

{ADRIAN,HAROON}@THINKST.COM

THE PRODUCTS WE DESERVE



THANKS!







**SYSADMIN
DEVELOPER
PEN-TESTER
ANALYST
CISO**

THINKST CANARY

- ▶ **SYSADMIN**
 - ▶ **DEVELOPER**
 - ▶ **PEN-TESTER**
 - ▶ **ANALYST**
 - ▶ **CISO**
-

- ▶ **THINKST CANARY**

STATE OF PLAY

**BY THE NUMBERS:
SECURITY PRODUCTS**

Network & Infrastructure Security

Advanced Threat Protection
 Barracuda BLUEDEKAGON BLUVECTOR Check Point Cisco CORSA FIREEYE FORTINET HUAWEI HYSDLATE
 JOESecurity JUNIPER lastline McAfee Mimecast OPSWAT paloalto REVERSING LABS
 RESEC Sasa Software SONICWALL SOPHOS SPAMINA Symantec VOTIRO WatchGuard

NAC
 aruba AUDUNET AXONIOUS CISCO Extreme FORESCOUT FORTINET Genians portnox Trustwave

SDN
 BlackRidge CERTES Cybera Cyxtera NanoSec SKYPORT SYSTEMS TEMPERED NETWORKS VERSA zenera zscaler

DDoS Protection
 Akamai Check Point Cloudflare Imperva neustar NEXUSGUARD NSFOCUS ORACLE SECURE 64™ StackPath

DNS Security
 BLUECAT CISCO efficient IP Infoblox neustar SECURE 64™ Threat STOP Verisign

Network Firewall
 algosec CISO Check Point Cisco Clavister endian FIREWALL FORCEPOINT FORTINET Hillstone Huawei OPAQ paloalto Sangfor securocloud SONICWALL SOPHOS STORMSHIELD tufin VMware

Deception
 ACALVIO Attivo Networks Craft CyberTrap CyMetrica FIDELIS Illusive IPER MOKESCREEN TRAPX

Web Security

ICS + OT
 APERIO BAYSHORE BELDEN CLARITY CRIMFENCE CyberX CYBERBIT DRAGOS endian FIRMITAS FORESCOUT HALO ANALYTICS Indegy dimension NextNine NOZOMI PAS PFP radiflow Rhebo RIPSentry #SCADAfence sentryo

Network Analysis & Forensics
 AWAKE BROTA CCS CISCO CloudShark Corelight CORE Corvil DARKTRACE ExtraHop FIDELIS Grey Cortex IronNet LUMETA MixMode NETSCOUT PERCH Plixer Sec7 SS8 utimaco VECTRA VERINT

Web Security
 Akamai auriopro authentic8 Barracuda copy CEQUENCE Check Point Cisco ContentKeeper CYREN DEFiant digicert distil networks ERICOM FORCEPOINT FORTINET GoSECURE GWAVA iboss Light Point Security McAfee Menlo Security NAMOGOO perimeterx proofpoint randed Reblaze SH=PE SHIELD SQUARE smoothwall SOPHOS SPAMINA Source Symantec TREND Micro Trustwave unbotify whiteops zscaler

Endpoint Security

Endpoint Prevention
 AhnLab avast Avecto Avira Barkly BINARY DEFENSE BitDefender BLUEBRIDGE Bromium BUFFERZONE Carbon Black. Check Point COMODO CYBERARK cyberason CYLANCE Desinfect ENDGAME ENSILO ERICOM ES&T F-Secure Kaspersky HYSOLATE intego ivanti McAfee Microsoft MORPHISEC OPSWAT paloalto panda RECEPTION POINT SentinelOne SOPHOS sparkcognition STORMSHIELD Symantec TEHRIS TREND VMware WEBROOT ZQANCE

Endpoint Detection & Response
 Belden BINARY DEFENSE Carbon Black. Check Point CYBERBIT CYBERSON CYBONET CYLANCE Cynet DIGITAL GUARDIAN Dtex ENDGAME ENSILO FENROR7 FIDELIS FIREEYE FORCEPOINT GoSECURE HUNTRESS Kaspersky NEXHEMIA nextthink NYOTRON paloalto panda promisc RSA SECPod SentinelOne SOPHOS Symantec TANIUM TEHRIS WatchGuard ziften

Application Security

WAF & Application Security
 6scan AIO Akamai ALERT LOGIC ARXAN Barracuda CEQUENCE citrix CloudFlare CONTRAST Cycliclabs DEAP Security denyall ergon FORTINET Imperva NETSPI netsparker onapsis ORACLE PentaSecurity portshift PULSE Secure PURSEC Quylis radware RAPID7 Reblaze riverbed SUCUN SANS SK=PE Signal Sciences sqreen StackPath TEMPLARBIT THREATX TREND Trustwave VERACODE Vicarius wallarm waratek WhiteHat

Application Security Testing
 acunetix beyond bugcrowd BUGFINDERS CHROMA ERPScan Fasoo hackerone IBM MICRO FOCUS N-Stalker NowSecure PARASOFT PERFORCE PORTSWIGGER Qualys RAPID7 SiteLock SecurityCompass sonarsource Synack SYNOPSIS tenable Trustwave VERACODE WhiteHat WhiteSource

MSSP

Traditional MSSP
 at&t BAE SYSTEMS BT CenturyLink CISO SYSTEMS CSC IBM INFOSIFIT Megapact nspire OPTIV Secureworks SOLUTIONARY Symantec Trustwave verizon

Advanced MSS & MDR
 APT ANTIAN ARCS WOOD APTER DOD Allen Hamilton CRITICAL SYSTEMS CYBERSECURE CYBERX CYBERES deepwatch distanced ONSIGHT ESSENTIAL eSPEL FIREWALL Cloudwatch HEMLOCK MEDIANIA nspire OPTIV PALADIN PRORICIO RAPID7 Raytheon redJanary RELIAQUEST UNISYS

Data Security

Encryption
 ANIUNA baffle Cryptosync CipherCloud CYBERARK COVERTIX CryptoMove CyberX DATALOCKER ENVEIL Fortanix KeyNexus AnCrypted Cloud NuCypher PKWARE SecurityFirst STORMSHIELD THALES TREND Micro virtru WINMAGIC

DLP
 clearswift CODE42 DOSOVS DIGITAL GUARDIAN FIDELIS FORCEPOINT ETE Technology INFOWATCH McAfee SEARCHINFORM SOMANSA Symantec ZECURION

Data Privacy
 Actifile BigID COVATA D.DAY LABS D-ID INTEGRIS minerva nuix OneTrust PRIFENDER SecuPI SPIRION TITUS VULNOMI TrustArc trusthub VERY GOOD SECURITY

Data Centric Security
 BlueTalon CODE42 Datex datify ESO CyberTech druuv egress GlobalVelocity IONIC opentext PRIVATAR SECLORE SPIRION StorageCraft THIMAIR VARONIS VERA

Mobile Security

Mobile Security
 appdome BETTER BlackBerry BlueCedar Check Point cellrox COMMUNITAKE CyberodAPT desinfect eMune Fyde HAVOS INIPIEDIC KATISA KODLSPRN Lookout mobileIron NowSecure ALSO pradeo PSAFE SaltDNA silent circle SOTI Symantec TeleSign ATESKALABS tigerText TRUSTLOOK VAULT VMware wandera wickr ZIMPERIUM

Risk & Compliance

Risk Assessment & Visibility
 AXONIOUS Balbix cavirin Coalition CyberSERVER CyberCube cyber GRX cyteleg DELVE odysium FIRMEN INQSec KENNA PHEHMAH SECURITY NOPSEC OPAQ Outpost24 panaseer PREVALENT REDSEAL riskrecon RISKSENSE SKYBOX tenable UpGuard VENAFFI zeguro

Security Ratings
 BITSIGHT COIAX FICO GUIDEWIRE Metasploit Panoras PREVALENT RiskLens riskrecon

Pen Testing & Breach Simulation
 AT&T Cobalt CHRONUS CYBERPAT CYCIGNTO CYMULATE DEPTH KORNADO MAZEBOLT NOPSEC PCVSYS PICUS SECURITY RAPID7 Safebreach SCYTHE VERODIN

GRC
 algosec AppTega SECURE Galvanize Lockpath MetricStream netwrix Onspring:RESOLVER riskconnect RSA SAI GLOBAL tufin

Security Awareness & Training
 Barracuda Coffee CyberVista BIRONALES KnowBe4 PHISHLABS proofpoint SANS SPACEFORCE

Security Operations & Incident Response

SIEM
 AT&T Cybersecurity BLACKSTRATUS CORRELOG CYGLANT DEVO Data Engine DNET EventTracker exabeam FORTINET HanSight Huntsman IBM IGLORSECURITY JASK logentries LOGPOINT LogRhythm logz.io McAfee MICRO FOCUS Palantir RSA SAWMILL SECURONIX solarwinds splunk sumologic TIBCO Trustwave

Security Incident Response
 arctis networks atarlabs ayehu CYBERBIT CYBERSENSE CYBER TRIAGE CS SECURITY DARK LIGHT DEMISTO DFLABS FIREEYE Microsoft paloalto radar RAPID7 Raytheon RESILIENT SEC3 servicenow SIEMPLIFY SIFT SECURITY splunk SWIMLANE SYNCRITY THREATCONNECT THREAT QUOTIENT UPLEVEL VERINT

Momentum CYBER

Threat Intelligence

Threat Intelligence
 4i@ ANOMALI Blueliv. BlueVoyant CENTRAL NETWORKS Cisco Cyberint digital shadows DOMAINTOOLS EclecticIQ FARSIGHT FLASHPOINT GROUP HAN SIGHT HYAS INTEL471 INTSIGHTS KELA LOOKINGGLASS Malware Patrol NUCLEON Recorded Future RiskBased SECURITY RISKIQ SenseCy Sixgill SpyCloud SURFWATCH THREATCONNECT ThreatMetrix THREATQUOTIENT Threat STOP TRU*STAR WEBROOT

IoT

IoT Devices
 ALLIANCE ARMIS Bastille CENTRI Convium Cybertool ETRITE MDX CYLIB delifer IONIC LABS IMUBIT KEYFACTOR LEVEL MagicCube MEDIGATE MOCANA Regulus RISCURE Rubicon SECURITYTHINGS BEPIO SENRIO ZingBox

Automotive
 BlackBerry Blue3 C2A security CARSDOME Continental cyCURO CYMOTIVE ENIGMATOS foretellix Guard KNOX HARMAN Karamba Security NNG otonomo SAFERIDE Trillium Upstream

Connected Home
 Bitdefender CUJO F-Secure S.A.M. SYMANTEC Fortress

Messaging Security

Messaging Security
 AGARI AREA 1 AstraID BAE SYSTEMS Barracuda Cisco clearswift CYBONET CYREN FIREEYE FORCEPOINT FORTINET GoSECURE GreatHorn GWAVA inky IRONSCALES mailguard McAfee Microsoft mimecast PHISHLABS proofpoint Sasa Software SONICWALL SOPHOS SPAMINA Symantec TREND Micro Trustwave VadeSecure VALIMAIL VOTIRO WEBROOT wickr ZERO SPAM zix

Identity & Access Management

Authentication
 ACCEDON Auth0 AVERON BehaviorSec BIOCATCH CallSign Centify CLEF CORE SECURITY EXOSTAR FOREROCK FUDO SECURITY Google HPR IDEE IMPRIVATA INTRINSIC JUMIO nok nok pindrop plainID SAASPASS SaferPass SECRET SECURE(SET) SECURETIDN SECUREPUSH ShoCard SILVERFORT tascent ThreatMetrix TRANSMIT SECURITY TransUnion TRUSONA UNBOUND UNIKEN V-KEY VIRGIL SECURITY

IDaaS
 AVATIER Centify IBM idaptive Ientus welcome Microsoft okta onelogin ORACLE PING RSA THALES

Privileged Management
 BeyondTrust Centify CYBERARK FUDO SECURITY HITACHI IBM ManageEngine MICRO FOCUS ONE IDENTITY Remediant SECURELINK thyotic

Identity Governance
 AXIOMATICS DeepIdentity helpsystems SailPoint SAVIYNT simeio

Consumer Identity
 Akamai Auth0 FOREROCK IDexperts ID.me JUMIO loginradius Microsoft PING PIREAN SAP SECURE KEY Trulioo vchain verato VERIFF

Security Analytics

Security Analytics
 AWAKE Bay Dynamics DARK TRACE Dtex empow exabeam Fluency FORTINET HanSight haystax IMVISION IronNet JASK MICRO FOCUS mistnet observe it paloalto patternex Reservoir Labs RSA SEC3 SECURONIX TERAMIND THETARAY TripleCyber VECTRA Veriato vmware

Digital Risk Management

Digital Risk Management
 QCEP crisp CYBERPRINT digital shadows DigitalBolsa EXPANSE LOOKINGGLASS NAMOGOO PHISHLABS RISKIQ SafeGuard source ZEROFOX

Blockchain

Blockchain
 BLOCK ARMOUR Chain GRAXEL edge guardtime IDEE Manifold NuID remme ShoCard vchain xage

Security Consulting & Services

Security Consulting & Services
 accenture ADAPTURE A-LIGN appsec BISHOPFOX BLACKCAP Booz | Allen | Hamilton BT CORVID Deloitte DENIM GROUP EY FIREEYE Ishtech GreyCastle IBM IOActive Komodo KUBELSO SECURITY leidos MindPoint nccgroup NEC NNTT OPTIV PWC REVEALRISK SECURITYCOMPASS SERA SYN SPECTER OPS STROZ FRIEDBERG SYGZA VERISITE

Fraud & Transaction Security

Fraud & Transaction Security
 AU TIX BIOCATCH BLOCK FRAUD Brighterian CARDINAL COMMERCE DATAVISOR EARLY WARNING emailage ethoca EverCompliant feedai FICO FirstData FORTER GROUP IdenTrust Kount MagicCube MAXIMING NetGuardians NS Data Security Pondera riskified Shift Technology sift SIGNIFYD simility SOCURE ThreatMetrix TokenID TransUnion UNIKEN technology

Cloud Security

Container
 anchore aqua CAPSULES deepfence guide Aporeto BetterCloud BRACKET cavirin Check Point CleanDATA Cloud Conformity CLOUDWAY CloudPassage CYBERARK EDGEWISE Guardicore StackRox Sysdig Twistlock

Infrastructure
 Akamai BetterCloud BRACKET cavirin Check Point CleanDATA Cloud Conformity CLOUDWAY CloudPassage CYBERARK EDGEWISE Guardicore StackRox Sysdig Twistlock

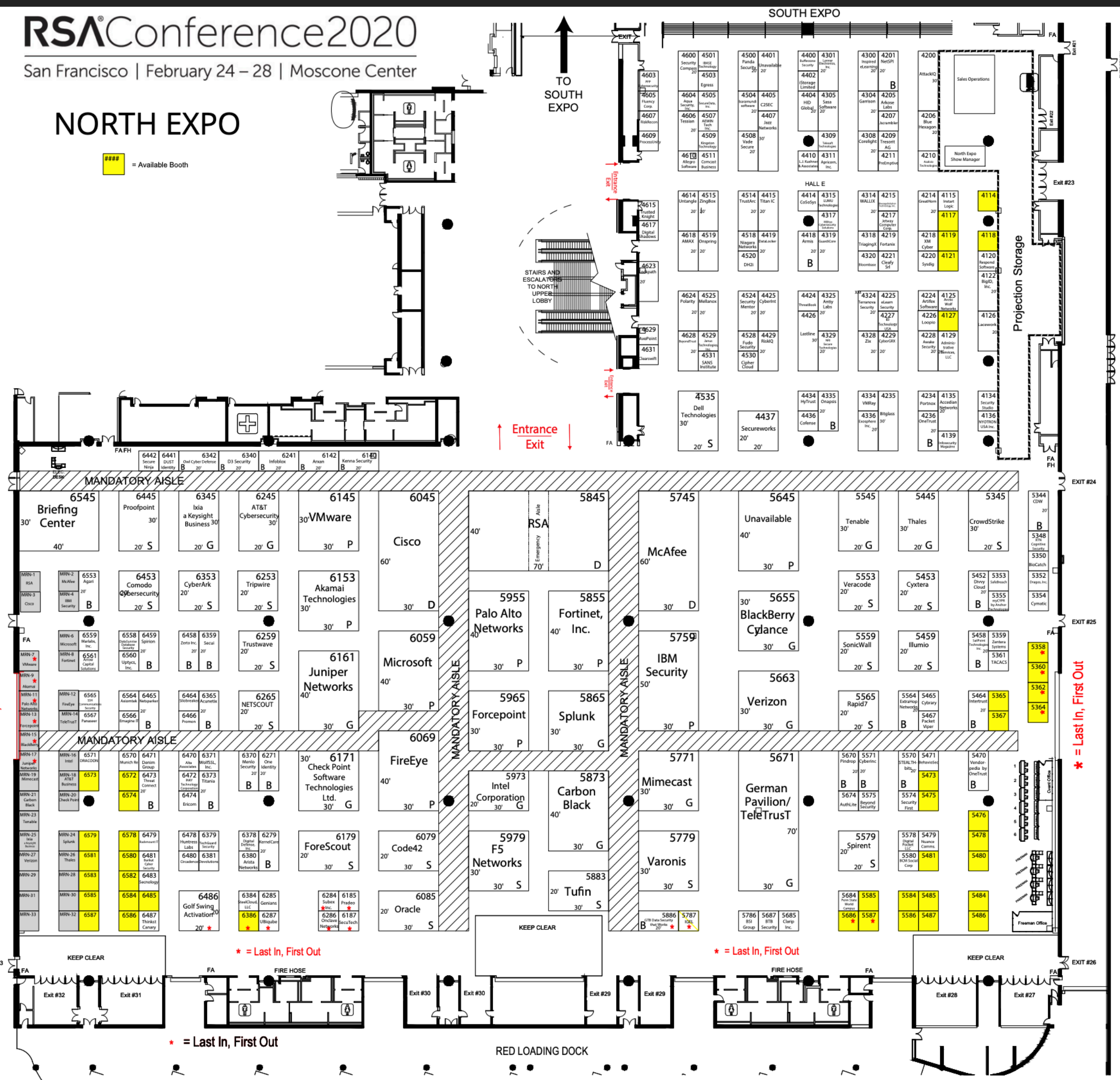
CASB
 AVANAN bitglass CipherCloud CISCO EORNET Managed Methods McAfee Microsoft netskope ORACLE proofpoint SECURIGO SKYFORMATION StratoKey Symantec

RSA[®] Conference 2020

San Francisco | February 24 – 28 | Moscone Center

NORTH EXPO

= Available Booth



* = Last In, First Out

* = Last In, First Out

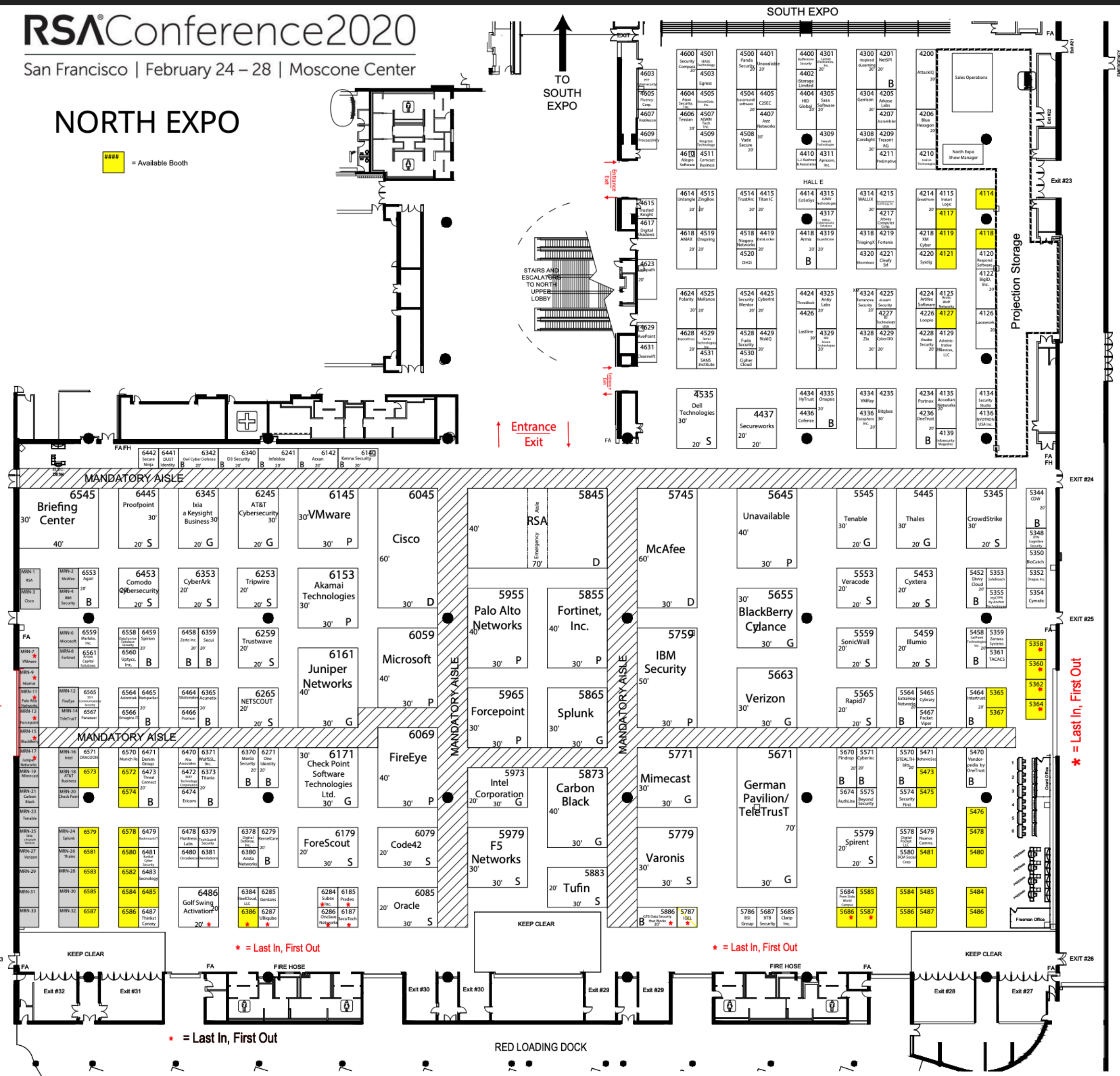
* = Last In, First Out

RSA[®] Conference 2020

San Francisco | February 24 – 28 | Moscone Center

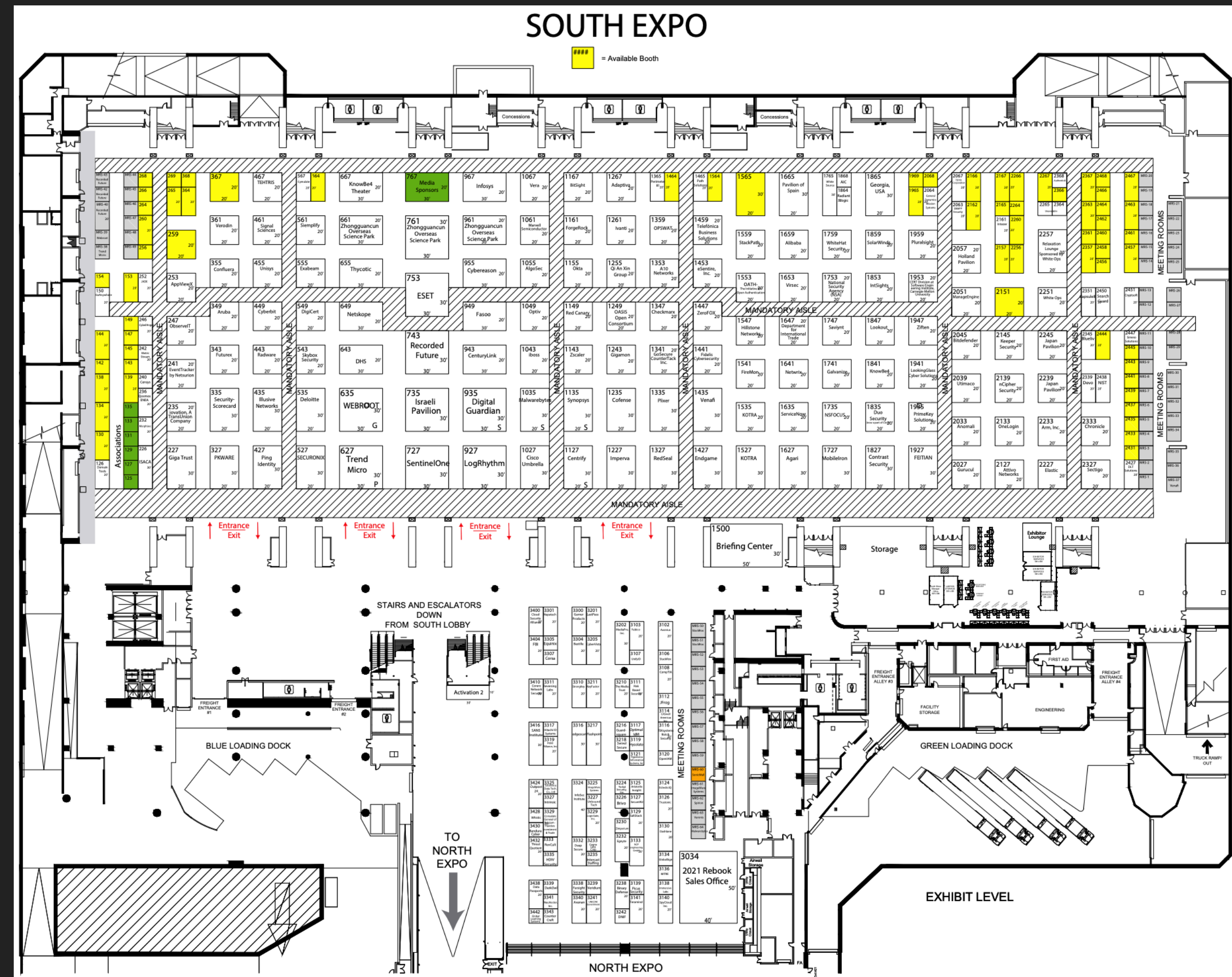
NORTH EXPO

■ = Available Booth



SOUTH EXPO

■ = Available Booth



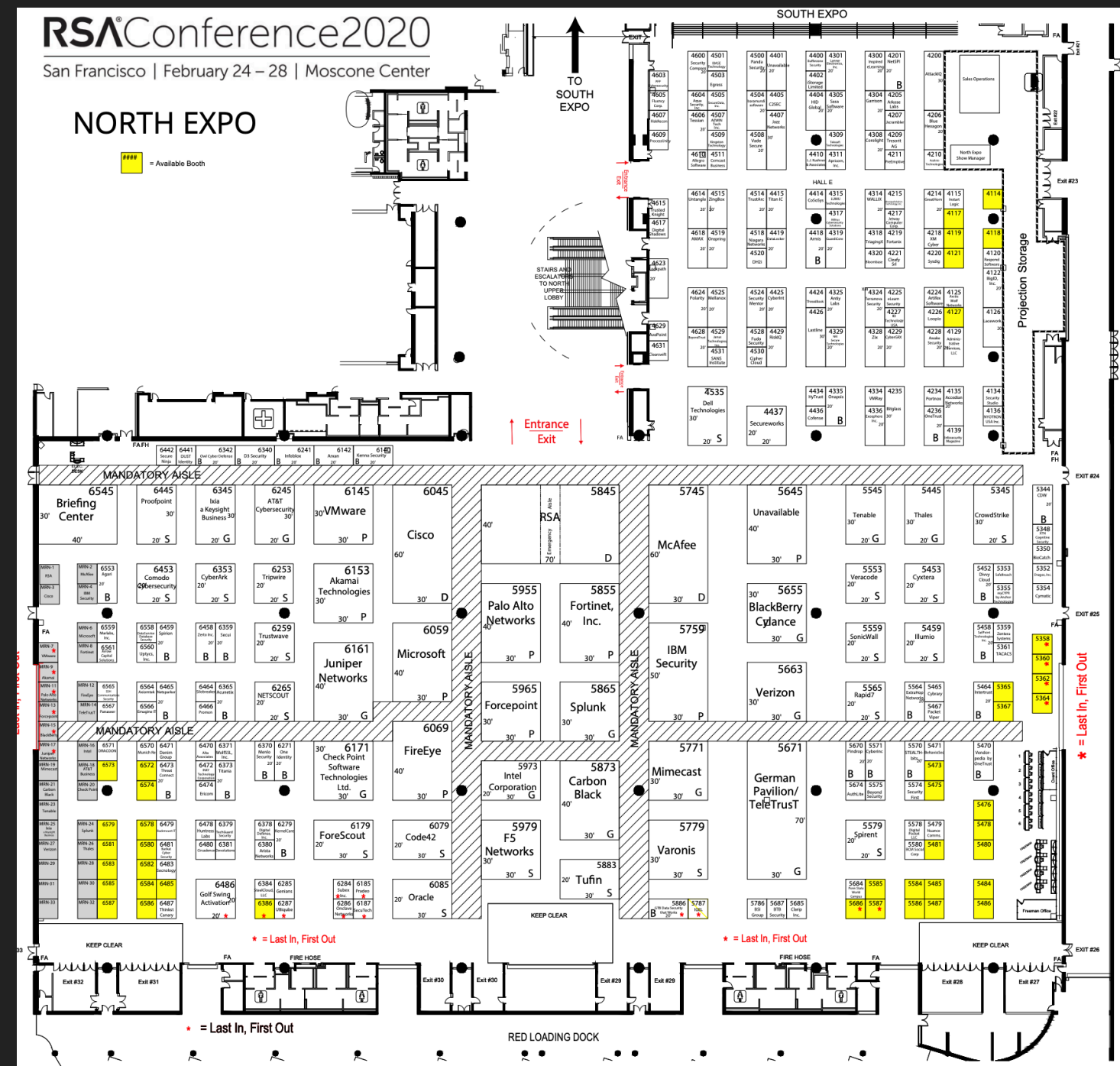
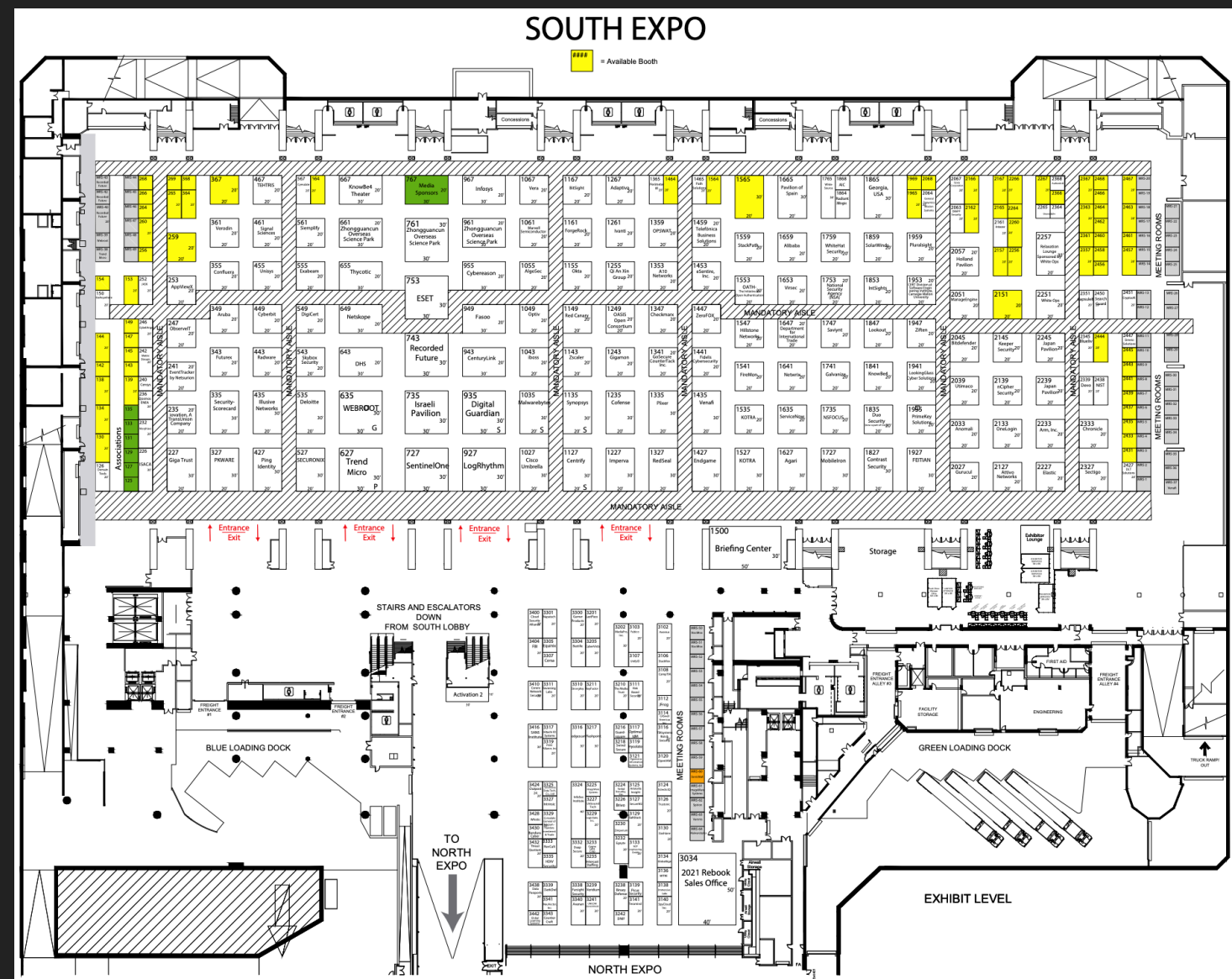
SOUTH EXPO

