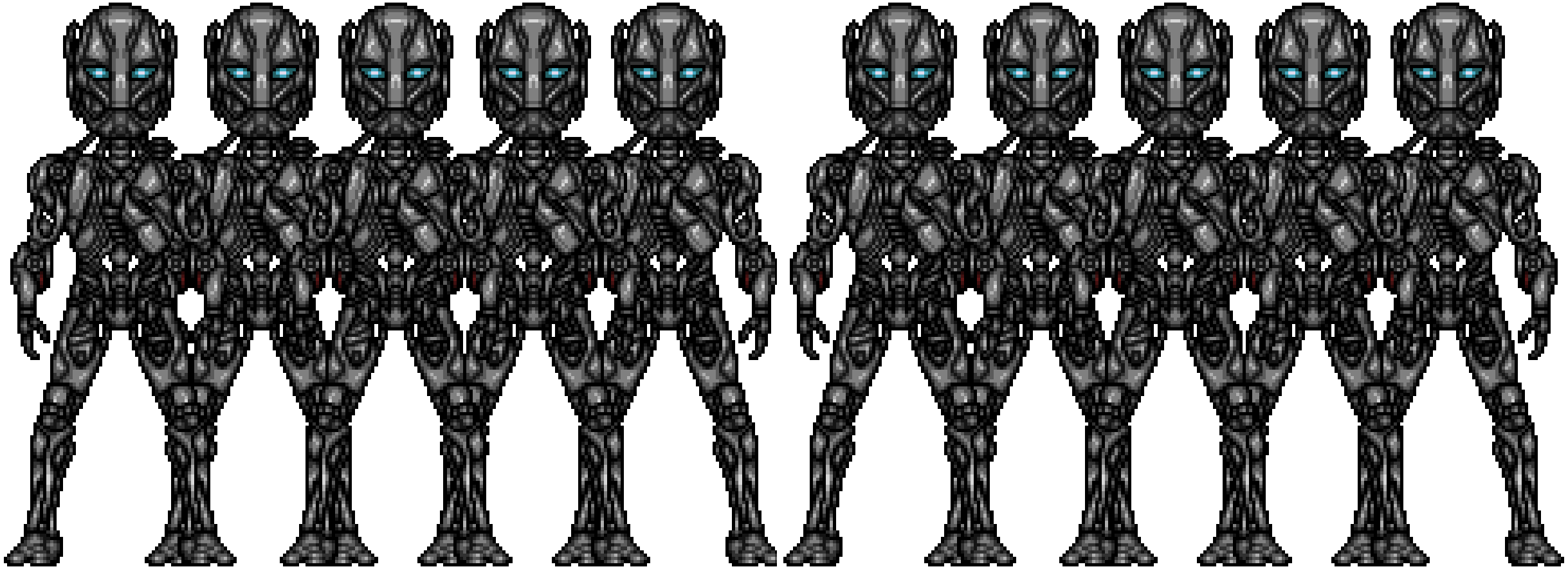


PROCESS

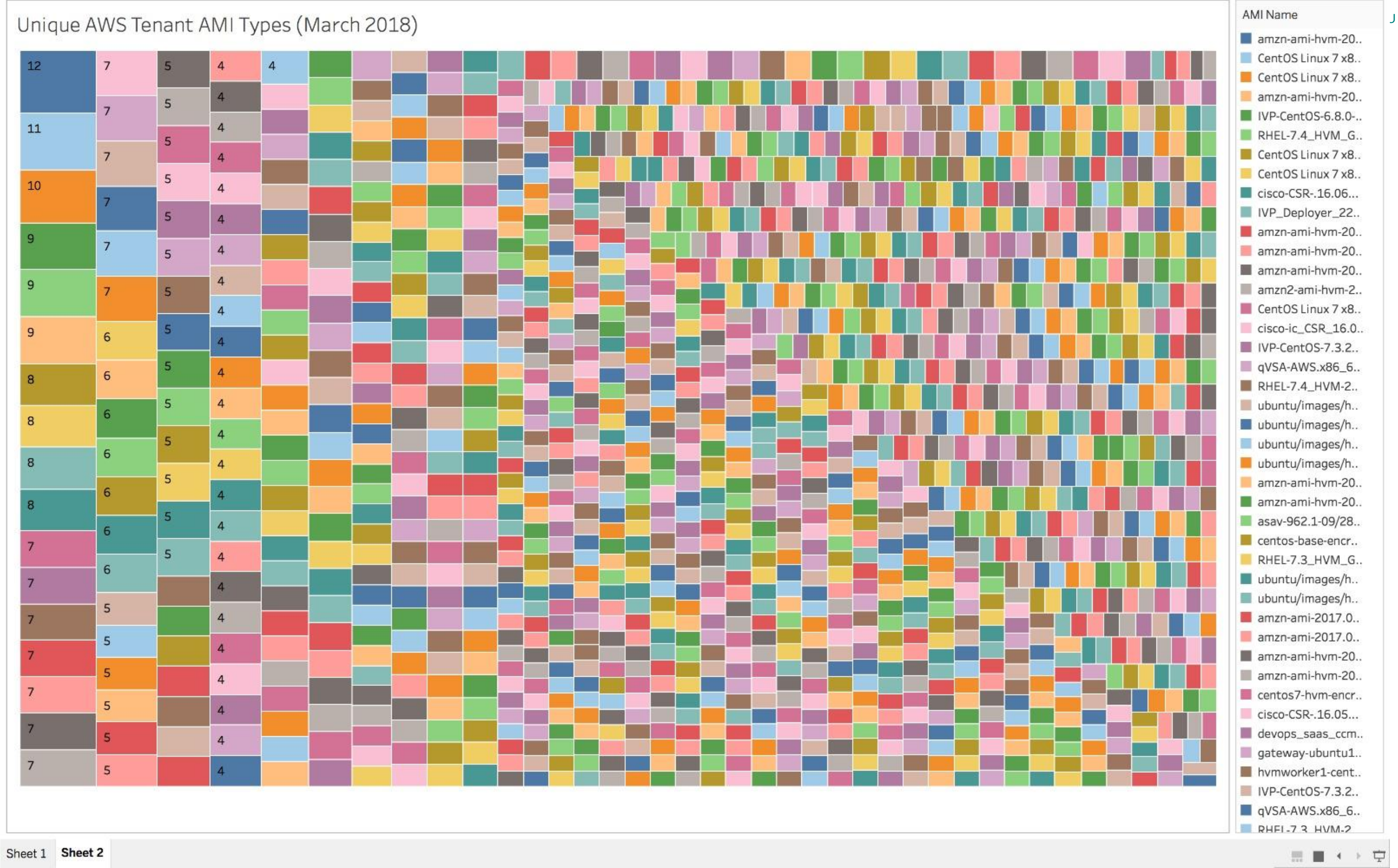


STANDARDS

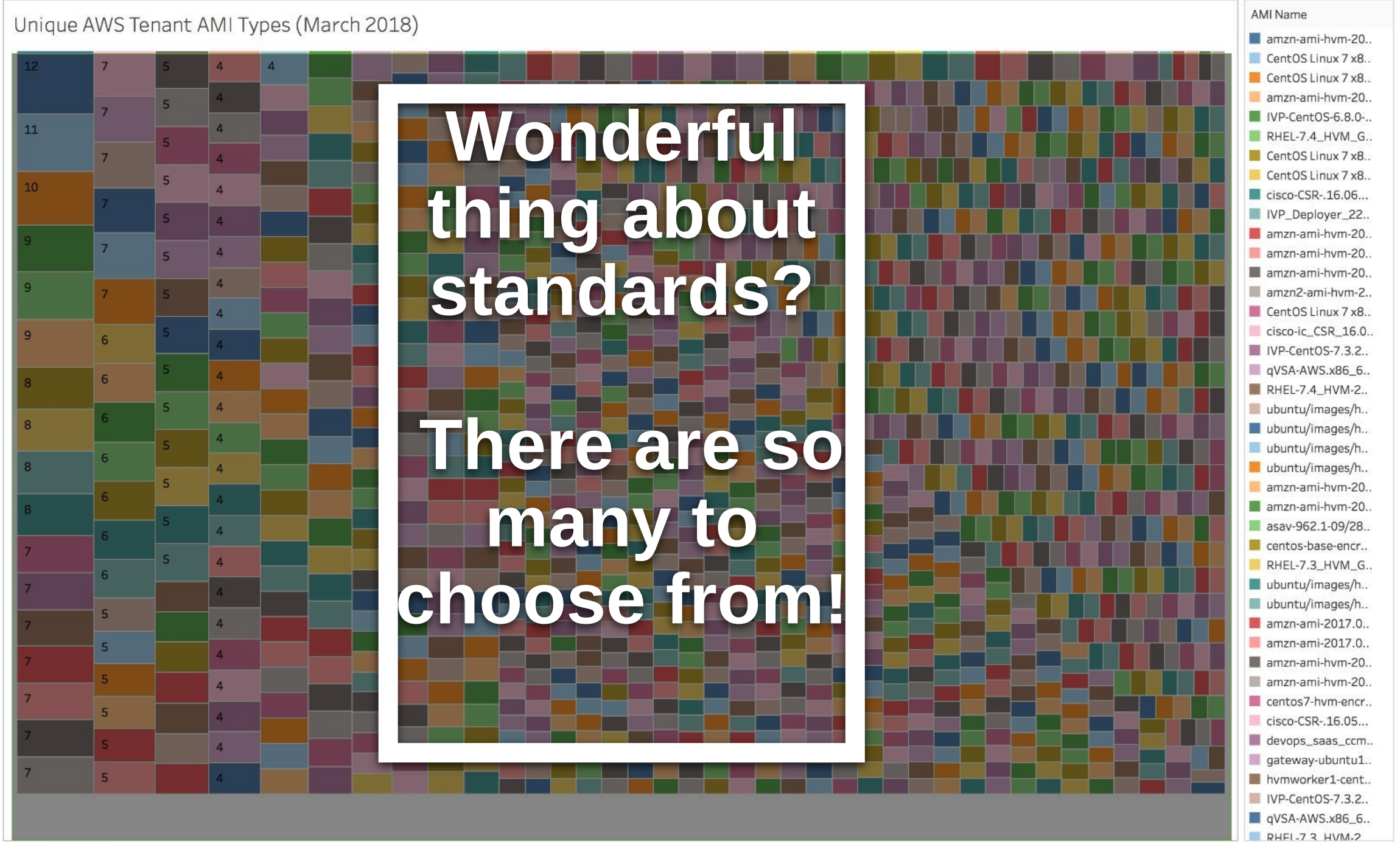
PROCESS



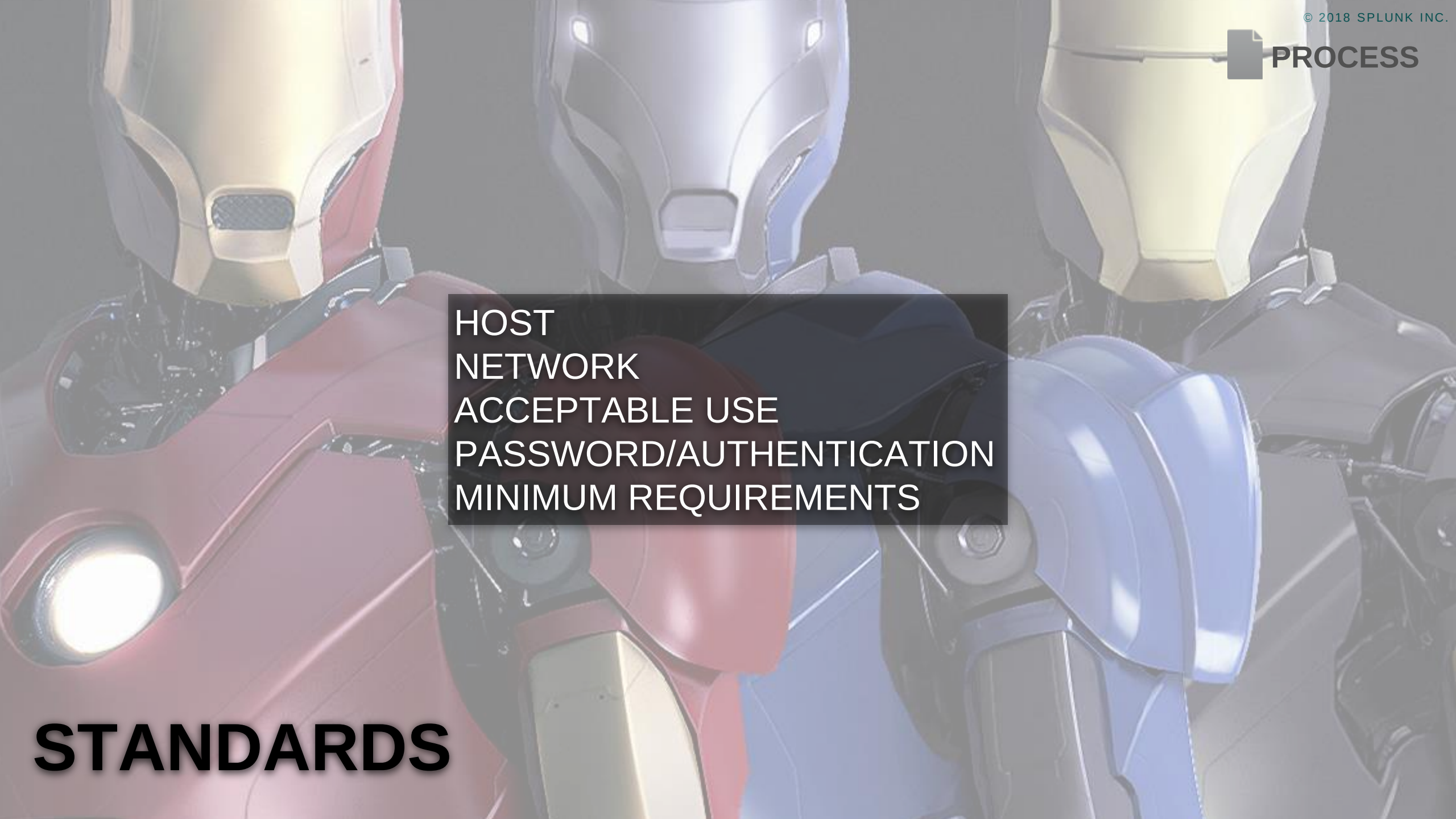
STANDARDS



Unique AWS Tenant AMI Types (March 2018)
12
11
10
9
9
9
8
8
8
8
7
7
7
7
7
7
7
AMI Name
amzn-ami-hvm-20..
CentOS Linux 7 x8..
CentOS Linux 7 x8..
amzn-ami-hvm-20..
IVP-CentOS-6.8.0-..
RHEL-7.4_HVM_G..
CentOS Linux 7 x8..
CentOS Linux 7 x8..
cisco-CSR-.16.06...
IVP_Deployer_22..
amzn-ami-hvm-20..
amzn-ami-hvm-20..
amzn-ami-hvm-20..
amzn2-ami-hvm-2..
CentOS Linux 7 x8..
cisco-ic_CSR_16.0..
IVP-CentOS-7.3.2..
qVSA-AWS.x86_6..
RHEL-7.4_HVM-2..
ubuntu/images/h..
ubuntu/images/h..
ubuntu/images/h..
ubuntu/images/h..
amzn-ami-hvm-20..
amzn-ami-hvm-20..
asav-962.1-09/28..
centos-base-encr..
RHEL-7.3_HVM_G..
ubuntu/images/h..
ubuntu/images/h..
amzn-ami-2017.0..
amzn-ami-2017.0..
amzn-ami-hvm-20..
amzn-ami-hvm-20..
centos7-hvm-encr..
cisco-CSR-.16.05...
devops_saas_ccm..
gateway-ubuntu1..
