secure delaware 2021

splunk> turn data into doing™

never losing the remote again

Mick Baccio

Global Security Advisor, SURGe
mbaccio@splunk.com
@nohackme

splunk> turn data into doing™

Agenda

- FLS & bio
- scene set/ransomware
- workload
- raising security posture
- we have the tools

Forward-Looking Statements

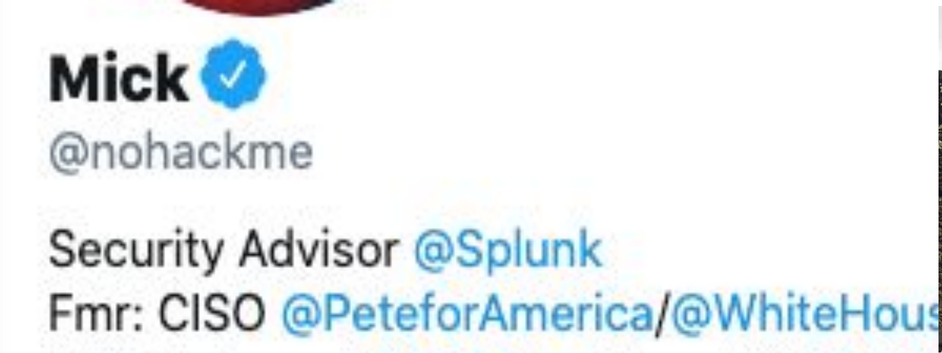
This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

A discussion of factors that may affect future results is contained in our most recent annual report on Form 10-K and subsequent quarterly reports on Form 10-Q, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov, including descriptions of the risk factors that may impact us and the forward-looking statements made in this presentation. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

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. We undertake no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

> Mick Baccio | Global Security Advisor, SURGe

- ❑ 20+ years of cybersecurity work, mostly in mil/gov and healthcare space
- ❑ Built cybersecurity incident response and threat intelligence programs at HHS
- ❑ White House Threat Intelligence Branch Chief POTUS 44/45
- ❑ First CISO of a US Presidential campaign
- ❑ Named Business Insider Top 50 cyber leaders 2020
- ❑ Featured in Splunk Security Predictions 2021
- ❑ DEFCon Goon, lockpicking instructor, sneakerhead
- ❑ Co-Host, Coffee talk with SURGe

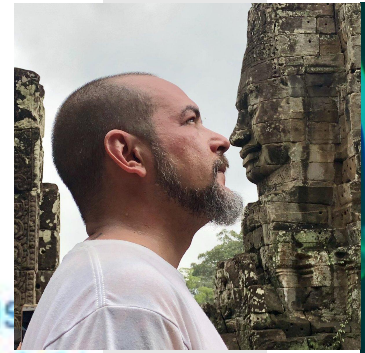


Mick

@nohackme

Security Advisor @Splunk

Fmr: CISO @PeteforAmerica/@WhiteHous

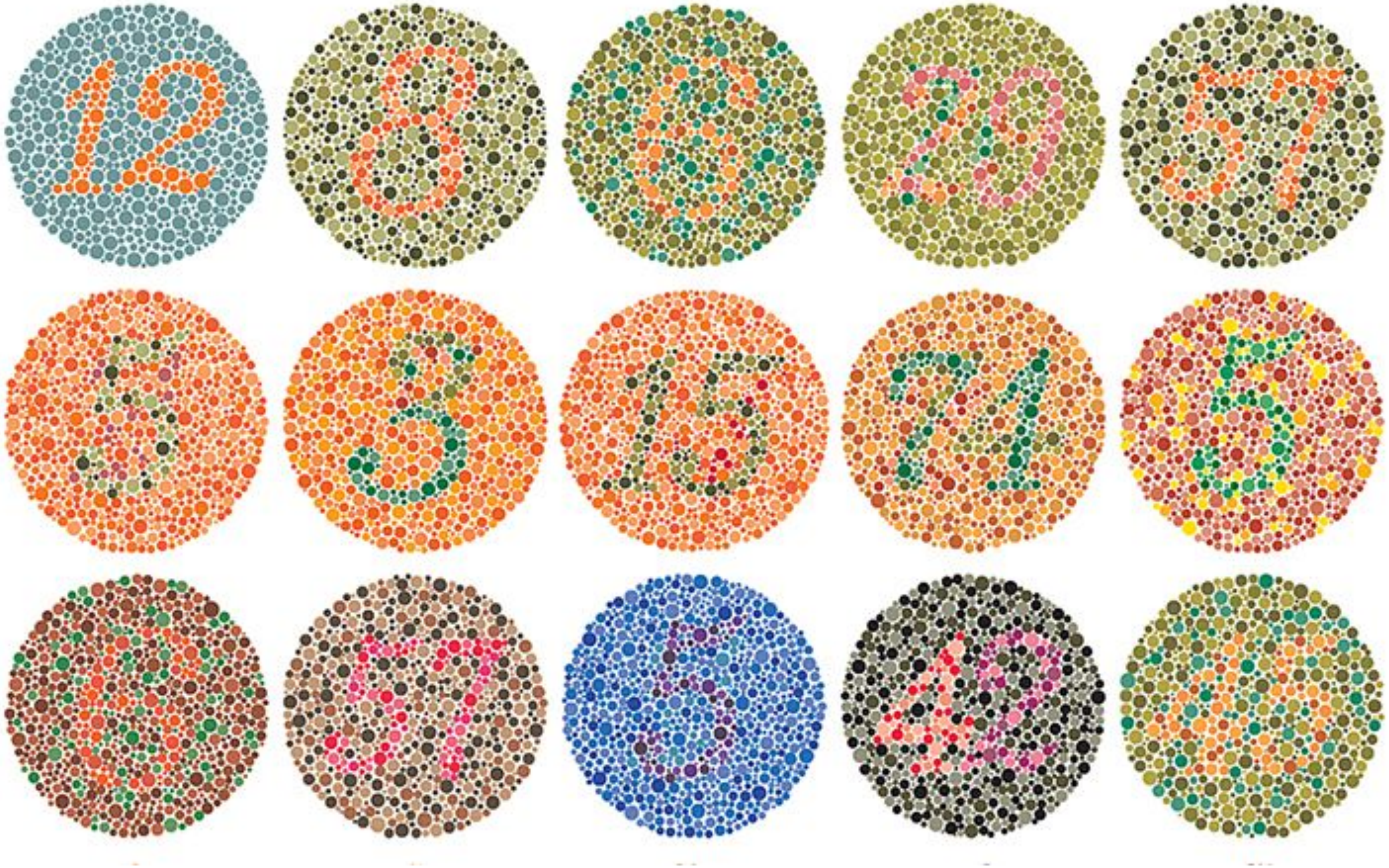


“I teach lockpicking

“I am a GOON at DEFCon

“I scuba dive

“dislikes onions, a lot



Power
TV Input
CH
VOL
Mute
Exit
Guide
xfinity
A
B
C
D
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0 Space

EDIFIER
OPT
COX
PC
AUX
RC600A

it all of us

I DON'T CARE HOW LONG IT TAKES.
I'LL SPEND TIME LOOKING FOR THE REMOTE KNOWING FULL WELL THAT THERE ARE ALSO BUTTONS ON THE TV.