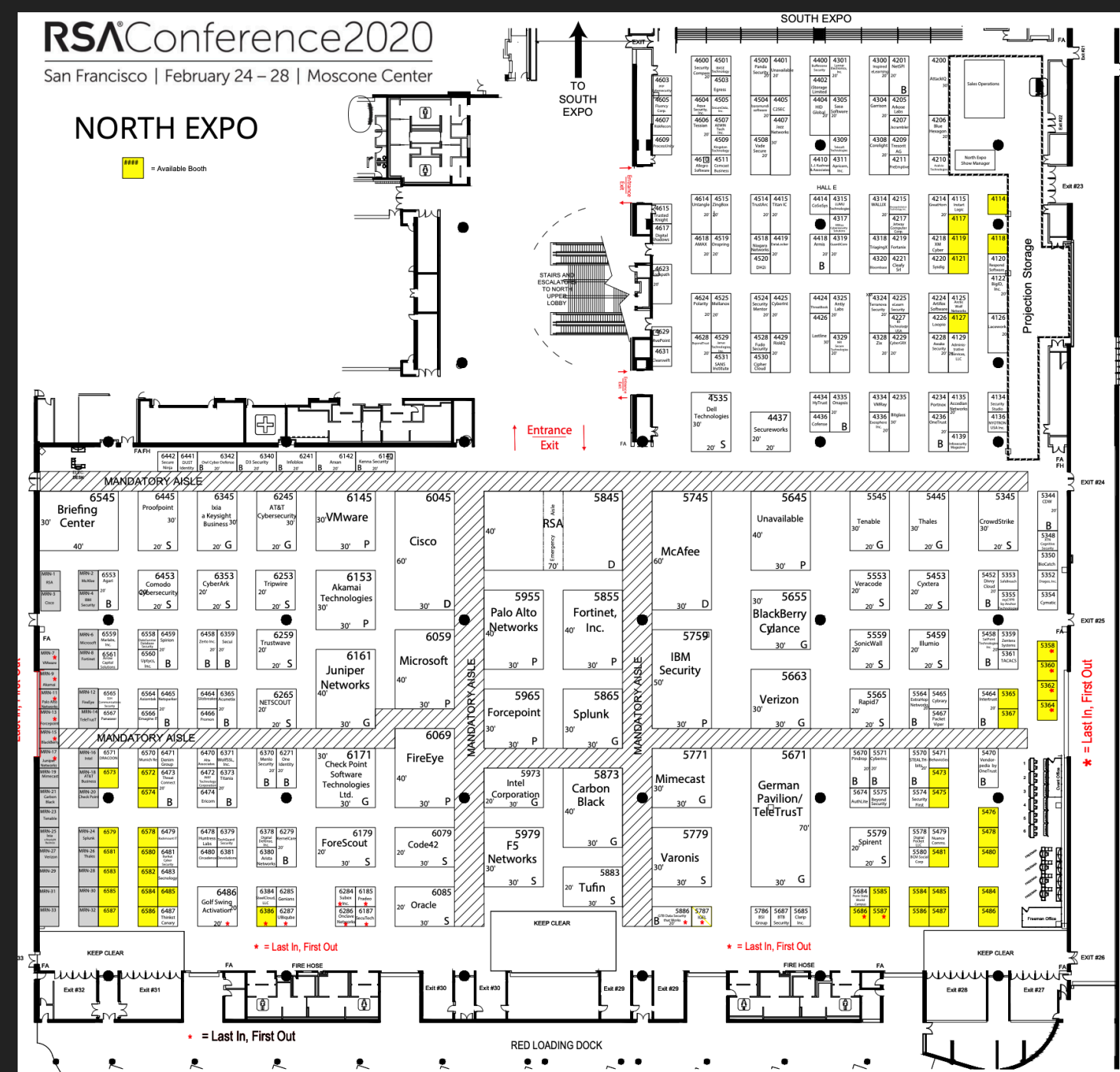
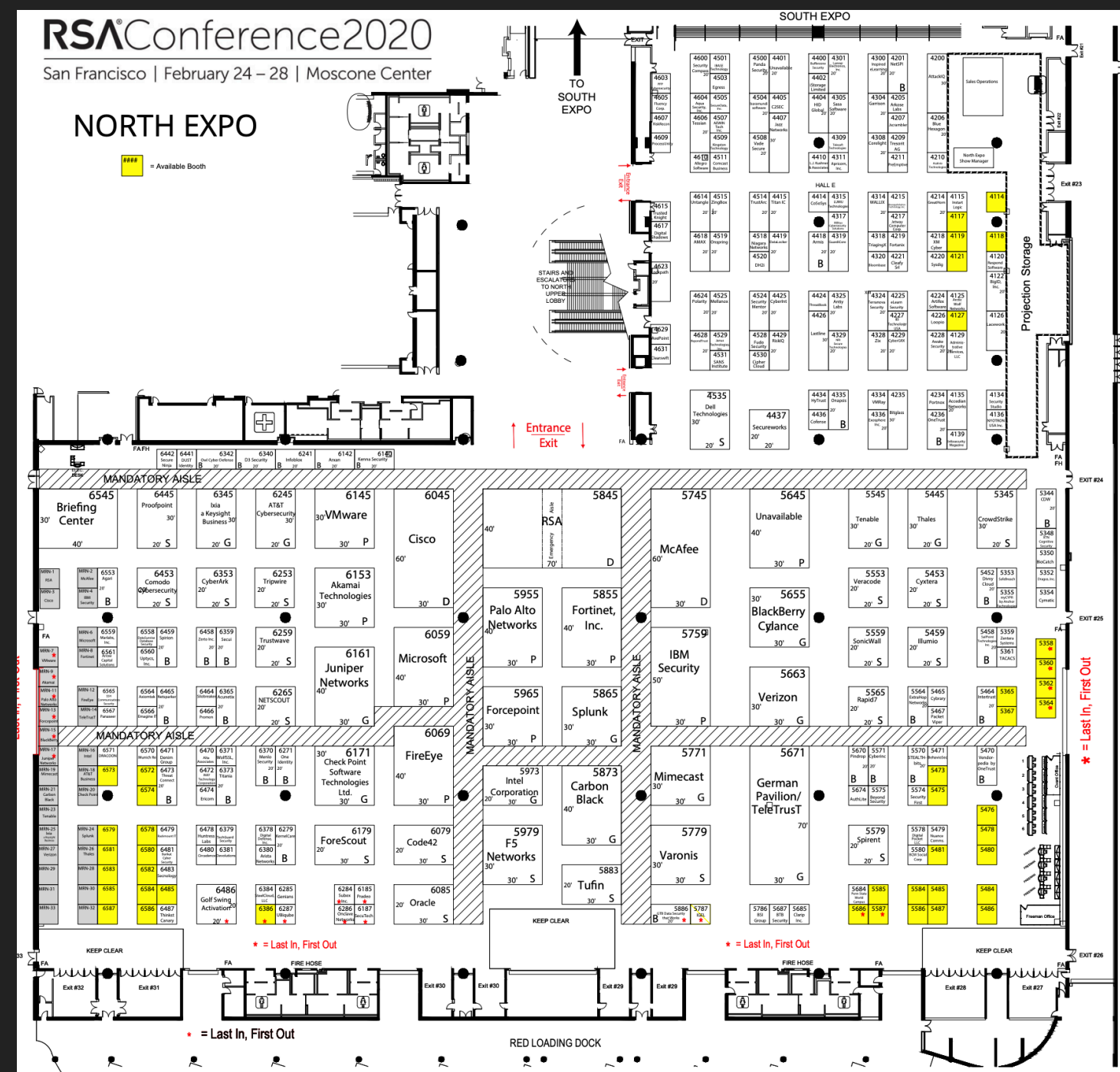
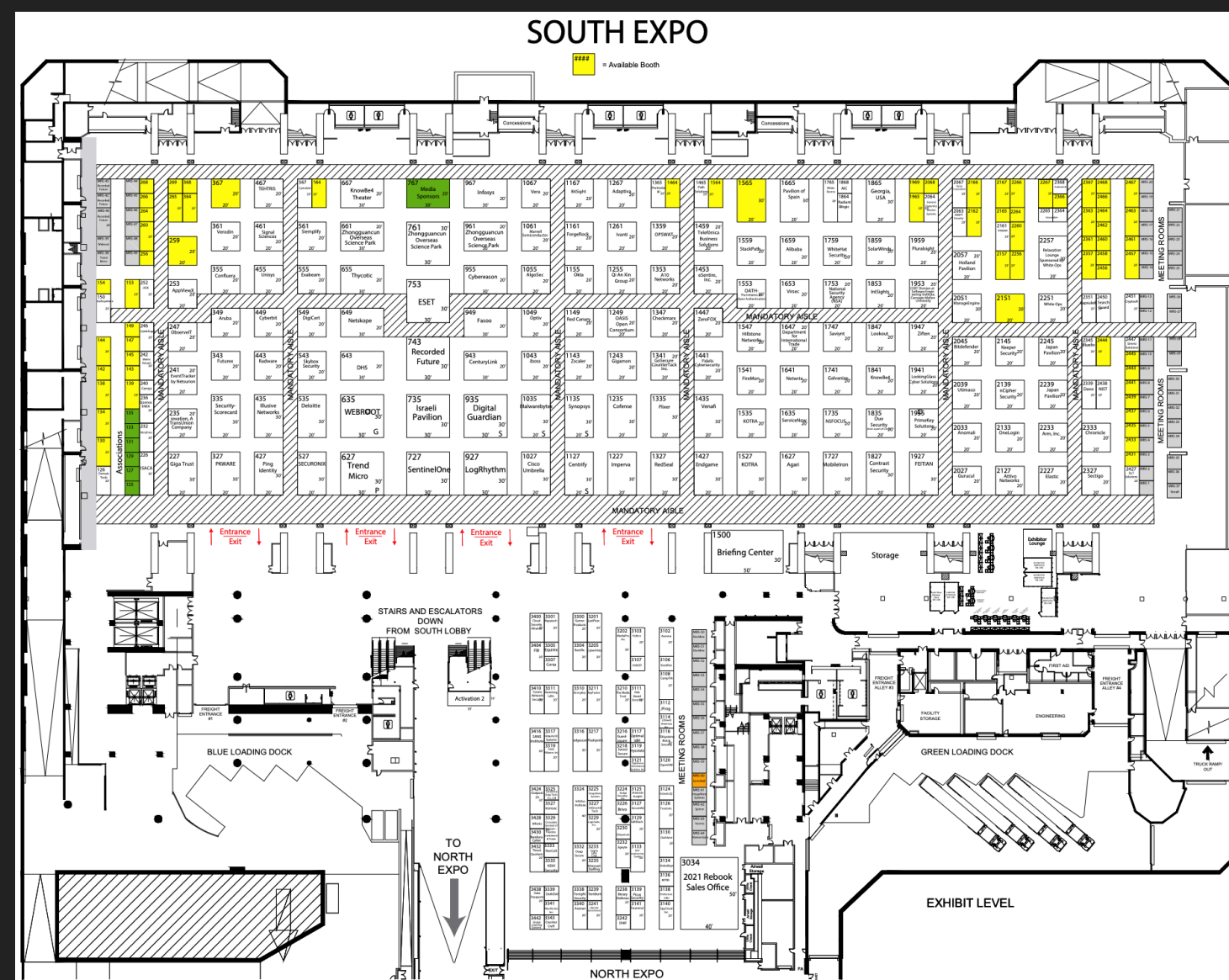
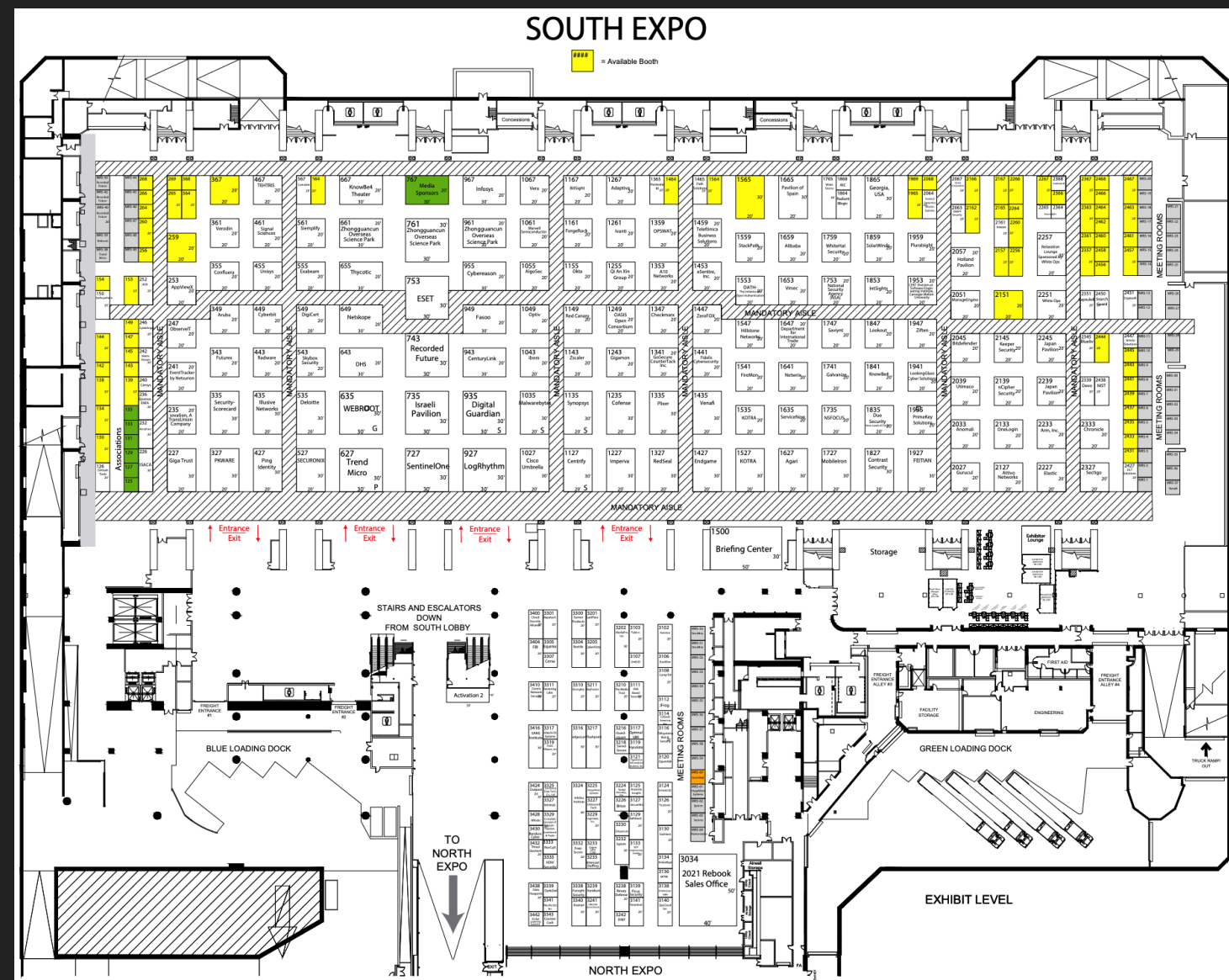
Available Booth

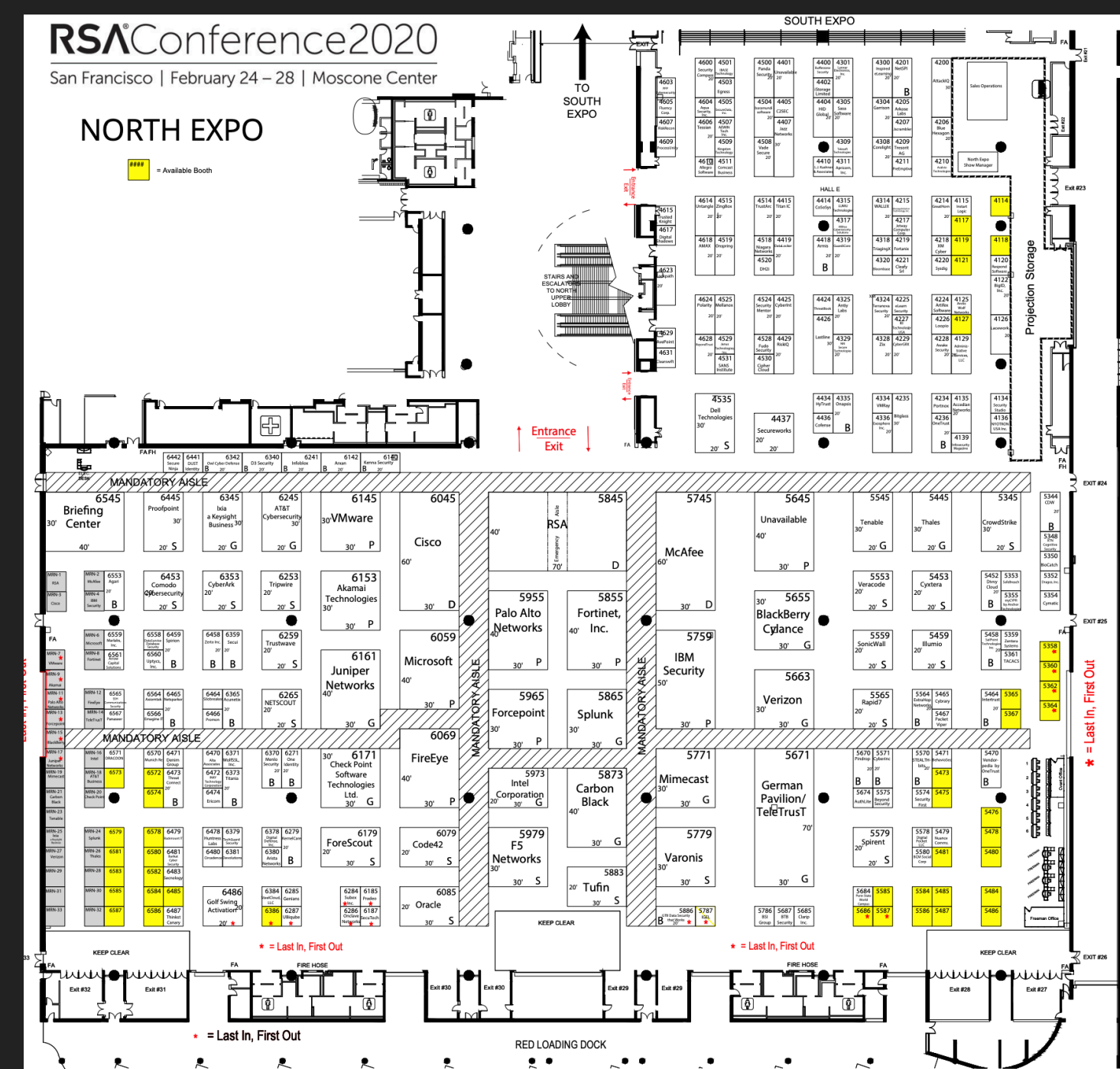
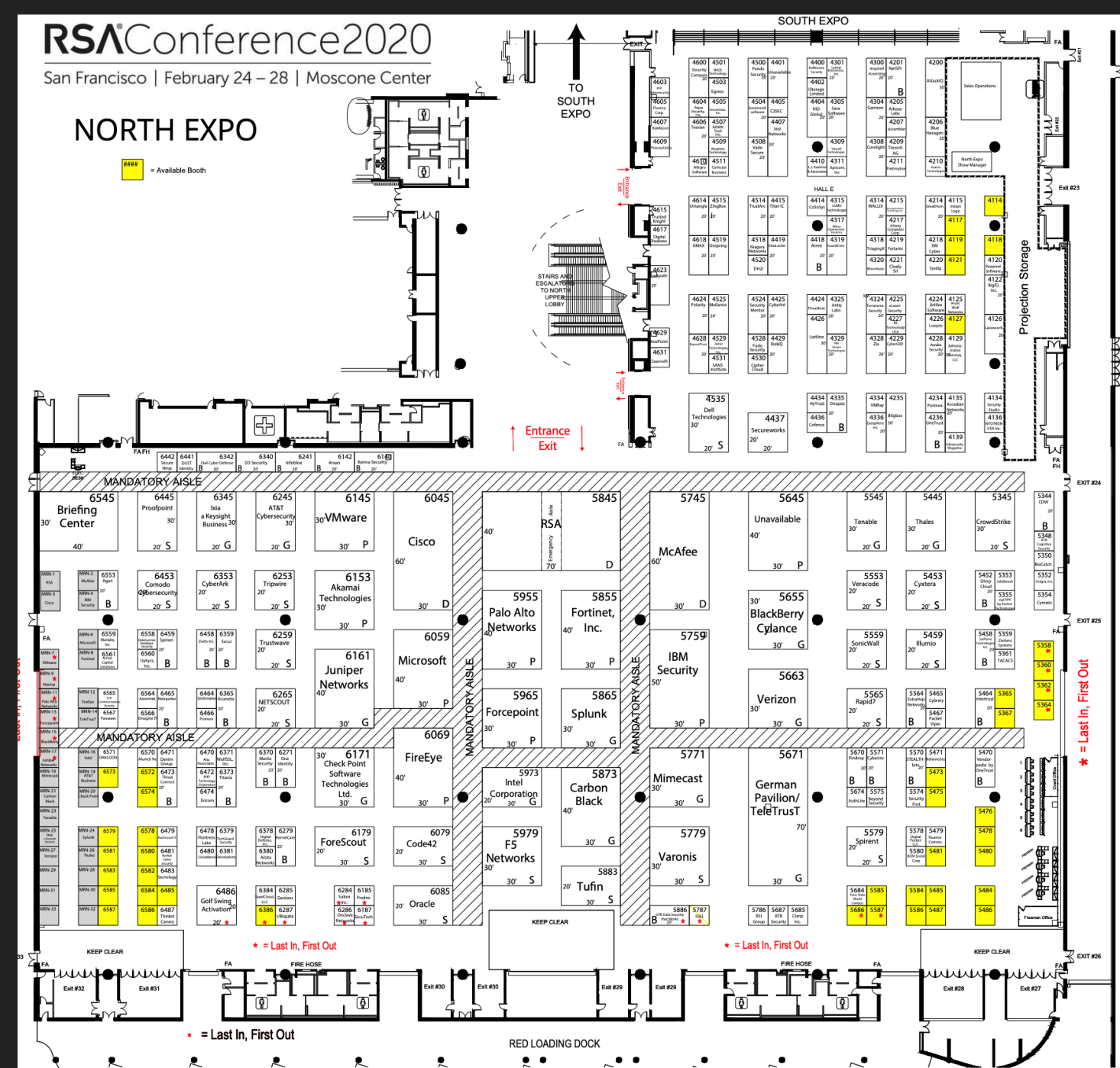
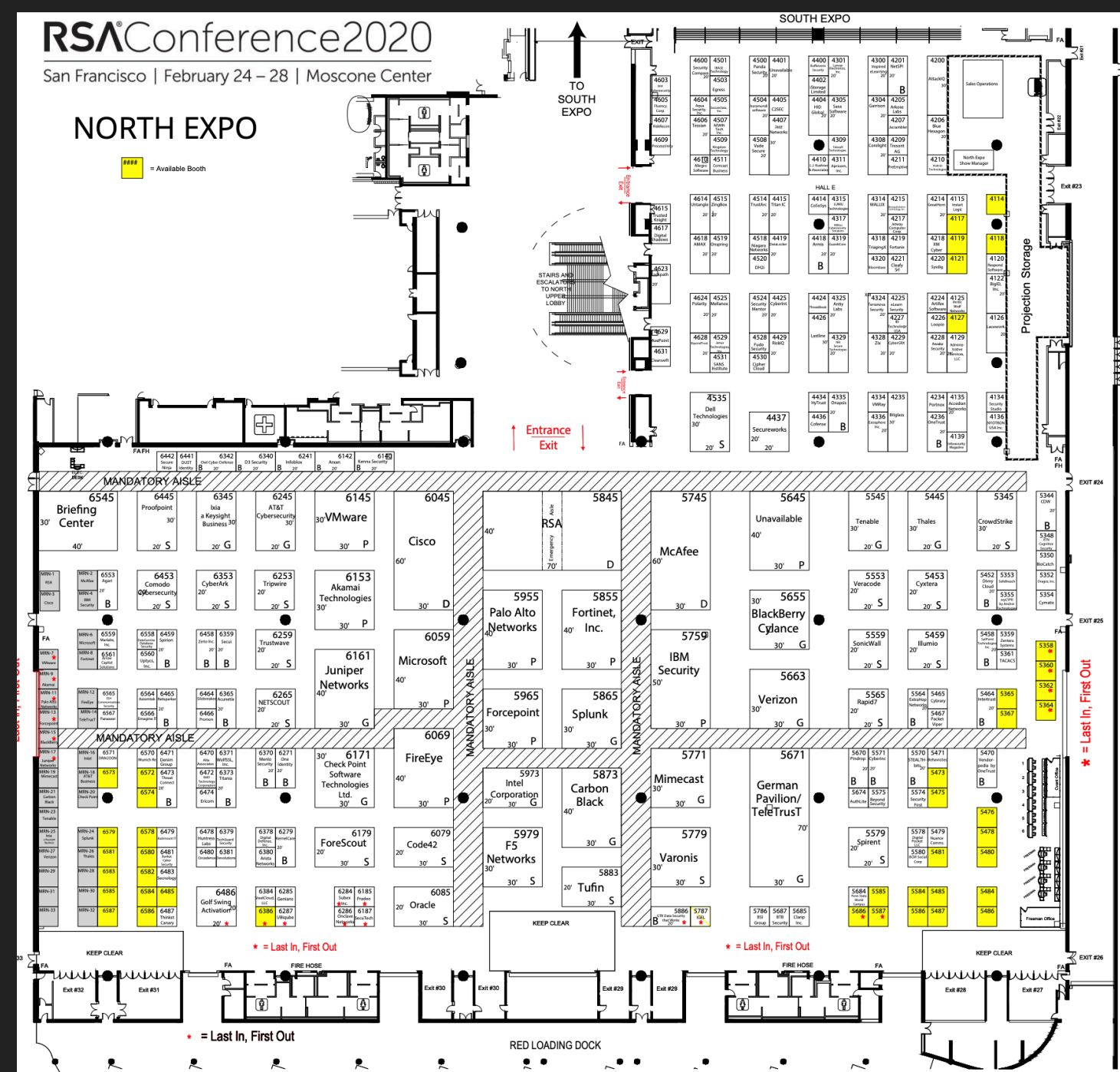
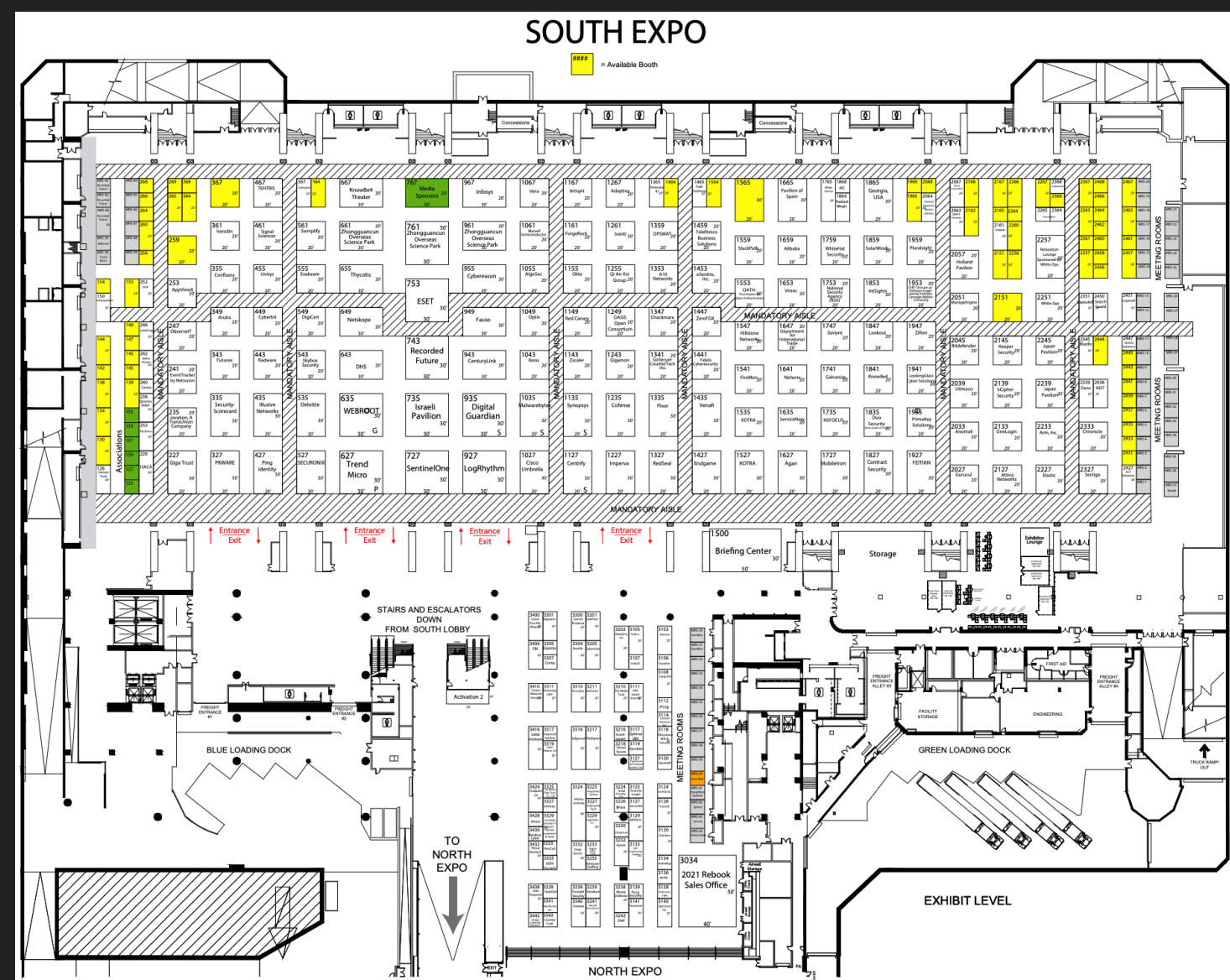
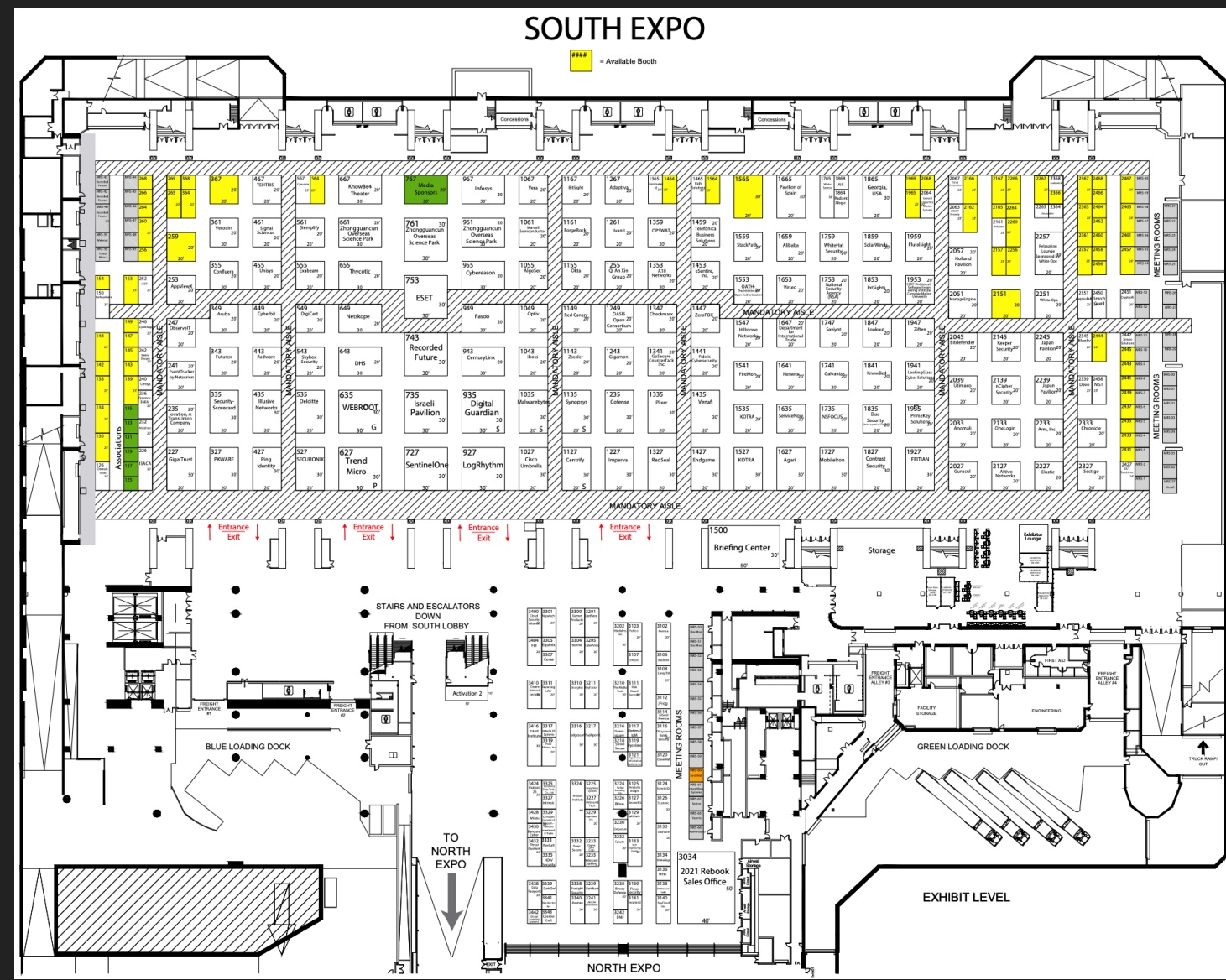