hvmworker1-cent..
IVP-CentOS-7.3.2..
qVSA-AWS.x86_6..
RHEL-7.3_HVM-2..
Sheet 1
Sheet 2


Unique AWS Tenant AMI Types (March 2018)
AMI Name
amzn-ami-hvm-20..
CentOS Linux 7 x8..
CentOS Linux 7 x8..
amzn-ami-hvm-20..
IVP-CentOS-6.8.0-..
RHEL-7.4_HVM_G..
CentOS Linux 7 x8..
CentOS Linux 7 x8..
cisco-CSR-.16.06...
IVP_Deployer_22..
amzn-ami-hvm-20..
amzn-ami-hvm-20..
amzn-ami-hvm-20..
amzn2-ami-hvm-2..
CentOS Linux 7 x8..
cisco-ic_CSR_16.0..
IVP-CentOS-7.3.2..
qVSA-AWS.x86_6..
RHEL-7.4_HVM-2..
ubuntu/images/h..
ubuntu/images/h..
ubuntu/images/h..
ubuntu/images/h..
amzn-ami-hvm-20..
amzn-ami-hvm-20..
asav-962.1-09/28..
centos-base-encr..
RHEL-7.3_HVM_G..
ubuntu/images/h..
ubuntu/images/h..
amzn-ami-2017.0..
amzn-ami-2017.0..
amzn-ami-hvm-20..
amzn-ami-hvm-20..
centos7-hvm-encr..
cisco-CSR-.16.05...
devops_saas_ccm..
gateway-ubuntu1..
hvmworker1-cent..
IVP-CentOS-7.3.2..
qVSA-AWS.x86_6..
RHEL-7.3_HVM-2..
Wonderful thing about standards?
There are so many to choose from!
Sheet 1
Sheet 2