LOST REMOTE
CAN'T TELL NETFLIX I'M STILL HERE
imgflip.com
SETS THE T.V. REMOTE DOWN
AAAAAAAAND IT'S GONE

big brain solution

losing more than the remote

Disappearing Perimeter

data is the new perimeter

Environment shift

i never want to go into an office again

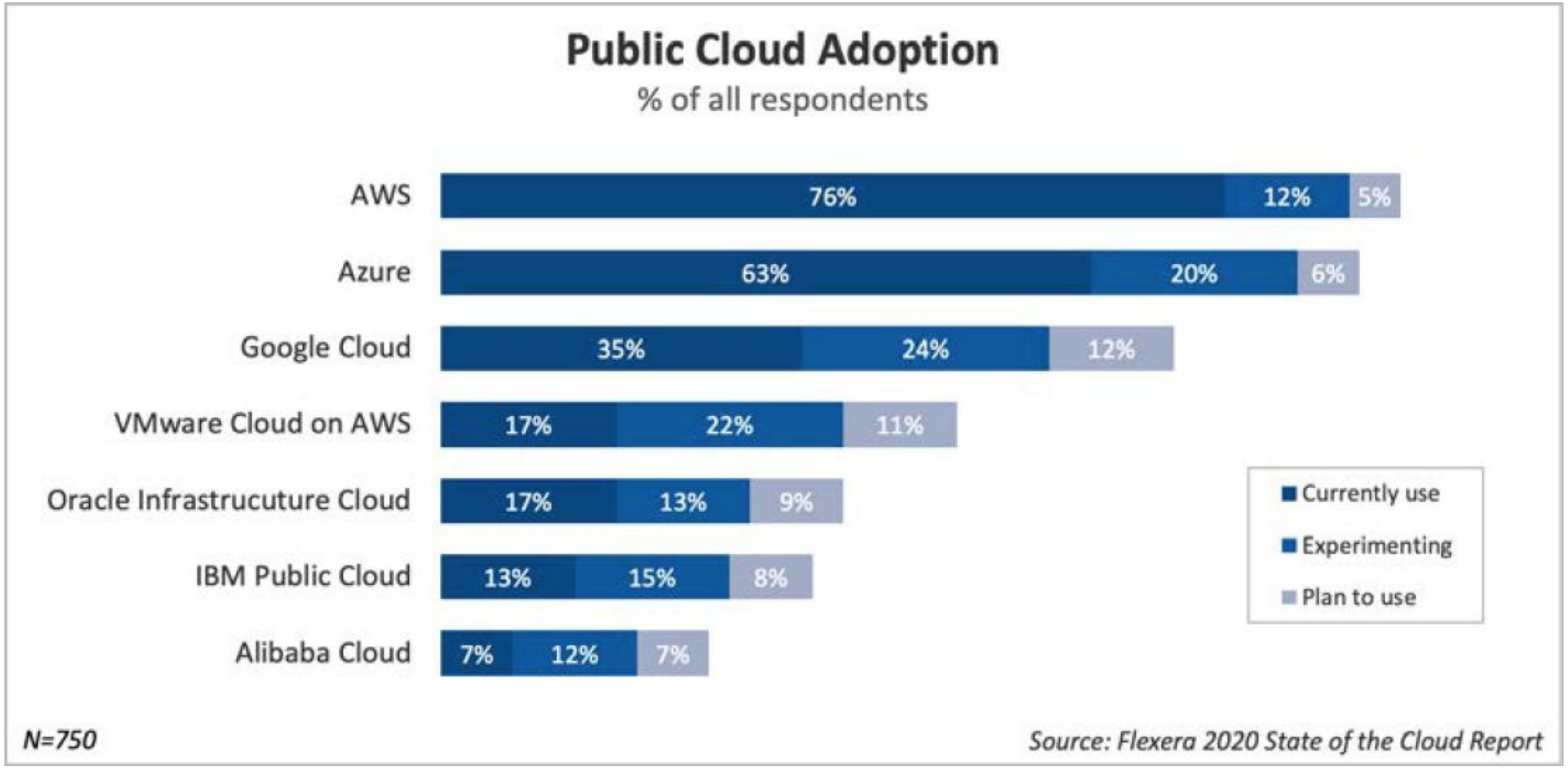
Devices and Users

identity is the new endpoint

MOVE
FAST AND
BREAK
THINGS

saas pass iass

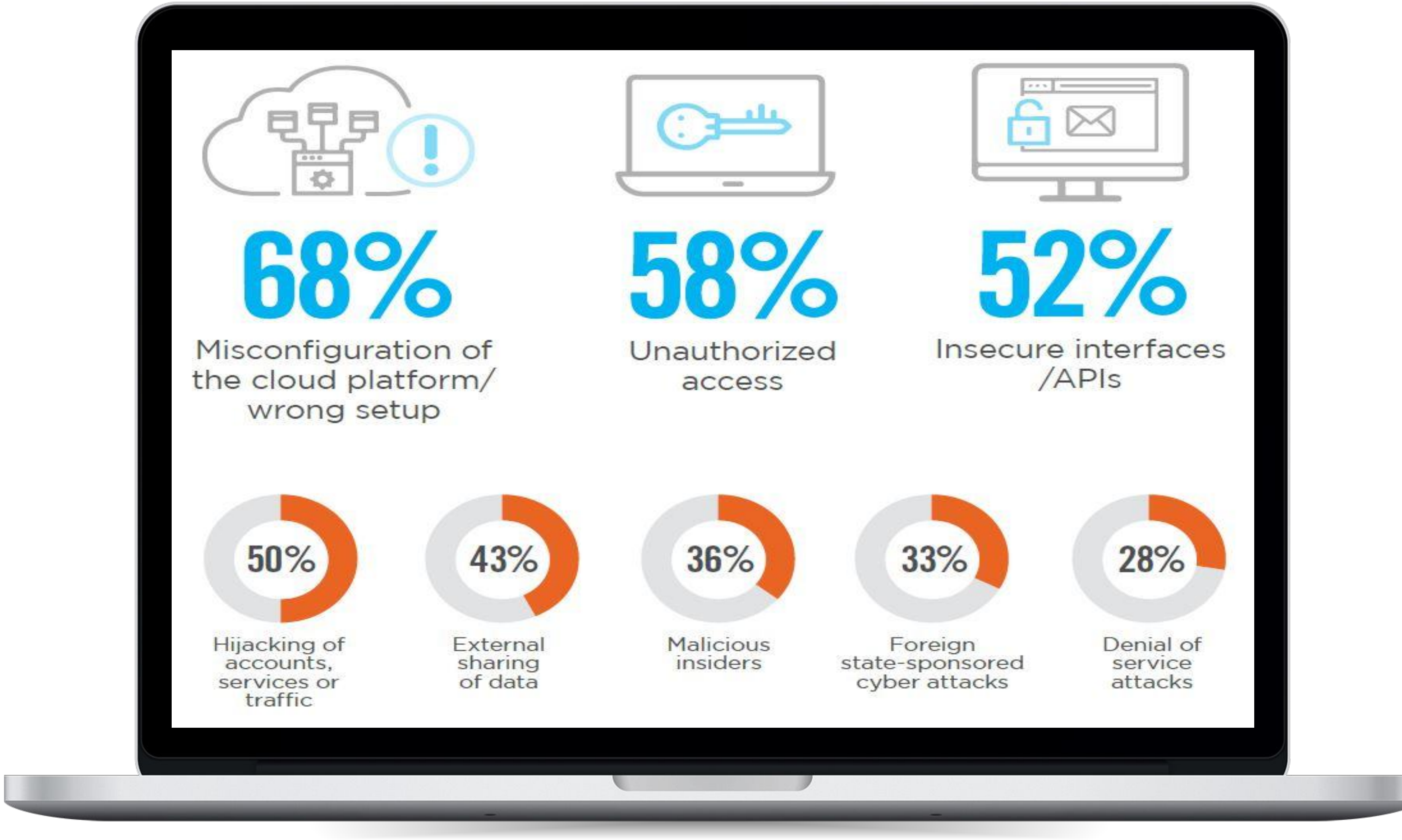
Top Cloud Providers for 2020



Source: Flexera 2020 State of the Cloud Report

my foot, i shot it

these are 100% preventable problems



68%
Misconfiguration of the cloud platform/ wrong setup

58%
Unauthorized access

52%
Insecure interfaces /APIs

50%
Hijacking of accounts, services or traffic

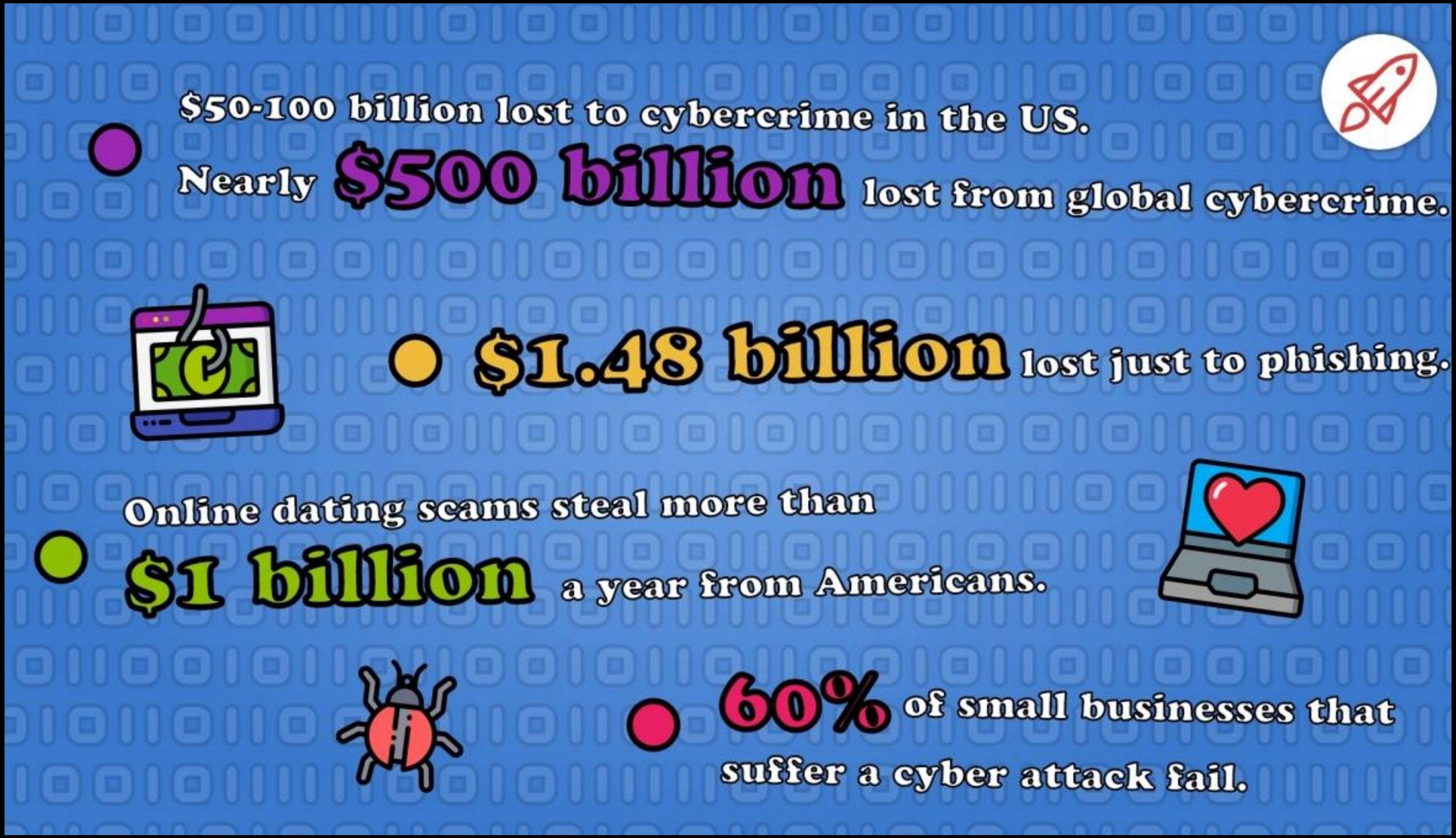
43%
External sharing of data

36%
Malicious insiders

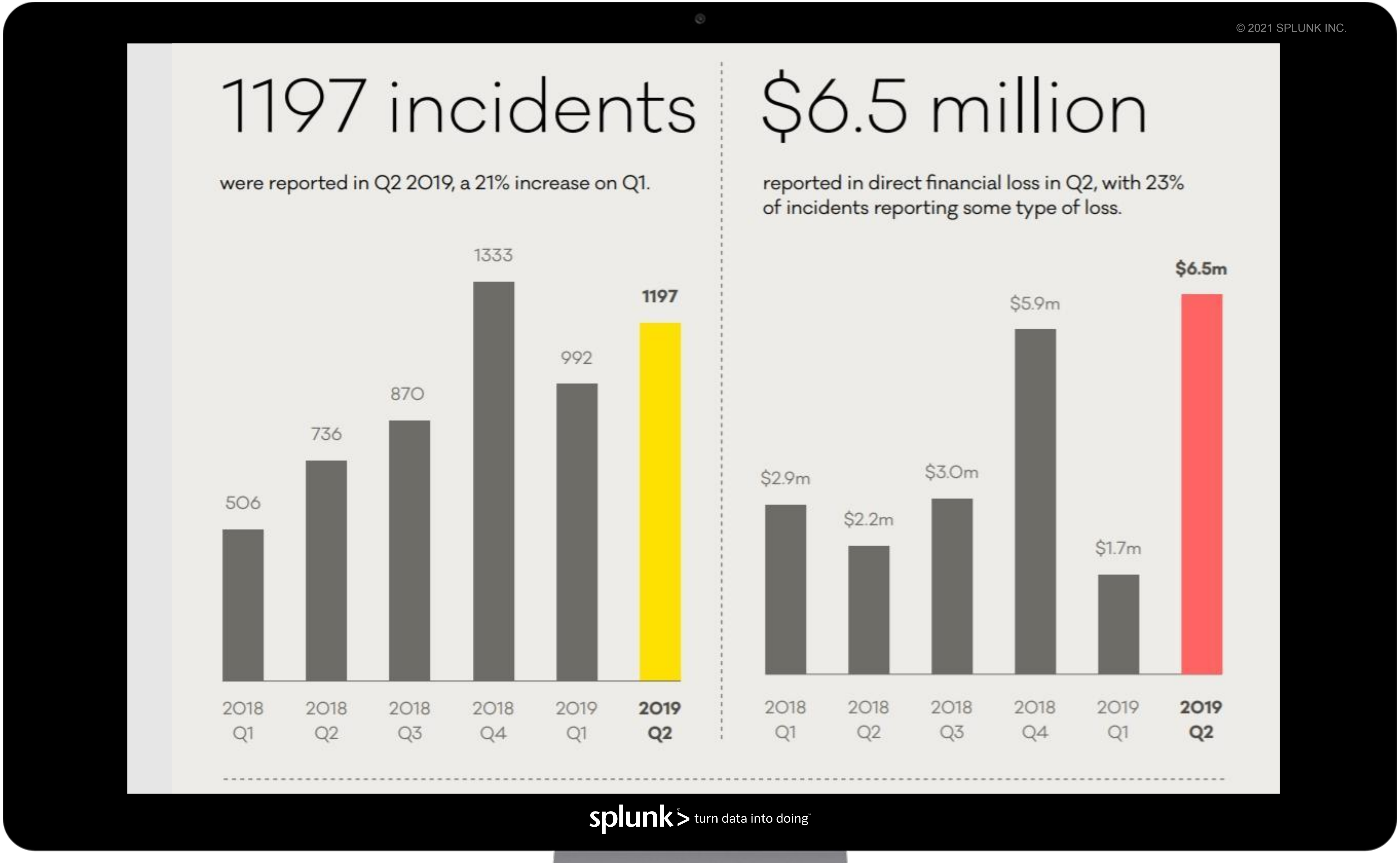
33%
Foreign state-sponsored cyber attacks

28%
Denial of service attacks

broken things cost money



- $50-100 billion lost to cybercrime in the US. Nearly **$500 billion** lost from global cybercrime.
- **$1.48 billion** lost just to phishing.
- Online dating scams steal more than **$1 billion** a year from Americans.
- **60%** of small businesses that suffer a cyber attack fail.



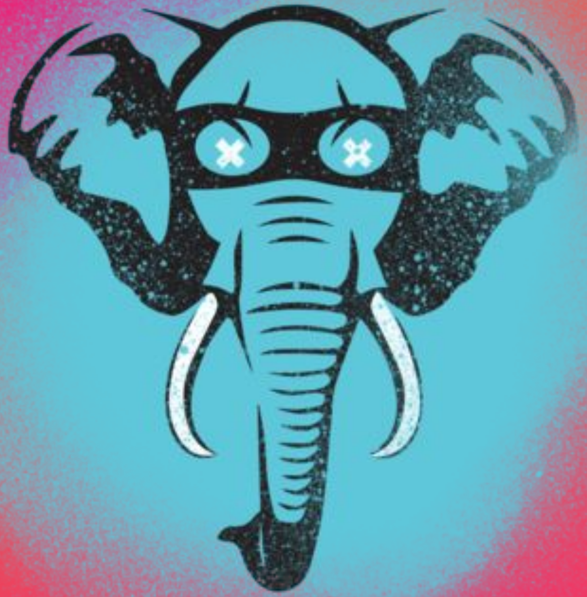
1197 incidents

were reported in Q2 2019, a 21% increase on Q1.

$6.5 million

reported in direct financial loss in Q2, with 23% of incidents reporting some type of loss.

relevant ransomware elephant

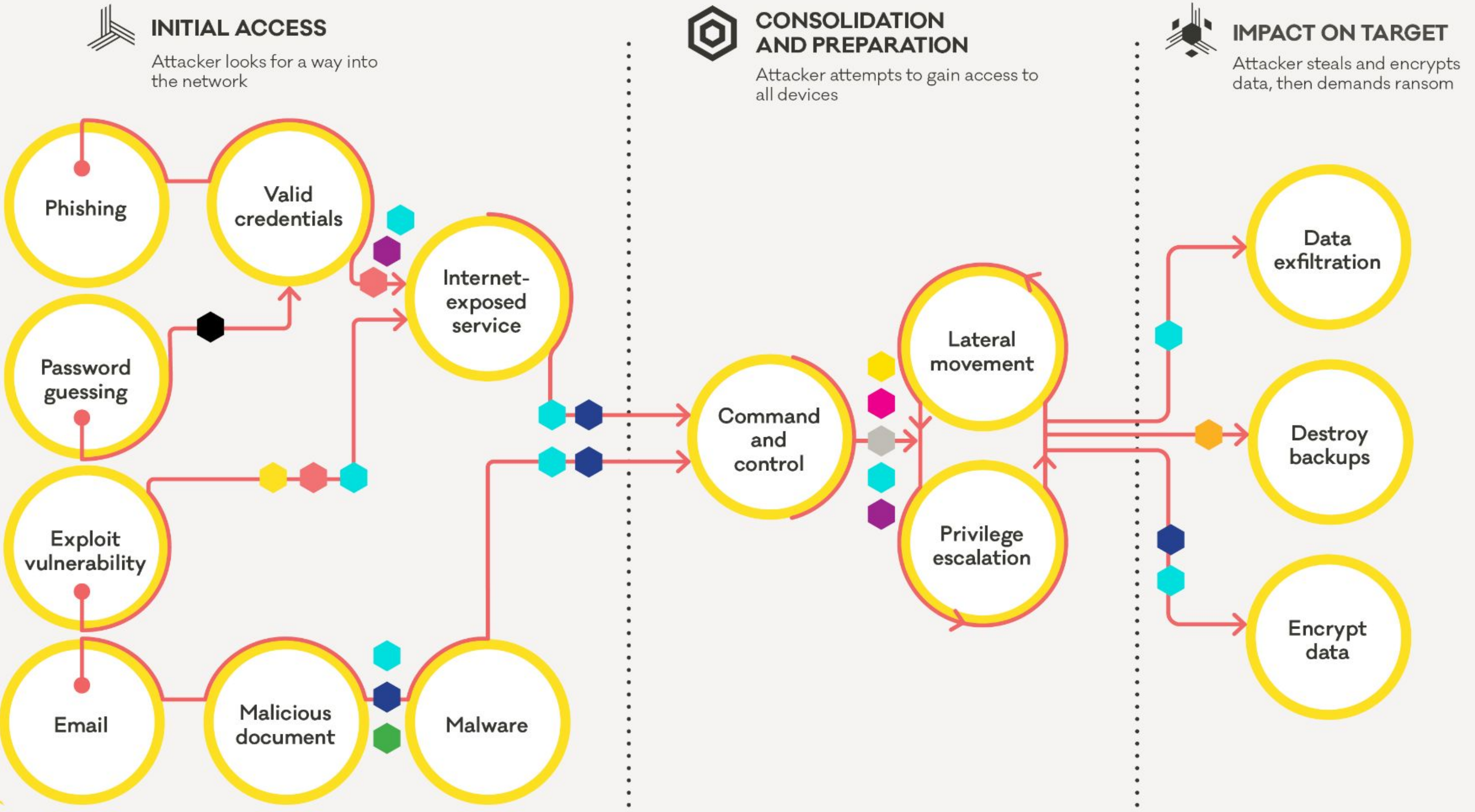


splunk> turn data into doing™

LIFECYCLE OF A RANSOMWARE INCIDENT

certnz

How the CERT NZ Critical Controls can help you stop a ransomware attack in its tracks.