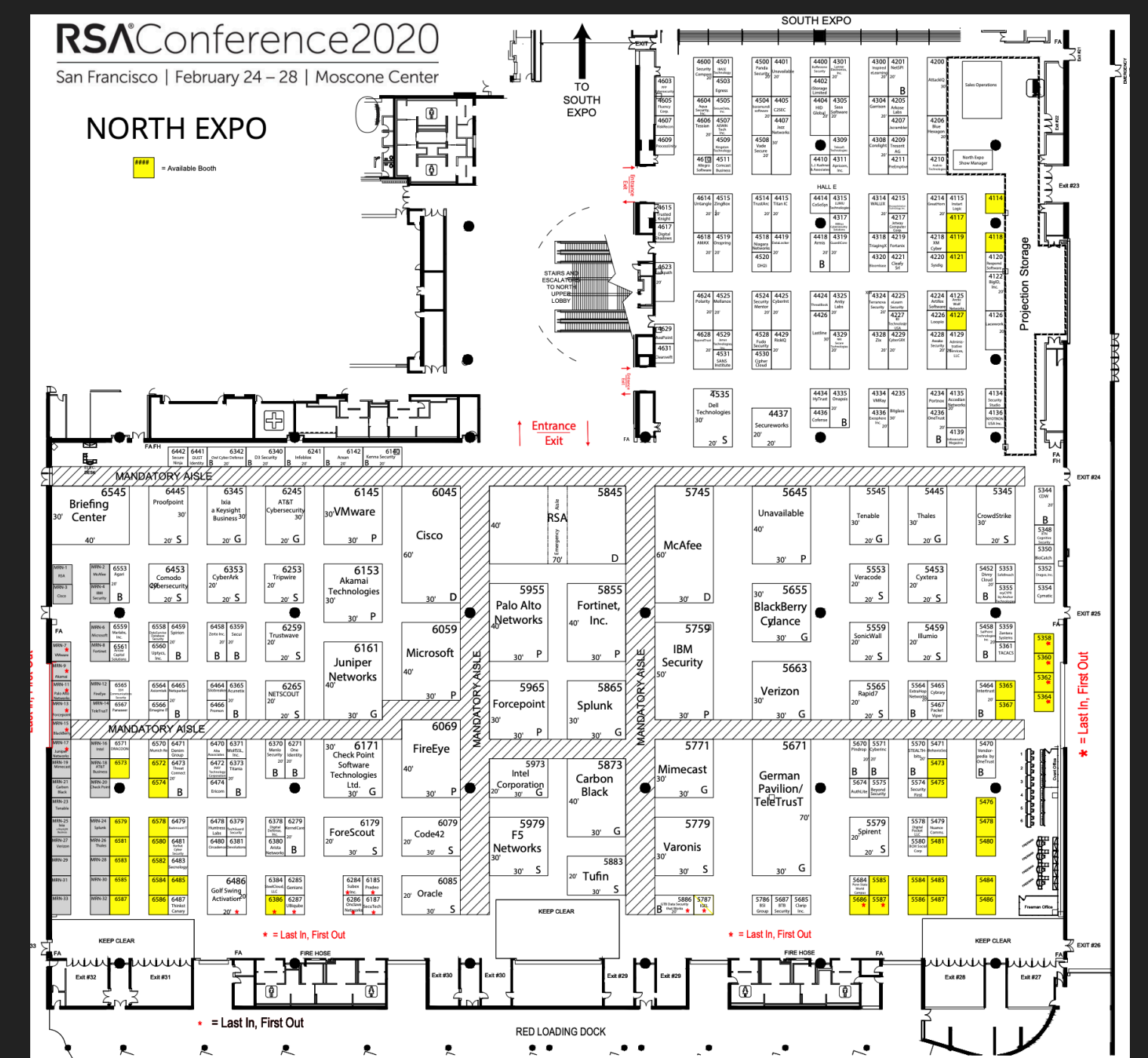
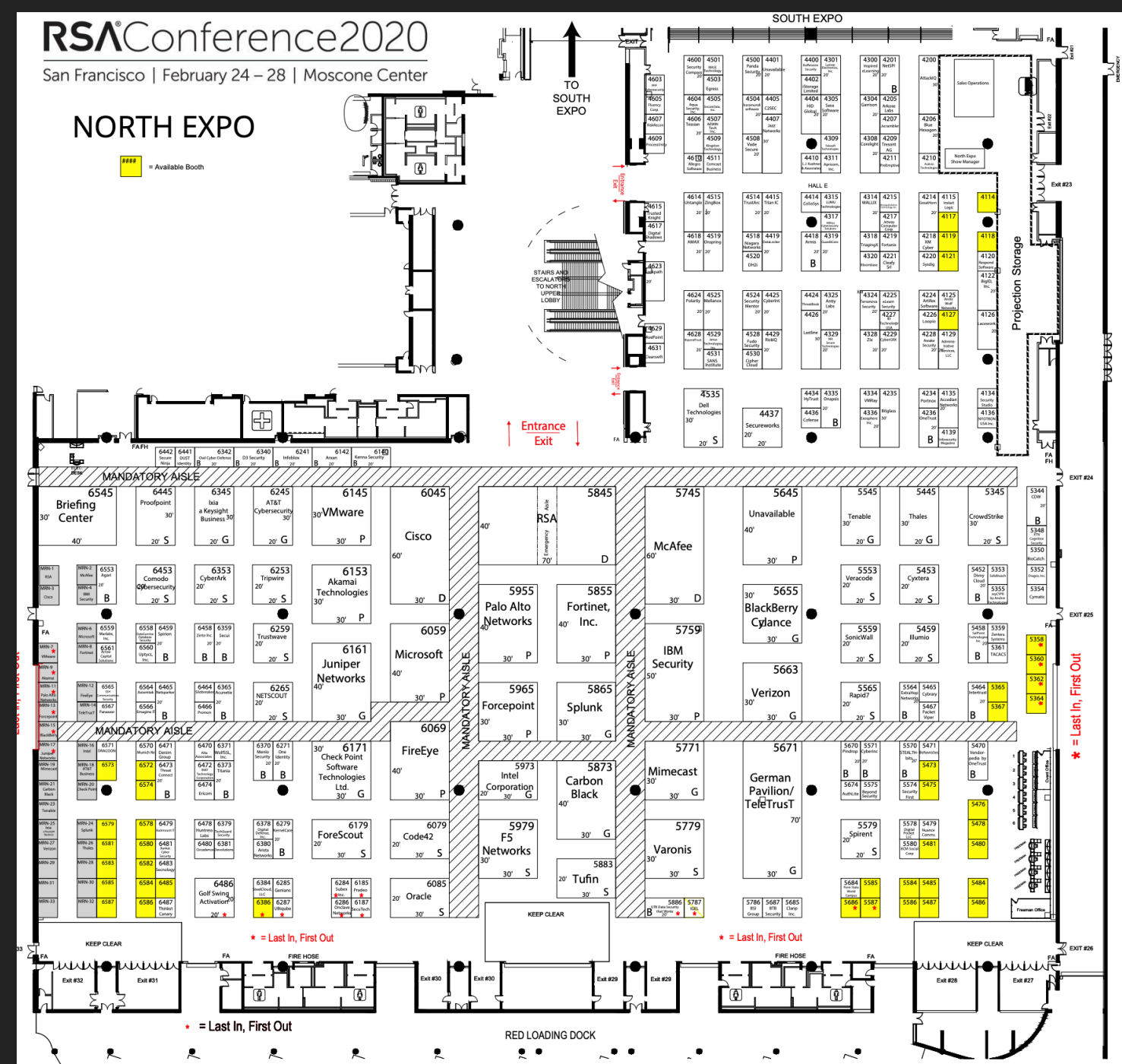
EXHIBIT LEVEL

NORTH EXPO









BY THE NUMBERS: SECURITY CONFERENCES

2019

111 CONFERENCES

585 TOTAL WORLDWIDE

173 CITIES

52 COUNTRIES

2019

111 CONFERENCES

585 TOTAL WORLDWIDE

173 CITIES

52 COUNTRIES

BOSIDES

2019

111 CONFERENCES

585 TOTAL WORLDWIDE

173 CITIES

52 COUNTRIES

BOSIDES **punk'd**

2019

2083 CONFERENCES

(DOESN'T INCLUDE TRAINING OR JOB FAIRS)

2019

2083 CONFERENCES

(DOESN'T INCLUDE TRAINING OR JOB FAIRS)

2010: "ALMOST A CON FOR EVERY DAY OF THE YEAR!"

2019: NORMAL TO ATTEND TWO CONS IN THE SAME DAY

2019

2083 CONFERENCES

(DOESN'T INCLUDE TRAINING OR JOB FAIRS)

2010: "ALMOST A CON FOR EVERY DAY OF THE YEAR!"

2019: NORMAL TO ATTEND TWO CONS IN THE SAME DAY

CON OVERLAP IS A THING NOW
HOW MUCH OVERLAP IS THERE?
I'M GLAD YOU ASKED...

**ON JUNE 4TH, 2019
19 SECURITY CONFERENCES
OVERLAPPED**

**ON JUNE 4TH, 2019
19 SECURITY CONFERENCES
OVERLAPPED**

New York State Cyber Security Conference

Noord Infosec Dialogue Benelux

CIO Benelux Dialogue

Digital Summit Austin

Rocky Mountain Information Security Conference (RMISC)

DOE Cyber Conference

DevSecOps Days Denver

The TU-Automotive Conference & Exhibition USA

Cyber Trends in 2019

National Cyber Summit

Infosecurity Europe

RANT Respite

BSides London

Southern California CISO Executive Summit Q2

AuSec Conference

**ON JUNE 4TH, 2019
19 SECURITY CONFERENCES
OVERLAPPED**

New York State Cyber Security Conference

Noord Infosec Dialogue Benelux

CIO Benelux Dialogue

Digital Summit Austin

Rocky Mountain Information Security Conference (RMISC)

DOE Cyber Conference

DevSecOps Days Denver

The TU-Automotive Conference & Exhibition USA

Cyber Trends in 2019

National Cyber Summit

Infosecurity Europe

RANT Respite

BSides London

Southern California CISO Executive Summit Q2

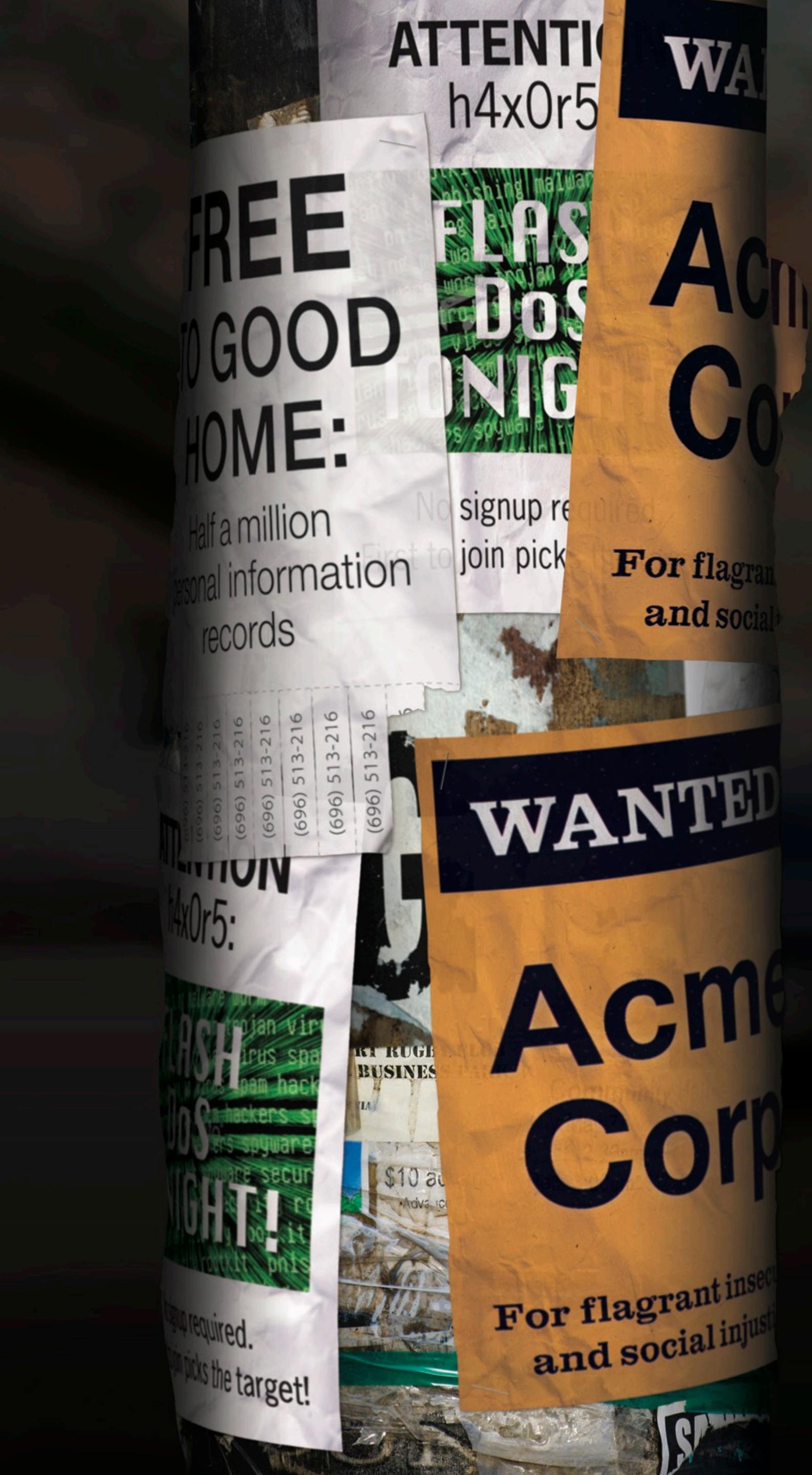
AuSec Conference

Philadelphia CISO Executive Summit Q2

Utah Digital Government Summit

CTCrypt

ITS America Annual Meeting



2012 DATA BREACH INVESTIGATIONS REPORT

A study conducted by the Verizon RISK Team with cooperation from the Australian Federal Police, Dutch National High Tech Crime Unit, Irish Reporting & Information Security Service, Police Central e-Crime Unit, and United States Secret Service.

92% OF THE VICTIM ORGANISATIONS INVESTIGATED WERE NOTIFIED ABOUT THE BREACH BY A 3RD PARTY

- 2012 Verizon DBIR

M-Trends[®] 2015:
**A VIEW FROM
THE FRONT LINES**

SECURITY
CONSULTING

205 DAYS IS THE
MEDIAN TIME FOR
ATTACKERS TO EXIST ON
A NETWORK BEFORE
BEING DISCOVERED

- 2015 M-Trends Report

Cost of a Data Breach Report²⁰¹⁹

**THE AVERAGE TIME TO
IDENTIFY A BREACH IN
2019 WAS 206 DAYS**

- 2019 IBM / Ponemon

Conducted by



Sponsored by

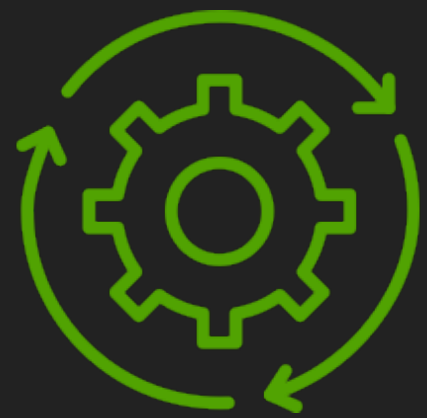
IBM Security

SO...

WHY THO'?



WE RAISE MONEY BADLY



WE BUILD PRODUCTS BADLY



WE DO SALES BADLY

(FOR INFOSEC COMPANIES)

**THE VC MODEL IS
BROKEN**



~~GROWTH / SCALE~~

~~“VC’S INVEST IN EXITS”~~



COMPLEXITY

PROXY-BOOST



**“WE CRAWL THE DARKWEB AT SCALE AND
THEN USE MACHINE LEARNING TO
EXTRACT IOC’S IN REAL-TIME TO
IDENTIFY APT”**

– STANFORD POSTGRADS



**“WE CRAWL THE DARKWEB AT SCALE AND
THEN USE MACHINE LEARNING TO EXTRACT
IOC’S IN REAL-TIME TO IDENTIFY APT”**

– STANFORD POSTGRADS

**“GET RID OF LOCAL-ADMIN
PASSWORDS”**

– A SYS-ADMIN



#RSAC - THEMES



COMPLEXITY

PROXY-BOOST



IS YOUR SEC SOFTWARE ACTUALLY GOOD?

MOST PEOPLE ACTUALLY CAN'T TELL









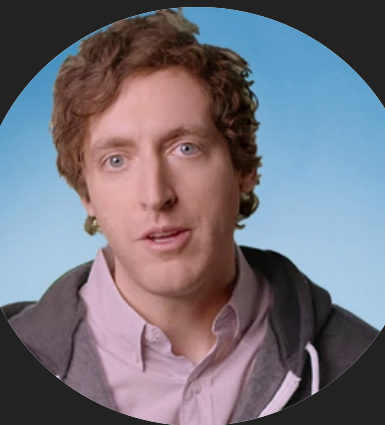


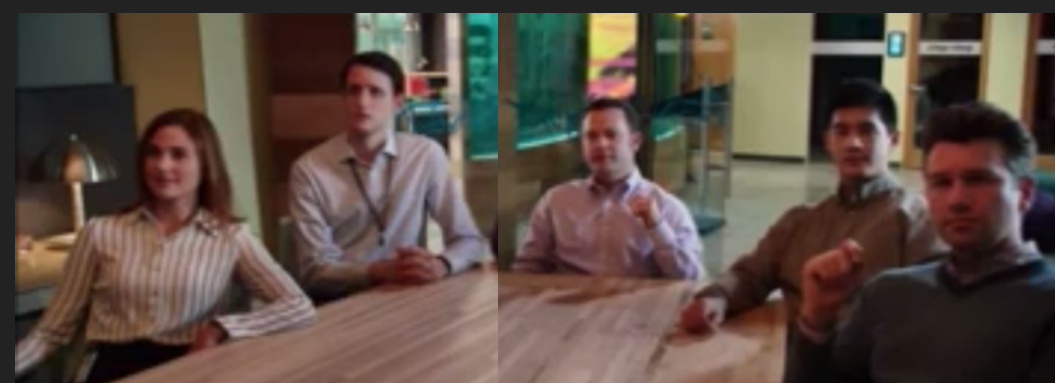




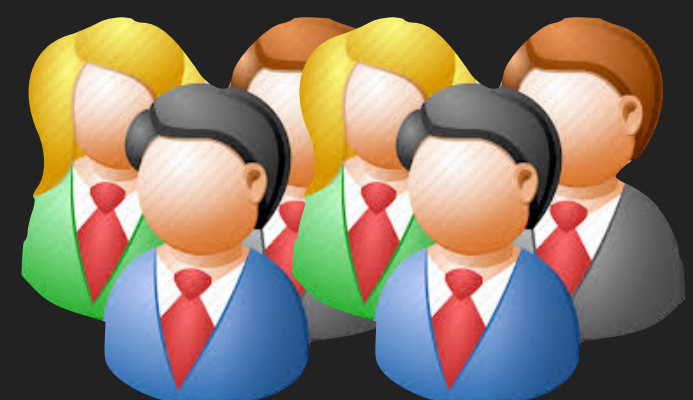
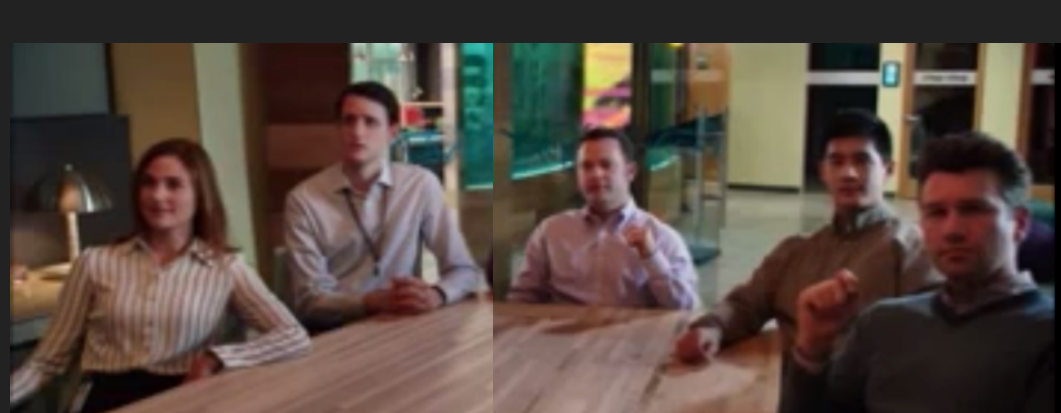
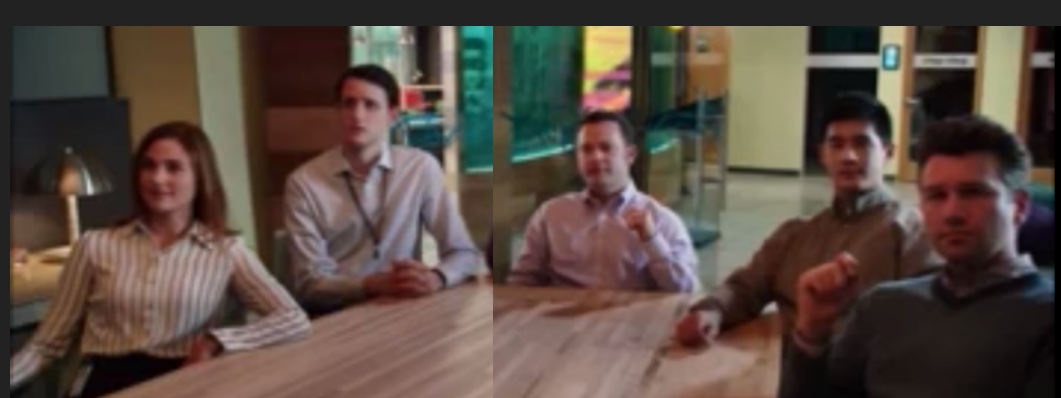
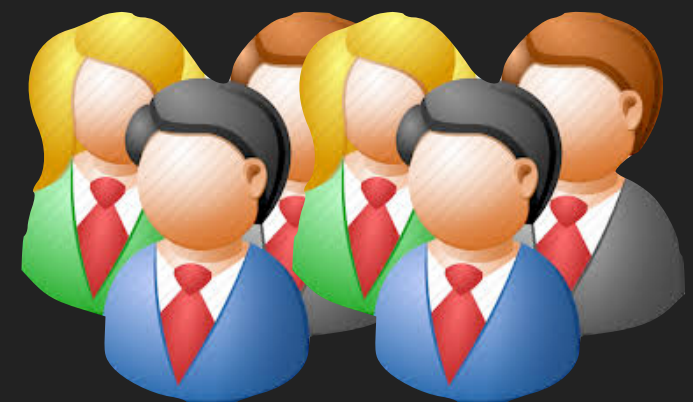
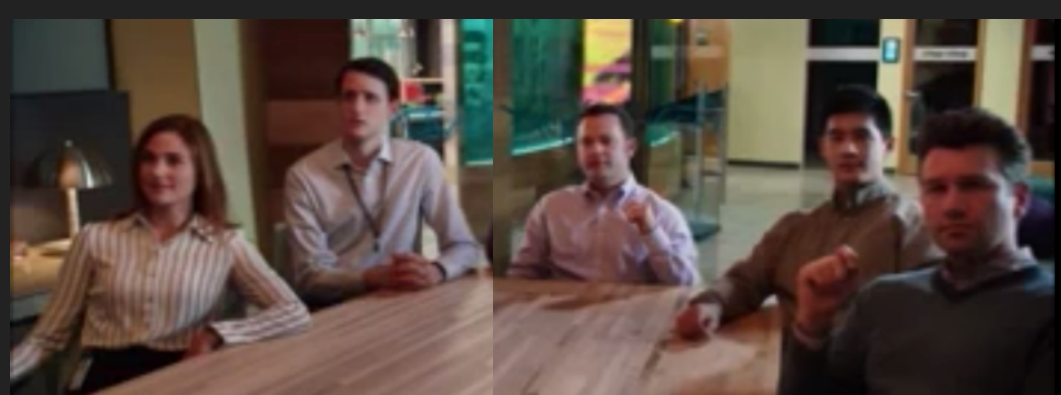
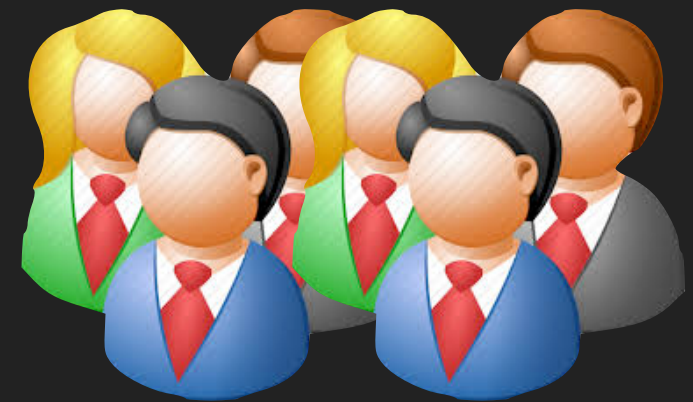
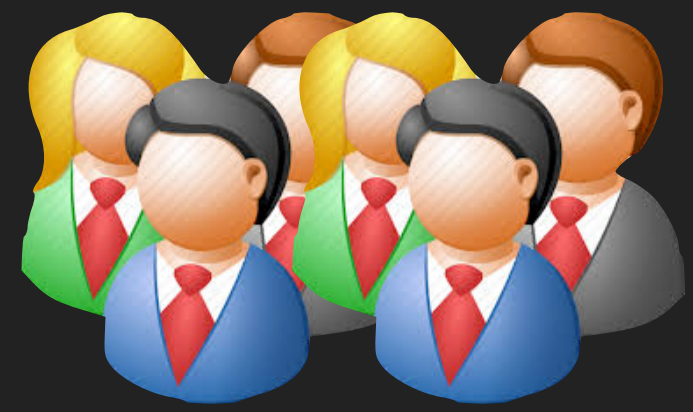










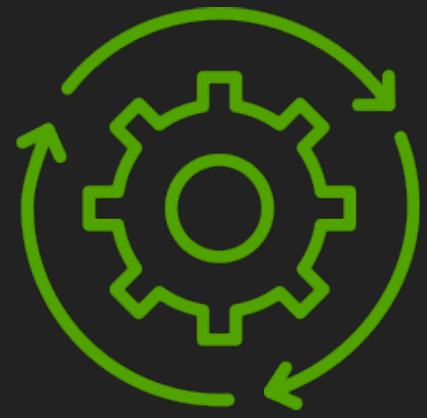


BAD FOR EVERYONE





WE RAISE MONEY BADLY

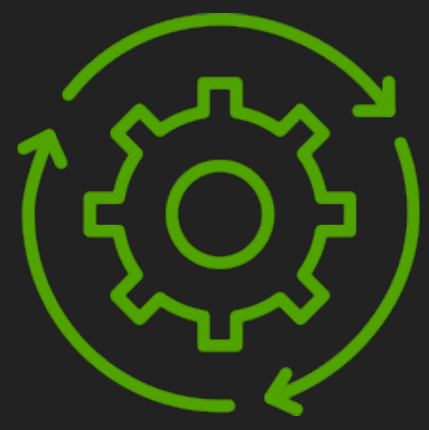


WE BUILD PRODUCTS BADLY



WE DO SALES BADLY

COMPLEXITY





[Essays](#) >

A Plea for Simplicity

You can't secure what you don't understand.