PROCESS



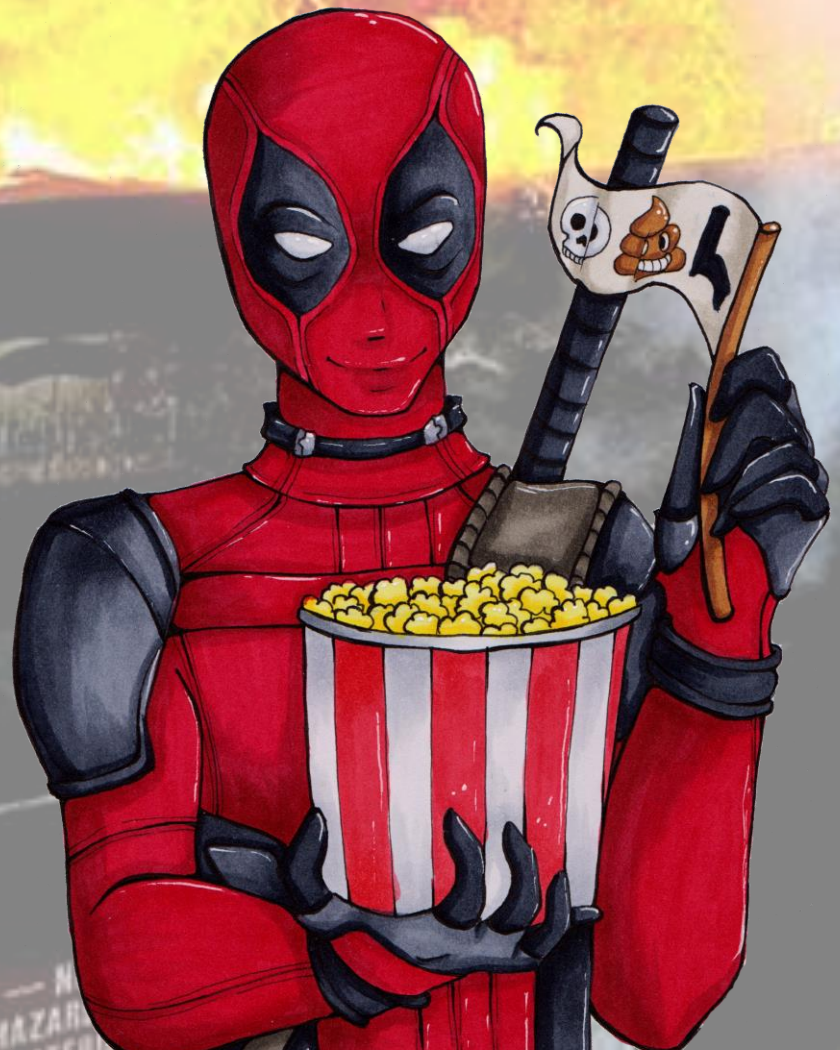
HOST
NETWORK
ACCEPTABLE USE
PASSWORD/AUTHENTICATION
MINIMUM REQUIREMENTS

STANDARDS

PROCESS

PREPARE FOR THE INEVITABLE

PREPARE FOR THE INEVITABLE



PROCESS


CHARTER


ESCALATION PATHS


ENGAGEMENT PROCESS

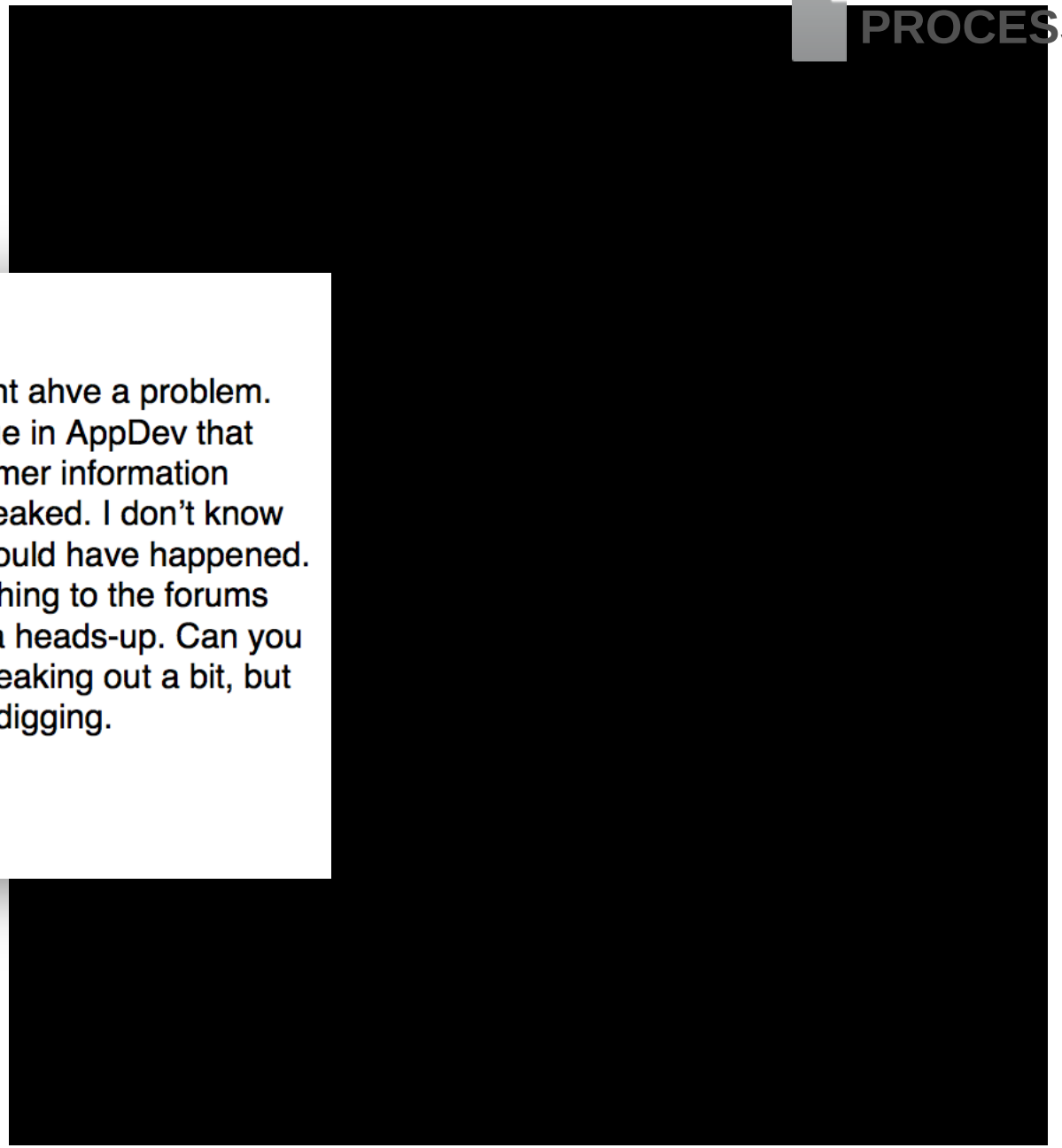

RESPONSE TEMPLATES


PARTNER DIRECTORY


SERVICE LEVEL AGREEMENTS

INCIDENT RESPONSE HANDBOOK

PROCESS



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.

CRISIS COMMS

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

PROCESS

SECURITY MONITORING PLAYBOOK

PROCESS

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

THREAT-BASED MONITORING PLAN

Image compliments of - on aminoapps.com

PROCESS

PLAYBOOK

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 Instance Created by Unusual User
Detects the first time a user creates a new instance.
Recommended
Searches Included
Audit Trail

AWS New API Call Per User
Looks for users that are using AWS APIs that they've never used before.
Recommended
Searches Included
Audit Trail
Blue Bubbles indicate the data source used by this example.

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
Audit Trail

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

Email Attachments With Lots Of Spaces
Attackers often use spaces as a means to obfuscate an attachment's file extension. This search looks for messages with email attachments that have a large number of spaces within the filename.
Recommended
Try ES Content Update
Email

Emails from Outside the Organization with Company Domains
Phishers will often try to send emails where the from address uses your organization's domain name, e.g., emailing finance from yourceo@yourcompany.com. Detect that now!
Recommended
Searches Included
Email

Fake Windows Processes
This example finds processes normally run from Windows\System32 or Windows\SysWOW64, running from some other location. This can indicate a malicious process trying to hide as a legitimate process.
Recommended
Searches Included
Endpoint Detection and Response
Windows Security

First Time Accessing an Internal Git Repository
Find users who accessed a git repository for the first time.
Recommended
Searches Included
Source Code Respository

Malicious PowerShell Process With Obfuscation Techniques
This search looks for powershell processes launched with arguments that have characters indicative of obfuscation on the command line.
Recommended
Try ES Content Update
Endpoint Detection and Response

Public S3 Bucket in AWS
Detects when new or existing S3 buckets are set to public.
Recommended
Searches Included
Audit Trail

Registry Keys Used For Persistence
The search looks for modifications to registry keys that can be used to launch an application or service at system start.
Recommended
Try ES Content Update
Endpoint Detection and Response

User with Increase in Outgoing Email
Both to detect data exfiltration and compromised account, we can analyze users that are sending out dramatically more data than normal. This search looks per source email address for big increases in volume.
Recommended
Searches Included
Email

Abnormally High Number of Endpoint Changes By User
Detects an abnormally high number of endpoint changes by user account, as they relate to restarts, audits, filesystem, user, and registry modifications.
Try Splunk ES
Endpoint Detection and Response

Anomalous New Process
Alerts when an anomalous number hosts are detected with a new process.
Try Splunk ES
Endpoint Detection and Response

Anomalous New Service
Alerts when an anomalous number hosts are detected with a new service.
Try Splunk ES
Endpoint Detection and Response

Attrib.exe used to hide files/directories via commandline
Attackers leverage an builtin Windows binary, attrib.exe, to mark specific as hidden by using specific flags so that the victim does not see the file. The search looks for specific command line arguments to detect the use of attrib.exe to hide files.
Try ES Content Update
Endpoint Detection and Response

AWS APIs Called More Often Than Usual Per User
Builds a per-user baseline for how many API calls is normal, and then alerts for deviations.
Searches Included
Audit Trail

AWS Cloud Provisioning Activity from Unusual IP
Looks for AWS Provisioning activities that occur from new IPs (for organizations with strict IP controls).
Searches Included
Audit Trail

AWS Instance Modified by Unusual User
Detects the first time a user modifies an existing instance.
Searches Included
Audit Trail

Chained Exploit Followed by Suspicious Events Detected
Host and Network IDS event categories, detect events with a category of 'backdoor' or 'trojan' followed by a signature categorized as 'post exploit' on a given host or network with a given time period.
Use Splunk PS
IDS or IPS
Host-based IDS