INITIAL ACCESS

Attacker looks for a way into the network

Phishing

Valid credentials

Password guessing

Exploit vulnerability

Email

Malicious document

Malware

Internet-exposed service

CONSOLIDATION AND PREPARATION

Attacker attempts to gain access to all devices

Command and control

Lateral movement

Privilege escalation

IMPACT ON TARGET

Attacker steals and encrypts data, then demands ransom

Data exfiltration

Destroy backups

Encrypt data

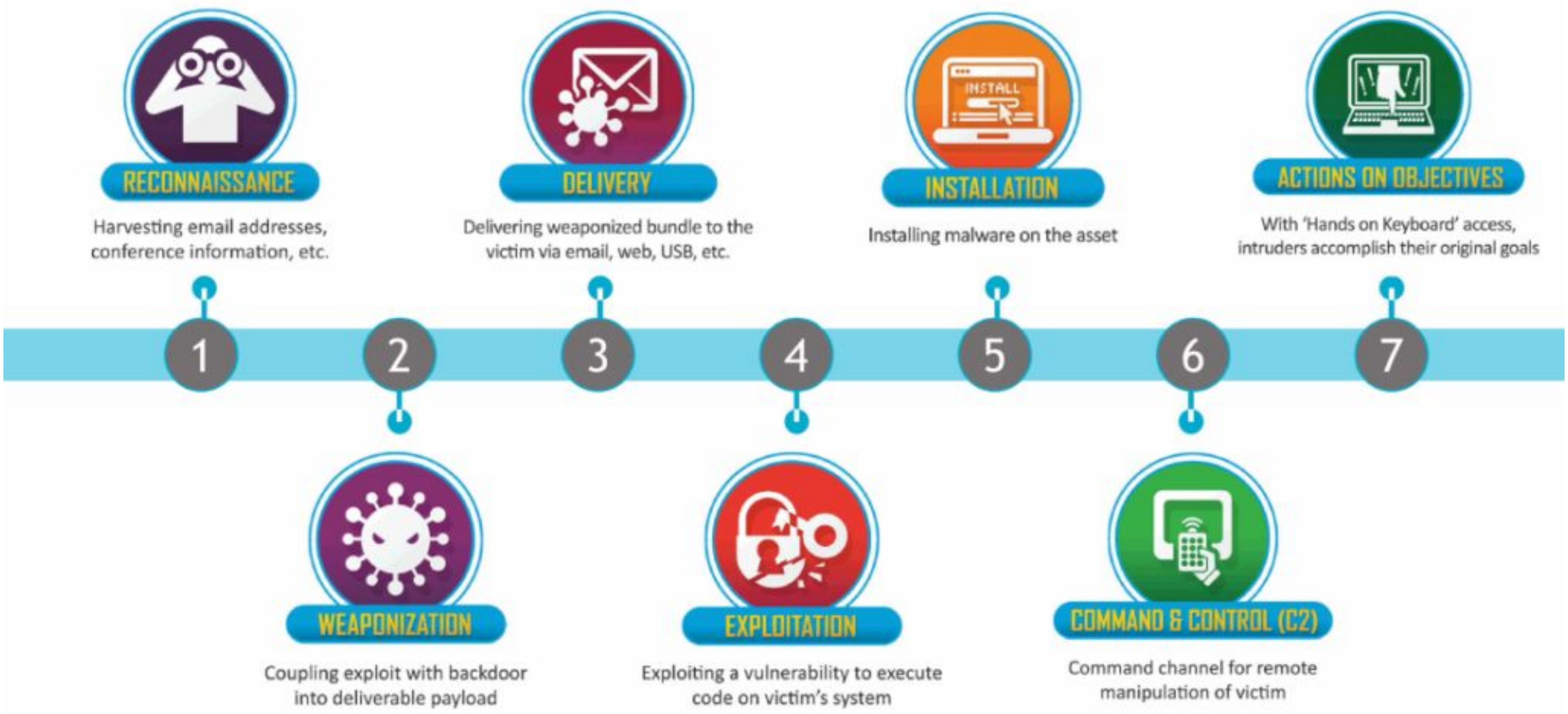
CRITICAL CONTROLS KEY

- Internet-exposed services
- Patching
- MFA
- Network segmentation
- Principle of least privilege
- Backups
- Application allowlisting
- Logging and alerting
- Disable macros
- Password manager

New Zealand Government

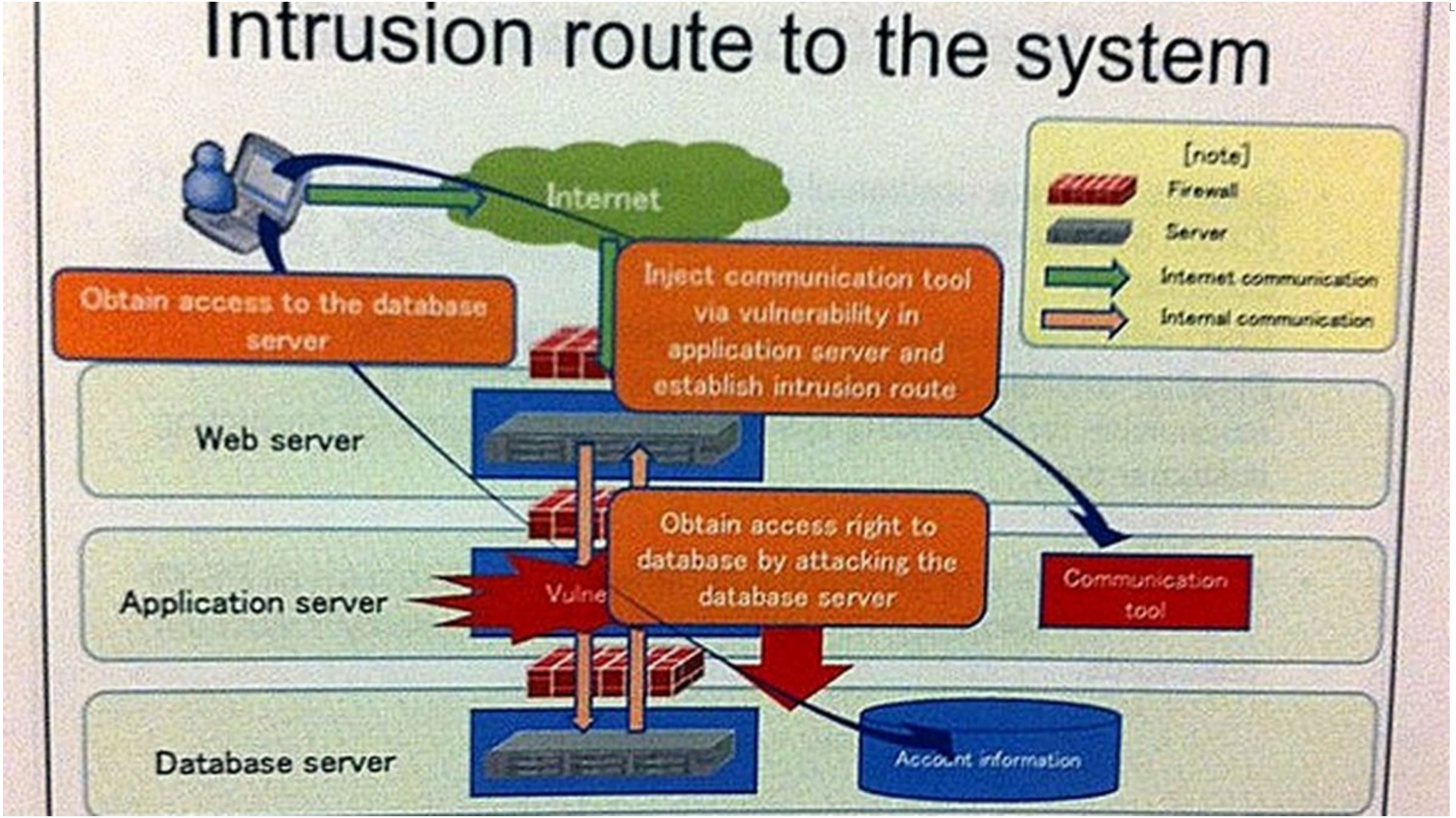
ata into doing™

LOCKHEED MARTIN KILL CHAIN



1. **RECONNAISSANCE** – Harvesting email addresses, conference information, etc.
2. **WEAPONIZATION** – Coupling exploit with backdoor into deliverable payload
3. **DELIVERY** – Delivering weaponized bundle to the victim via email, web, USB, etc.
4. **EXPLOITATION** – Exploiting a vulnerability to execute code on victim's system
5. **INSTALLATION** – Installing malware on the asset
6. **COMMAND & CONTROL (C2)** – Command channel for remote manipulation of victim
7. **ACTIONS ON OBJECTIVES** – With 'Hands on Keyboard' access, intruders accomplish their original goals

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html



Intrusion route to the system

Internet

Obtain access to the database server

Inject communication tool via vulnerability in application server and establish intrusion route

Web server

Application server

Vulne

Obtain access right to database by attacking the database server

Communication tool

Database server

Account information

[note]

- 🟥 Firewall
- ▬ Server
- ➡ Internet communication
- ➡ Internal communication

APT vs Cybercrime

does it matter anymore?

splunk> turn data into doing™

BEC is king

By the end of 2017, the average user was receiving 16 phishing emails per month. 66% of malware is installed via malicious email attachments.

49% of non-point-of-sale malware was installed via malicious email. 21% of ransomware involved social actions, such as phishing.

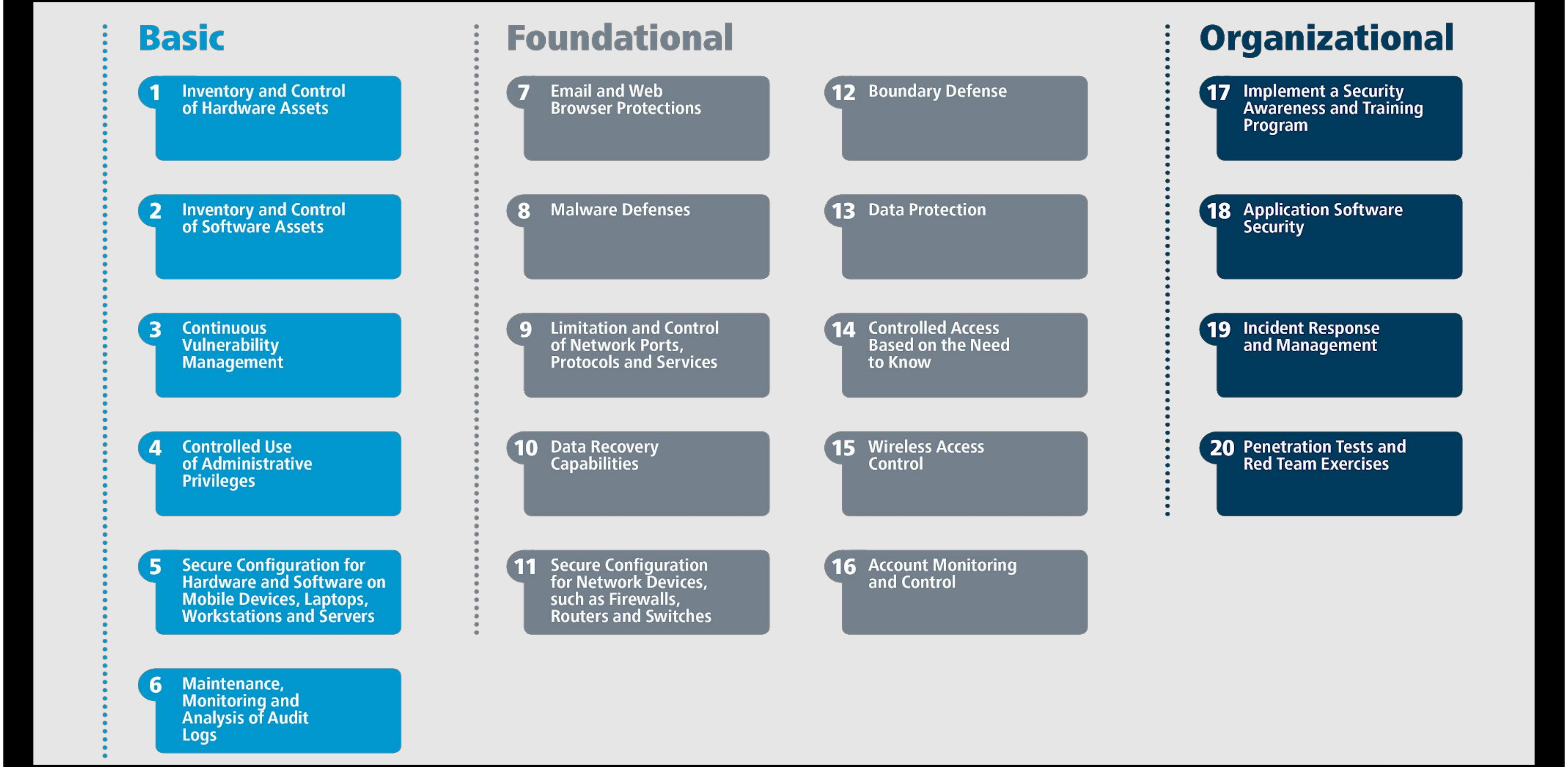
- Nearly 1,000 U.S. Organizations Impacted by Ransomware Attacks in 2019
- Ransomware Attacks Against Municipalities Increased 60% in 2019