Bruce Schneier
Information Security

Ask any 21 experts to predict the future, and they're likely to point in 21 different directions. But whatever the future holds--IP everywhere, smart cards everywhere, video everywhere, Internet commerce everywhere, wireless everywhere, agents everywhere, AI everywhere, *everything* everywhere--the one thing you can be sure of is that it will be complex. For consumers, this is great. For security professionals, this is terrifying. The worst enemy of security is complexity. This has been true since the beginning of computers, and it's likely to be true for the foreseeable future.

We all know the amount of testing that goes into any major software product, and we all know the number of bugs that still slip through. The testing process--implement, test, fix, test, repeat--is imperfect, but it's the best we've found. Security doesn't lend itself to this process, because security properties cannot be "tested" in the same way as functional properties. Products are useful for what they do, while security products are useful solely because of what they *prevent* from being done. A security product may work fine, but you have no idea if it is secure. No amount of beta testing can uncover a security flaw. Ever.

The only way to evaluate the security of a system is to analyze it. This is a time-consuming and expensive process, and almost no one bothers to go through it. If they did, they would quickly realize that most systems are far more complex to analyze, and that there are security flaws everywhere.

We've seen security bugs in almost everything: operating systems, applications programs, network hardware and software, and security products themselves. This is a direct result of the complexity of these systems. The more complex a system is--the more options it has, the more functionality it has, the more interfaces it has, the more interactions it has--the harder it is to analyze. Everything is more complicated: the specification, the design, the implementation, the use. And everything is relevant to

Search

Powered by *DuckDuckGo*

blog essays whole site

Subscribe



About Bruce Schneier



I am a **public-interest technologist**, working at the intersection of security, technology, and people. I've been writing about security issues on my **blog** since 2004, and in my monthly **newsletter** since 1998. I'm a fellow and lecturer at Harvard's **Kennedy School** and a board member of **EFF**. This personal website expresses the opinions of neither of those organizations.

Featured Essays

[The Value of Encryption](#)

[Data Is a Toxic Asset, So Why Not Throw It Out?](#)

[How the NSA Threatens National Security](#)

[Terrorists May Use Google Earth, But Fear Is No Reason to Ban It](#)

[In Praise of Security Theater](#)

[Refuse to be Terrorized](#)

[The Eternal Value of Privacy](#)

[Terrorists Don't Do Movie Plots](#)

THE WORST ENEMY OF SECURITY IS COMPLEXITY.



[Essays](#) >

A Plea for Simplicity

You can't secure what you don't understand.

Bruce Schneier
Information Security

Ask any 21 experts to predict the future, and they're likely to point in 21 different directions. But whatever the future holds--IP everywhere, smart cards everywhere, video everywhere, Internet commerce everywhere, wireless everywhere, agents everywhere, AI everywhere, *everything* everywhere--the one thing you can be sure of is that it will be complex. For consumers, this is great. For security professionals, this is terrifying. The worst enemy of security is complexity. This has been true since the beginning of computers, and it's likely to be true for the foreseeable future.

We all know the amount of testing that goes into any major software product, and we all know the number of bugs that still slip through. The testing process--implement, test, fix, test, repeat--is imperfect, but it's the best we've found. Security doesn't lend itself to this process, because security properties cannot be "tested" in the same way as functional properties. Products are useful for what they do, while security products are useful solely because of what they *prevent* from being done. A security product may work fine, but you have no idea if it is secure. No amount of beta testing can uncover a security flaw. Ever.

The only way to evaluate the security of a system is to analyze it. This is a time-consuming and expensive process, and almost no one bothers to go through it. If they did, they would quickly realize that most systems are far more complex to analyze, and that there are security flaws everywhere.

We've seen security bugs in almost everything: operating systems, applications programs, network hardware and software, and security products themselves. This is a direct result of the complexity of these systems. The more complex a system is--the more options it has, the more functionality it has, the more interfaces it has, the more interactions it has--the harder it is to analyze. Everything is more complicated: the specification, the design, the implementation, the use. And everything is relevant to

Search

Powered by *DuckDuckGo*

blog essays whole site

Subscribe



About Bruce Schneier



I am a **public-interest technologist**, working at the intersection of security, technology, and people. I've been writing about security issues on my **blog** since 2004, and in my monthly **newsletter** since 1998. I'm a fellow and lecturer at Harvard's **Kennedy School** and a board member of **EFF**. This personal website expresses the opinions of neither of those organizations.

Featured Essays

[The Value of Encryption](#)

[Data Is a Toxic Asset, So Why Not Throw It Out?](#)

[How the NSA Threatens National Security](#)

[Terrorists May Use Google Earth, But Fear Is No Reason to Ban It](#)

[In Praise of Security Theater](#)

[Refuse to be Terrorized](#)

[The Eternal Value of Privacy](#)

[Terrorists Don't Do Movie Plots](#)

A SECURITY PRODUCT MAY WORK FINE, BUT YOU HAVE NO IDEA IF IT IS SECURE. NO AMOUNT OF BETA TESTING CAN UNCOVER A SECURITY FLAW. EVER.



[Essays](#) >

A Plea for Simplicity

You can't secure what you don't understand.

Bruce Schneier
Information Security

Ask any 21 experts to predict the future, and they're likely to point in 21 different directions. But whatever the future holds--IP everywhere, smart cards everywhere, video everywhere, Internet commerce everywhere, wireless everywhere, agents everywhere, AI everywhere, *everything* everywhere--the one thing you can be sure of is that it will be complex. For consumers, this is great. For security professionals, this is terrifying. The worst enemy of security is complexity. This has been true since the beginning of computers, and it's likely to be true for the foreseeable future.

We all know the amount of testing that goes into any major software product, and we all know the number of bugs that still slip through. The testing process--implement, test, fix, test, repeat--is imperfect, but it's the best we've found. Security doesn't lend itself to this process, because security properties cannot be "tested" in the same way as functional properties. Products are useful for what they do, while security products are useful solely because of what they *prevent* from being done. A security product may work fine, but you have no idea if it is secure. No amount of beta testing can uncover a security flaw. Ever.

The only way to evaluate the security of a system is to analyze it. This is a time-consuming and expensive process, and almost no one bothers to go through it. If they did, they would quickly realize that most systems are far more complex to analyze, and that there are security flaws everywhere.

We've seen security bugs in almost everything: operating systems, applications programs, network hardware and software, and security products themselves. This is a direct result of the complexity of these systems. The more complex a system is--the more options it has, the more functionality it has, the more interfaces it has, the more interactions it has--the harder it is to analyze. Everything is more complicated: the specification, the design, the implementation, the use. And everything is relevant to

Search

Powered by *DuckDuckGo*

blog essays whole site

Subscribe



About Bruce Schneier



I am a **public-interest technologist**, working at the intersection of security, technology, and people. I've been writing about security issues on my **blog** since 2004, and in my monthly **newsletter** since 1998. I'm a fellow and lecturer at Harvard's **Kennedy School** and a board member of **EFF**. This personal website expresses the opinions of neither of those organizations.

Featured Essays

[The Value of Encryption](#)

[Data Is a Toxic Asset, So Why Not Throw It Out?](#)

[How the NSA Threatens National Security](#)

[Terrorists May Use Google Earth, But Fear Is No Reason to Ban It](#)

[In Praise of Security Theater](#)

[Refuse to be Terrorized](#)

[The Eternal Value of Privacy](#)

[Terrorists Don't Do Movie Plots](#)

THE OTHER CHOICE IS TO SLOW DOWN, SIMPLIFY AND TRY TO ADD SECURITY. CUSTOMERS WON'T DEMAND THIS-- THE ISSUES ARE TOO COMPLEX FOR THEM TO UNDERSTAND



[Essays](#) >

A Plea for Simplicity

You can't secure what you don't understand.

Bruce Schneier
Information Security
November 19, 1999

Ask any 21 experts to predict the future, and they're likely to point in 21 different directions. But whatever the future holds--IP everywhere, smart cards everywhere, video everywhere, Internet commerce everywhere, wireless everywhere, agents everywhere, AI everywhere, *everything* everywhere--the one thing you can be sure of is that it will be complex. For consumers, this is great. For security professionals, this is terrifying. The worst enemy of security is complexity. This has been true since the beginning of computers, and it's likely to be true for the foreseeable future.

We all know the amount of testing that goes into any major software product, and we all know the number of bugs that still slip through. The testing process--implement, test, fix, test, repeat--is imperfect, but it's the best we've found. Security doesn't lend itself to this process, because security properties cannot be "tested" in the same way as functional properties. Products are useful for what they do, while security products are useful solely because of what they *prevent* from being done. A security product may work fine, but you have no idea if it is secure. No amount of beta testing can uncover a security flaw. Ever.

The only way to evaluate the security of a system is to analyze it. This is a time-consuming and expensive process, and almost no one bothers to go through it. If they did, they would quickly realize that most systems are far more complex to analyze, and that there are security flaws everywhere.

We've seen security bugs in almost everything: operating systems, applications programs, network hardware and software, and security products themselves. This is a direct result of the complexity of these systems. The more complex a system is--the more options it has, the more functionality it has, the more interfaces it has, the more interactions it has--the harder it is to analyze. Everything is more complicated: the specification, the design, the implementation, the use. And everything is relevant to

Search

Powered by *DuckDuckGo*

blog essays whole site

Subscribe



About Bruce Schneier



I am a **public-interest technologist**, working at the intersection of security, technology, and people. I've been writing about security issues on my **blog** since 2004, and in my monthly **newsletter** since 1998. I'm a fellow and lecturer at Harvard's **Kennedy School** and a board member of **EFF**. This personal website expresses the opinions of neither of those organizations.

Featured Essays

[The Value of Encryption](#)

[Data Is a Toxic Asset, So Why Not Throw It Out?](#)

[How the NSA Threatens National Security](#)

[Terrorists May Use Google Earth, But Fear Is No Reason to Ban It](#)

[In Praise of Security Theater](#)

[Refuse to be Terrorized](#)

[The Eternal Value of Privacy](#)

[Terrorists Don't Do Movie Plots](#)



[Essays](#) >

A Plea for Simplicity

You can't secure what you don't understand.

Bruce Schneier
Information Security
November 19, 1999

Ask any 21 experts to predict the future, and they're likely to point in 21 different directions. But whatever the future holds--IP everywhere, smart cards everywhere, video everywhere, Internet commerce everywhere, wireless everywhere, agents everywhere, AI everywhere, *everything* everywhere--the one thing you can be sure of is that it will be complex. For consumers, this is great. For security professionals, this is terrifying. The worst enemy of security is complexity. This has been true since the beginning of computers, and it's likely to be true for the foreseeable future.

We all know the amount of testing that goes into any major software product, and we all know the number of bugs that still slip through. The testing process--implement, test, fix, test, repeat--is imperfect, but it's the best we've found. Security doesn't lend itself to this process, because security properties cannot be "tested" in the same way as functional properties. Products are useful for what they do, while security products are useful solely because of what they *prevent* from being done. A security product may work fine, but you have no idea if it is secure. No amount of beta testing can uncover a security flaw. Ever.

The only way to evaluate the security of a system is to analyze it. This is a time-consuming and expensive process, and almost no one bothers to go through it. If they did, they would quickly realize that most systems are far more complex to analyze, and that there are security flaws everywhere.

We've seen security bugs in almost everything: operating systems, applications programs, network hardware and software, and security products themselves. This is a direct result of the complexity of these systems. The more complex a system is--the more options it has, the more functionality it has, the more interfaces it has, the more interactions it has--the harder it is to analyze. Everything is more complicated: the specification, the design, the implementation, the use. And everything is relevant to

Search

Powered by *DuckDuckGo*

blog essays whole site

Subscribe



About Bruce Schneier



I am a **public-interest technologist**, working at the intersection of security, technology, and people. I've been writing about security issues on my **blog** since 2004, and in my monthly **newsletter** since 1998. I'm a fellow and lecturer at Harvard's **Kennedy School** and a board member of **EFF**. This personal website expresses the opinions of neither of those organizations.

Featured Essays

[The Value of Encryption](#)

[Data Is a Toxic Asset, So Why Not Throw It Out?](#)

[How the NSA Threatens National Security](#)

[Terrorists May Use Google Earth, But Fear Is No Reason to Ban It](#)

[In Praise of Security Theater](#)

[Refuse to be Terrorized](#)

[The Eternal Value of Privacy](#)

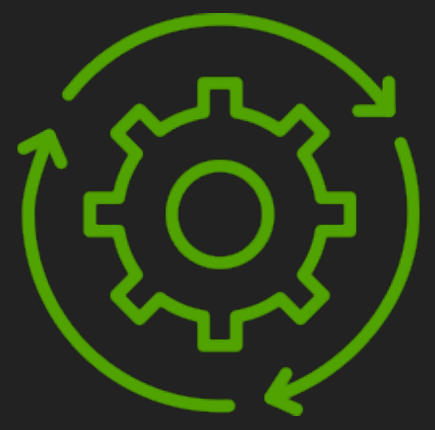
[Terrorists Don't Do Movie Plots](#)

BRUCE SCHNEIER

INFORMATION SECURITY

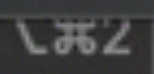
NOVEMBER 19, 1999

\$ gpg --version





bash

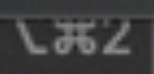


maru:~ haroon\$ ma

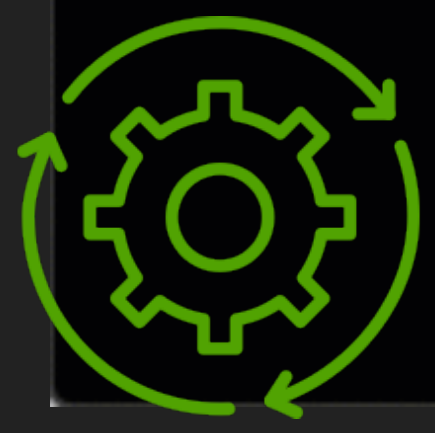
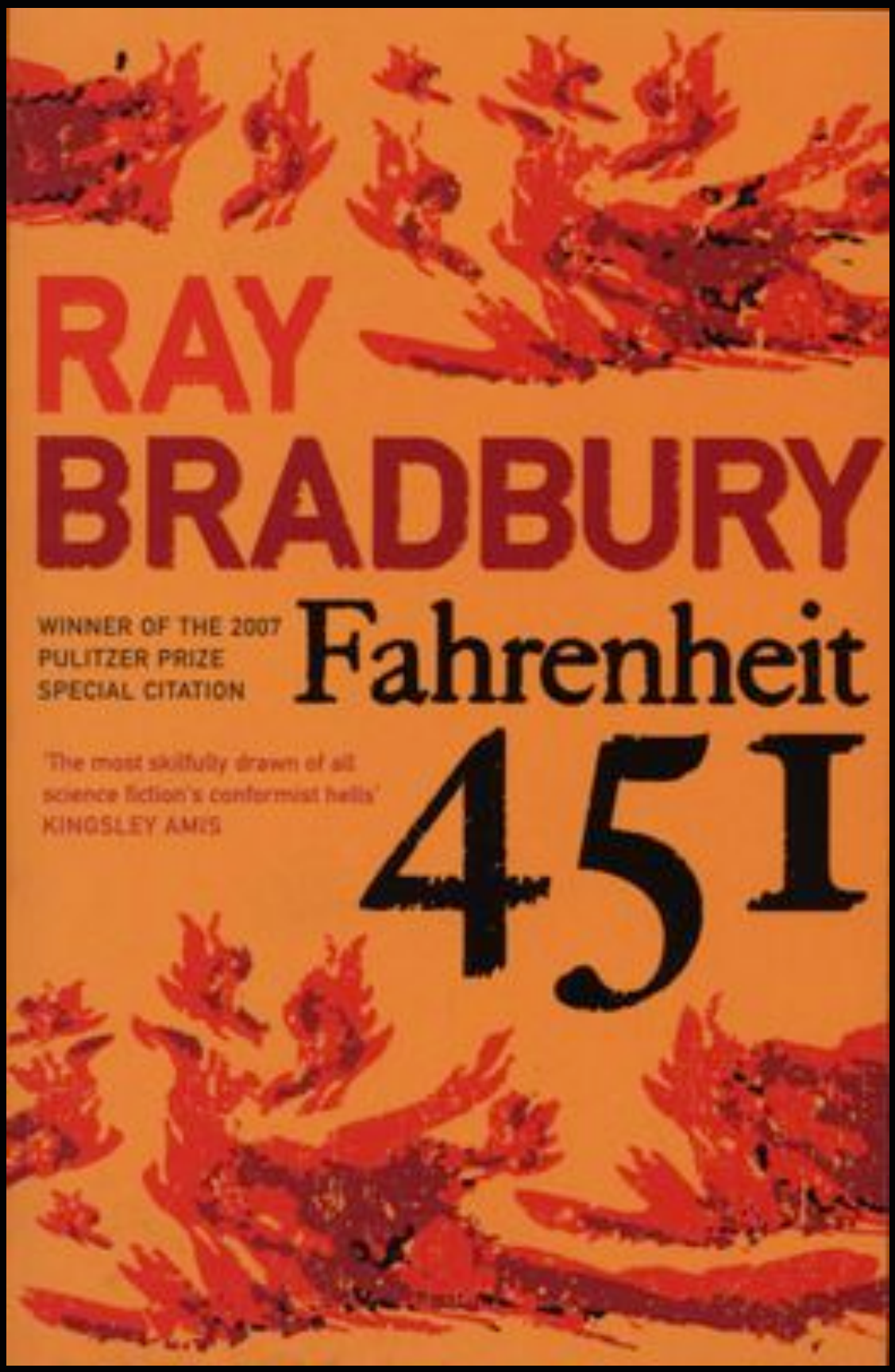




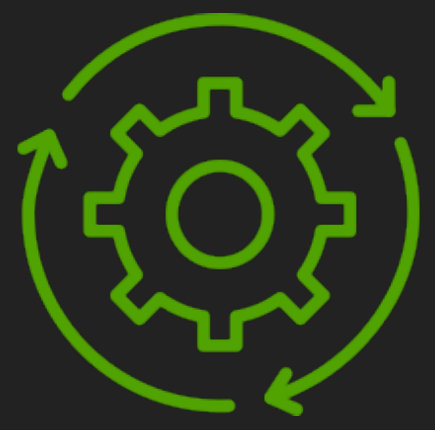
bash



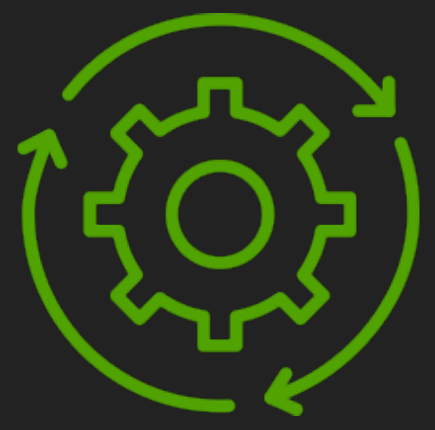
maru:~ haroon\$ ma



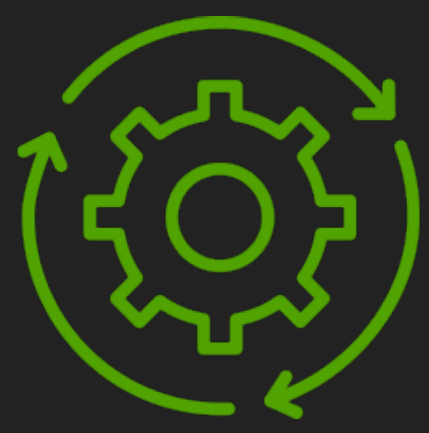
BUT WHY THO'?



- INVESTORS
- BOFH HISTORY
- OLD CANARDS



INSECURE SECURITY PRODUCTS





haroon meer

@haroonmeer

FireEye exists to stop 0days. Raft of 0days reported in FireEye boxes.

Obviously we need another box that stops 0days in front of FE boxes.

RETWEETS

219

LIKES

130



11:26 AM - 8 Sep 2015



Dino A. Dai Zovi

@dinodaizovi



Following

Security anti-pattern #34: Attempting to mitigate vulnerable attack surfaces with higher-privileged *and more vulnerable* attack surfaces.

RETWEETS

46

LIKES

57



9:13 PM - 16 Apr 2016



Tavis Ormandy @taviso · May 11

Many remote stack overflows in Symantec Endpoint. No big deal, because /GS is the default since 2005, right? Hahaha.

```
ModLoad 07710000 07800000 C:\Windows\System32\Kernel32.dll
ModLoad 07710000 07801000 C:\Windows\System32\advapi32.dll
ModLoad 0eef0000 0ef20000 C:\ProgramData\Symantec\Symantec Endpoint Protection\12.1.4304.4100\105-Data-Definitions\FirusDefa-20140510-DOT-POWER32.dll
ModLoad 0a710000 0a740000 C:\ProgramData\Symantec\Symantec Endpoint Protection\12.1.4304.4100\105-Data-Definitions\FirusDefa-20140510-DOT-BAYERN32.dll
ModLoad 0e9c0000 0eaf0000 C:\ProgramData\Symantec\Symantec Endpoint Protection\12.1.4304.4100\105-Data-Definitions\FirusDefa-20140510-DOT-BAYERN32.dll
[Ext obj]: Cse KR exception = code 0007163 (first chance)
ModLoad 0ea70000 0eab0000 C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\12.1.4304.4100\105-Data\sw1.dll
[Ext obj]: Access violation = code 0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00000000 ebx=00000000 ecx=00000000 edx=00000000 iax=00000000
esp=41414141 ebp=07107100 iopl=0         up=up  ip=ip             op=0023 00*0023 00*0023 00*0023 00*0023 00*0023 00*0023 00*0023
41414141 75
0 070> !avr & cc0c080
ntext  eax  ebx  ecx  edx  iax
01110000 02114000 cc0c080 (Deferred)
Image path: C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\12.1.4304.4100\105-Data\cc0c080.exe
Image name: cc0c080.exe
Timestamp: Fri May 29 17:26:40 2015 (55928AC0)
CheckSum: 00029F12
ImageSize: 00024000
File Version: 12.12.0.15
Product Version: 12.12.0.15
File flags: 0 (NONE)
File OS: 40004 NT Win32
File type: 1.0 App
File date: 00000100 00000000
Translations: 0409 0409
Company Name: Symantec Corporation
Product Name: Symantec Security Technologies
Internal Name: cc0c080
OriginalFilename: cc0c080.exe
Product Version: 12.12.0.15
File Version: 12.12.0.15
File Description: Symantec Service Framework
Legal Copyright: Copyright (c) 2013 Symantec Corporation. All rights reserved.
```

← ↻ 340 ❤️ 249 I ...



Retweeted by Ben Nagy



Joxean Koret @matalaz · 30m

It took me longer to install your AV, Comodo, than finding the first bug on it. Thanks for playing, wait for results...

RETWEETS

8

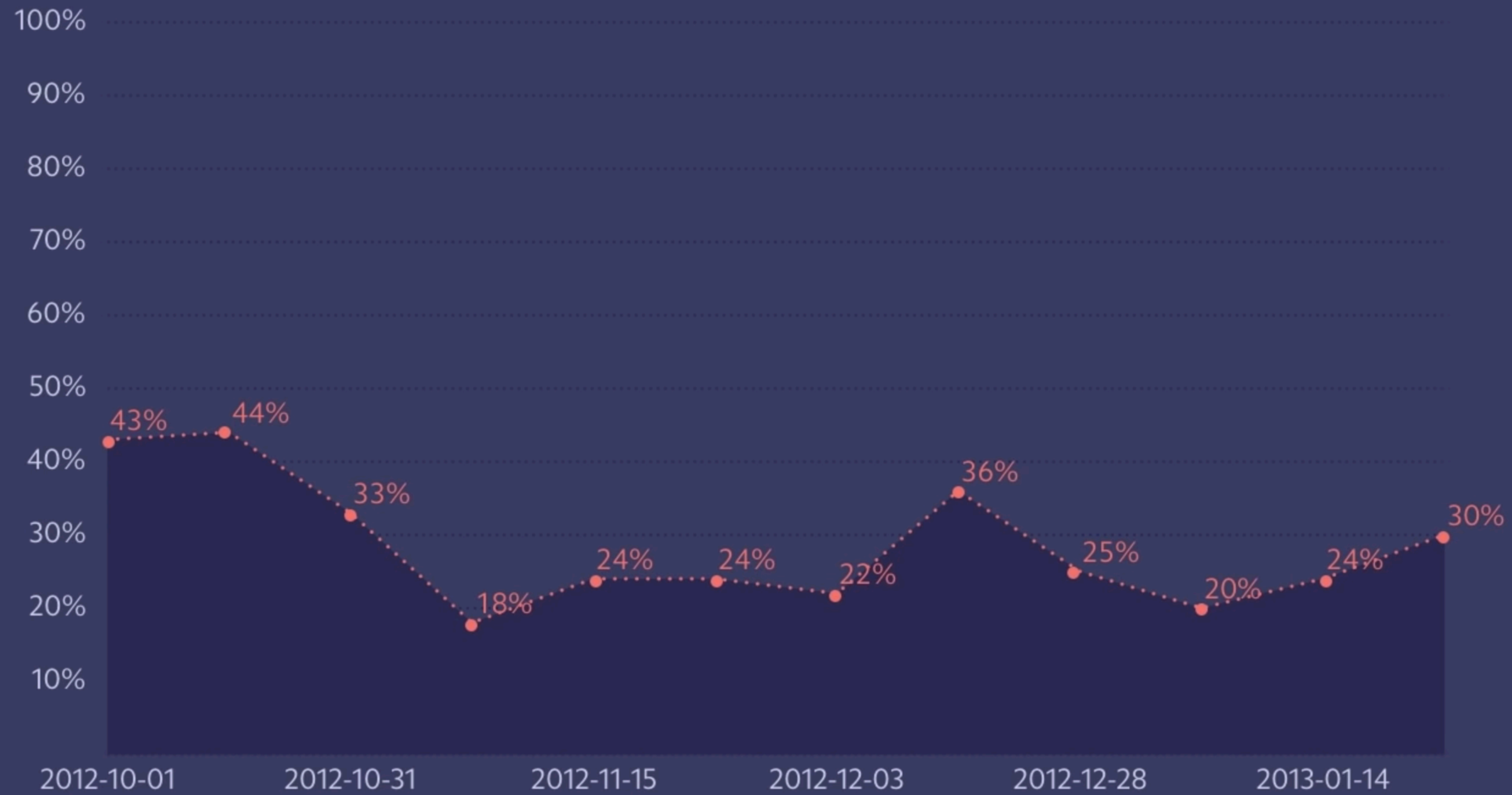
FAVORITES

4



2:02 PM - 25 Aug 2014 · Details

Layered Security Solutions



Source: DARPA Cyber Analytical Framework. Peiter Zatko primary author.