Clients Connecting to Multiple DNS Servers
This search allows you to identify the endpoints that have connected to more than five DNS servers over the timeframe of the search.
Try ES Content Update
DNS

Common Filename Launched from New Path
Simpler malware will hide in plain sight with a filename like explorer.exe, running in the user profile. This detection will look for new paths, for common / expected executables. (MITRE CAR Reference)
Searches Included
Endpoint Detection and Response
Windows Security

Communication outbound to regions without business relationship
Outbound communication with servers hosted in regions where the organization does not expect to have employees, customers, or suppliers.
Use Splunk PS
IDS or IPS

Concentration of Attacker Tools by SHA1 Hash
It's uncommon to see attacker tools used in rapid succession on an endpoint. This search will identify tools by file hash, and look for multiple executions. (MITRE CAR Reference)
Searches Included
Endpoint Detection and Response

Concentration of Discovery Tools by Filename
It's uncommon to see many host discovery tools launched on an endpoint, except in very specific situations. This search will identify tools by filename, and look for many launches. (MITRE CAR Reference)
Searches Included
Endpoint Detection and Response
Windows Security

Concentration of Discovery Tools by SHA1 Hash
It's uncommon to see many discovery tools launched on an endpoint, except in specific situations. This search will identify tools by file hash, and look for several in quick succession. (MITRE CAR Reference)
Searches Included
Endpoint Detection and Response

Detect hosts connecting to dynamic domain providers
Malicious actors often abuse legitimate Dynamic DNS services to host malicious payloads or interactive command and control nodes. Attackers will automate domain resolution changes by routing dynamic domains to countless IP addresses to circumvent firewall blocks, blacklists as well as frustrate a network defenders analytic and investigative processes. This search will look for DNS queries made from within your infrastructure to suspicious dynamic domains

Detect Journal Clearing
This use case looks for the fsutil process clearing the update sequence number (USN) change journal.
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 creation of this file in the C:\ drive is driven by a motive to perform path interception.
Try ES Content Update
Endpoint Detection and Response

Detect Prohibited Applications Spawning cmd.exe
This search looks for executions of cmd.exe spawned by a process that is often abused by attackers and does not typically launch cmd.exe.
Try ES Content Update
Endpoint Detection and Response

Detect Use of cmd.exe to Launch Script Interpreters
This search looks for the execution of cscript.exe or wscript.exe with a parent of cmd.exe. The search will return the full command lines for these executions, as well as the target system, sorted by time.
Try ES Content Update
Endpoint Detection and Response

Detection of DNS Tunnels
This search is used to detect DNS tunneling, by calculating the sum of the length of DNS queries and DNS answers. The search also filters out potential false positives by filtering out queries made to internal systems and the queries originating from internal DNS, Web, and Email servers. 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 an unusually large volume of DNS traffic

Disabling Remote User Account Control
The search looks for modifications to registry keys that control the enforcement of Windows User Account Control (UAC).
Try ES Content Update
Endpoint Detection and Response

DNS Query Length With High Standard Deviation
This search allows you to identify DNS requests and compute the standard deviation on the length of the names being resolved, then filter on two times the standard deviation to show you those queries that are unusually large for your environment.
Try ES Content Update
DNS

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 Queries
Alerts when a host starts sending excessive DNS queries
Try Splunk ES
DNS

Excessive Proxy Denies by Single Host
Excessive proxy blocks can be a good indicator of a potential automated beacon or malware phone home.
Use Splunk PS
Web Proxy

Familiar Filename Launched with New Path on Host
Processes are typically launched from the same path. When those paths change, it can be a malicious process masquerading as a valid one, to hide in task manager. (MITRE CAR Reference)
Searches Included

Find Processes with Renamed Executables
Oftentimes, attackers will execute a temporary file, and rename it to something innocuous (e.g. svchost.exe) to maintain persistence. This search will look for renamed executables. (MITRE CAR Reference)

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

splunkbase™

Search App by keyword, technology...