Easy
?
Shift

posture via process

splunk> turn data into doing™

but cyber



Basic

1 Inventory and Control of Hardware Assets

2 Inventory and Control of Software Assets

3 Continuous Vulnerability Management

4 Controlled Use of Administrative Privileges

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7 Email and Web Browser Protections

8 Malware Defenses

9 Limitation and Control of Network Ports, Protocols and Services

10 Data Recovery Capabilities

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring and Control

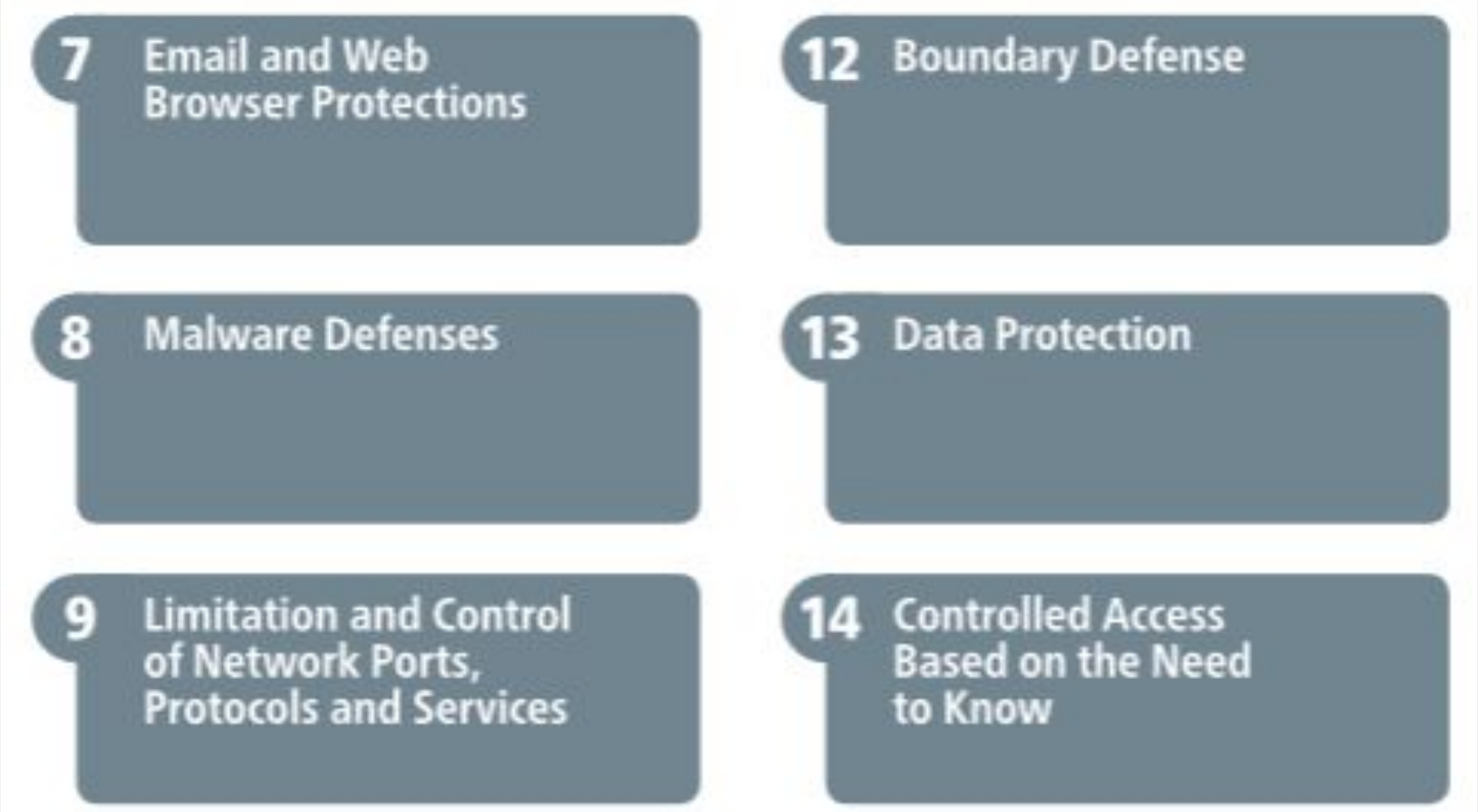
Organizational

17 Implement a Security Awareness and Training Program

18 Application Software Security

19 Incident Response and Management

20 Penetration Tests and Red Team Exercises



7 Email and Web Browser Protections

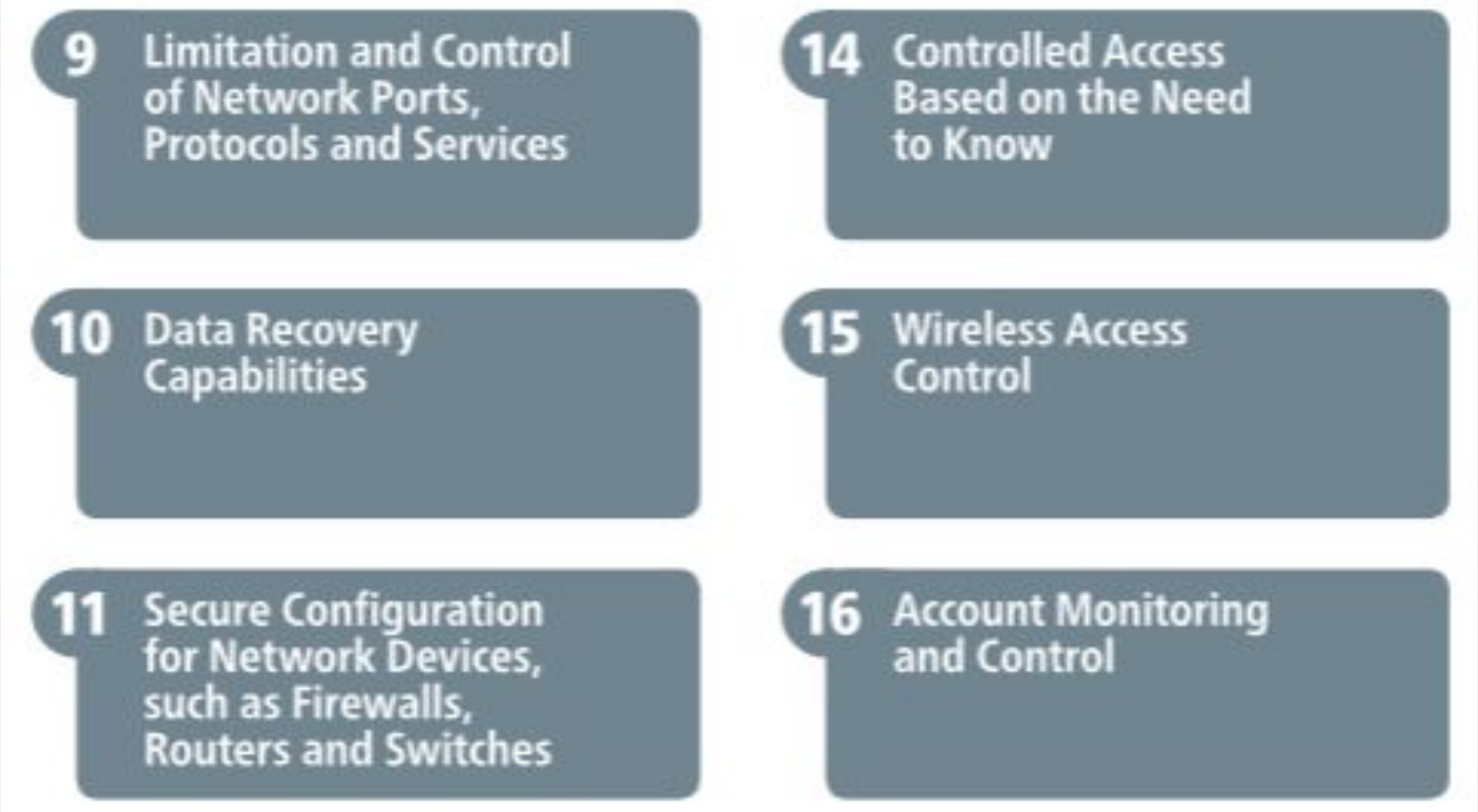
12 Boundary Defense

8 Malware Defenses

13 Data Protection

9 Limitation and Control of Network Ports, Protocols and Services

14 Controlled Access Based on the Need to Know



9 Limitation and Control of Network Ports, Protocols and Services

10 Data Recovery Capabilities

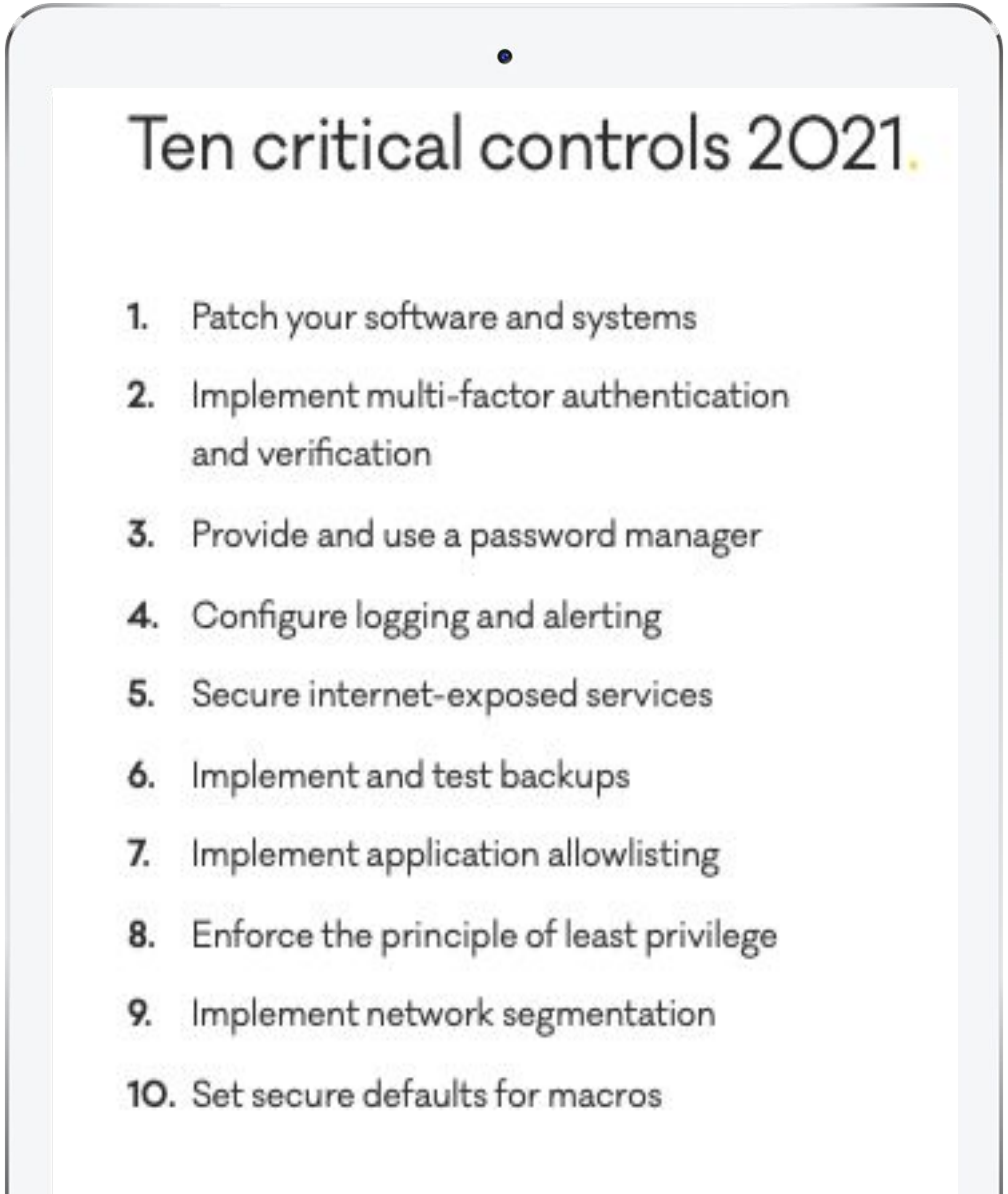
11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring and Control

NZ CERT top ten



Ten critical controls 2021.