When data contradicts best practices – <https://www.youtube.com/watch?v=S0QgABDSYZE>

Software Sub-segment Performance on First Submission

■ Acceptable ■ Not Acceptable

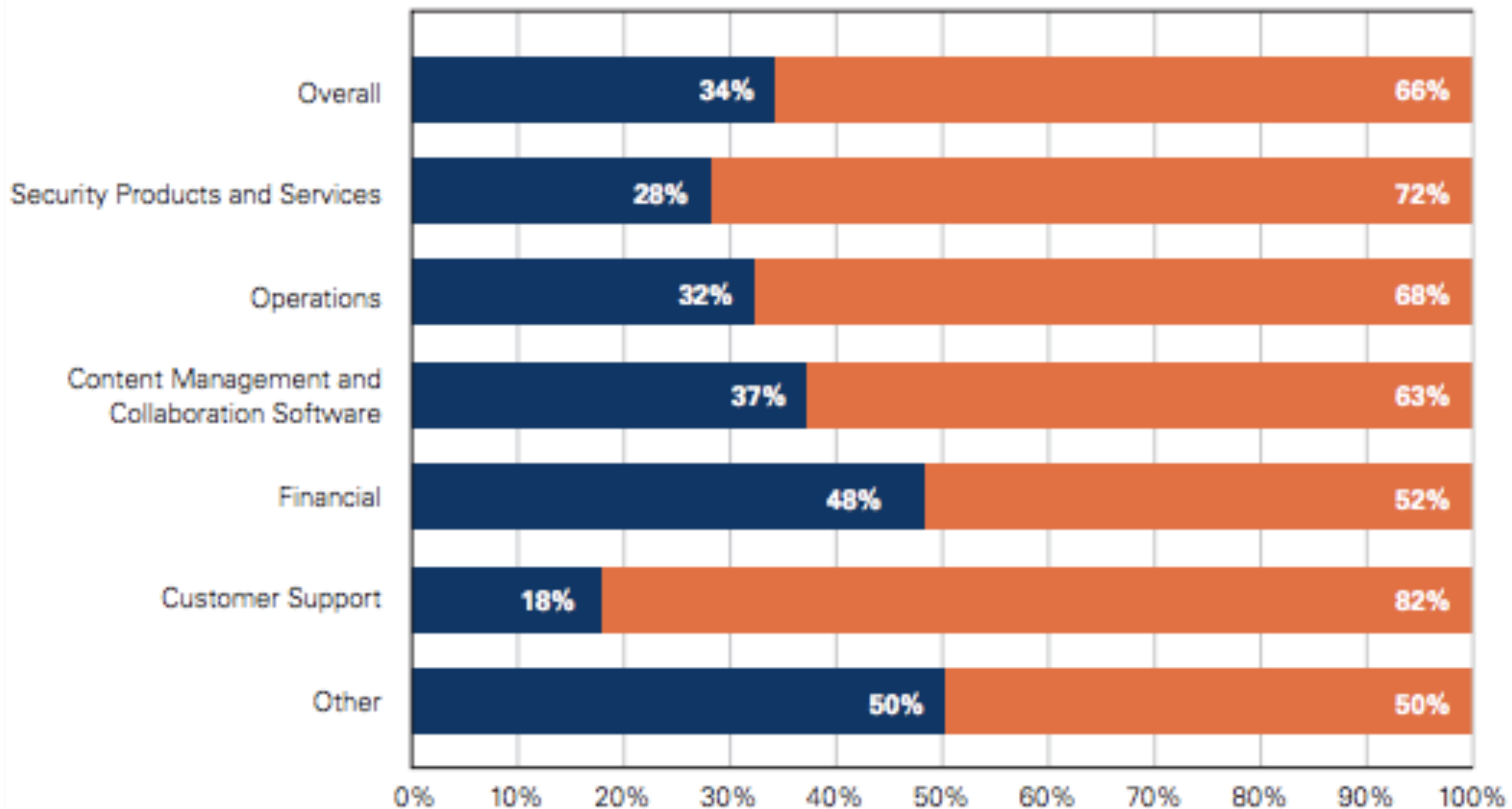
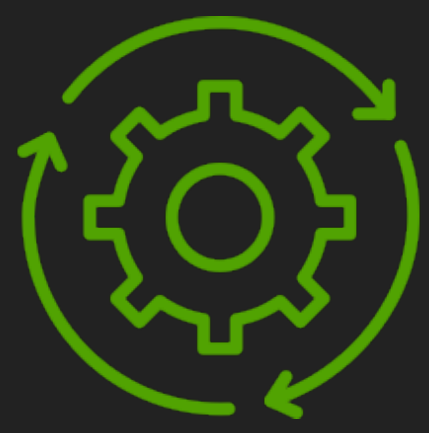
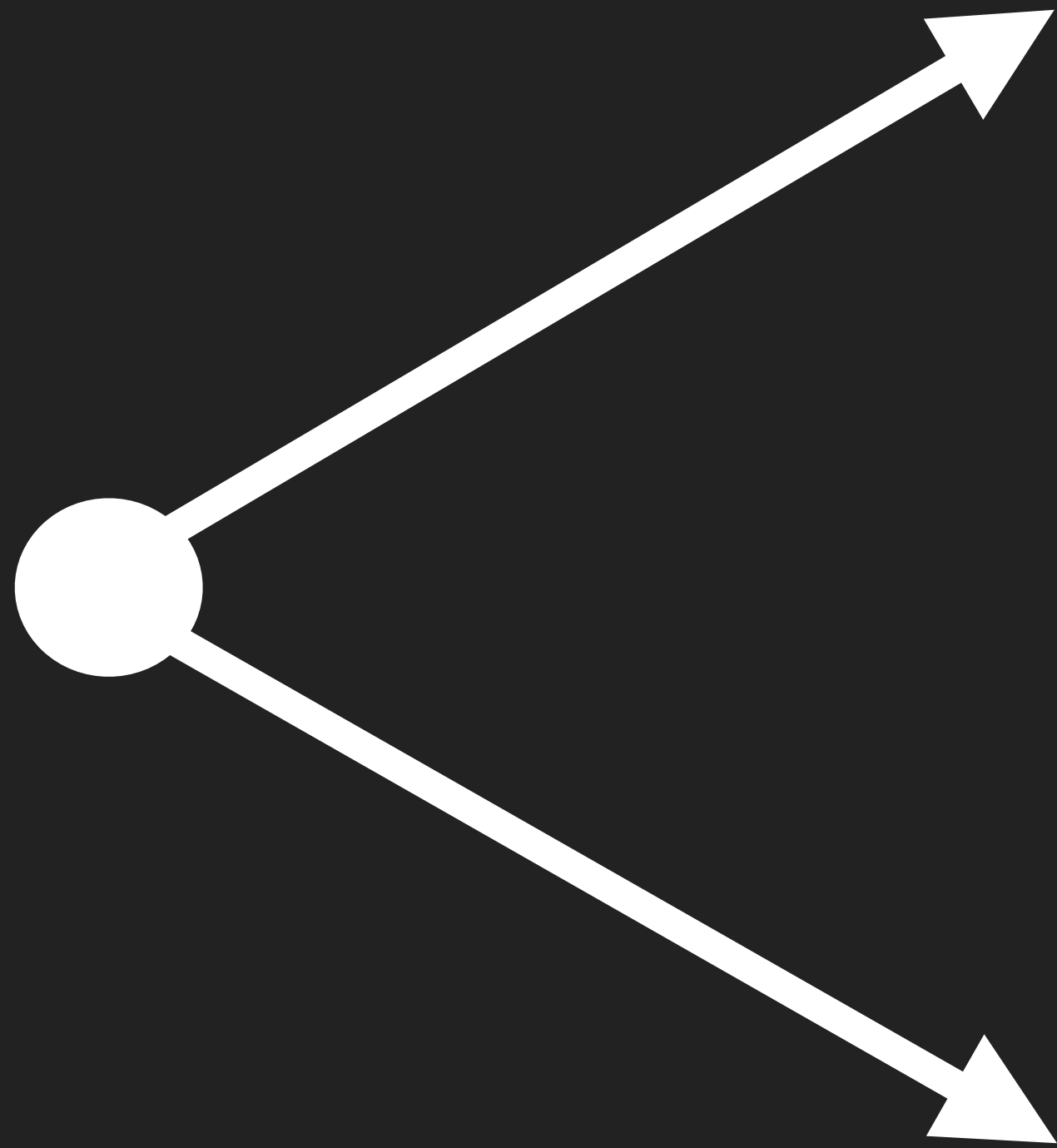


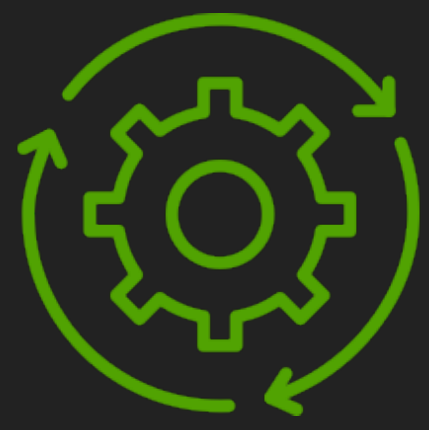
Figure 28: Software Sub-segment Performance on First Submission



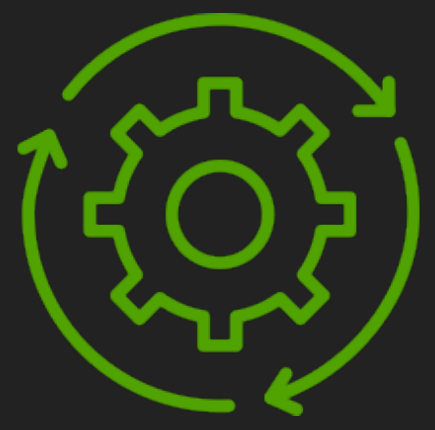


VLAN

REVIEW

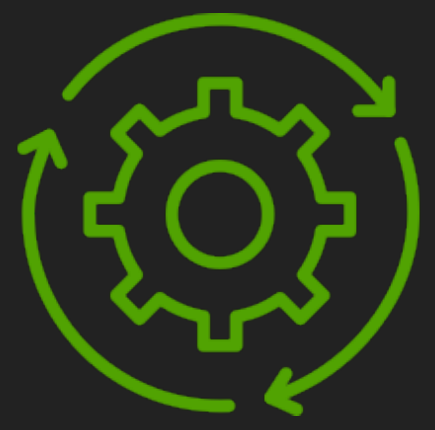


BUT WHY THO'?



- **NO PUSHBACK**

- **INABILITY TO TELL THE DIFFERENCE?**





WE RAISE MONEY BADLY



WE BUILD PRODUCTS BADLY

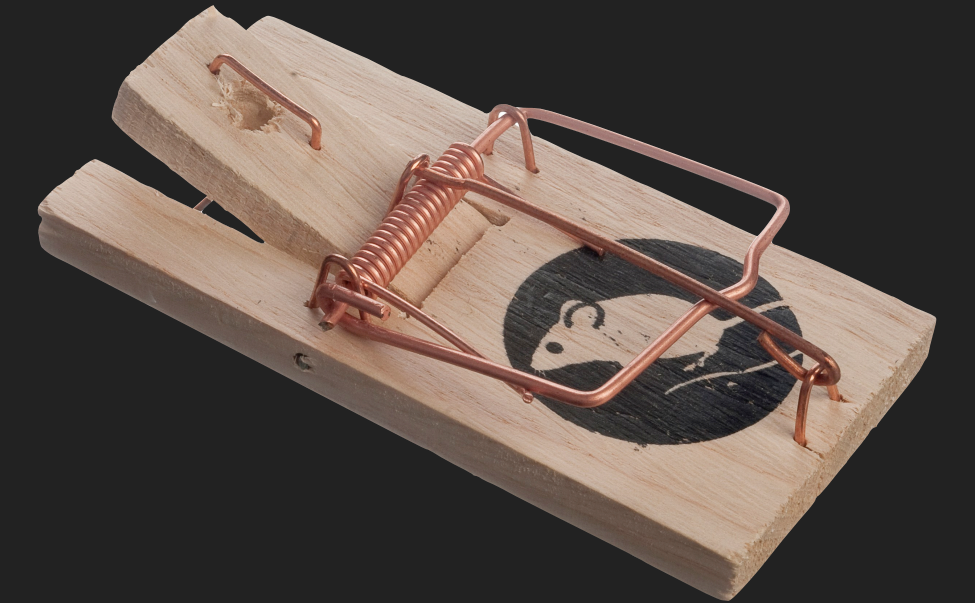


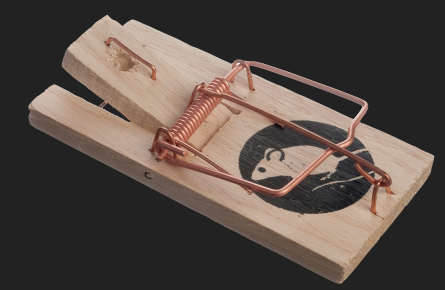
WE DO SALES BADLY

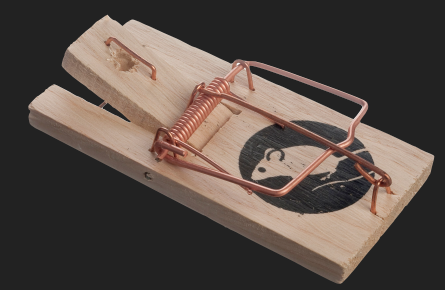
If You Build It, They Will Not Come

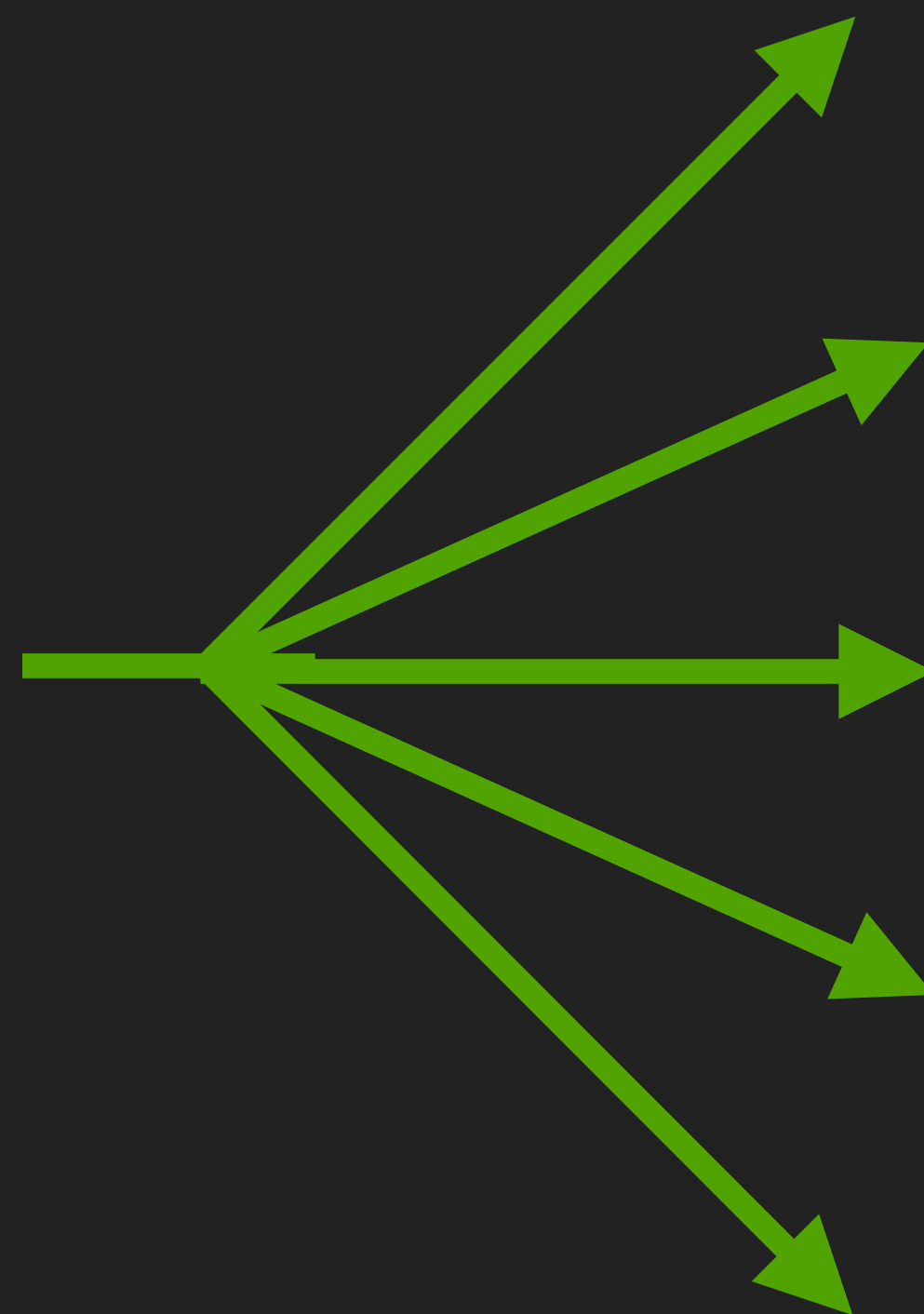


Add to Queue











What was the single biggest security challenge that you needed to deal with?



<https://cisoserries.com/simple-tool-to-visualize-the-security-vendor-ecosystem/>



Sounil Yu

Creator, Cyber Defense Matrix



The bazillion vendors that came knocking on my door trying to take a little bit of the BoA budget for security

PREPARED TO DEFEND

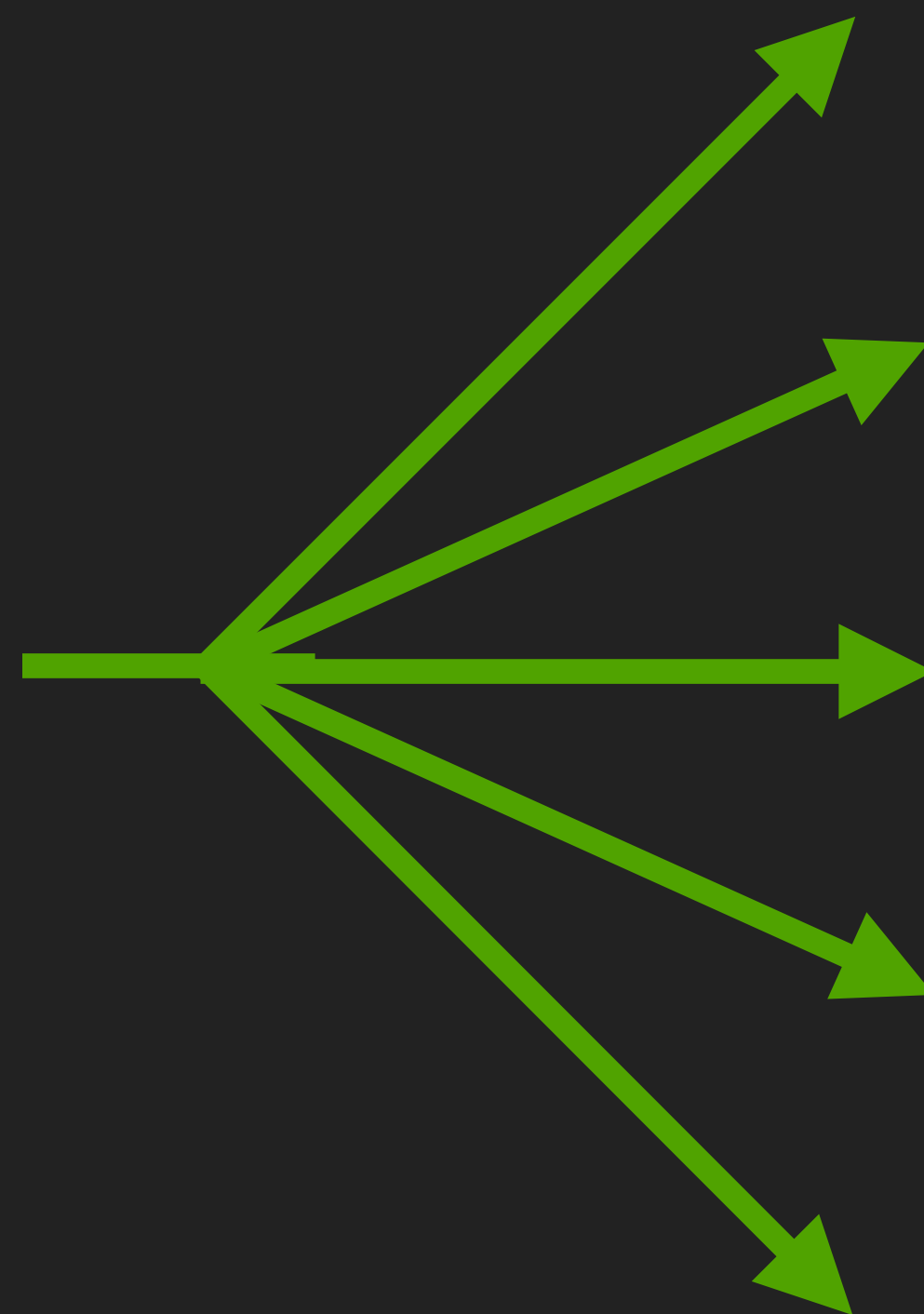
Powered by AI, Darktrace Antigena fights back against the most advanced cyber-attacks. From rapid ransomware to stealthy insider threats, our world-leading technology responds in seconds - giving you time to catch up.

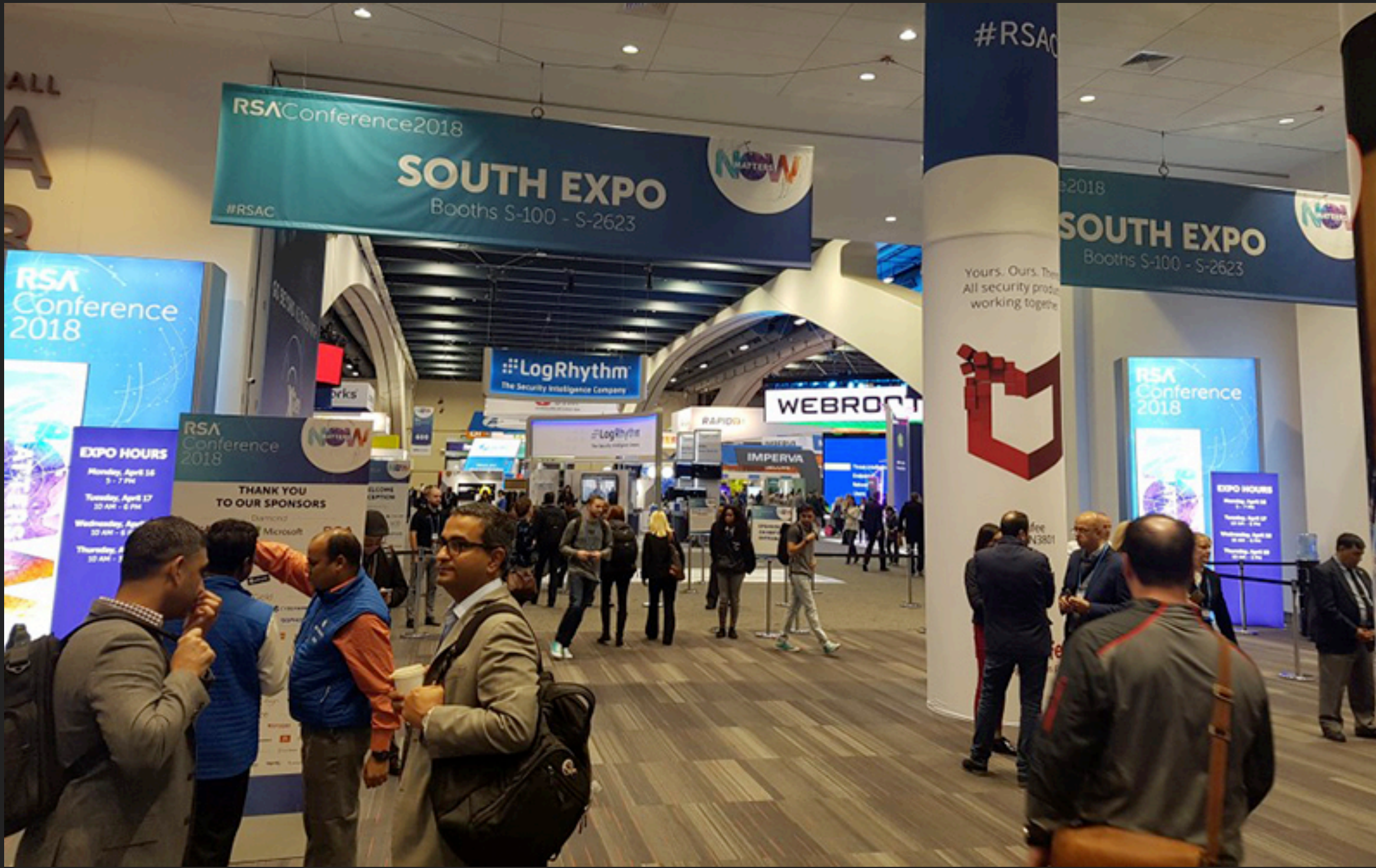
Learn more at darktrace.com



 **DARKTRACE**
World-Leading Cyber AI








thinkst Thoughts...: Considerin x +

blog.thinkst.com/p/we-found-expo-incredibly-worthwhile.html

Considering an RSAC Expo booth? Our Experience, in 5,000 words or less



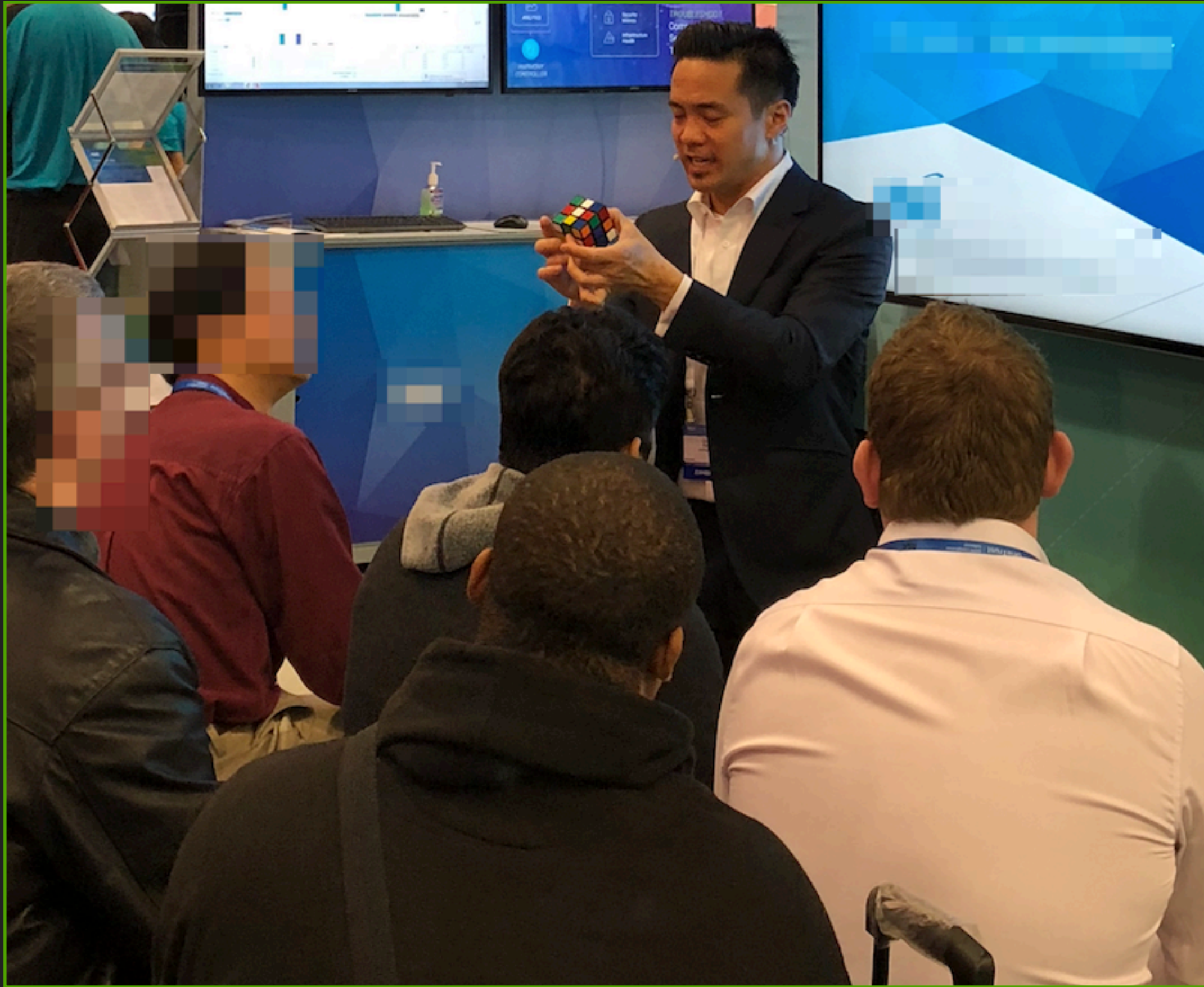
Introduction

Thinkst'ers have spoken at a heap of security conferences across careers spanning decades, and yet last year (2017) was the first time any of us actually attended RSAC (<https://www.rsaconference.com/>), when I attended the expo (almost accidentally). At the time I was surprised by a bunch of things, from its insane size to the bizarre vendor shenanigans. As I walked the expo floor I asked an array of vendors if they felt the show was worth it for them. The answers were mixed but most gravitated towards an uninspiring "We don't get huge value, but it will send a negative signal if we aren't here". While this confirmed my old bias that RSAC is exhibit-A of everything wrong with the industry, I was able to set-up multiple meetings for every one of my days in town and all the folks I met were (or became) Canary customers. Last year's tiny foray seemed promising and a proper run at the expo was something we had to test ourselves.

So we decided to try a booth for 2018, and figured we'd document our experience (and thoughts) along the way. In this post you'll find a full breakdown of all our costs for attending and boothing at RSAC, including what it takes to get a space; kitting it out with furniture, equipment, swag and more; staffing the booth; the crazy that is conference pricing; and the logistics for actually making it happen.