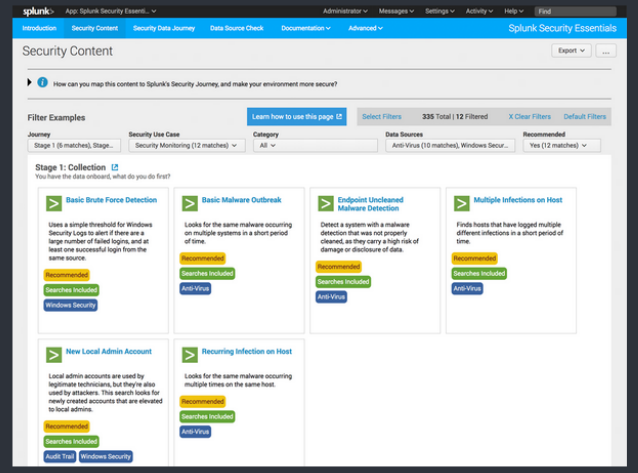
My Account

Support & Services

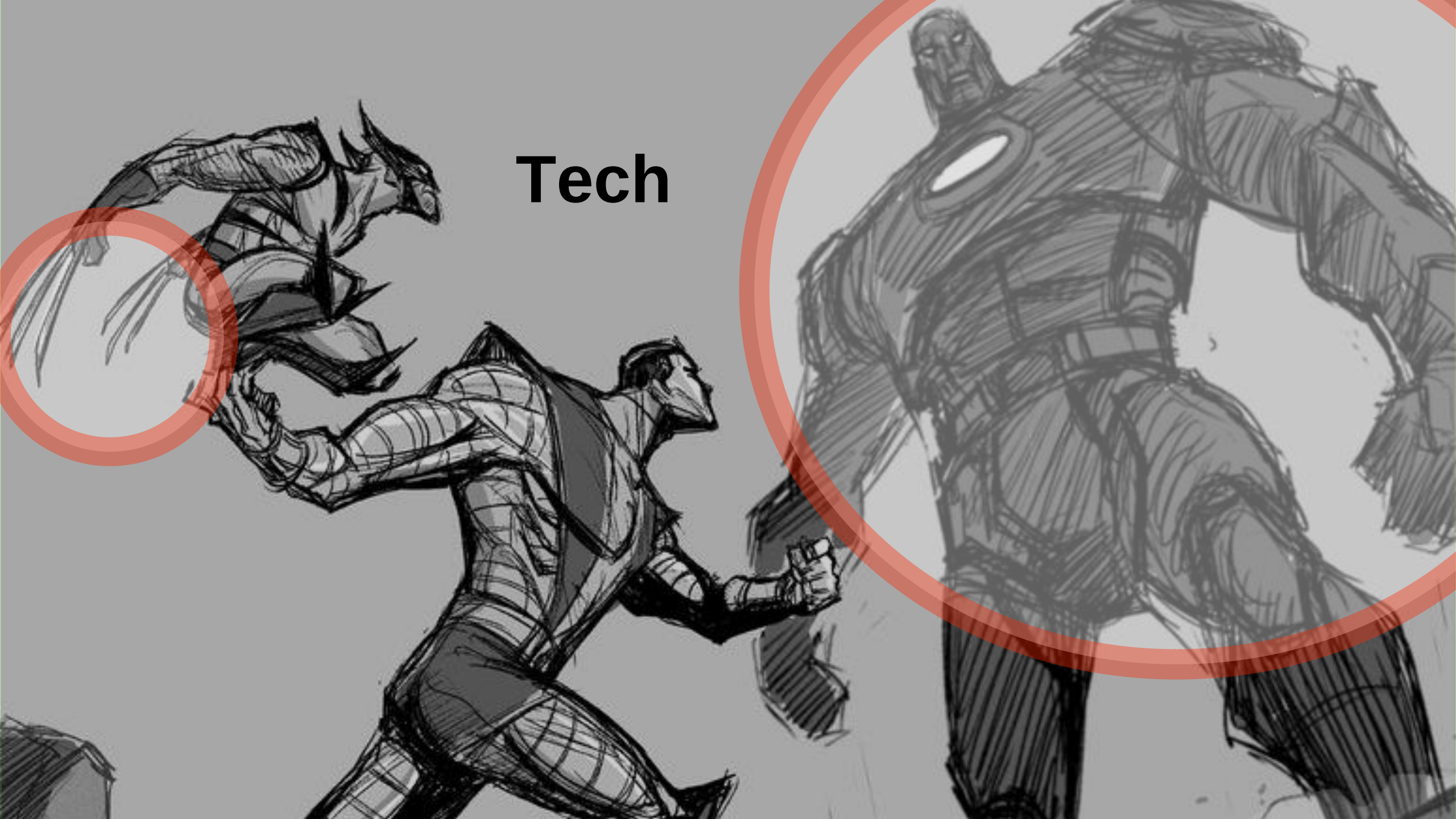
Splunk Security Essentials

22 ratings

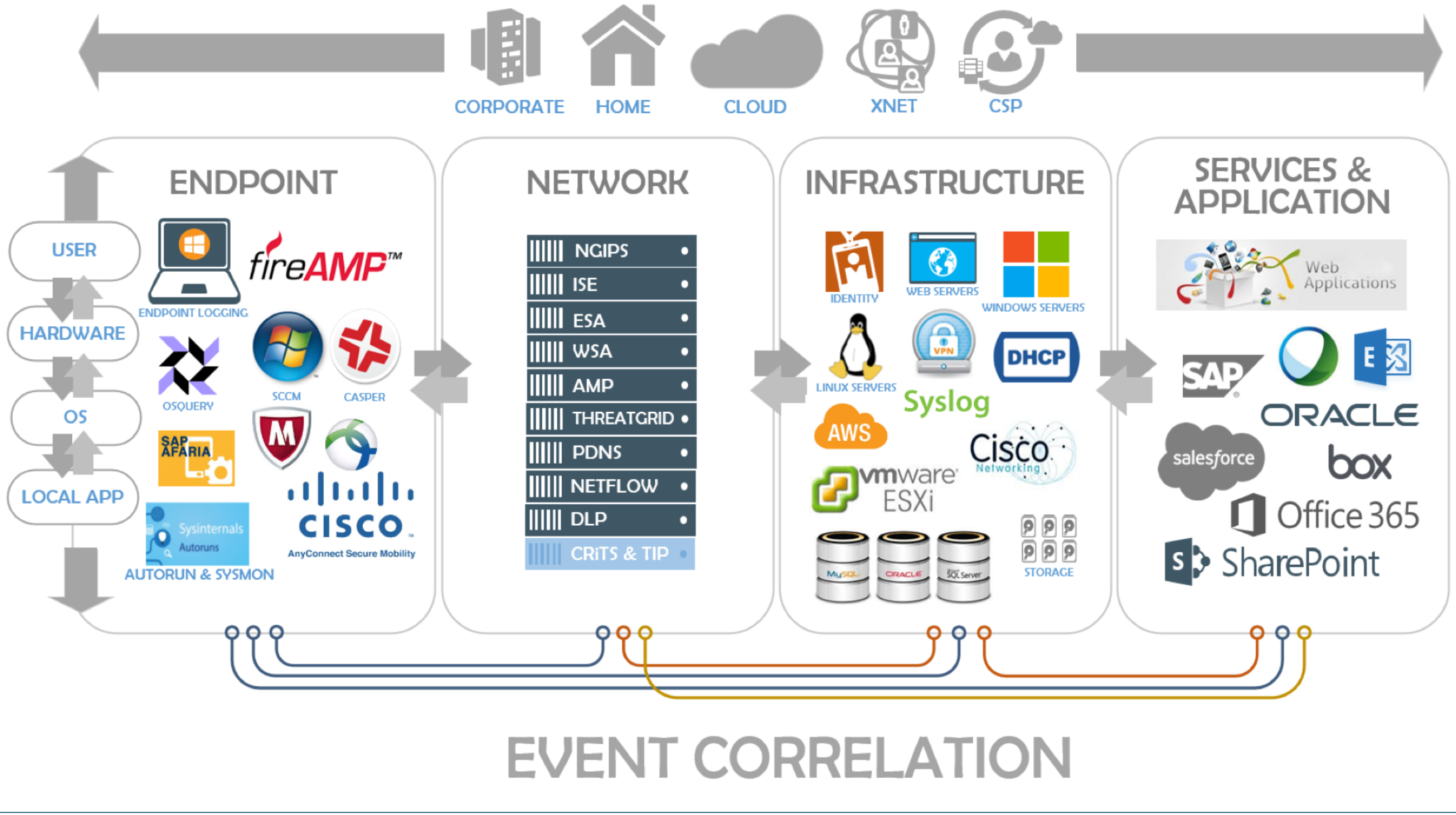
Splunk Built



Tech

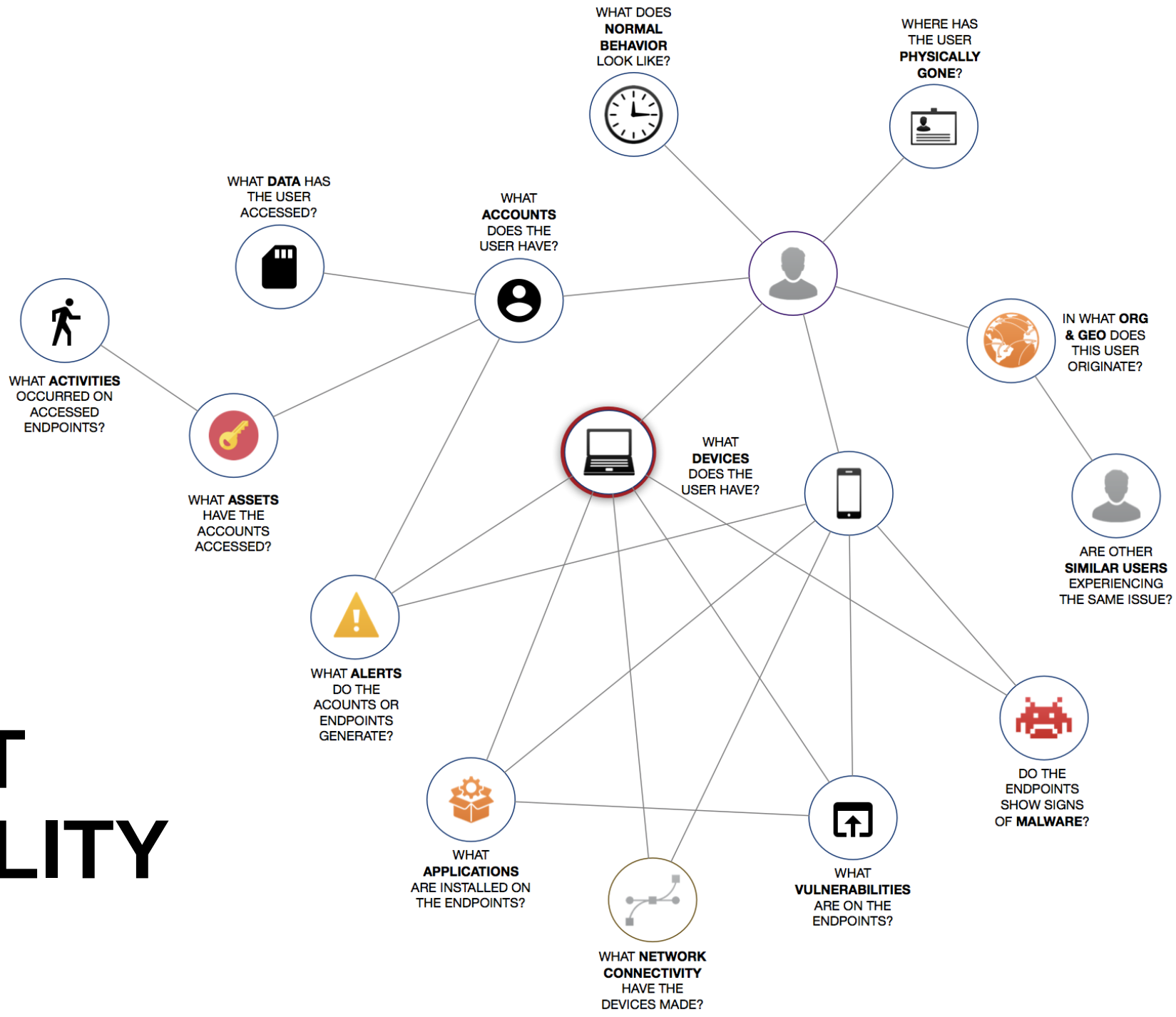


UNDERSTAND YOUR ENVIRONMENT



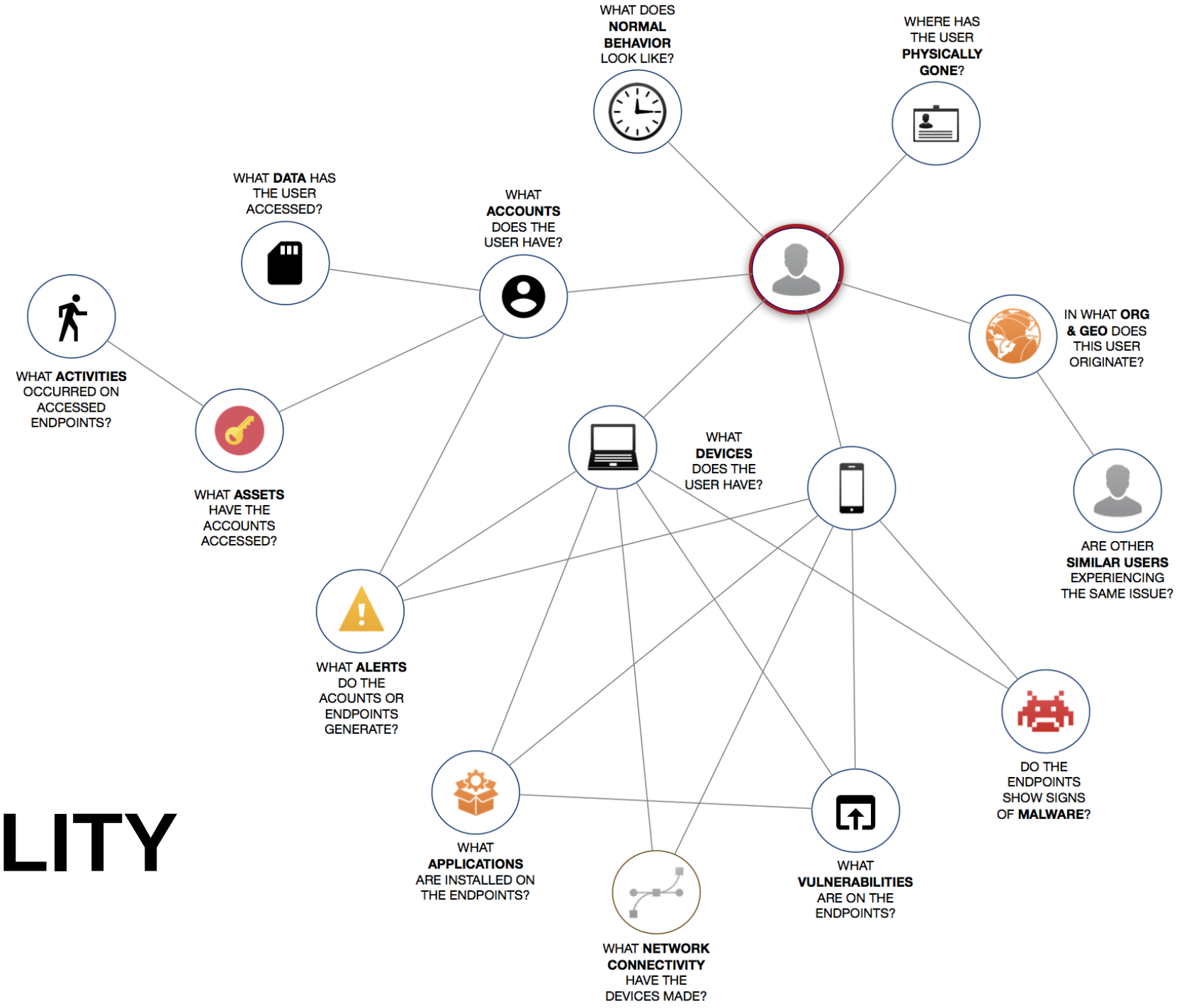
TECH

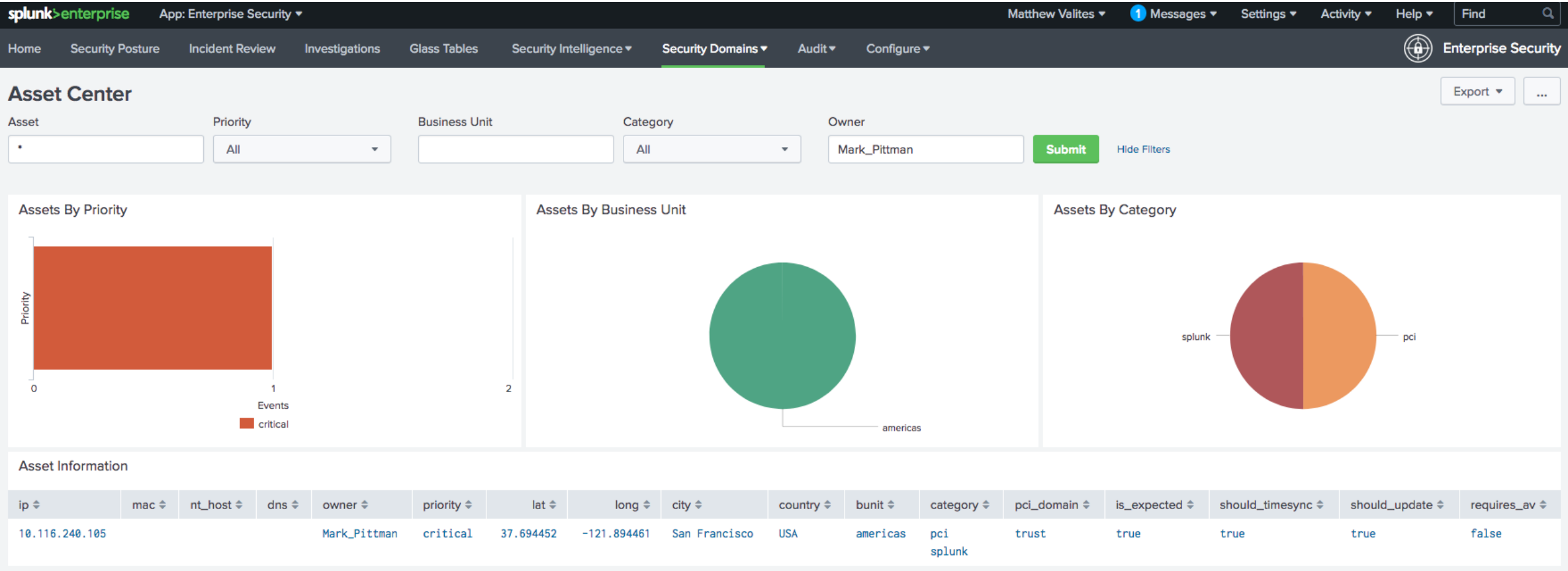
ASSET VISIBILITY



TECH

USER VISIBILITY





SYSTEM OF RECORD

TECH

Session Center

Export ▾ ...

Search: 10.116.240.105

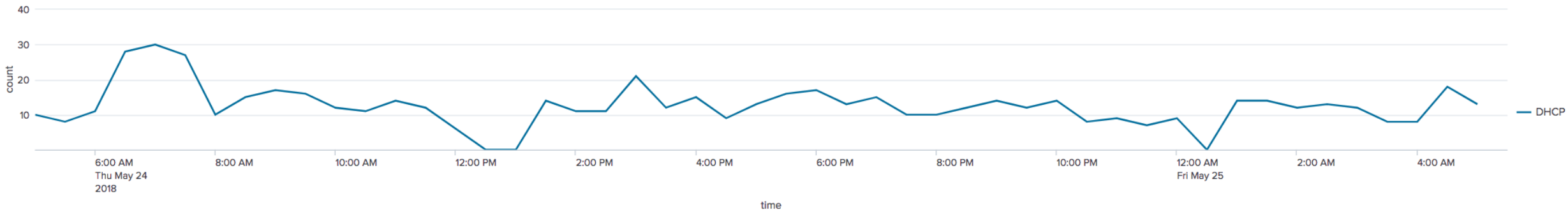
Select entity type: Device

Last 24 hours

Submit | Hide Filters

Network Sessions Data Model | User Behavior Analytics

Sessions Over Time



Session Details

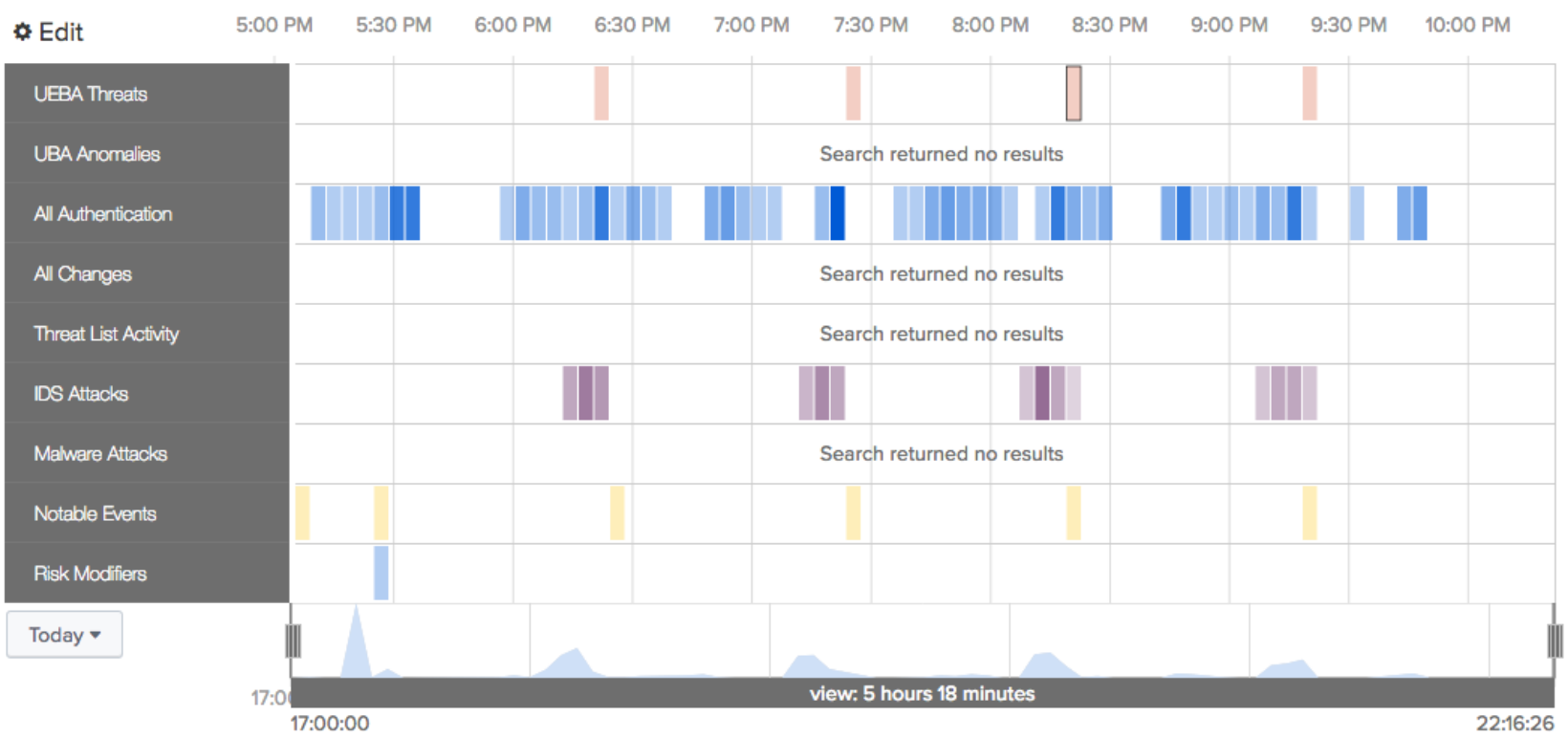
_time	src	ip	mac	nt_host	dns	user