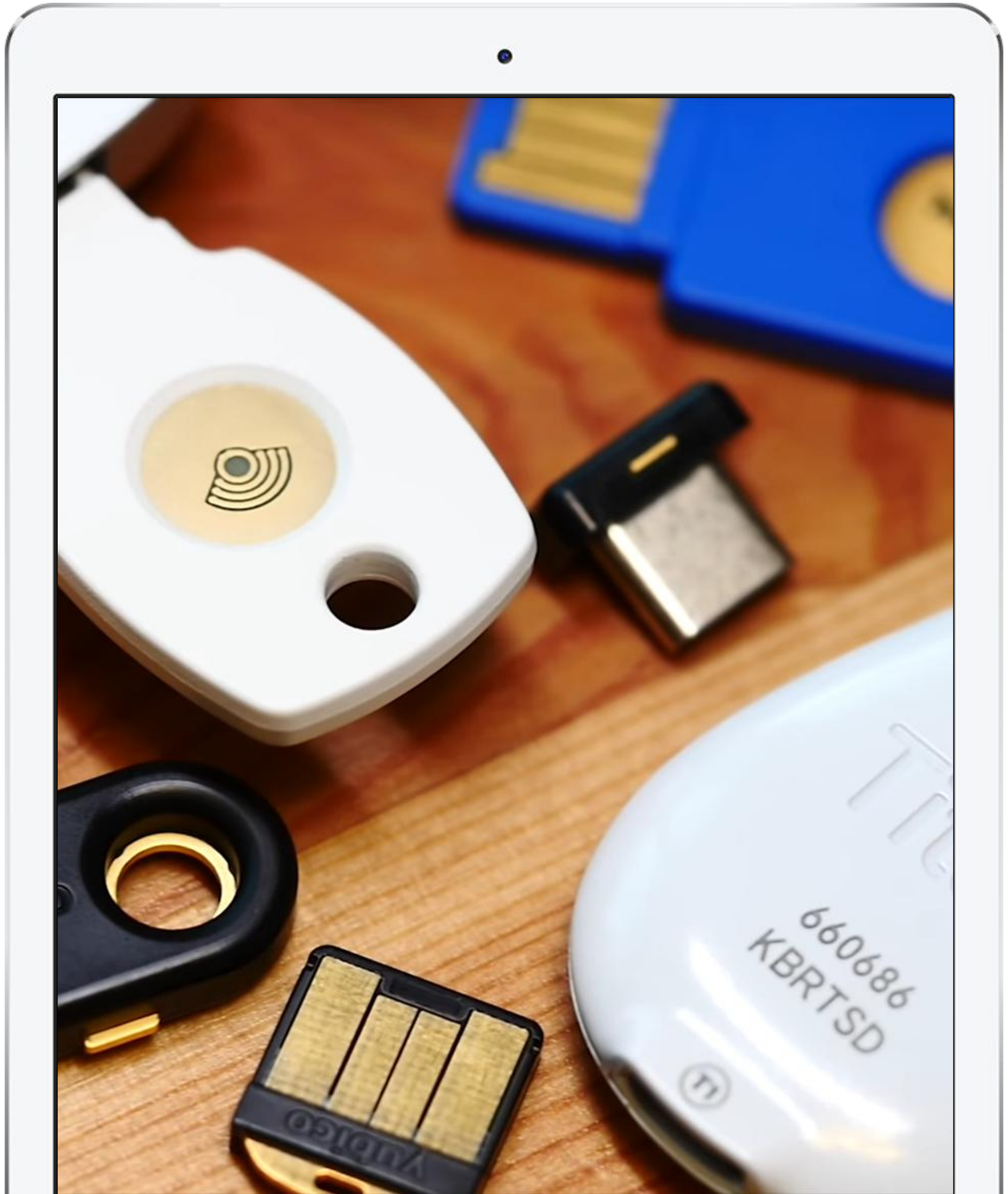
1. Patch your software and systems
2. Implement multi-factor authentication and verification
3. Provide and use a password manager
4. Configure logging and alerting
5. Secure internet-exposed services
6. Implement and test backups
7. Implement application allowlisting
8. Enforce the principle of least privilege
9. Implement network segmentation
10. Set secure defaults for macros

mandate MFA

avoid SMS

crawl/walk/run to tokens

monitor failed logins



hardware tokens work

Security Keys are inexpensive USB-based devices that offer an alternative approach to two-factor authentication (2FA), which requires the user to log in to a Web site using something they know (the password) and something they have (e.g., a mobile device).

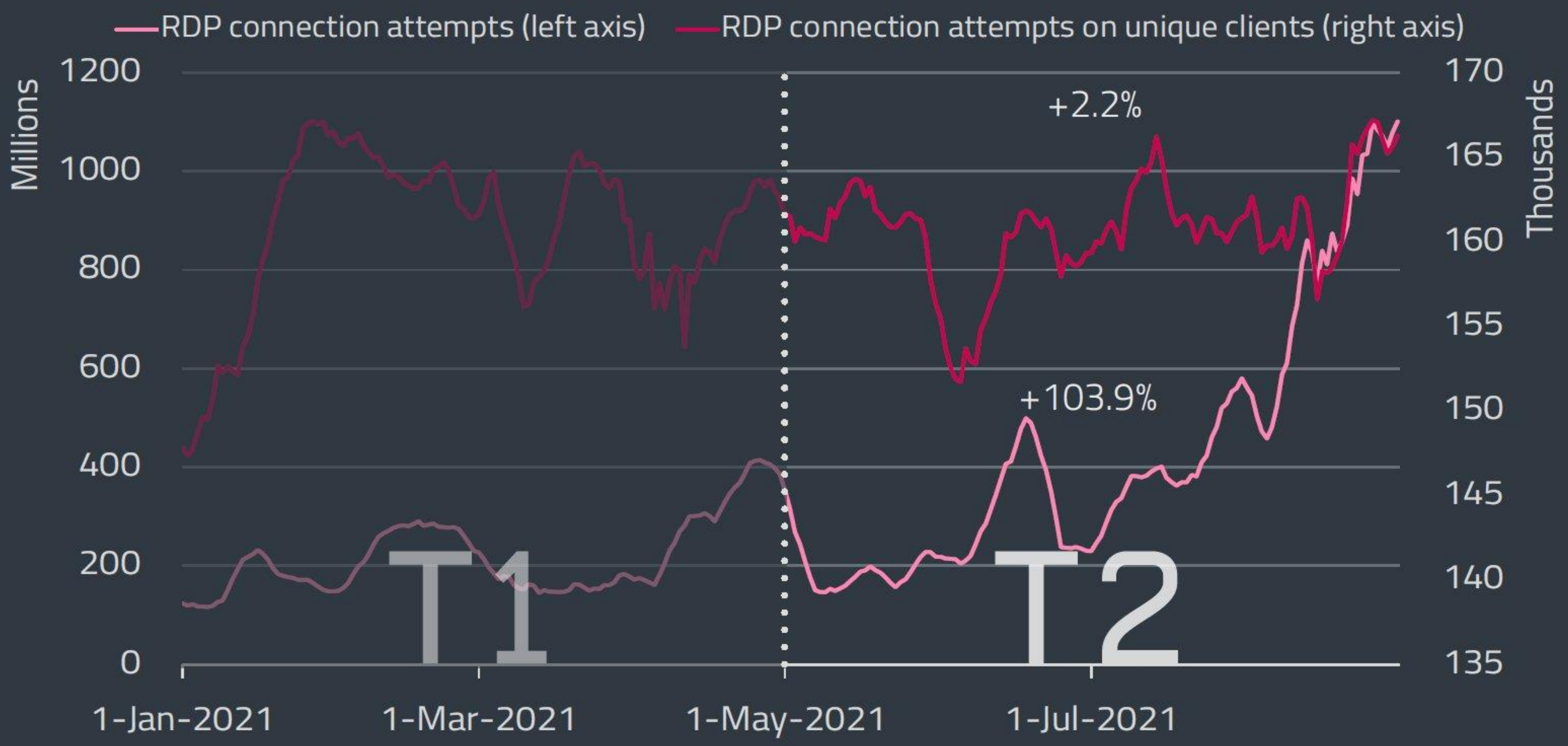
everyone loves patching

splunk> turn data into doing™

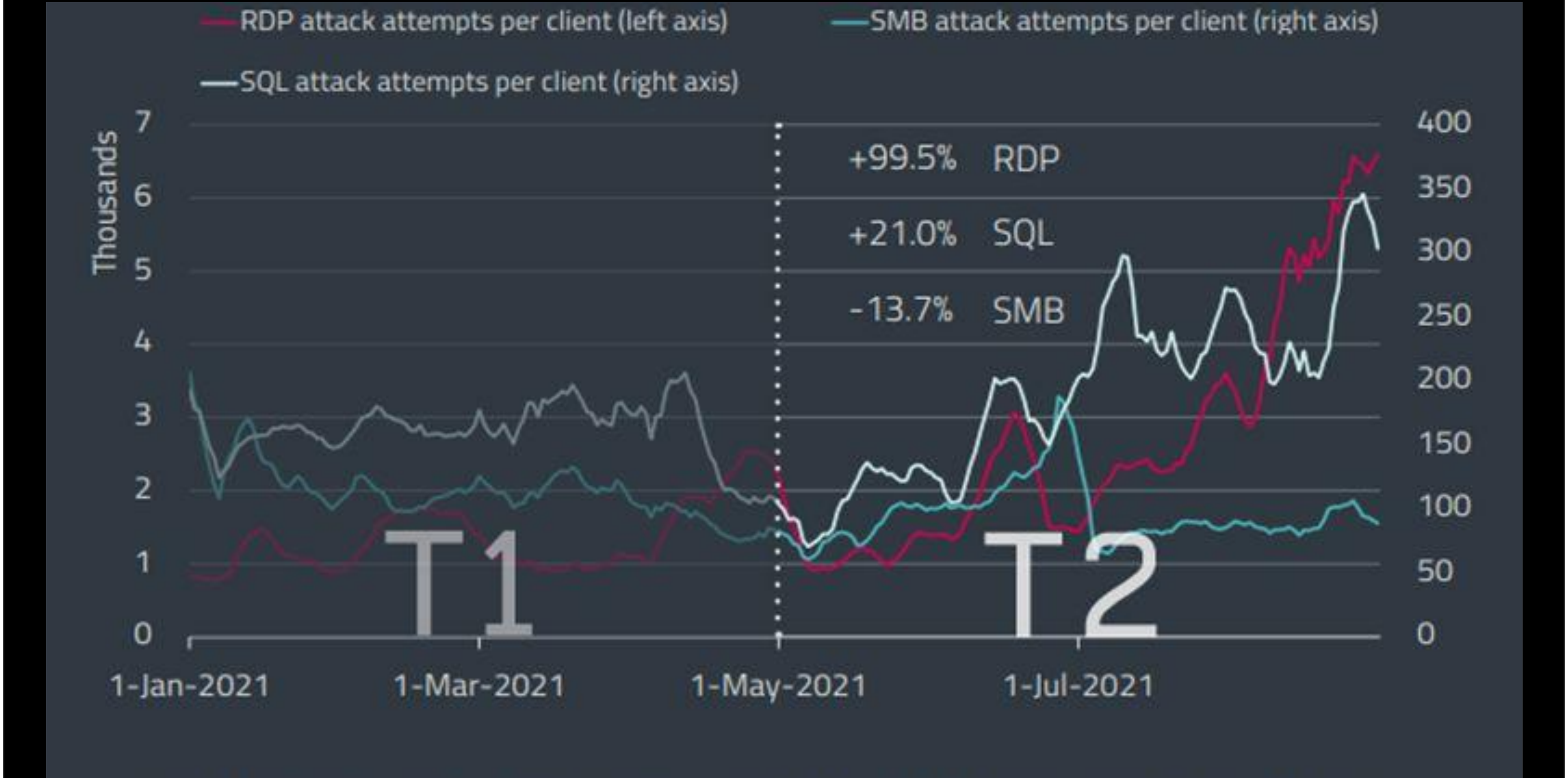
secure internet facing assets

Close and disable port 3389

Make RDP available only through a corporate VPN...Use Network Level Authentication (NLA)...Enable multi factor authentication... At the very least, use strong passwords.