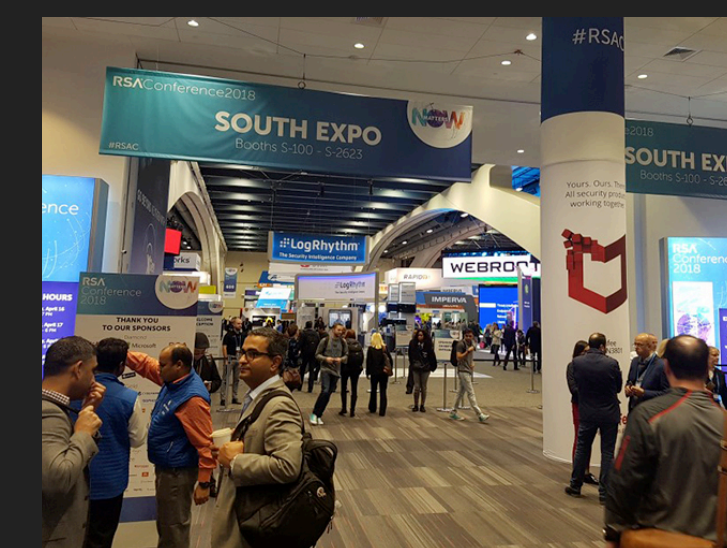
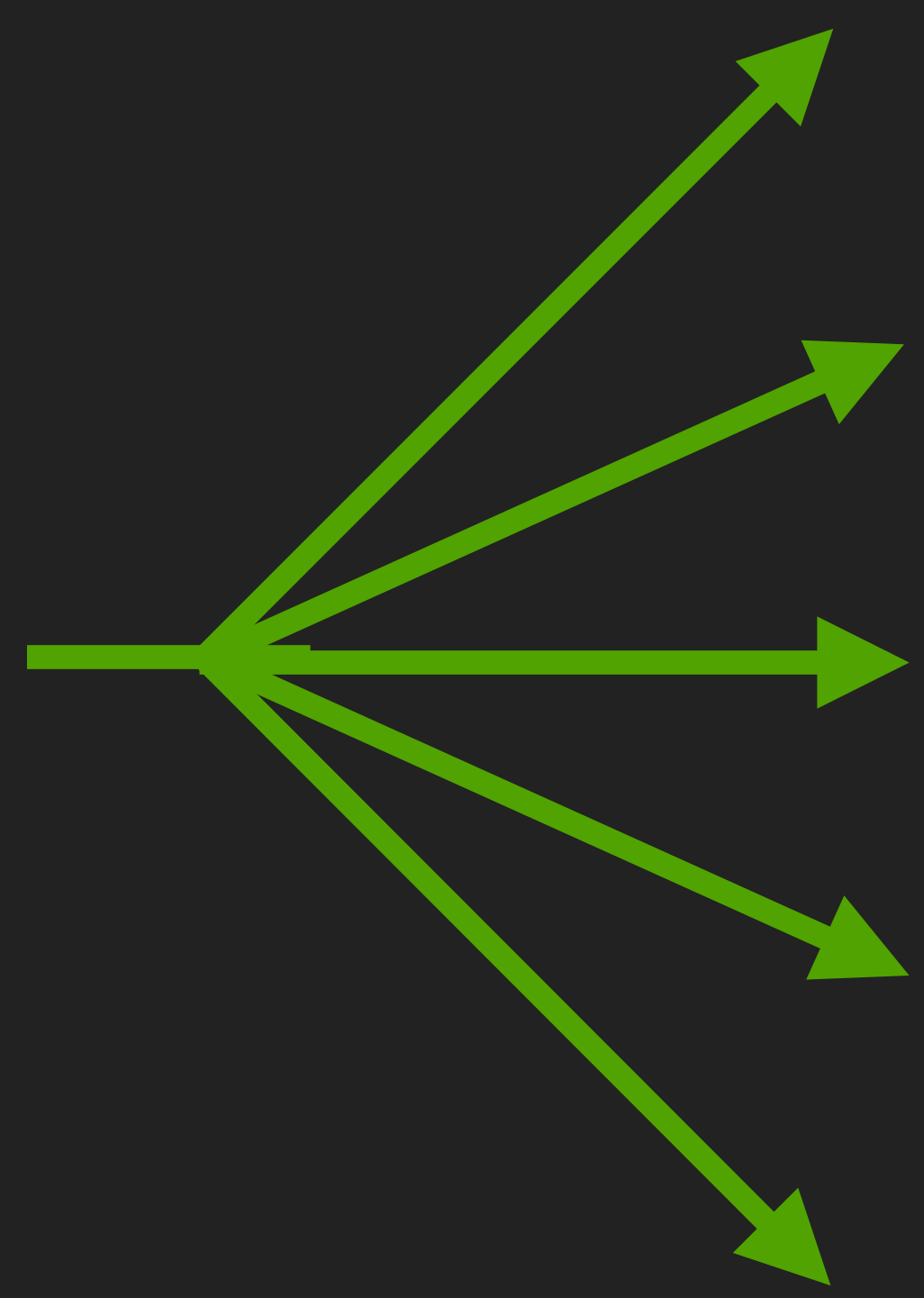
<https://blog.thinkst.com/p/we-found-expo-incredibly-worthwhile.html>



**IF A COMPANY DEDICATES 90% OF
THEIR FLOORSPACE TO THEIR RSAC
GIMMICK, AND JUST 10% TO ONE
DEMO STATION...**

me





Thank You for Making Us No. 1



McCarran INTERNATIONAL AIRPORT

HIGHEST RANKED IN AIRPORT CUSTOMER SATISFACTION AMONG MEGA AIRPORTS

For J.D. Power 2018 award information visit jdpower.com/awards

NanoLumens LAMAR

OUR PEOPLE MAKE US AMERICA'S MOST AWARDED AIRLINE.



#DELTAPROUD

11-1096-999

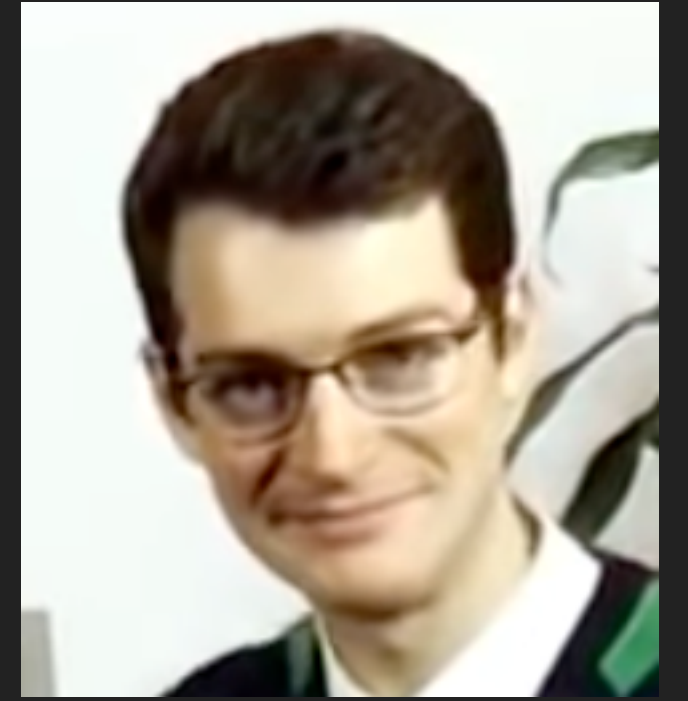
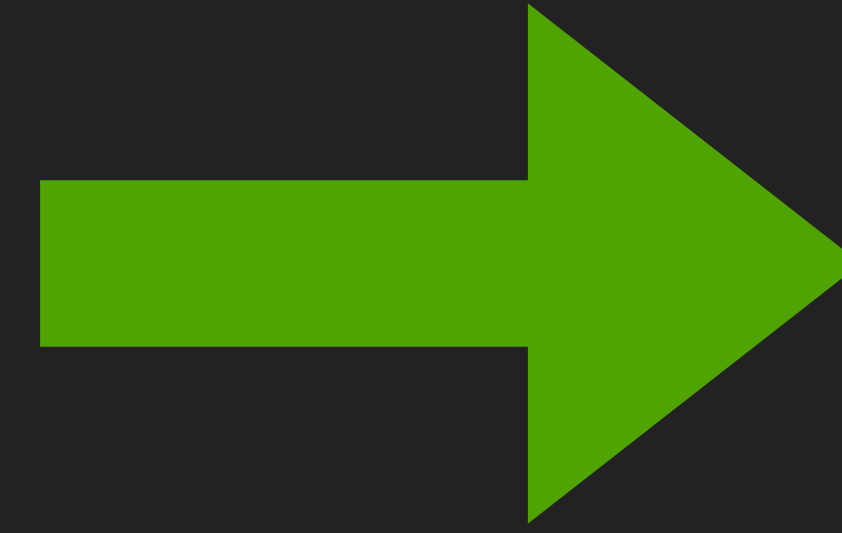
Flor de Caña

WINNER GLOBAL RUM PRODUCER OF THE YEAR

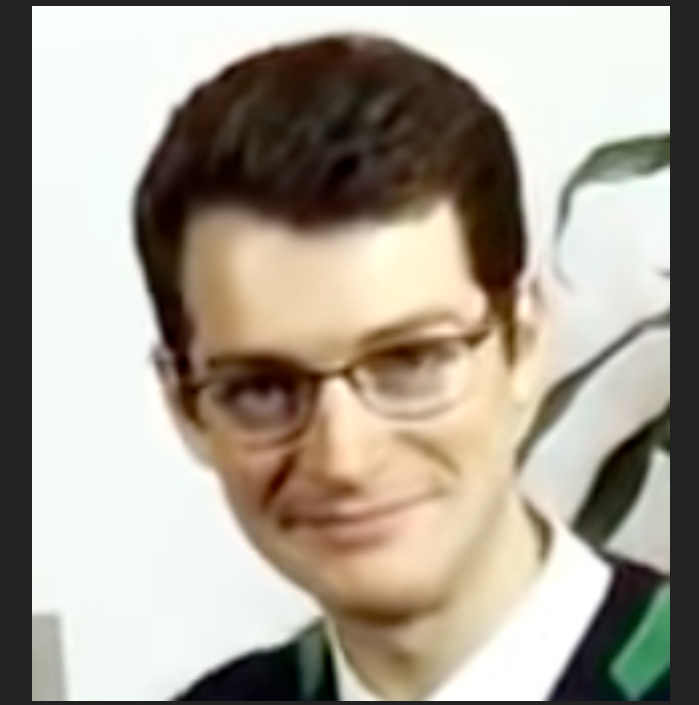
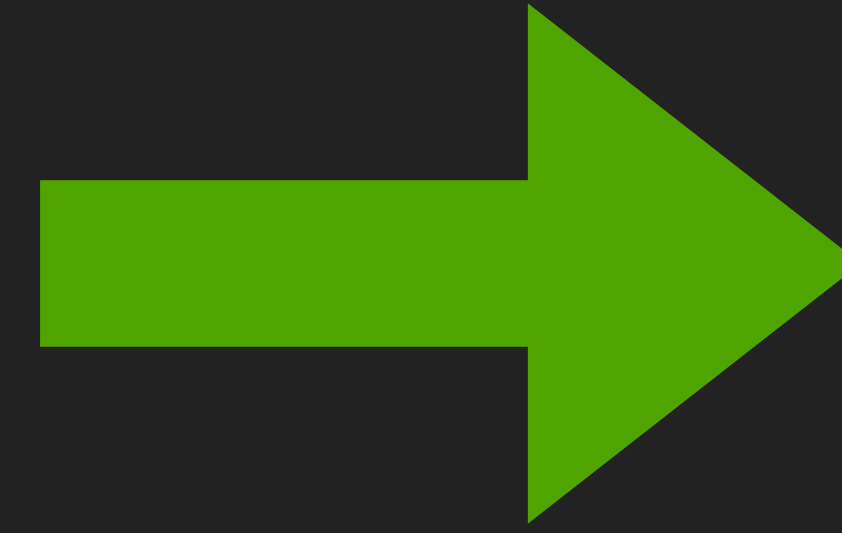
IWSC, '17



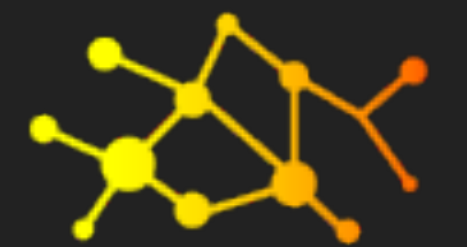
MEET PAUL



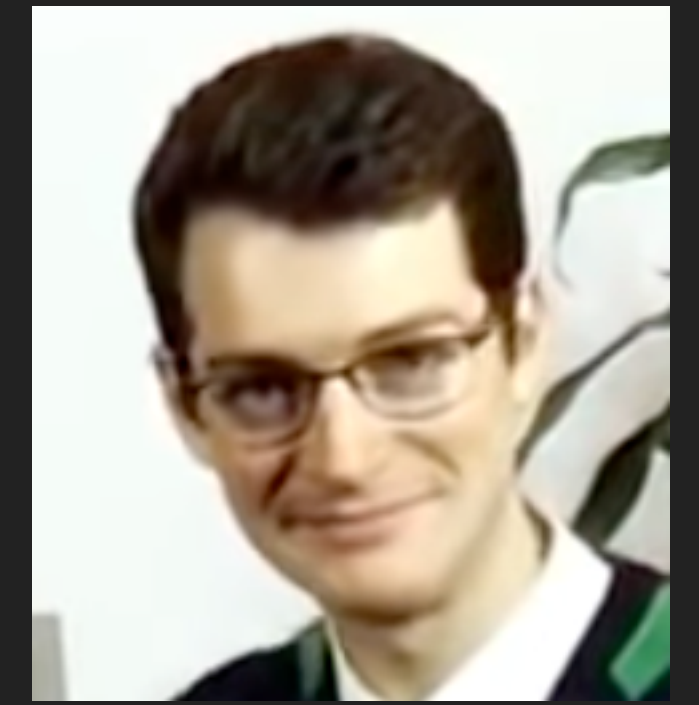
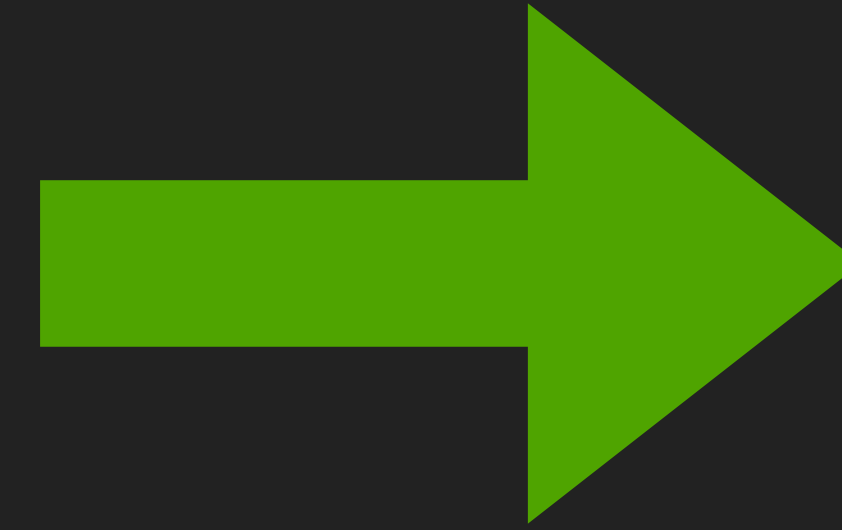
MEET PAUL



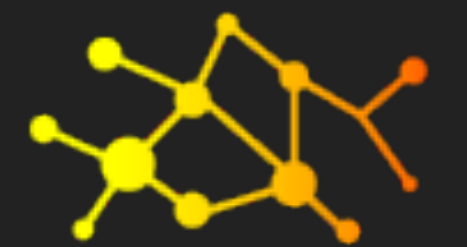
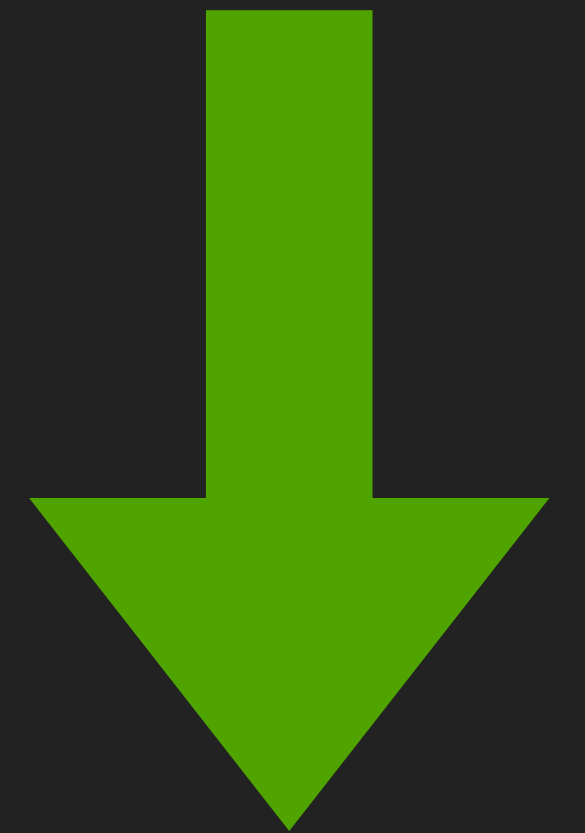
MEET PAUL



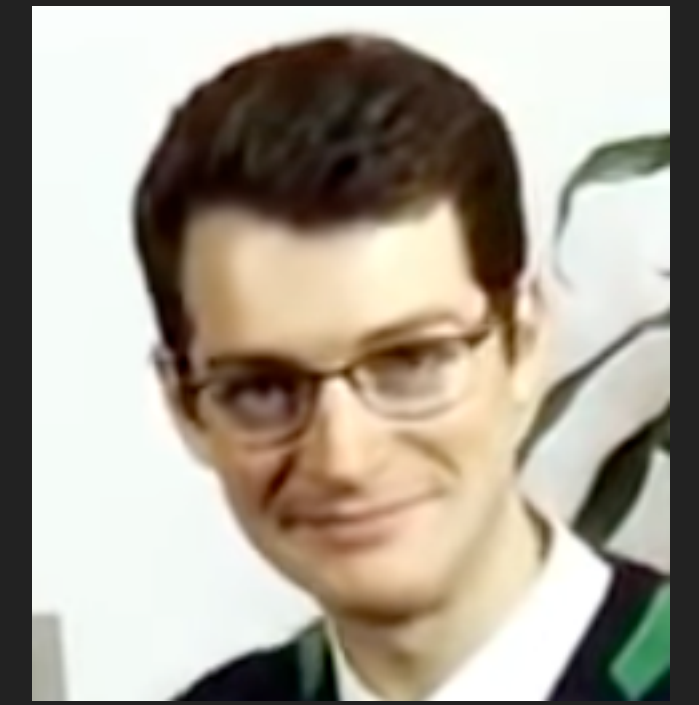
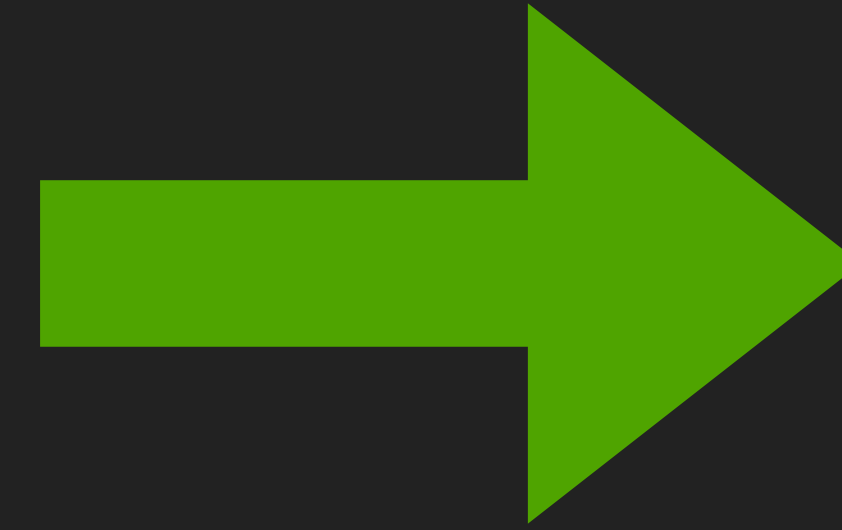
AccipiterMon



MEET PAUL

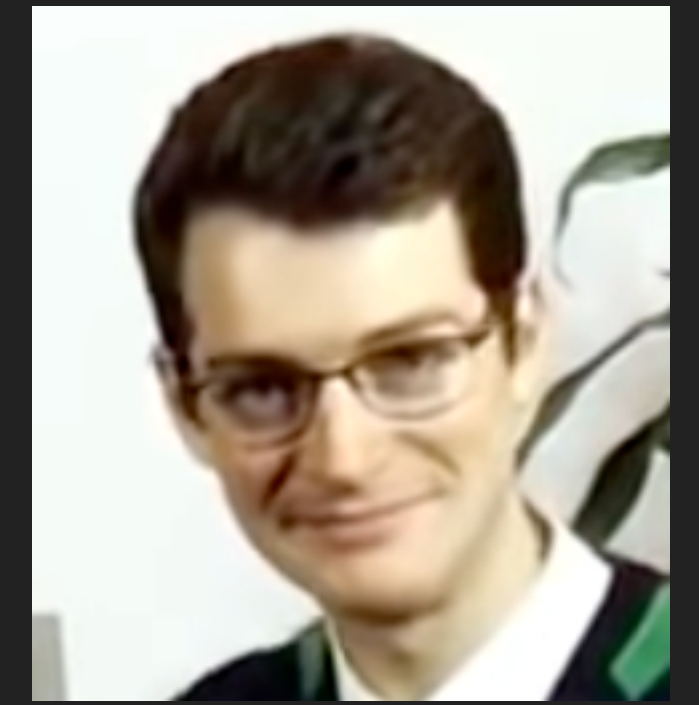
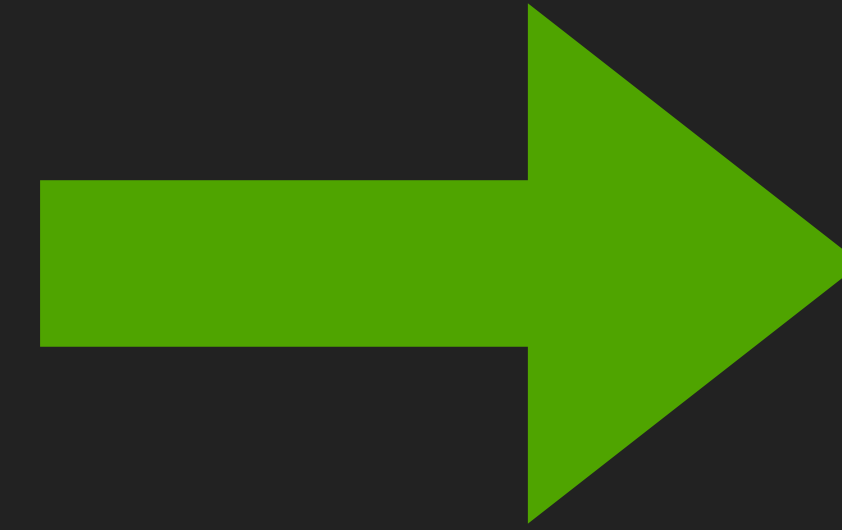


AccipiterMon



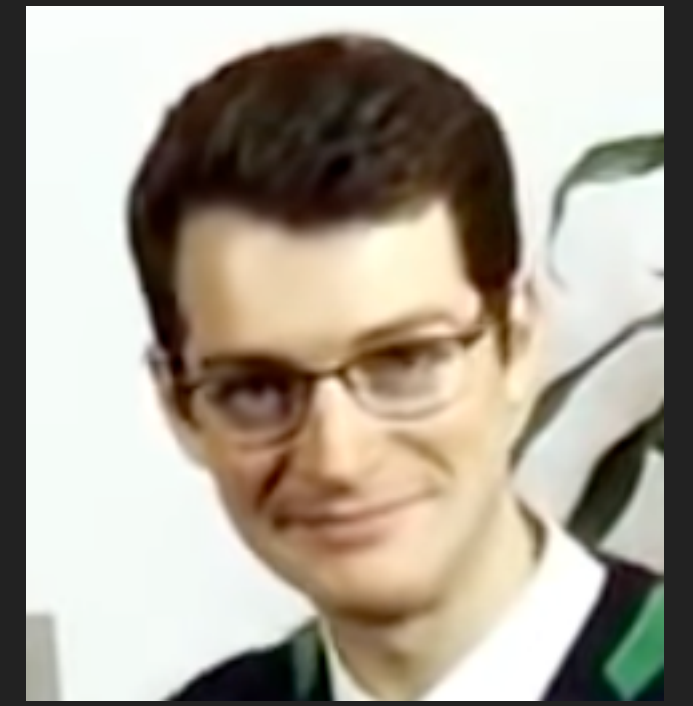
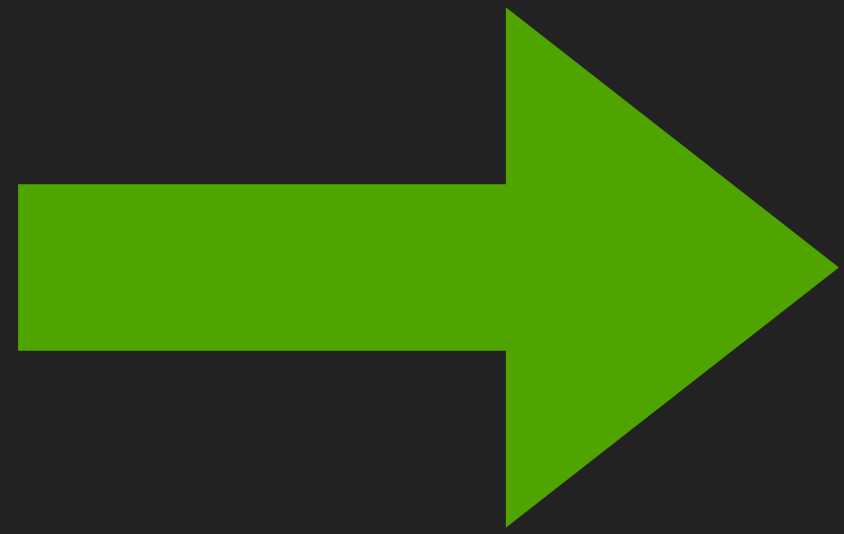
MEET PAUL





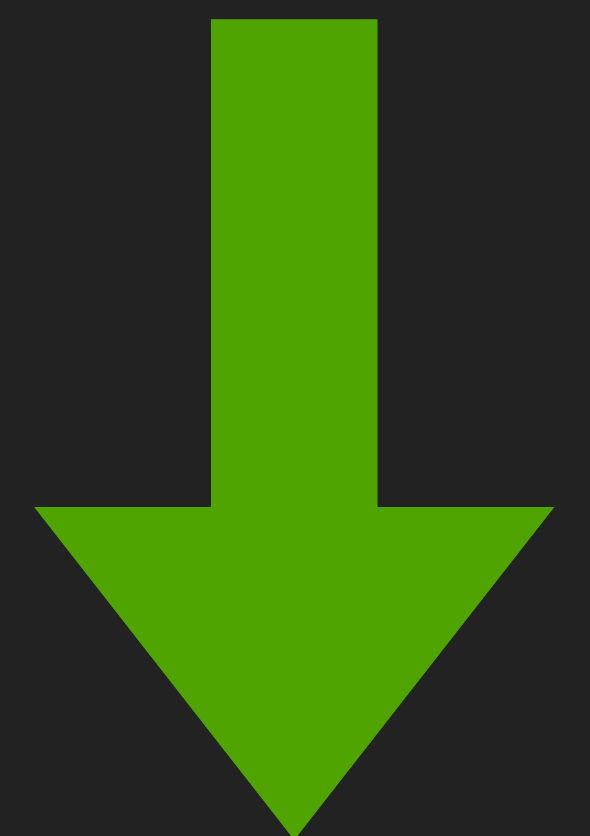
MEET PAUL

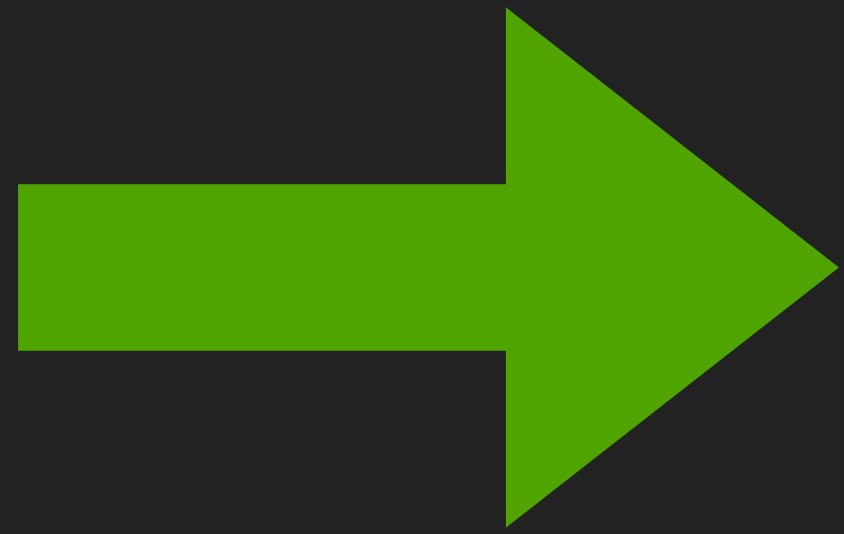




#CRUSHINGIT
(APPLAUSE)

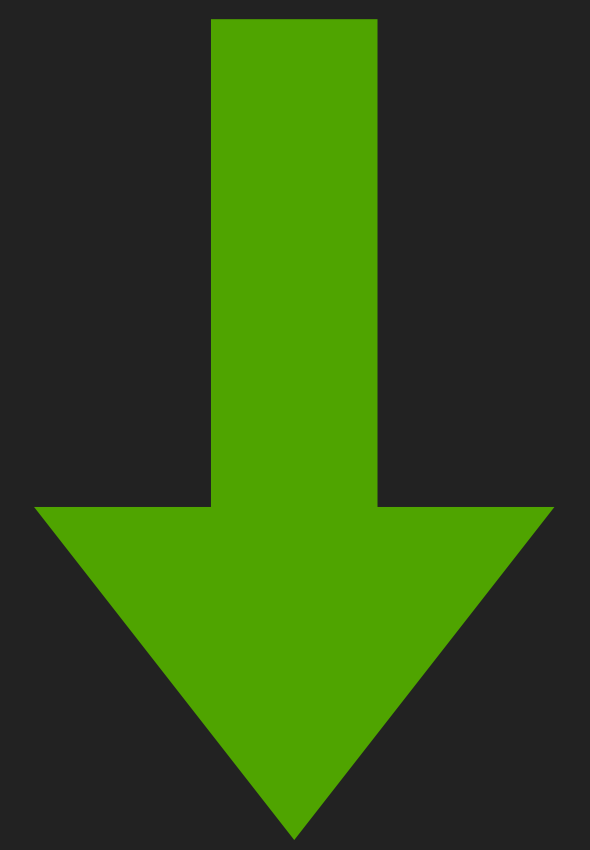
MEET PAUL

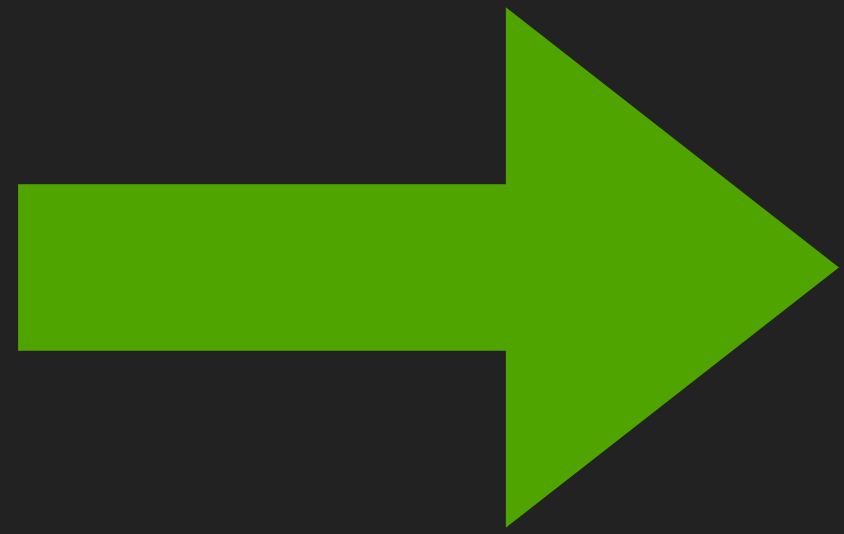




#CRUSHINGIT
(APPLAUSE)

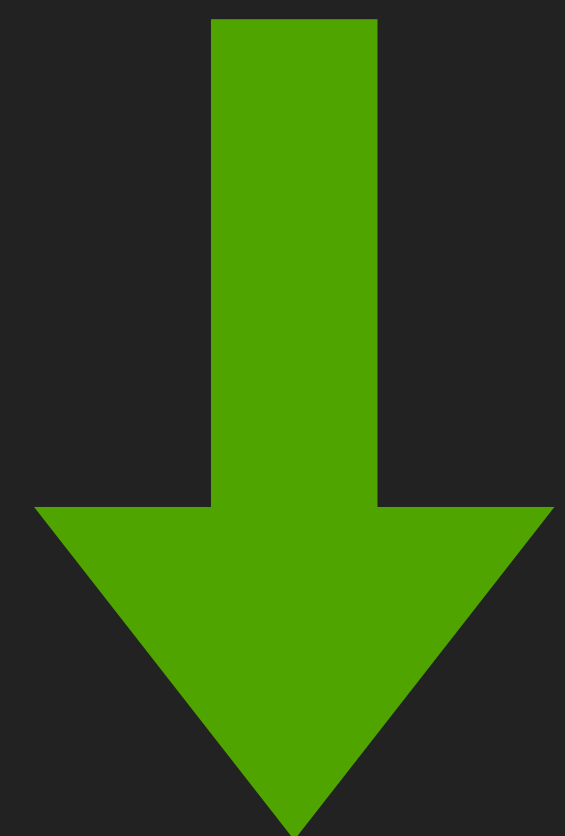
MEET PAUL



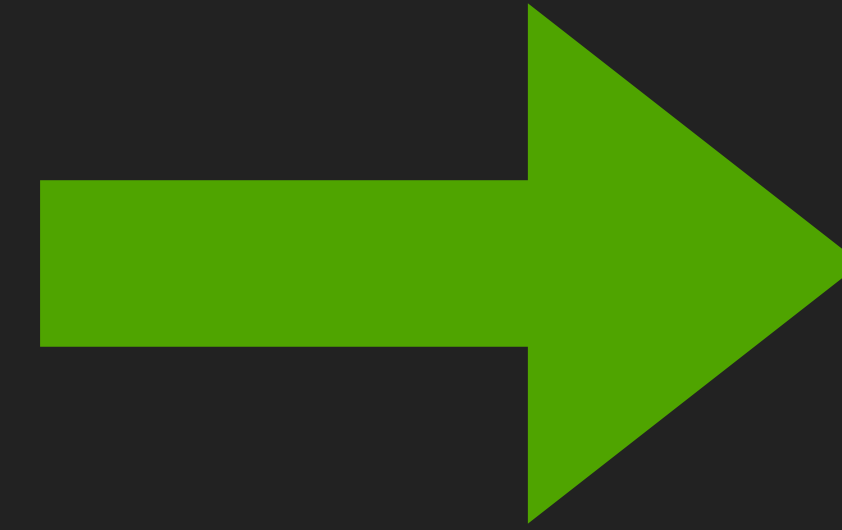


#CRUSHINGIT
(APPLAUSE)

MEET PAUL



JOB OFFER #1: CONFIDENTIAL – LEADERSHIP ROLE AT A PUBLIC SECURITY COMPANY
JOB OFFER #2: TOP MARKETING ROLE FOR A PE-BACKED, INFORMATION SECURITY COMPANY
JOB OFFER #3: LOOKING FOR A HEAD OF MARKETING FOR A VC-BACKED START-UP SECURITY COMPANY



#CRUSHINGIT
(APPLAUSE)

MEET PAUL



WHO JUDGES THE AWARDS?