2018-05-25 05:16:25		10.116.240.105	unknown	unknown	unknown	unknown
2018-05-25 05:13:51		10.116.240.105	c7:df:23:1a:e8:ba	SEP001BD4587CFF	unknown	unknown
2018-05-25 05:13:47		10.116.240.105	af:fd:16:4f:9e:d8	D2D6HLJ1	unknown	unknown
2018-05-25 05:13:34		10.116.240.105	af:fd:16:4f:9e:d8	SEP001BD4587CFF	unknown	unknown
2018-05-25 05:12:36		10.116.240.105	d3:da:83:05:5e:2a	RLDP	unknown	unknown
2018-05-25 05:11:10		10.116.240.105	72:3d:78:de:38:ec	SEP001BD4587CFF	unknown	unknown
2018-05-25 05:10:31		10.116.240.105	ba:b7:72:7a:16:30	SEP001BD4587CFF	unknown	unknown
2018-05-25 05:10:00		10.116.240.105	1a:ae:35:d8:b8:52	SEP001BD4587CFF	unknown	unknown
2018-05-25 05:09:14		10.116.240.105	c7:df:23:1a:e8:ba	SEP001BD4587CFF	unknown	unknown
2018-05-25 05:08:30		10.116.240.105	c7:df:23:1a:e8:ba	632-IMAC-04	unknown	unknown