Trends of RDP connection attempts and unique clients in T1 2021 – T2 2021, seven-day moving average

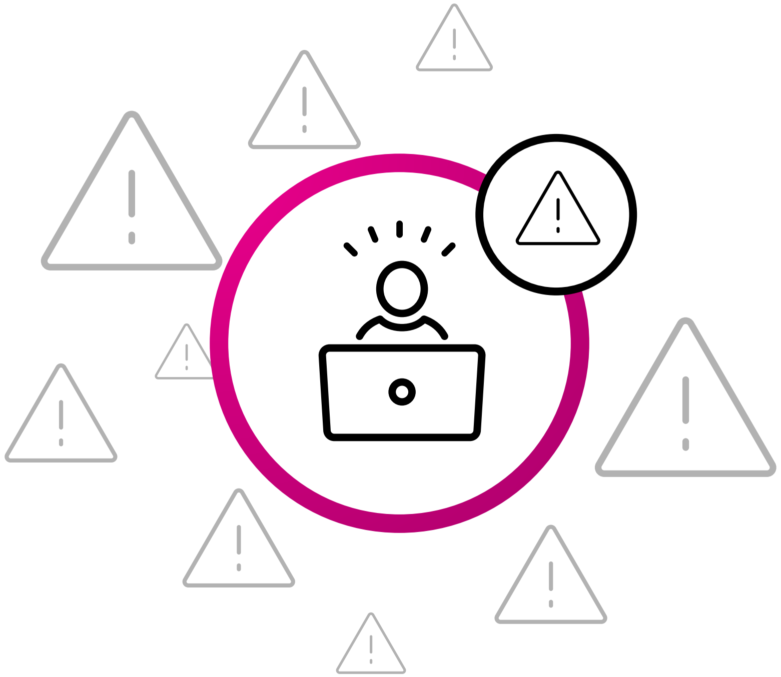


Trends of RDP, SMB and SQL attack attempts per client in T1 2021 – T2 2021, seven-day moving average

more data, more problems

Alert Volumes Are Overwhelming SOCs

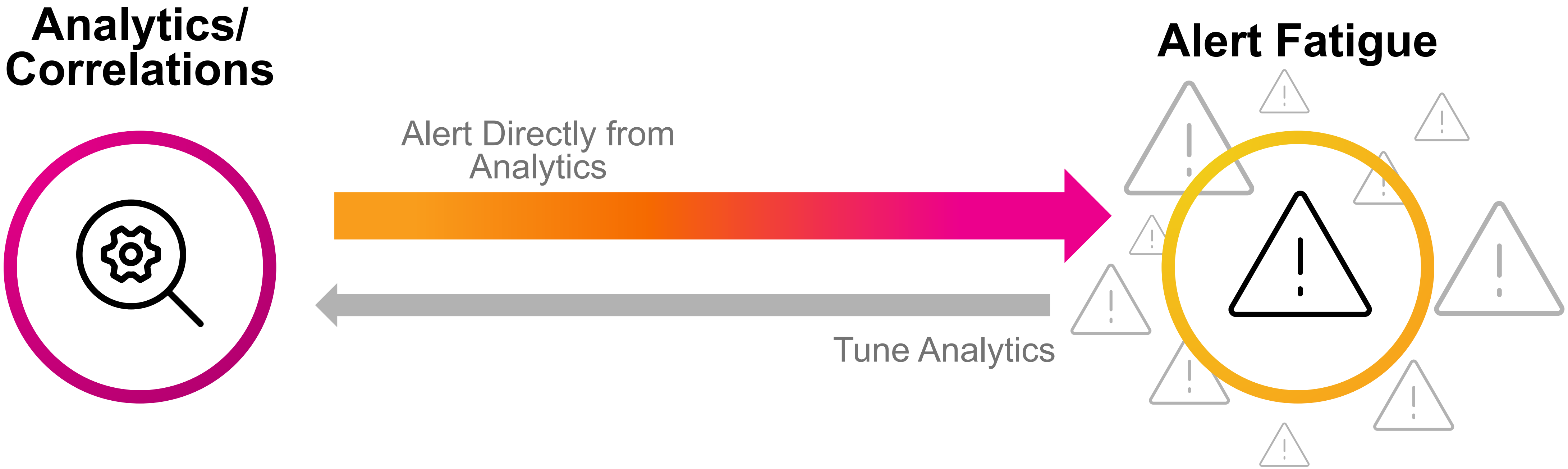
Over 40% of orgs receive 10,000+ alerts per day; experience 50%+ false positives



- Abandoned alerts
- Suppressed alerts
- Slow detection / response
- Analyst burnout

But What Alternatives Do SOCs Have?

There are no perfect correlation searches; alert fatigue seems inevitable



Analytics/ Correlations

Alert Directly from Analytics

Tune Analytics

Alert Fatigue

How can SOCs **reduce alert volumes** while **improving their security** coverage?

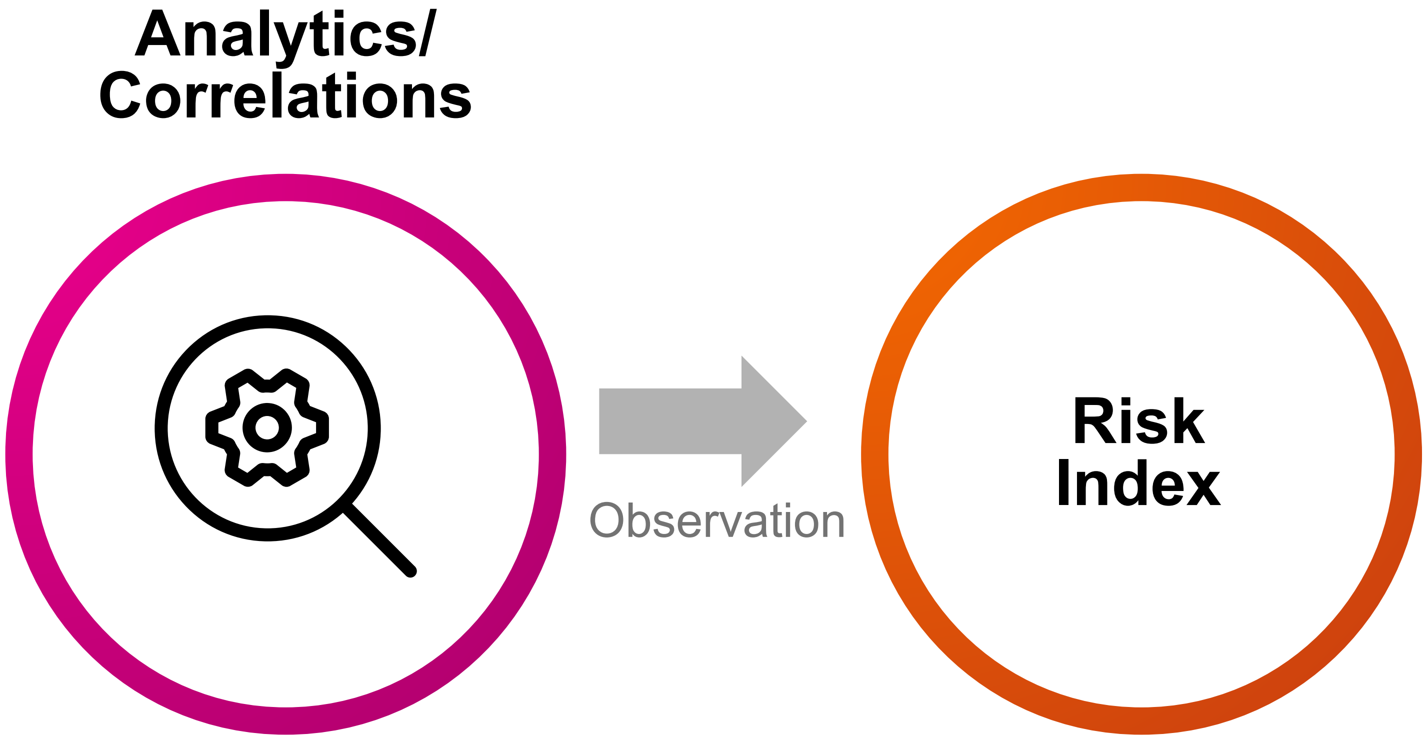
splunk> turn data into doing™

alert fatigue is real

data explosion indeed.

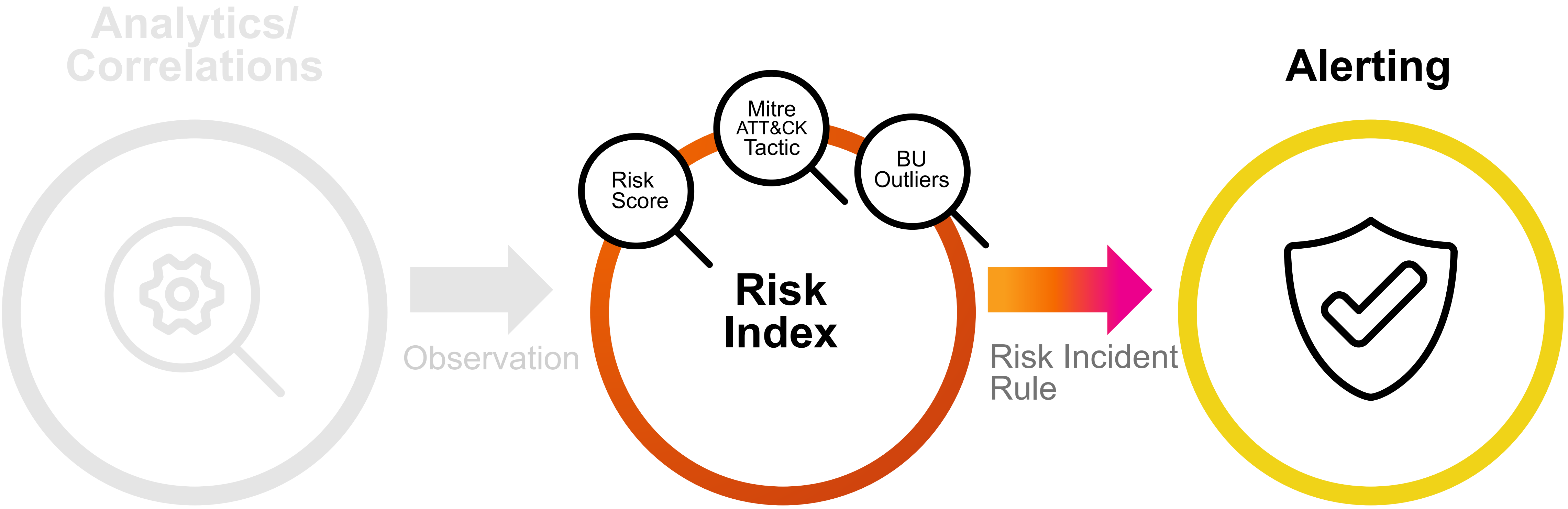
Risk-Based Alerting to the Rescue

Dramatically reduce alert volumes while increasing analyst productivity and efficiency



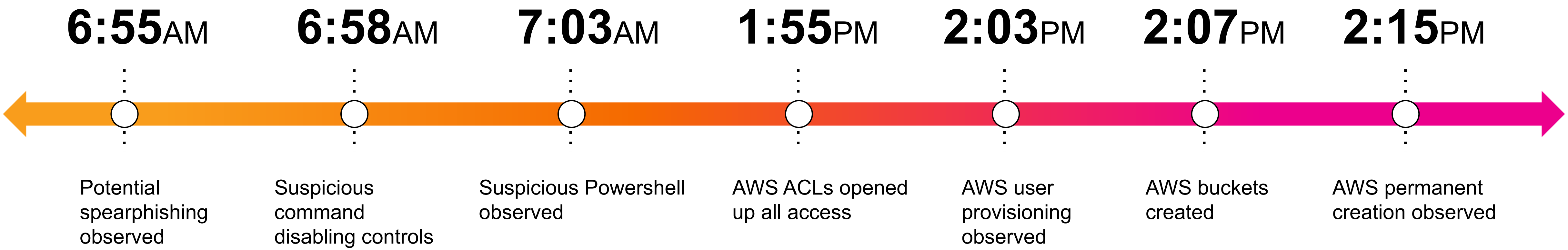
Risk-Based Alerting to the Rescue

Dramatically reduce alert volumes while improving your security posture



How Does This Look in Practice?

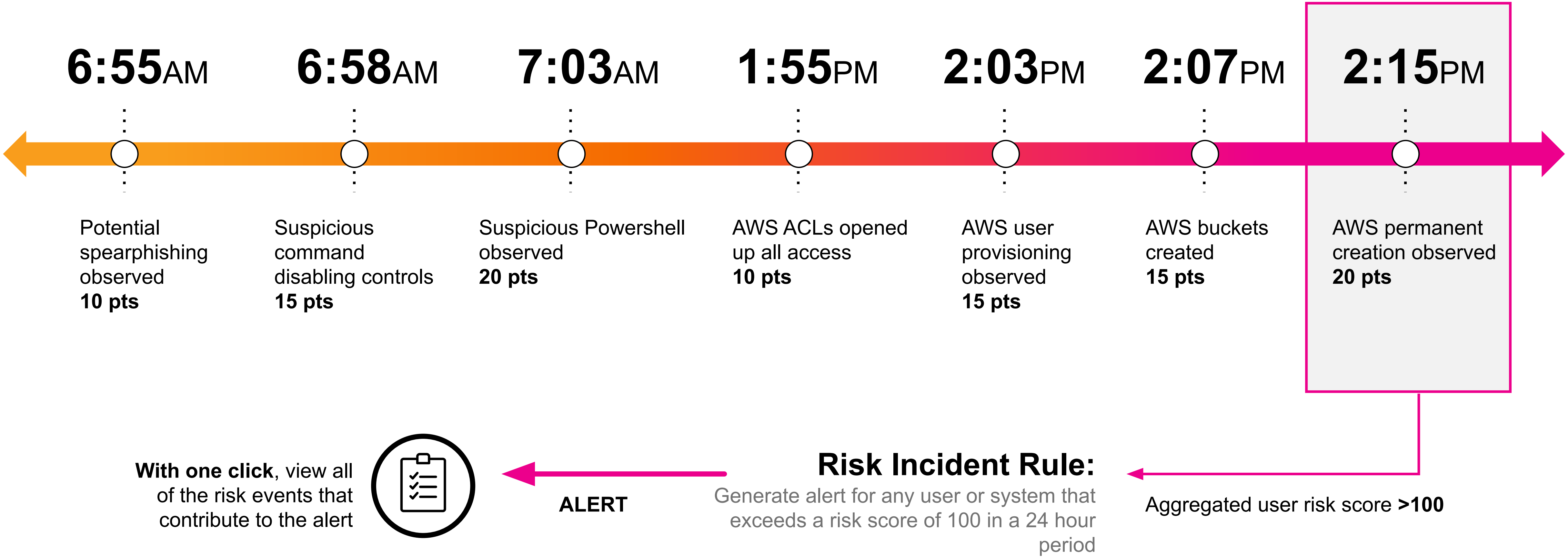
Traditionally, the events below would be considered too noisy and would be abandoned



6:55AM	6:58AM	7:03AM	1:55PM	2:03PM	2:07PM	2:15PM
Potential spearphishing observed	Suspicious command disabling controls	Suspicious Powershell observed	AWS ACLs opened up all access	AWS user provisioning observed	AWS buckets created	AWS permanent creation observed

How Does This Look in Practice?