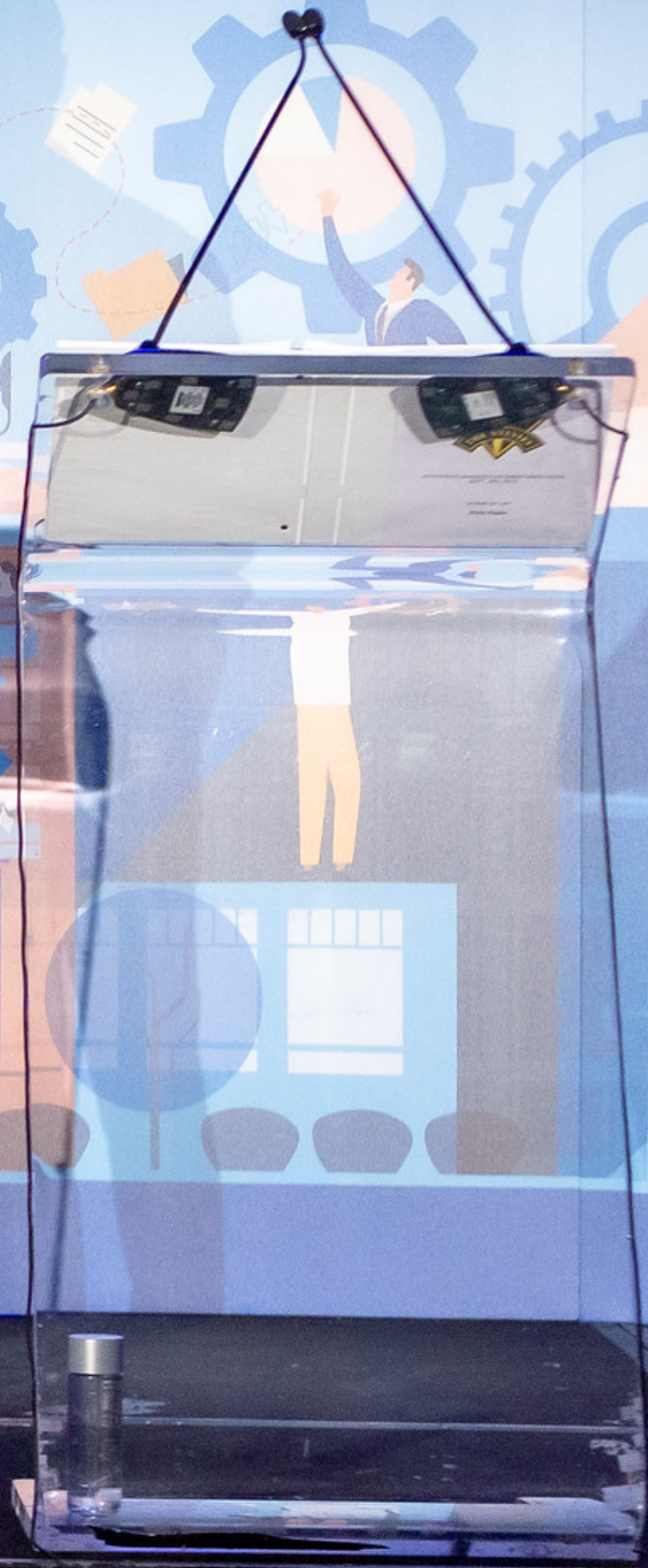
WHO JUDGES THE AWARDS?



WHO JUDGES THE AWARDS?



NEW YORK 2019 THE STEVIE AWARDS FOR GREAT EMPLOYERS





SVUS AWARDS GOLD

SVUS AWARDS GOLD

SVUS AWARDS GOLD

SVUS AWARDS GOLD

SVUS AWARDS GOLD

SVUS AWARDS GOLD

SVUS AWARDS GOLD

SVUS AWARDS GOLD

SVUS AWARDS GOLD

SVUS AWARDS GOLD

SVUS AWARDS GOLD

SVUS AWARDS GOLD

NETI PRODU
www.netiproducts.com

B2X Care Solutions

Century Corporation

Coca-Cola Inc.

NETI PRODU
www.netiproducts.com







Network Products Guide

PUBLISHED FROM SILICON VALLEY UNITED STATES | IT WORLD AWARDS

SATURDAY | JULY 20TH, 2019

- HOME
- IT WORLD AWARDS
- JUDGES
- STORE
- THE STORY

-  Recommendations for improving the security posture of your organization
-  What are the advantages of adopting cloud computing for any type of business
-  Why understanding ERP Security is important for CIOs
-  Advice for CIOs on implementing a strategy that unifies multiple platforms and technologies



14th Annual Network PG's 2019 IT World Awards | June 20 Final Deadline

- Startups
 - Interviews
 - Technology


What CIOs need to know when integrating SDN into their monitoring strategy

Net Optics specializes in designing visibility into networks to address challenges related to virtualization, compliance and security. The company is the leading provider of Total Application and Network Visibility solutions that deliver [...]

A CIOs guide to "must have" methods needed to protect against Advanced Persistent Threats and even cyber-threats from other nations

Plixer International is one of the fastest growing companies, and a leading provider of NetFlow-based network traffic monitoring and threat detection technology, historical reporting and capacity base-lining for both physical and virtual [...]

14th Annual Network PG's 2019 IT World Awards | June 20 Final Deadline

 Second Early Bird Deadline is February 15 We invite you to participate in the IT industry's premier excellence awards program IT World Awards® honoring achievements in every facet of the information technology [...]

Headline News

- SAIC Achieves Microsoft Gold Cloud Platform, Application Development, and Datacenter Competencies
- Garmin® shareholders approve quarterly dividend through March 2020 and Garmin announces record dates and payment dates for June 2019 dividend installment
- Ellucian Senior Vice President and Chief Architect Brian Knotts to Speak at AWS Public Sector Summit
- Washington Virtual Academy to Hold Commencement Ceremony June 9

Follow me on Twitter

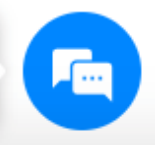
Tweets by @networkpg

NetworkProductsGuide Retweeted

 **Info Security PG**
@infosecuritypg

Join the Cyber Community g...
linkedin.com/
@infosecurity...

We may be busy right n...
For help leave a message



Golden Bridge Awards

BUSINESS AWARDS RECOGNIZING ACHIEVEMENTS AND INNOVATIONS ALL OVER THE WORLD

Search... 

SATURDAY, JULY 20TH, 2019

HOME

ABOUT

START AN ENTRY

JUDGES

WINNERS

CEREMONY

STORE

THE STORY



Nidhi Raina | Creating a purposeful and meaningful direction



Navdeep Reddy: Relentlessly Driven to Create The Best Possible Solution



Georgette Pascale: Fine-Tuning the Virtual Workplace – Managing a Business From Afar



Vladimir Chernavsky: Emerging trends in small business communications



Participate today on one of the juries for Golden Bridge Awards

(LEAVE A COMMENT)



Volunteer as a judge. As a judge it will be an opportunity for you to learn how other individuals, teams, and organizations are performing, confronting challenges and achieving success in the industry. [...]

Linda Taddonio: Meeting the eCommerce Imperative



Insite Software is a leading provider of B2B and B2C eCommerce technology and internationally enabled shipping solutions, serving more than 950 customers worldwide. Headquartered in Minneapolis, Insite Software's solutions enable leading manufacturers [...]

Chris Fedde: Big Data Security Challenges



Hexis Cyber Solutions, a subsidiary of The KEYW Holding Corporation based in Hanover, Maryland, provides complete cybersecurity solutions for commercial companies, government agencies, and the Intelligence Community (IC). Cyber terrorists, organized crime, [...]

11th Annual 2019 Golden Bridge Business and Innovation Awards | Final Deadline August 9

(LEAVE A COMMENT)



Translate

Select Language

Powered by  Google Translate

HOW TO SUBMIT



REQUEST AN ONLINE ENTRY KIT NOW

WE WILL EMAIL IT TO YOU INSTANTLY

ORDER ORIGINAL TROPHIES, MEDALLIONS, & PLAQUES



We may be busy right n...
For help leave a message



GOOGLE ANALYTICS ACCOUNT NUMBER

UA-60725595



REVEALS A SHARED CONNECTION

WWW.PILLARWORLDWARDS.COM

WWW.PRWORLDWARDS.COM

WWW.GOLDENBRIDGEAWARDS.COM

WWW.INFOSECURITYPRODUCTSGUIDE.COM

WWW.ONEPLANETAWARDS.COM

WWW.CSSWORLDWARDS.COM

WWW.WOMENWORLDWARDS.COM

WWW.GLOBEEAWARDS.COM

WWW.NETWORKPRODUCTSGUIDE.COM

WWW.SVUSAWARDS.COM

WWW.CEOWORLDWARDS.COM

WWW.CONSUMERWORLDWARDS.COM

WWW.BUSINESSAMERICAWARDS.COM

WWW.SVCAWARDSUSA.COM



awardcontact.org - awardcont: x +

Not Secure | www.awardcontact.org

This Domain Name Has Expired - Renewal Instructions.

awardcontact.org

روابط ذات صلة

- Car Insurance
- Life Insurance
- AARP
- Cheap Flights
- Credit Cards

نوع الخصوصية

البحث في الإعلانات



CYBER SECURITY 2017
CDM LEADER ★★★★★

INFOSEC AWARDS WINNER
CYBER DEFENSE MAGAZINE
2019

ASTORS AMERICAN SECURITY TODAY
2016
PLATINUM AWARD WINNER
HOMELAND SECURITY AWARDS

2019
Inc. BEST WORK-PLACES

CYBERSECURITY BREAKTHROUGH AWARDS

Info Security Products Guide
2016
GLOBAL EXCELLENCE AWARDS
★★★★★

★★★★★
NETWORK PRODUCTS GUIDE
IT World Awards
2016
BRONZE

★★★★★
ONE PLANET AWARDS
2016
SILVER

Info Security Products Guide
2017
GLOBAL EXCELLENCE
GOLD
★★★★★

NETWORK PRODUCTS GUIDE
★★★★★
IT World Awards
2017
SILVER

CYBER DEFENSE GLOBAL AWARDS
CYBER DEFENSE MAGAZINE
2018
WINNER

CDM | **INFOSEC AWARD WINNERS**
★ 2017 ★

REBOOT
SC Media Reboot Leadership **18** Awards

CIO Review 20 MOST PROMISING
JUNIPER NETWORKS
SOLUTION PROVIDERS - 2016

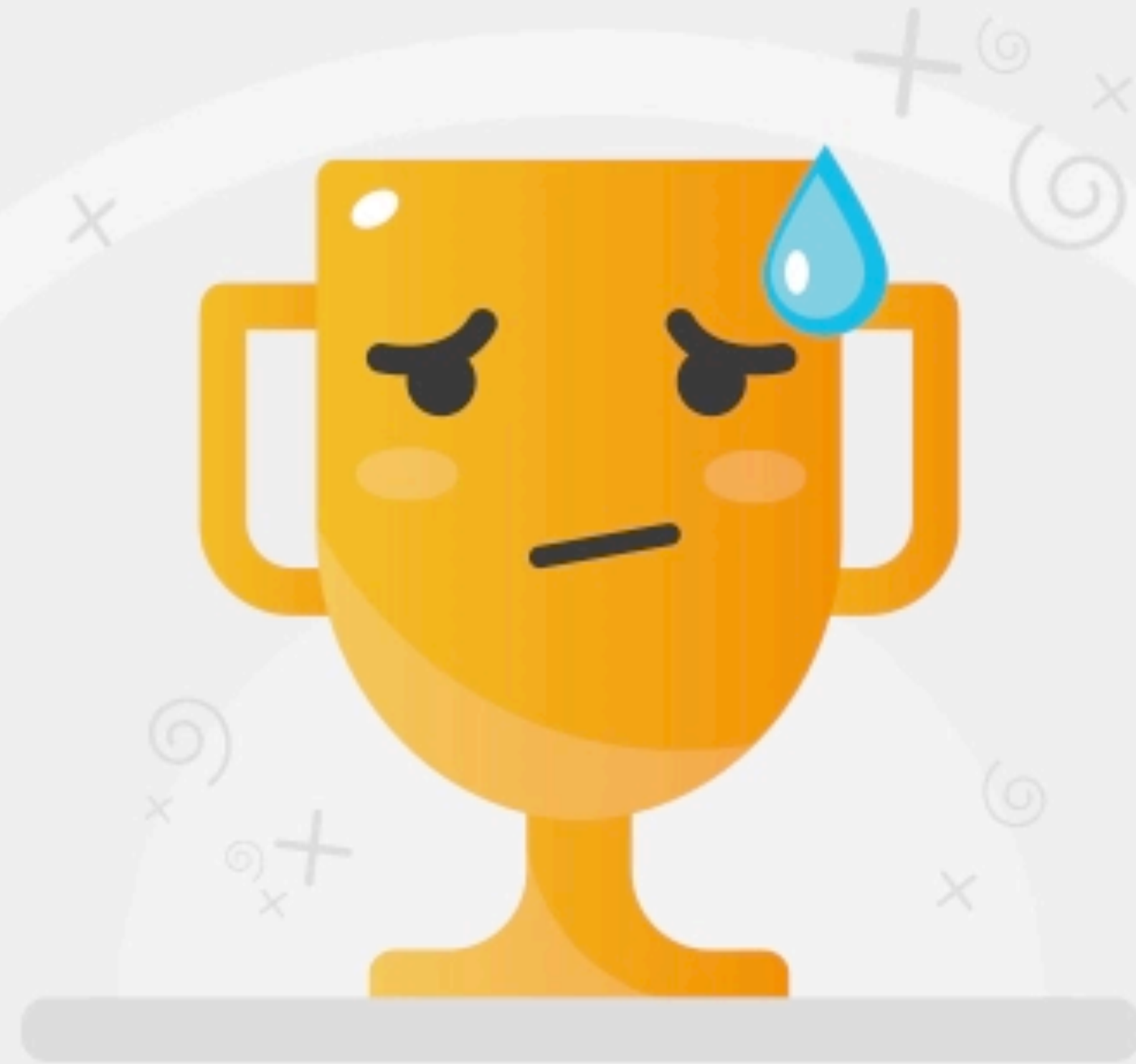


OOOPS!

This may not be the best way
to gain credibility

82% OF PURCHASING
DECISIONS ARE NOT
INFLUENCED BY
BUSINESS-RELATED
AWARDS

n=108



OOOPS!

This may not be the best way
to gain credibility

38% OF SECURITY
BUYERS AVOID
COMPANIES
PERCIEVED AS USING
MISLEADING
MARKETING

n=108

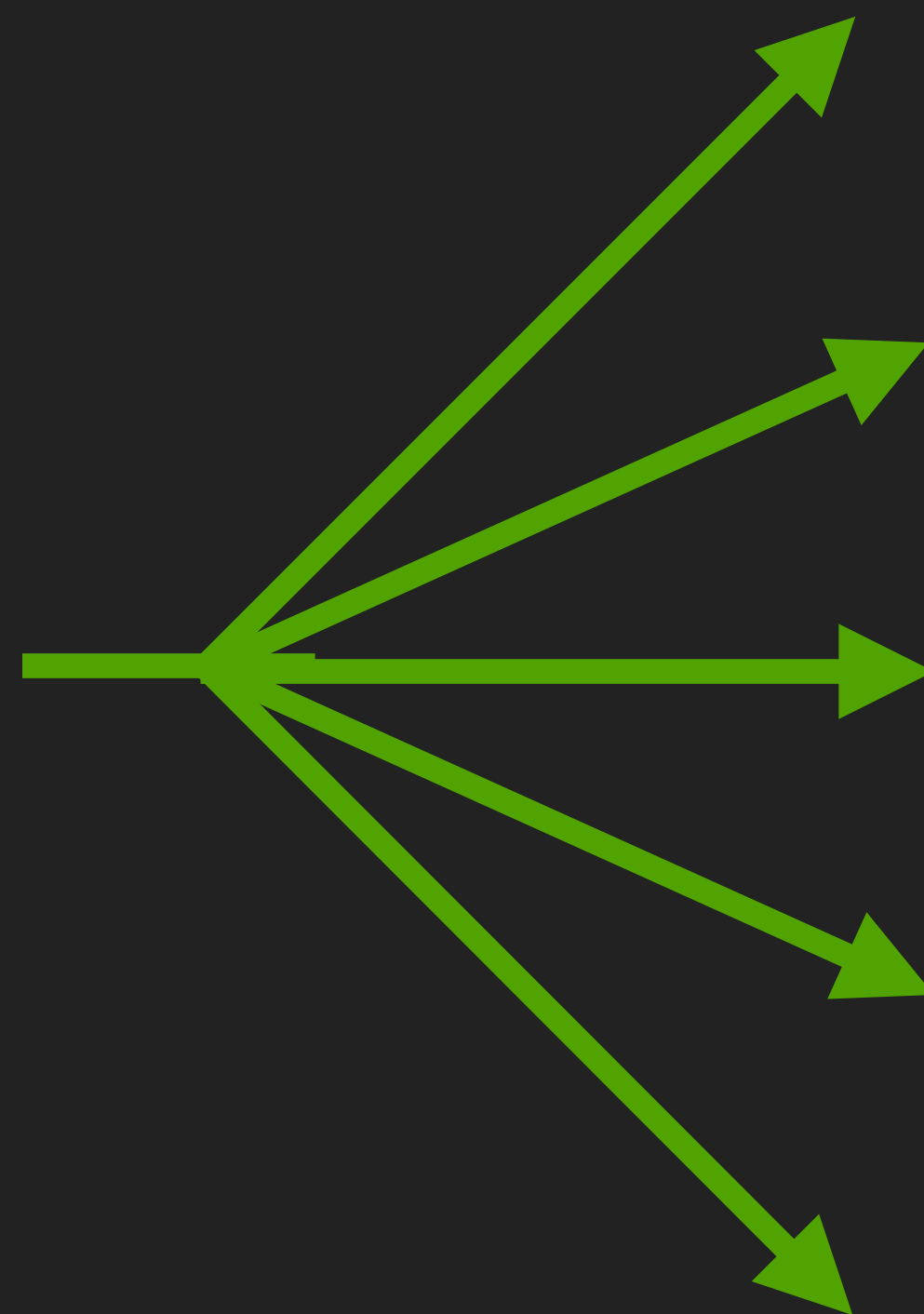




Figure 1. Magic Quadrant for Endpoint Protection Platforms



Source: Gartner (August 2019)



(1)

**ABSOLUTELY
NOT
PAY-FOR-PLAY**

(2)

**ANYONE CAN
SCHEDULE &
BRIEF ANALYST**

(3)

**KEEP IN THEIR
EAR & KEEP
THEM UPDATED**



(3)

**KEEP IN THEIR
EAR & KEEP
THEM UPDATED**

HOW?





I FEEL LIKE I'M TAKING CRAZY PILLS



I FEEL LIKE I'M TAKING CRAZY PILLS

CRAZY DOUBLE GAME



**1) WE WILL GIVE YOU THE ADVICE
TO MAKE YOUR PRODUCT ROCK!**

**2) WE WILL BE NEUTRAL & WILL
RATE YOU AND YOUR PEERS!**

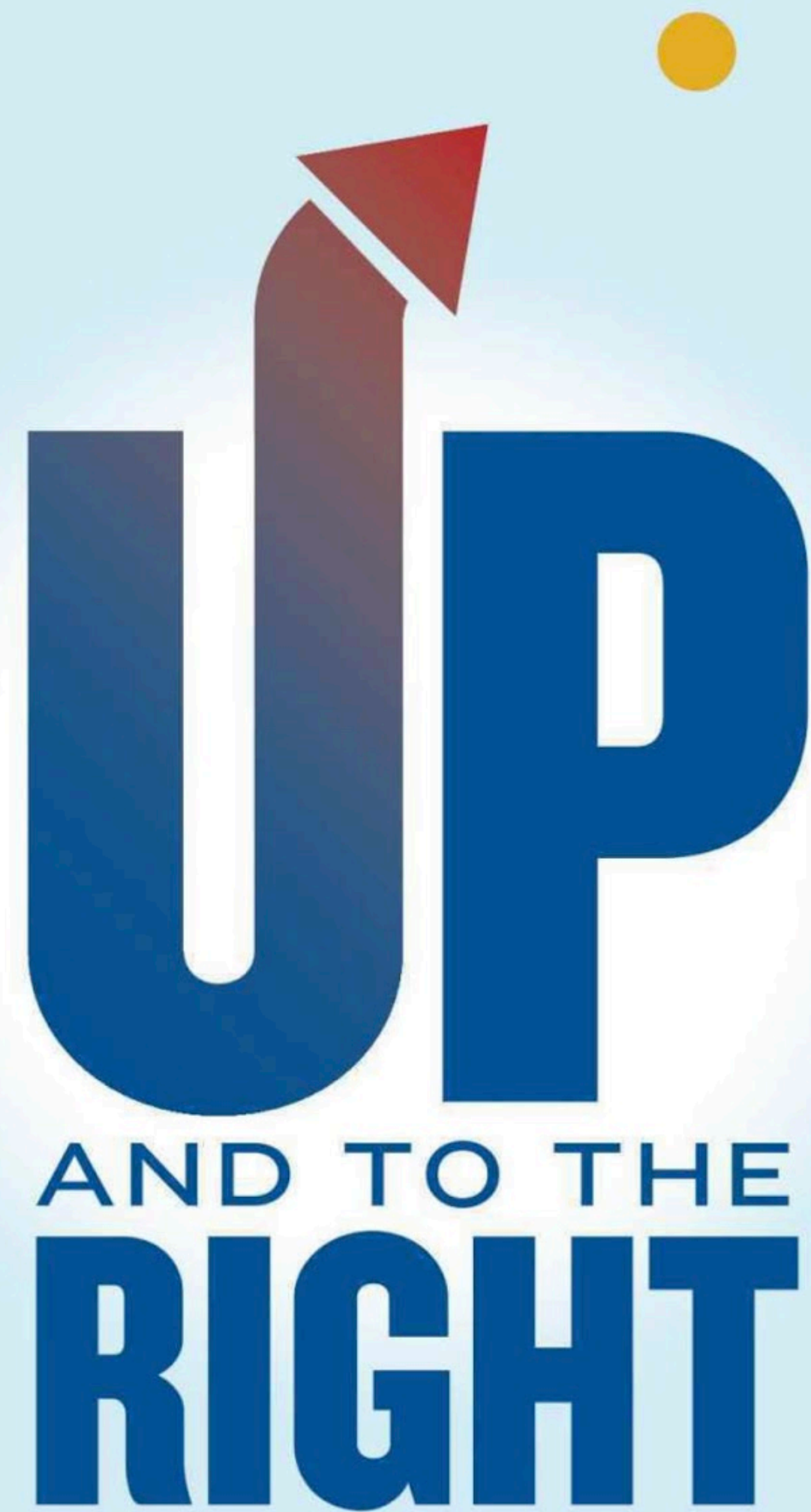




AND TO THE
RIGHT

STRATEGY AND TACTICS
OF ANALYST INFLUENCE

RICHARD STIENNON




UP AND TO THE RIGHT

STRATEGY AND TACTICS
OF ANALYST INFLUENCE

RICHARD STIENNON

HAVE YOUR AD AGENCY ATTEMPT TO GET DISPLAY ADS IN YOUR ANALYST'S HOME AIRPORT. ANALYSTS TRAVEL--A LOT. THEY ARE GOING TO BE PASSING THROUGH THEIR HOME AIRPORT AT LEAST TWICE A WEEK. WHAT IF THEY SAW YOUR DISPLAY AD THAT OFTEN? WHAT IF IT WAS THE VERY AD THEY HAD CHOSEN? THIS MAY BE OVER THE TOP, BUT WHAT IF THE AD WAS A PICTURE OF THE ANALYST WITH A COGENT SIDE-BAR QUOTE? YOU WOULD HAVE TO WORK WITH GARTNER TO ACCOMPLISH THAT.




UP AND TO THE RIGHT

STRATEGY AND TACTICS
OF ANALYST INFLUENCE

RICHARD STIENNON

NOW LEAD HIM TO **YOUR BEST CONFERENCE ROOM**. DON'T MAKE EXCUSES FOR HOLDING THE MEETING IN A CORNER OF THE CAFETERIA BECAUSE THE CEO IS MEETING WITH THE BOARD OR AN IMPORTANT SALES MEETING IS GOING ON (YES, THESE ARE ALL EXAMPLES FROM SAS DAYS I HAVE BEEN ON.) HAVE COFFEE, TEA OR REDBULL READY IN THE MEETING ROOM. (**YOU DO KNOW WHAT THE ANALYST'S FAVORITE MORNING BEVERAGE IS DON'T YOU?**) HAVE A SUPPLY OF CALORIC FUEL HANDY TOO. KEEP IN MIND THAT ANALYSTS EITHER EAT UNWISELY OR THEY ARE VERY HEALTH CONSCIOUS DEPENDING ON HOW LONG THEY BEEN AN ANALYST. THE SENIOR ANALYSTS ARE TRYING TO LOSE WEIGHT AND STAY FIT, SO OFFERING THEM BAKED GOODS IS A PROBLEM. BESIDES, YOU DON'T WANT THEM FALLING ASLEEP FROM A CARB COMA. AT LEAST HAVE YOGURT AND FRUIT ON HAND IN ADDITION TO THE USUAL BAGELS AND CREAM CHEESE.



UP AND TO THE RIGHT

STRATEGY AND TACTICS
OF ANALYST INFLUENCE

RICHARD STIENNON

GET THE ANALYST PROMOTED. PROMOTE THE ANALYST TO GARTNER MANAGEMENT. START WITH YOUR GARTNER SALES REP. SUMMITS AND THE IT SYMPOSIUM ARE OPPORTUNE MOMENTS TO CHAT WITH GARTNER EXECUTIVE MANAGEMENT. UPPER MANAGEMENT MAY NOT EVEN KNOW THE NAME OF YOUR ANALYST. MAKE SURE THEY DO. **OF COURSE YOU DO NOT HAVE TO LAY IT ON THICK.** YOU CAN EVEN BE NEGATIVE. ANALYSTS ARE JUDGED BY HOW MUCH IMPACT THEY HAVE. PISSING OFF THE VENDORS COULD BE A GOOD THING FOR THE ANALYST. NEGATIVE COMMENTS FROM END-USER CLIENTS ARE OF COURSE BAD, SO **GET YOUR FRIENDS WHO ARE CIOS AT MAJOR COMPANIES TO DROP THE ANALYST'S NAME OFTEN.**



WTAF???



WTAF???