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

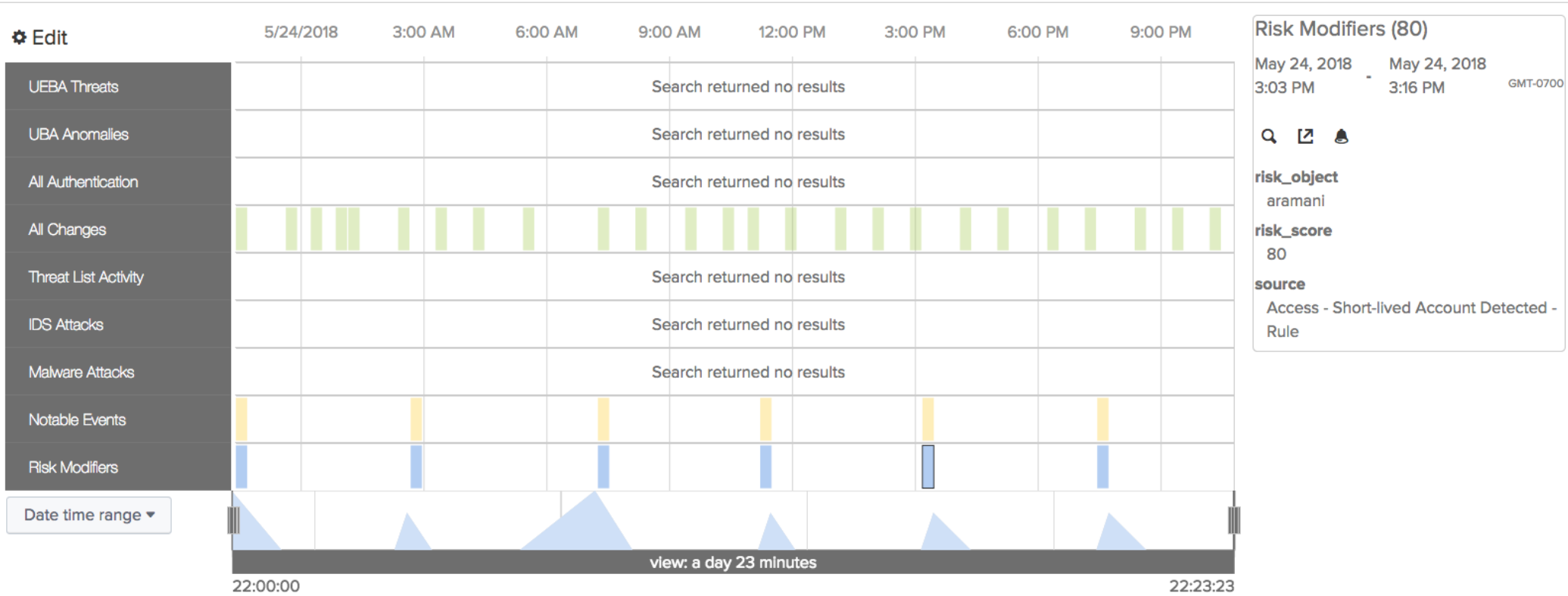
Devices
1.94.32.234
10.1.1.26
+11 more

Domains

Identity Investigator

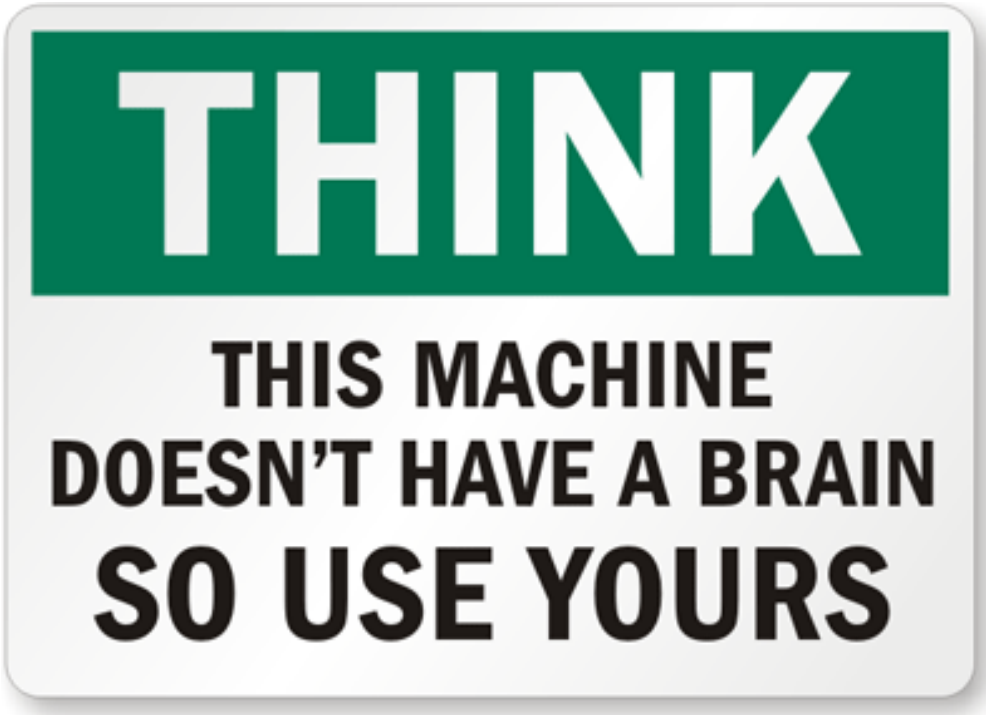
aramani Search

aramani is not a known identity.



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

Awe…

Sorry buddy.

Image courtesy of ClipartXtras

Models

Streaming Models | Batch Models

Streaming Models (18)

Search

NAME	EVENTS	EPS	LAST PROCESSED
Anomaly Aggregation Task Creates descriptive analytics from all generated anomalies.	127	4K	May 26, 2018 1:31 PM
Browser Exploitation Model Detects sequences of HTTP requests within a short period of time that suggests infection has taken place.	40.3K	43K	May 24, 2018 3:34 AM
Event Aggregation Task Creates aggregates based on configured cube definitions. The aggregates are stored for further analysis.	1M	8.2K	May 24, 2018 3:41 AM
Fixed Patterns in Microsoft Windows Logs Model Raises anomalies when the input data matches a set of predefined patterns in Microsoft Windows logs.	162K	18.9K	May 24, 2018 3:29 AM
Fixed Patterns in Network Traffic Model	903K	0	May 24, 2018 3:42 AM