With risk-based alerting, these events become context that informs high-fidelity alerts



6:55AM
Potential spearphishing observed
10 pts

6:58AM
Suspicious command disabling controls
15 pts

7:03AM
Suspicious Powershell observed
20 pts

1:55PM
AWS ACLs opened up all access
10 pts

2:03PM
AWS user provisioning observed
15 pts

2:07PM
AWS buckets created
15 pts

2:15PM
AWS permanent creation observed
20 pts

Aggregated user risk score **>100**

Risk Incident Rule:
Generate alert for any user or system that exceeds a risk score of 100 in a 24 hour period

ALERT

With one click, view all of the risk events that contribute to the alert

RBA Reduces Alerts, and Much More

RBA initially reduces alert volumes (and fast) but ultimately streamlines the entire SOC

Reduce Alerts

Improve Detections

Quantify SOC Maturity

Reduce Operational Costs

Large Technology Company

Streamline Investigations with Risk-Based Alerting

“With risk-based alerting in Splunk Enterprise Security, investigations went from taking days to taking fifteen minutes, and our true positive rate has increased from 40% to 90% in under two months. We’re discovering things that weren’t possible to detect before.”

“With risk-based alerting in Splunk Enterprise Security, we’re detecting more threats while doing less work. Our investigations process is now consistent and centers on high-fidelity alerts. Our analysts are excited to focus on real security issues, not Alerts.”

— Senior Cybersecurity Engineer

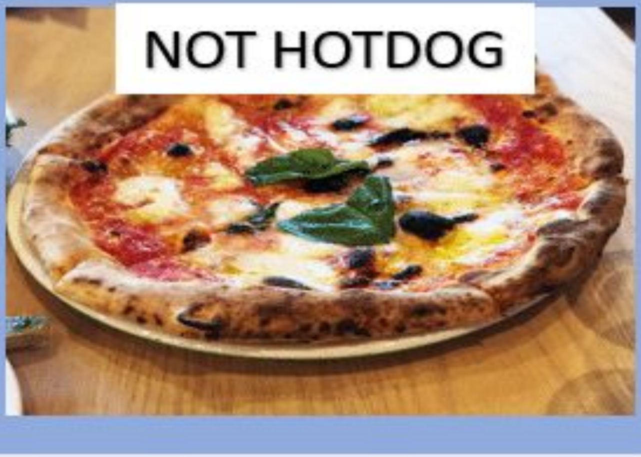
posture via technology

let’s talk about AI/ML

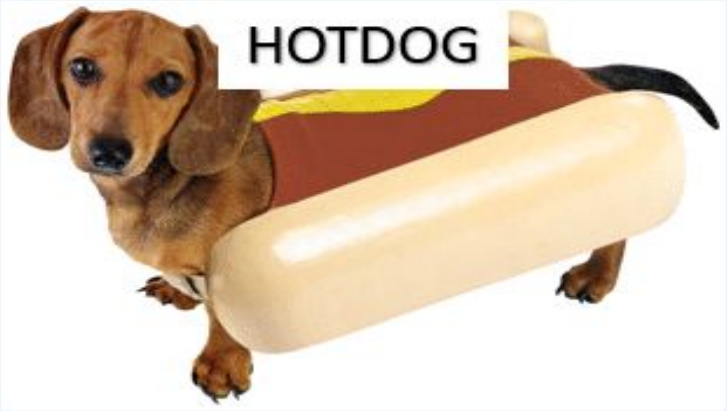
interpretability
training
explainability

True negative Predicted negative Actual negative	**False positive** Predicted positive Actual negative
False negative Predicted negative Actual positive	**True positive** Predicted positive Actual positive

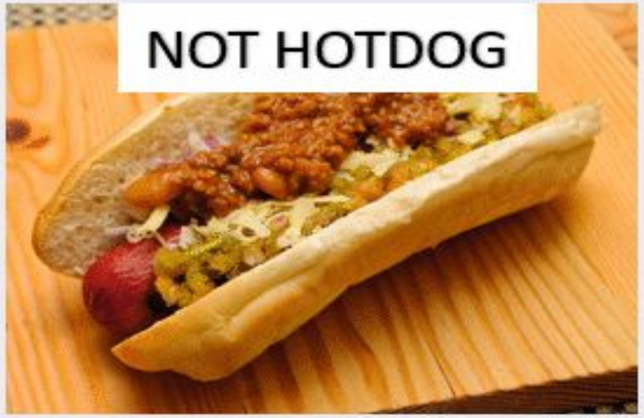
True negative



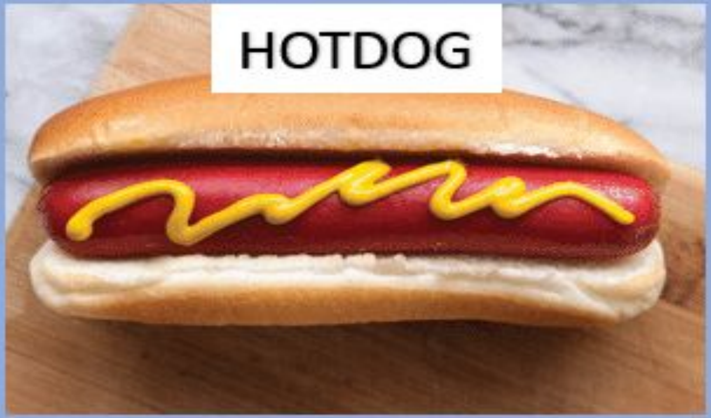
False positive



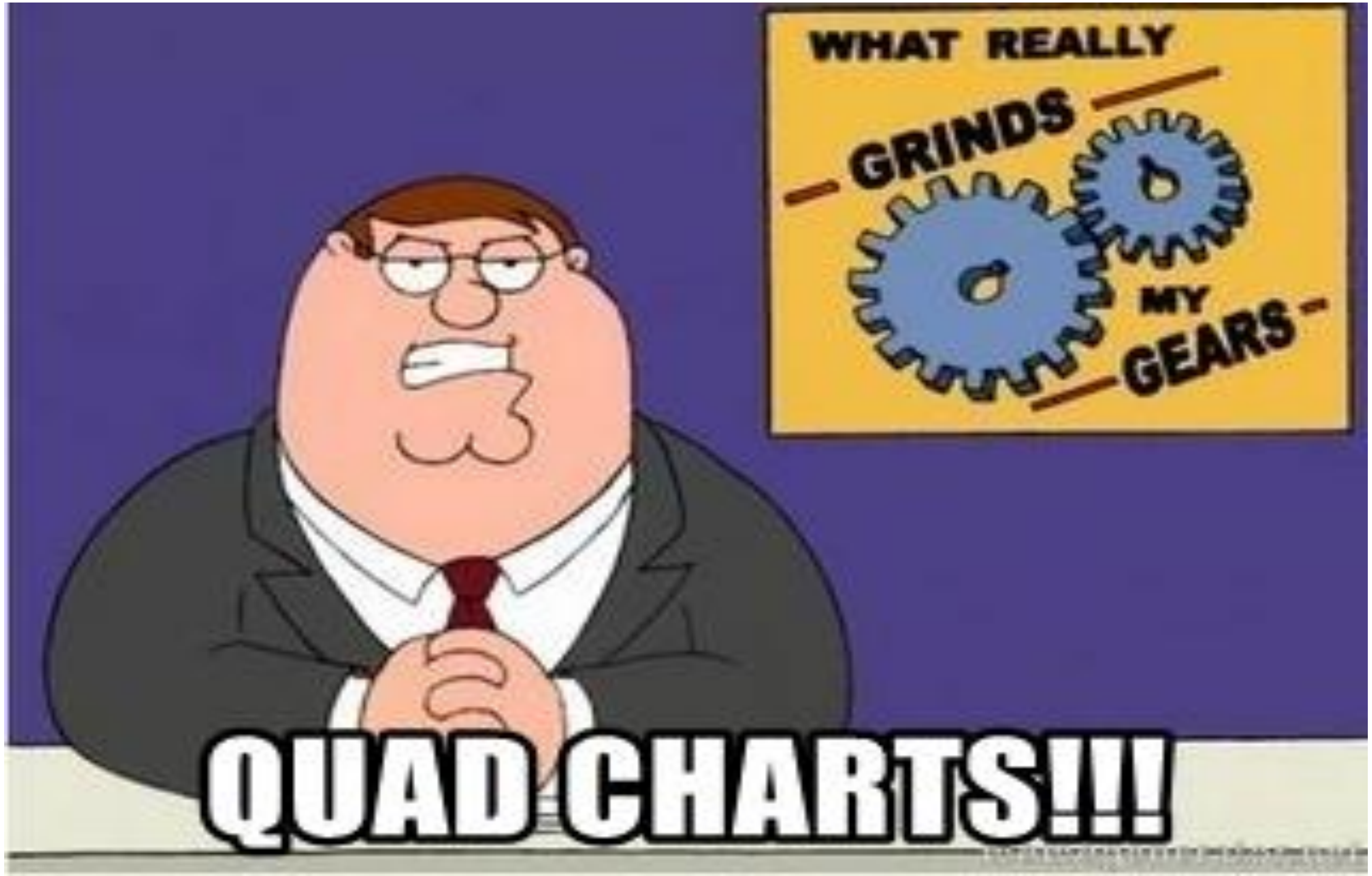
False negative



True positive



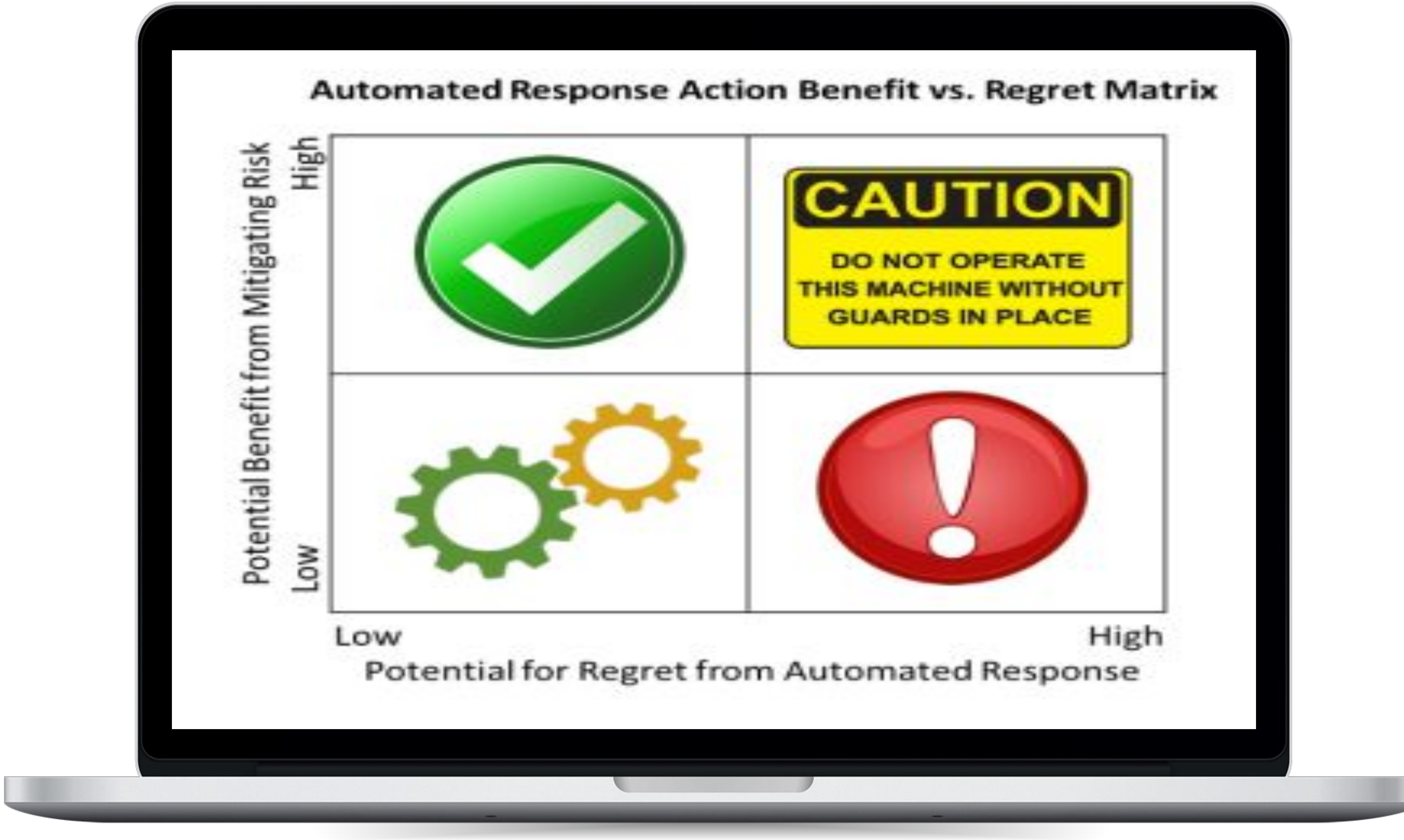
lean into automation



benefit vs regret

the other matrix

The idea is that organizations should focus on when to take an action in an automated manner instead of whether the action should be automated.