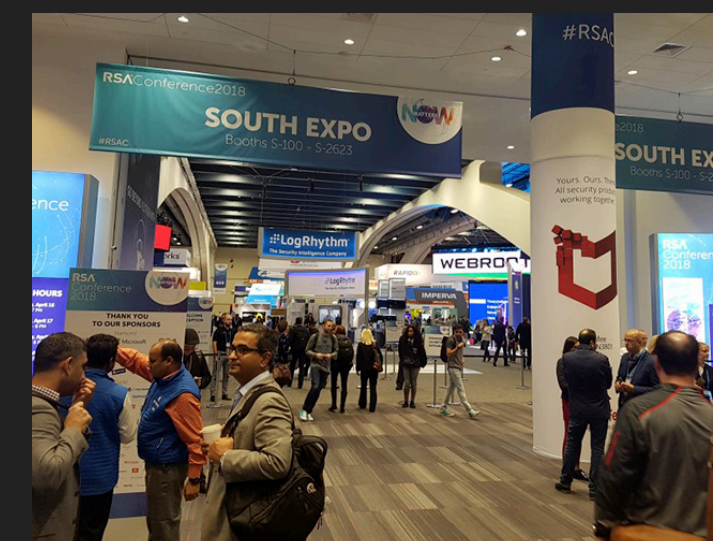
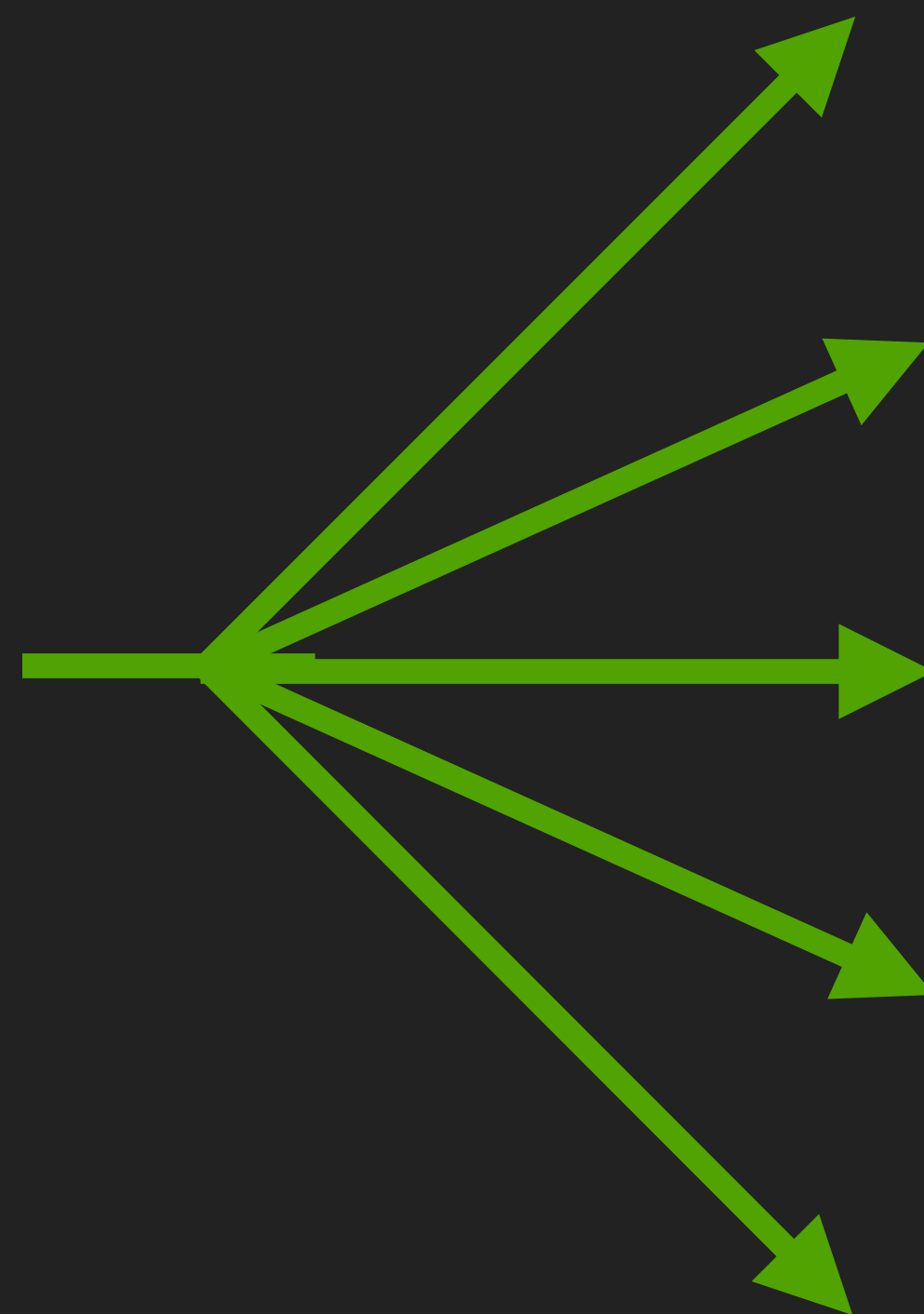
**Make
something
people
want.**



**Make
something**
AN ANALYST THINKS
**people
want.**





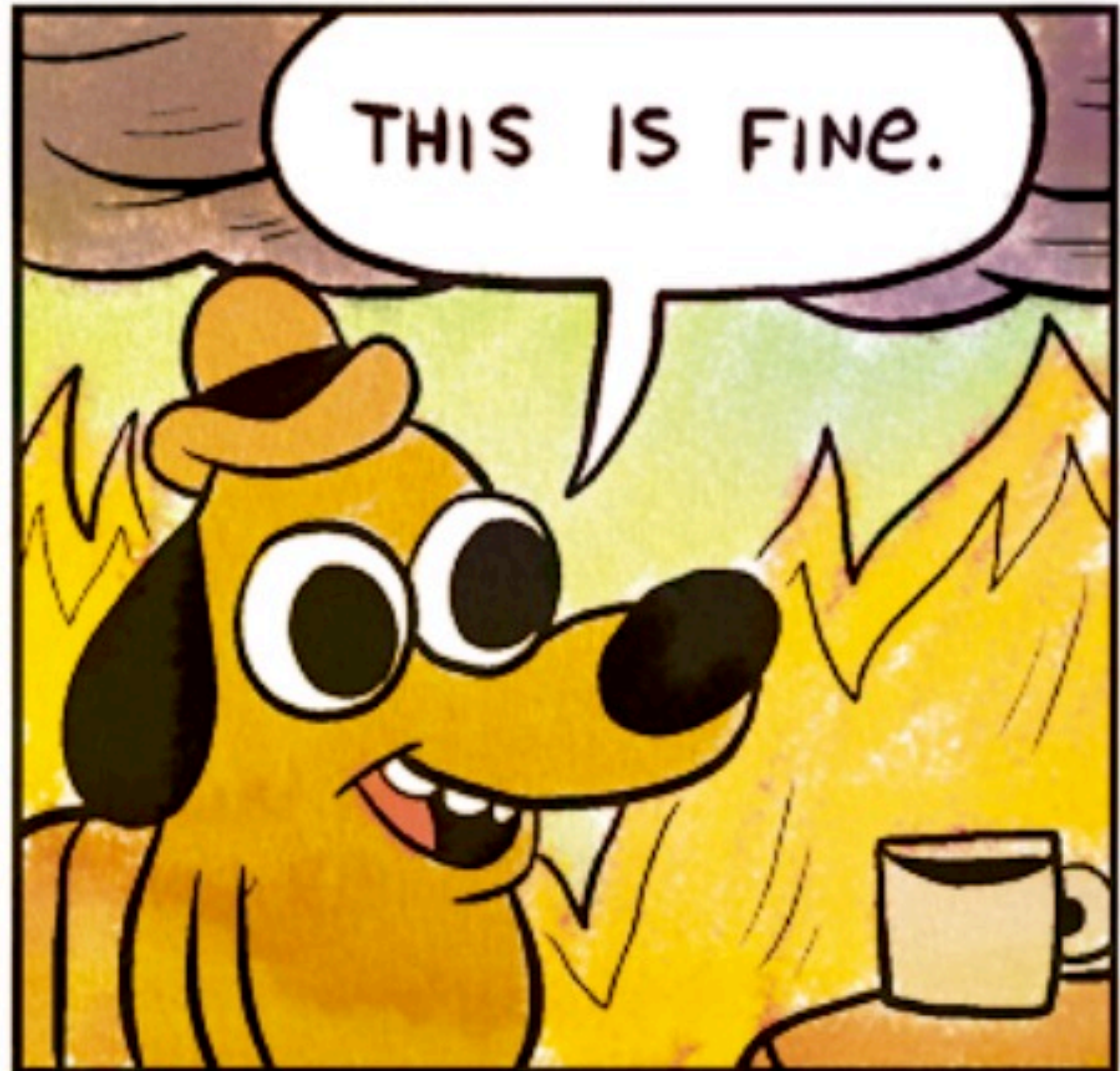


BUT WHY THO'?



- ITS WORKED TILL NOW (KINDA)
- NO PUSHBACK
- IT WAS THE WAY





- ITS WORKED TILL NOW (KINDA)
- NO PUSHBACK
- IT WAS THE WAY



BUT,, HOPE

facebook

2FAC: Facebook's internal multi-factor auth platform

Facebook Security



<https://www.youtube.com/watch?v=pY4FBGI7bHM>



slack

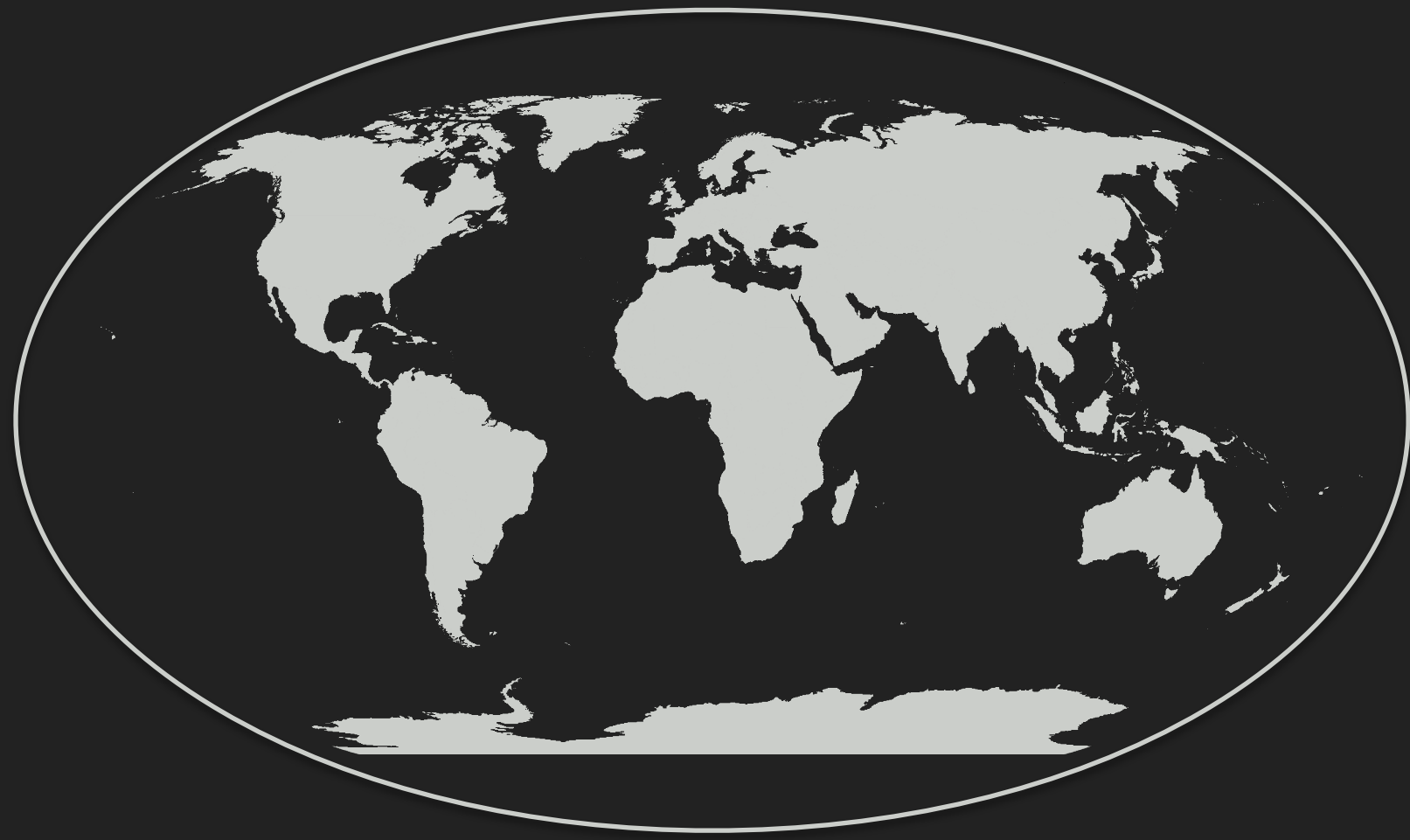


ATLASSIAN

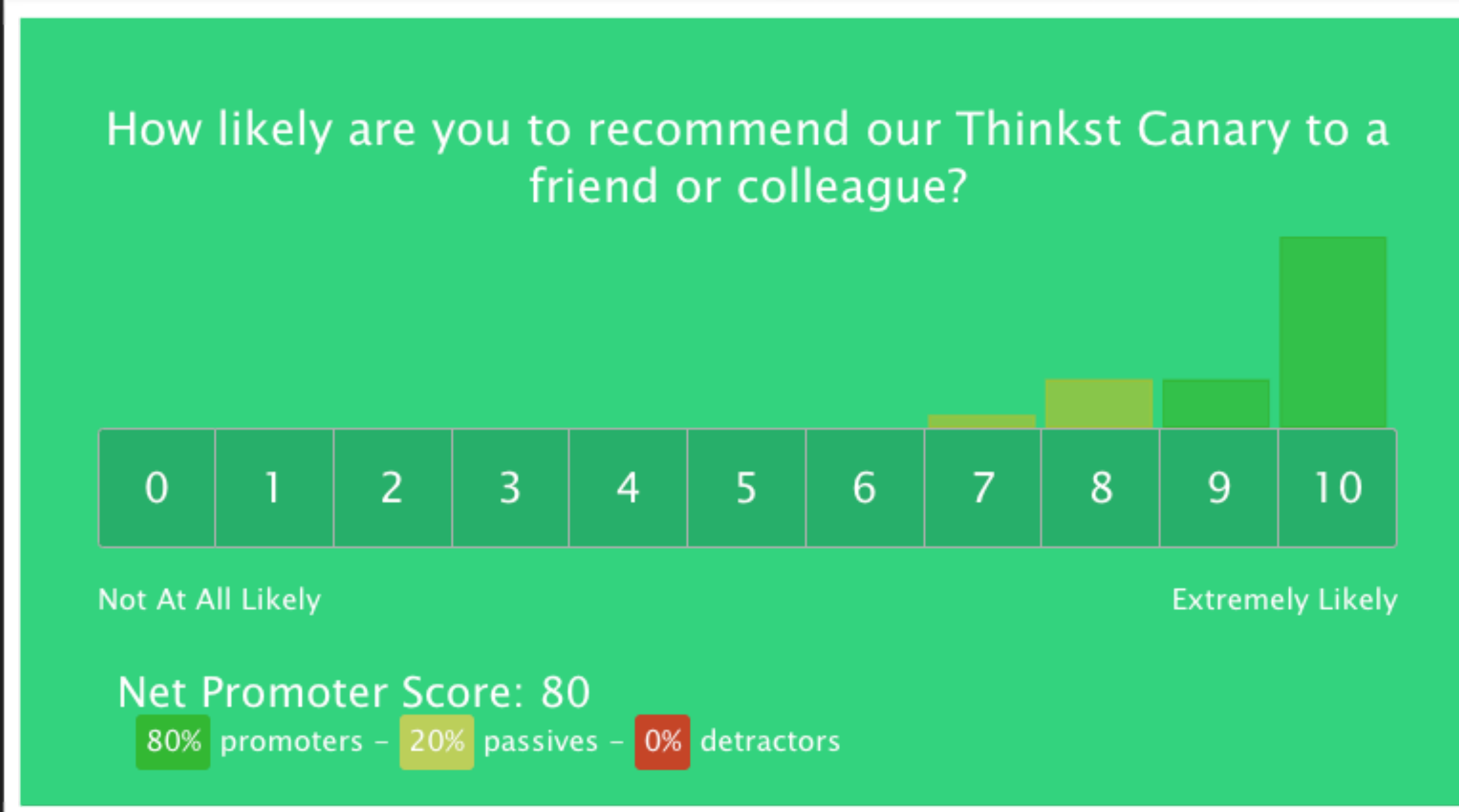
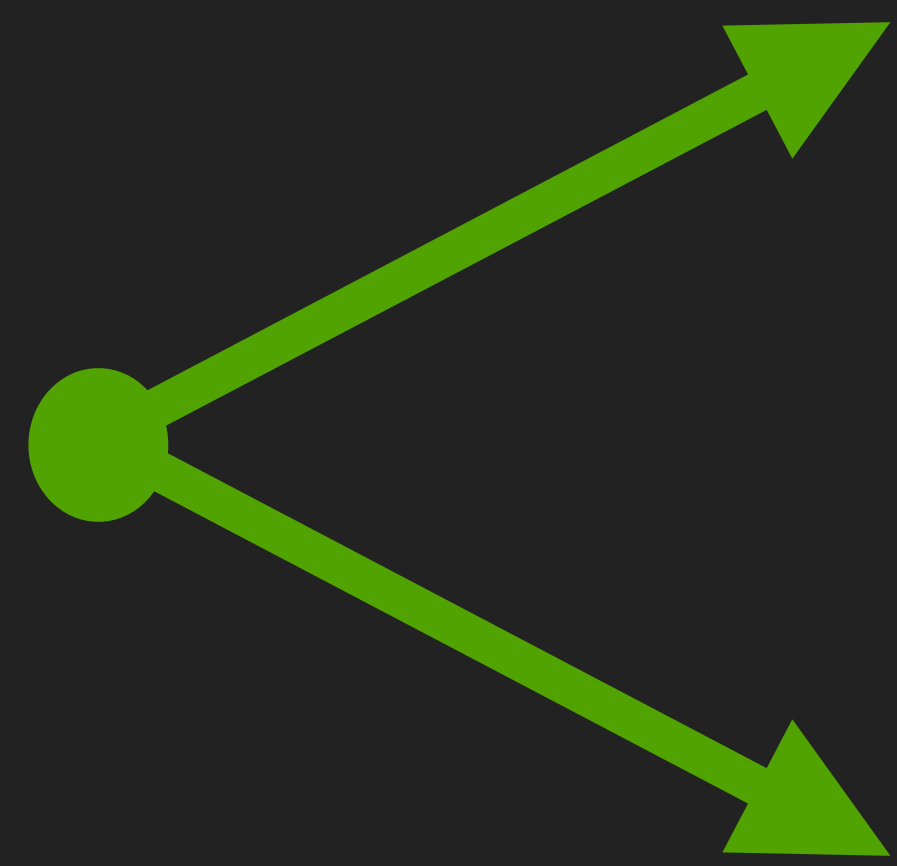


GitHub









ryan huber
@ryanhuber

Complete list of enterprise security products I recommend (evergreen edition):

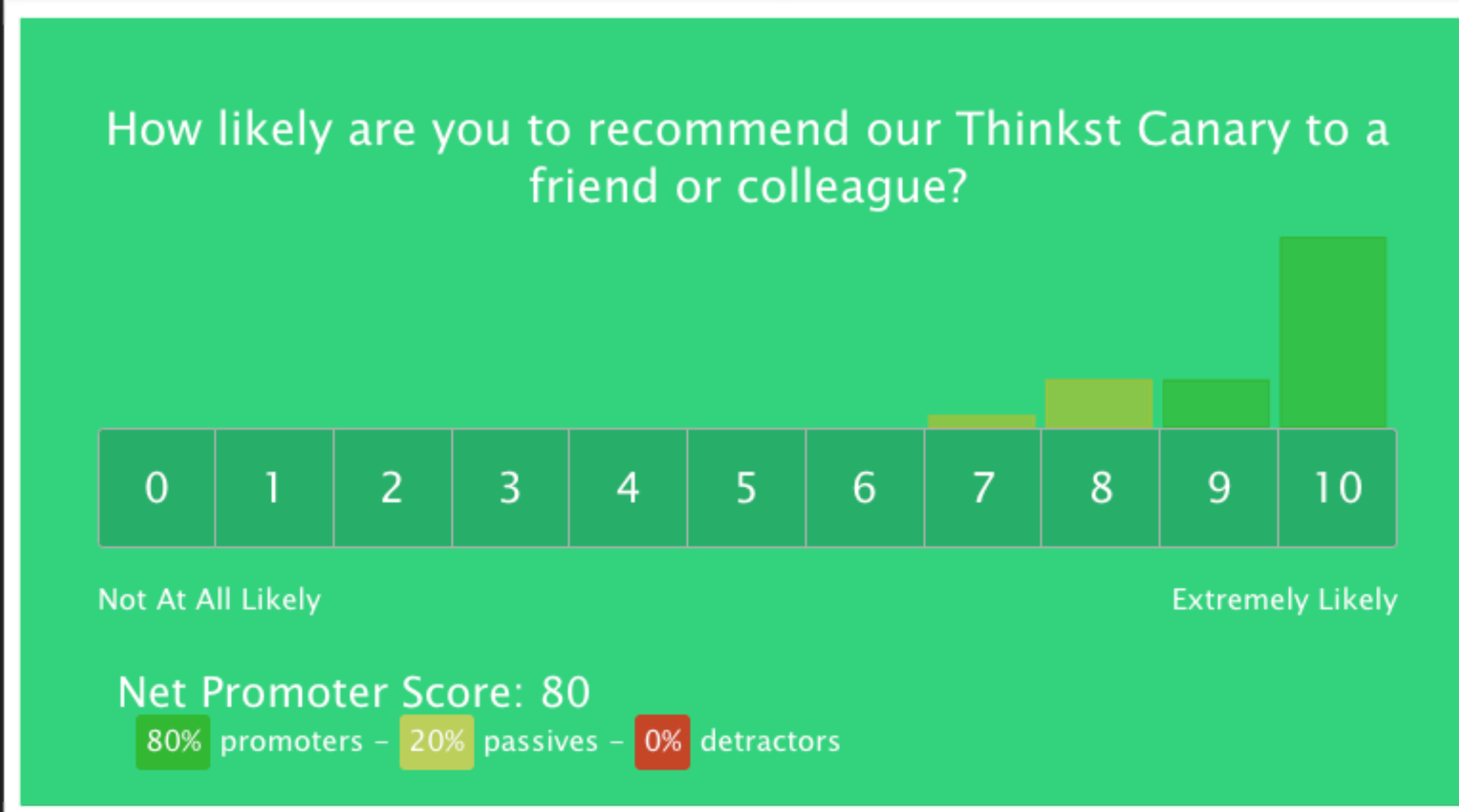
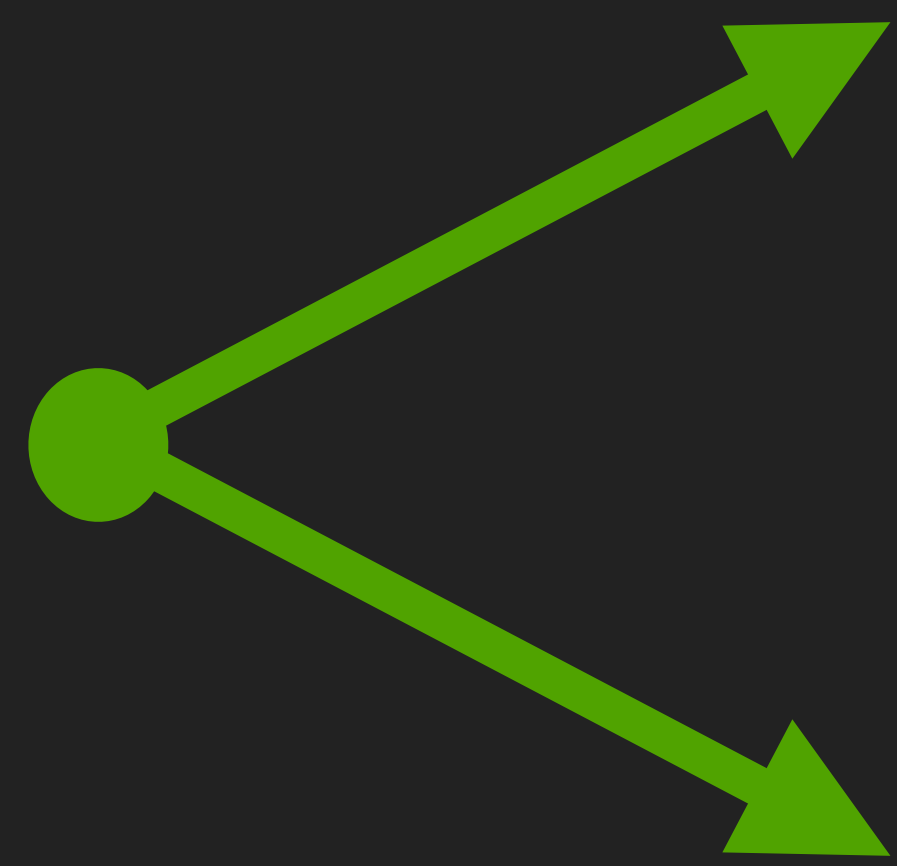
- 1) @ThinkstCanary
- 2) @duosec
- 3) @Yubico

8:11 PM - Jul 10, 2017

82 likes 24 people are talking about this

<https://canary.tools/love>





ryan huber
@ryanhuber

Complete list of enterprise security products I recommend (evergreen edition):

- 1) @ThinkstCanary
- 2) @duosec
- 3) @Yubico

8:11 PM - Jul 10, 2017

82 likes 24 people are talking about this

<https://canary.tools/love>

THE OLD WAY SAID:

- **YOUR PRODUCT DIDN'T MATTER;**
- **YOU COULD HAVE "0" USERS BUT WALL TO WALL ANALYST COVERAGE;**
- **YOU COULD FOOL PEOPLE WITH FAKE AWARDS;**
- **YOUR USABILITY COULD BE TERRIBLE AS LONG AS YOUR AIRPORT ADS WERE SLICK;**
- **YOUR SECURITY PRODUCT COULD BE INSECURE, AS LONG AS YOU HAD THE BIGGEST BOOTH AT RSAC;**



**MAYBE ITS TIME TO
LET THE OLD WAYS
DIE...**

A Star is Born

BUYERS:

- DEMAND MORE
- PUSH BACK MORE

STARTUPS:

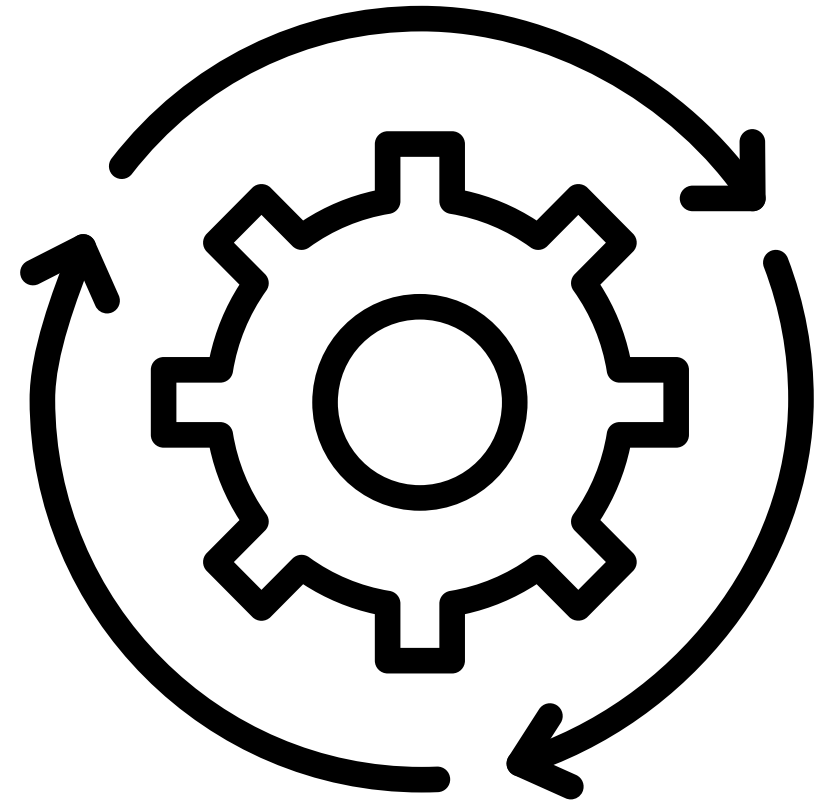
- THE OLD WAY FAILED
- WE CAN BE THE CHANGE



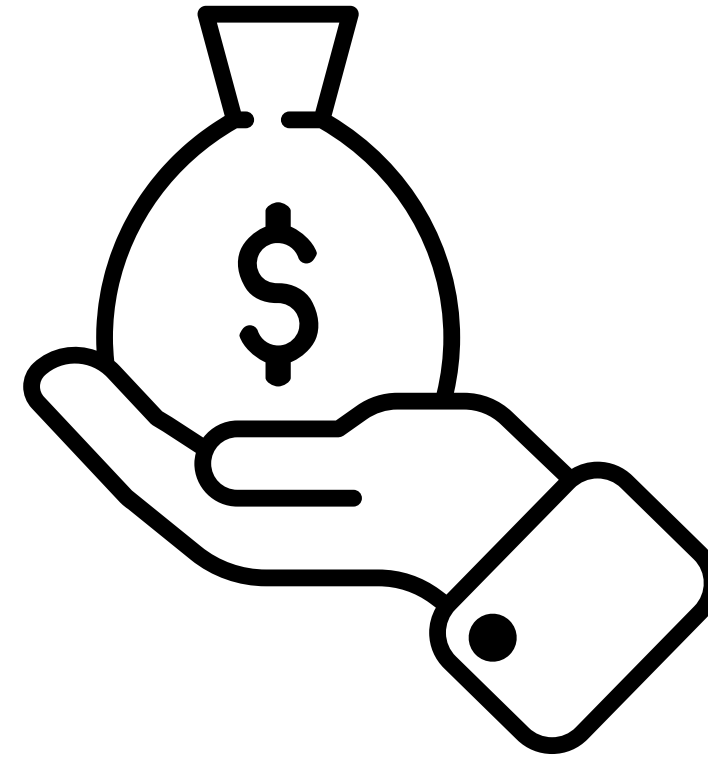
QUESTIONS?

[@sawaba](#)

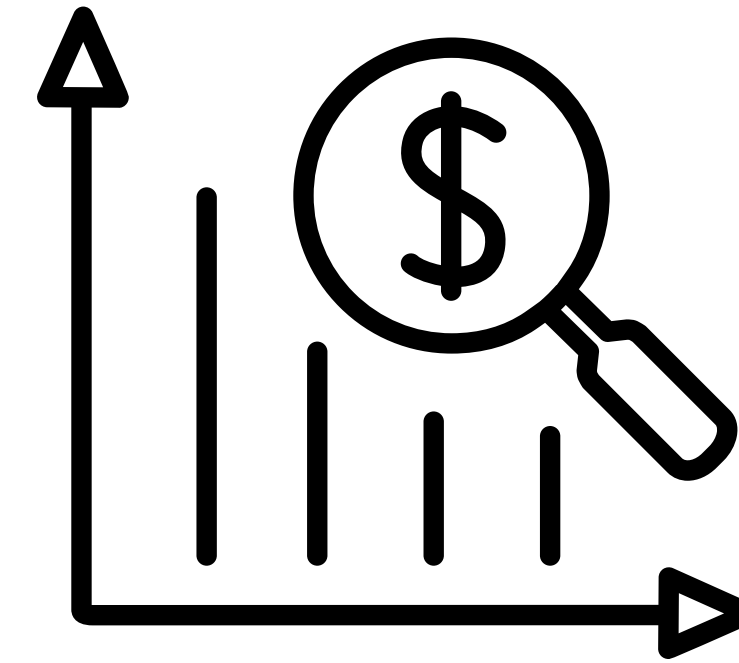
[@haroonmeer](#)



Created by SBTS
from the Noun Project



Created by Maxim Kulikov
from the Noun Project



Created by H Alberto Gongora
from the Noun Project

NOUN PROJECT

BATTLE CARDS