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

Image compliments of movieplayer.net

TECH

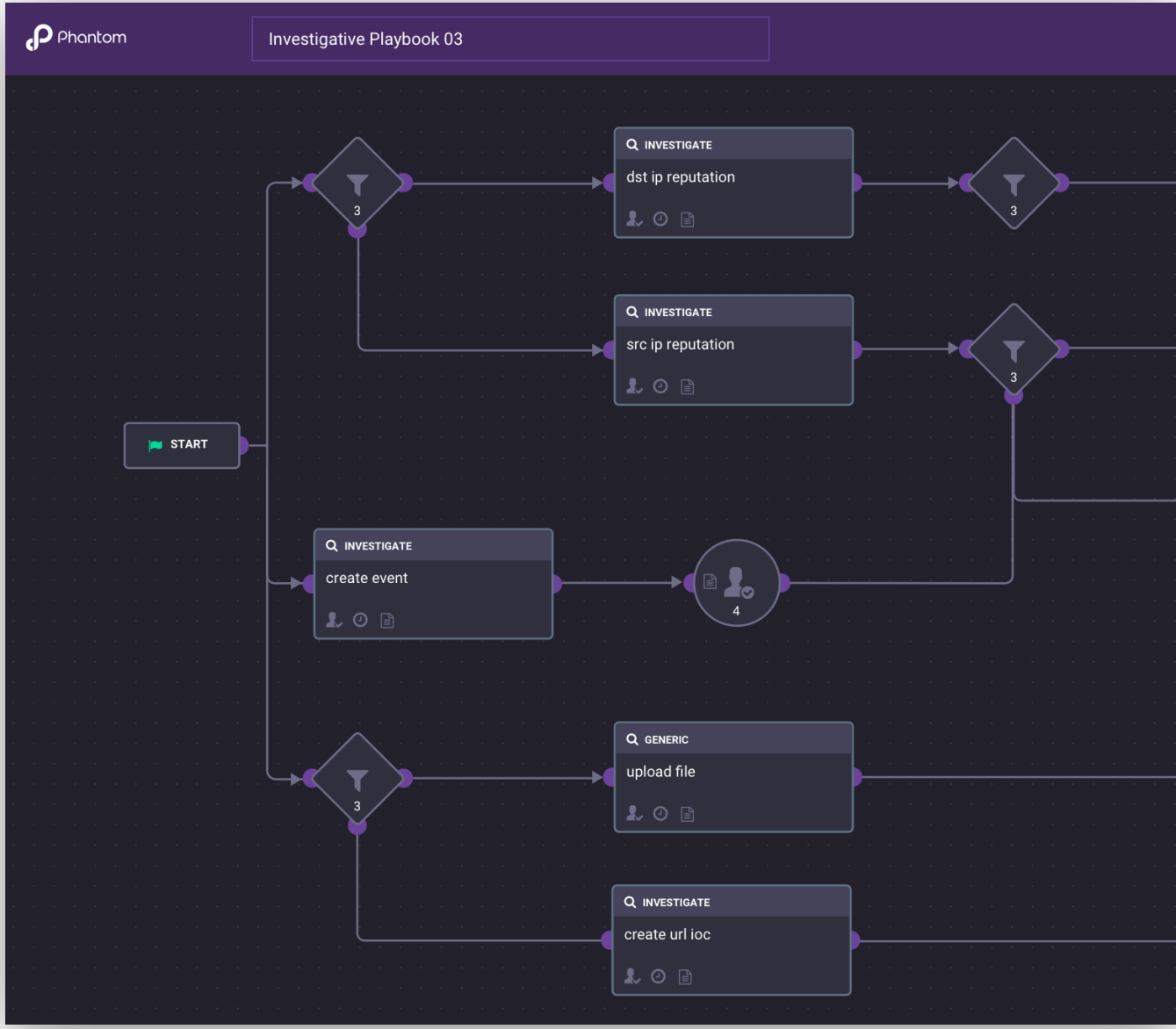
Automation

- 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



SHOWING VALUE

Image compliments of wooser on pinterest

SECURITY & TRUST ORGANIZATION REPORTING DASHBOARD

SELECT METRICS REPORTING

EXECUTIVE_NAME | SELECT ORGANIZATION | SELECT DEPARTMENT | SELECT SERVICE | SELECT ENVIRONMENT

DATE RANGE

Q4 FY17

INCIDENT OVERVIEW

CSIRT INCIDENTS	DATA INCIDENTS	VULNERABILITIES	POLICY VIOLATIONS	STOE
23	6	68	39	1

INCIDENT COST

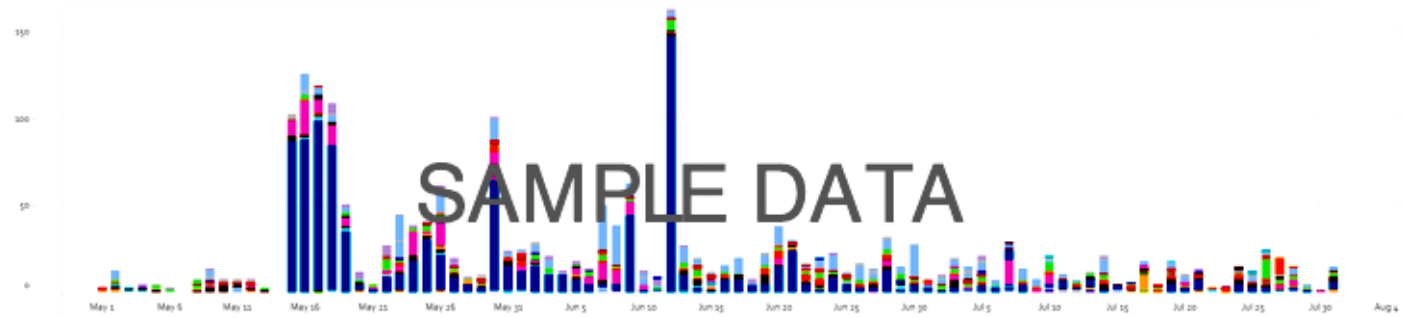
$6.8m

RISK SCORE

Q1	Q2	Q3	Q4
88	82	74	61

57

CSIRT | DATA | VULN | POLICY | STOE



DATA CENTER	DBU HOST	DESKTOP	EXTRANET	GUESTNET	HOME	LAB	OTHER HOST	VPN
3	2	570	53	35	30	1,376	3	140

FILTER LAB
FILTER PARTNER
FILTER DATACENTER
FILTER DBU
FILTER DMZ
FILTER CSB

SELECT COUNTRY
SELECT CITY
SELECT OFFICE

FILTER PLAYBOOK
FILTER CATEGORY

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

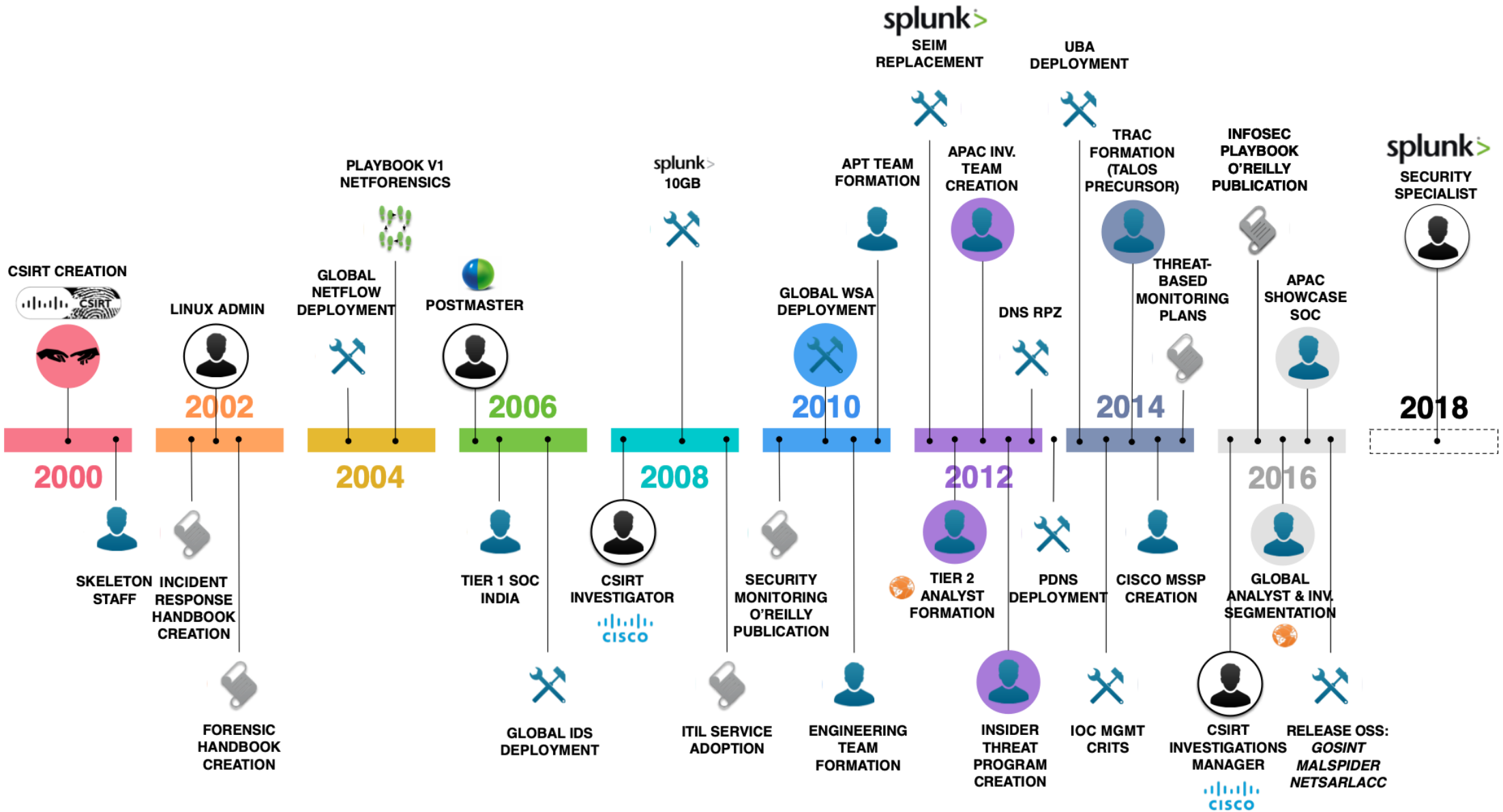
Industry Participation
Publications
Bake Sales
Conference hosting
Executive Briefings
Threat Data Contribution
Foosball Championships
Showcase SOC
Release open source tools

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

SHOWING SECURITY COMMUNITY VALUE

THE EVOLUTION OF A SOC

epoch - present



FULLY BALANCED SOC

Image compliments of Disney

Thank You

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

splunk>

Thank You

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

.conf18

splunk>

Thank You

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

splunk>

Thank You

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

splunk>

Thank You

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

.conf18

splunk>

Thank You

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

.conf18

splunk>

Thanks for rating the session!

PEOPLE

A
BIG
THANKS

Fox
Disney
Marvel
Ryan Reynolds
Mom
Brodsky
Aguero