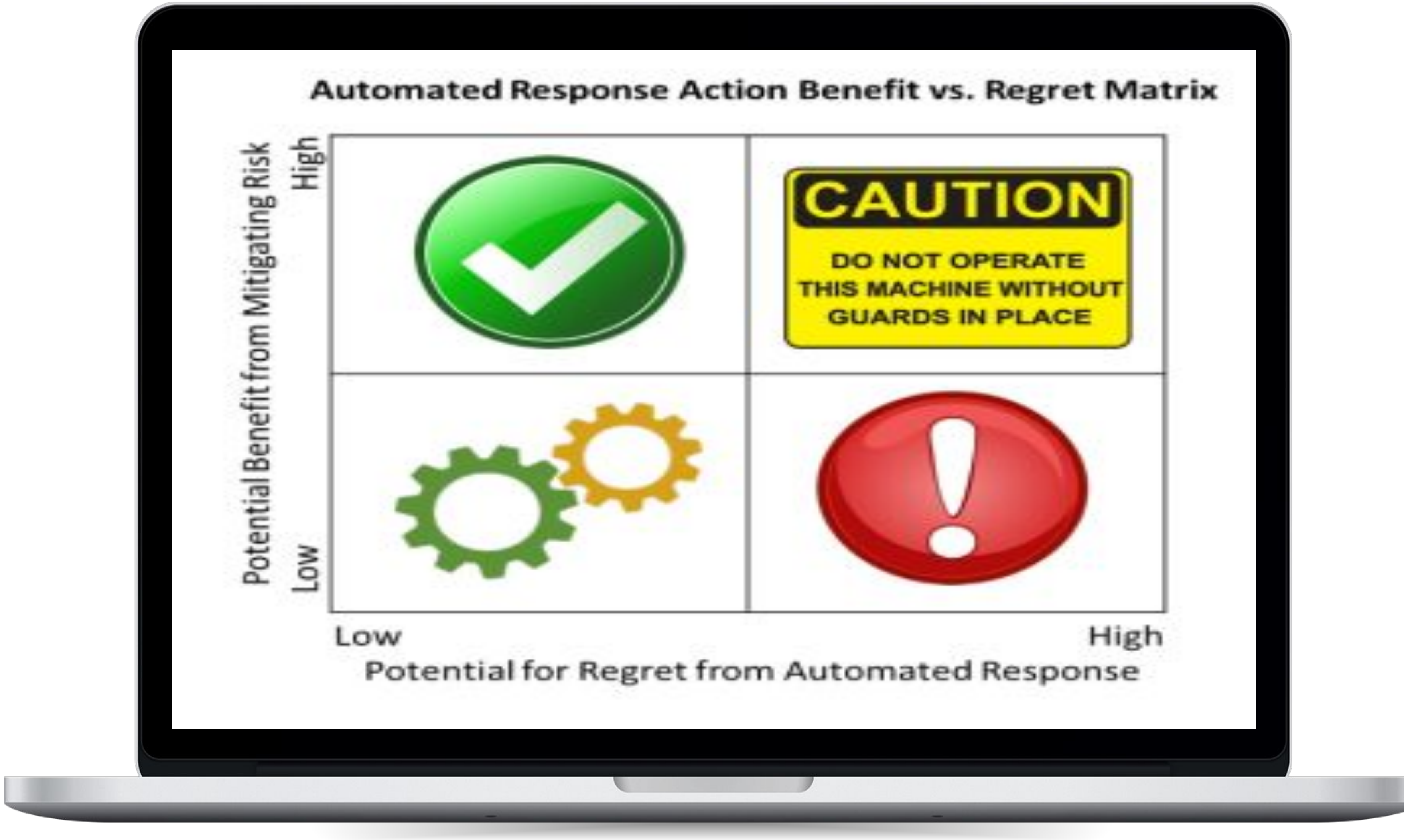

Automated Response Action Benefit vs. Regret Matrix
Potential Benefit from Mitigating Risk
High
Low
CAUTION
DO NOT OPERATE THIS MACHINE WITHOUT GUARDS IN PLACE
Low
High
Potential for Regret from Automated Response

not so fast

but still, fast

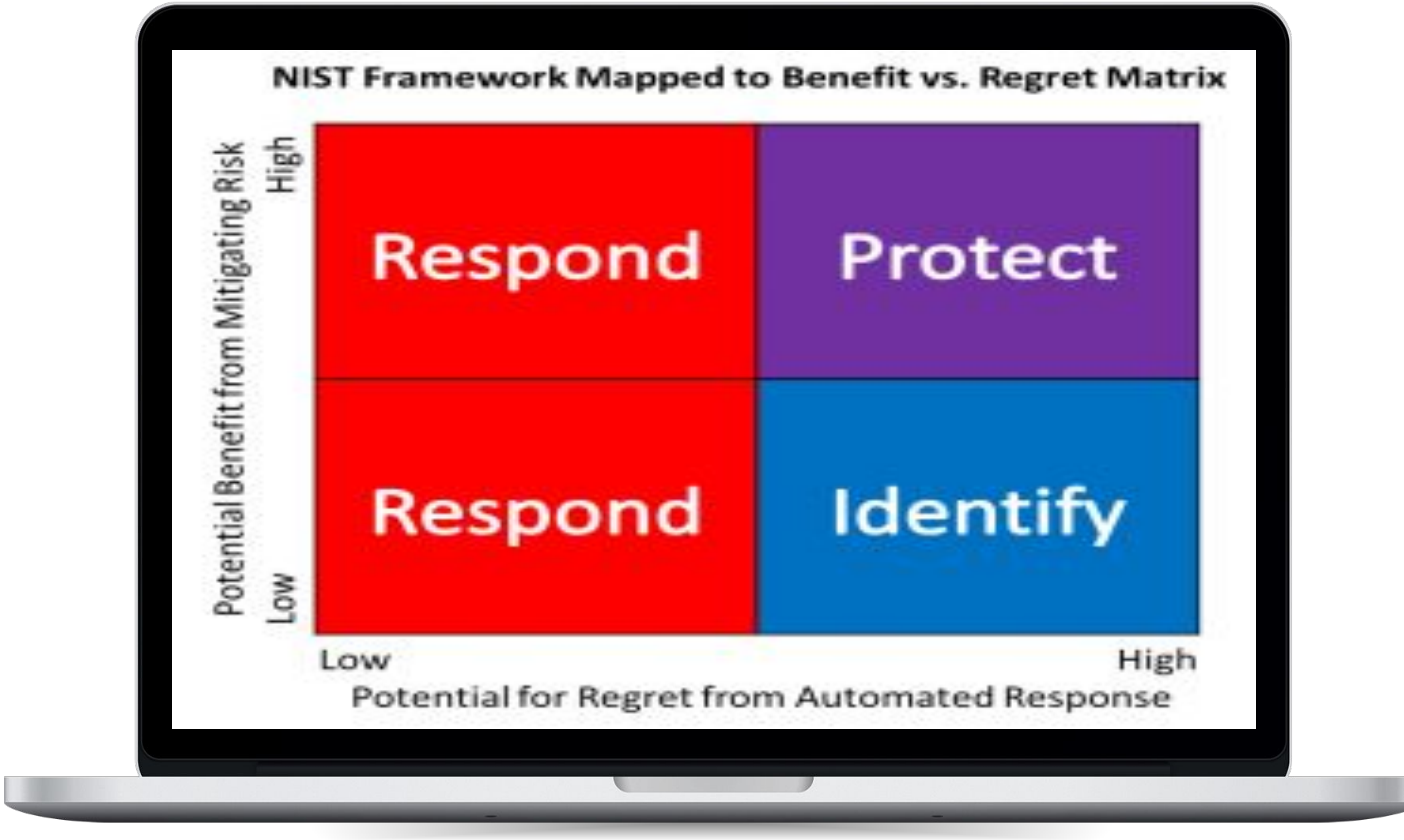
move too fast here, and you will break things and it will cost monies.

:(


Automated Response Action Benefit vs. Regret Matrix
Potential Benefit from Mitigating Risk
High
Low
CAUTION
DO NOT OPERATE THIS MACHINE WITHOUT GUARDS IN PLACE
Low
High
Potential for Regret from Automated Response

now with 100% more NIST

benefit vs regret



NIST Framework Mapped to Benefit vs. Regret Matrix

Respond

Protect

Respond

Identify

Potential Benefit from Mitigating Risk
High
Low
Low
High
Potential for Regret from Automated Response

*SOAR*ing into secure

USE CASE: Process Employee-Submitted Phishing Emails

Report Phishing
Deleting helps you, reporting helps everyone.
USERNAME
PASSWORD
Forward suspicious emails to
phishing@my.org

USE CASE: Process Employee-Submitted Phishing Emails

Step 1: Intake and Triage

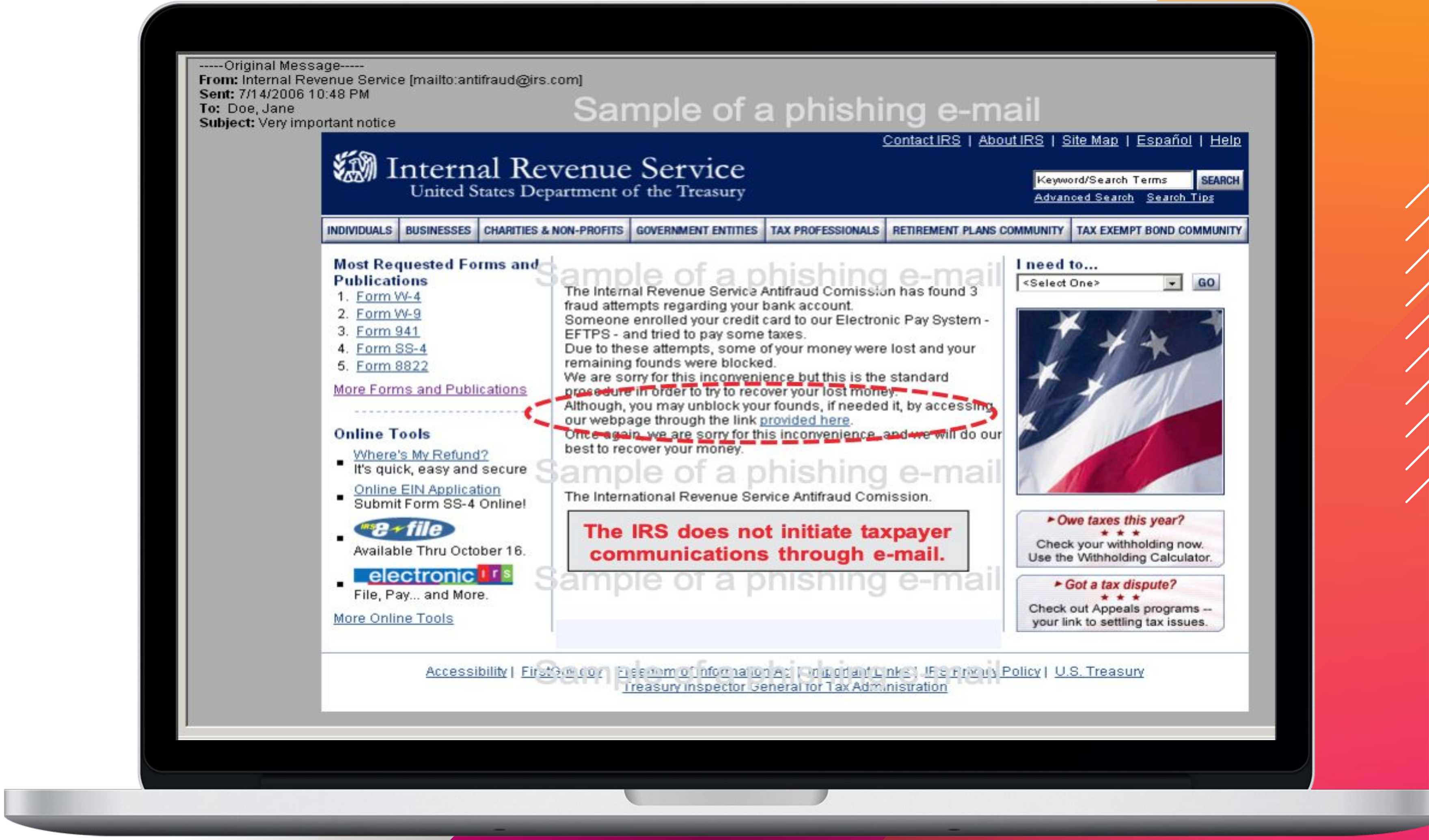
- Monitor mailbox for new samples
- Compare to known samples
- Match / link known samples
- Investigate new samples

splunk> turn data into doing

USE CASE: Process Employee-Submitted Phishing Emails

Step 2: Extract Artifacts and Indicators

- Domain names
- IP Addresses
- URLs
- File attachments



-----Original Message-----
From: Internal Revenue Service [mailto:antifraud@irs.com]
Sent: 7/14/2006 10:48 PM
To: Doe, Jane
Subject: Very important notice

Most Requested Forms and Publications

1. Form W-4
2. Form W-9
3. Form 941
4. Form SS-4
5. Form 8822

More Forms and Publications

Online Tools

- Where's My Refund?
  It's quick, easy and secure
- Online EIN Application
  Submit Form SS-4 Online!
- IRS e-file
  Available Thru October 16.
- electronic irs
  File, Pay... and More.

More Online Tools

The Internal Revenue Service Antifraud Comission has found 3 fraud attempts regarding your bank account.
Someone enrolled your credit card to our Electronic Pay System - EFTPS - and tried to pay some taxes.
Due to these attempts, some of your money were lost and your remaining founds were blocked.
We are sorry for this inconvenience but this is the standard procedure in order to try to recover your lost money.
Although, you may unblock your founds, if needed it, by accessing our webpage through the link provided here.
Once again, we are sorry for this inconvenience, and we will do our best to recover your money.

The International Revenue Service Antifraud Comission.

The IRS does not initiate taxpayer communications through e-mail.

I need to...

<Select One> GO

Owe taxes this year?
★ ★ ★
Check your withholding now.
Use the Withholding Calculator.

Got a tax dispute?
★ ★ ★
Check out Appeals programs -- your link to settling tax issues.

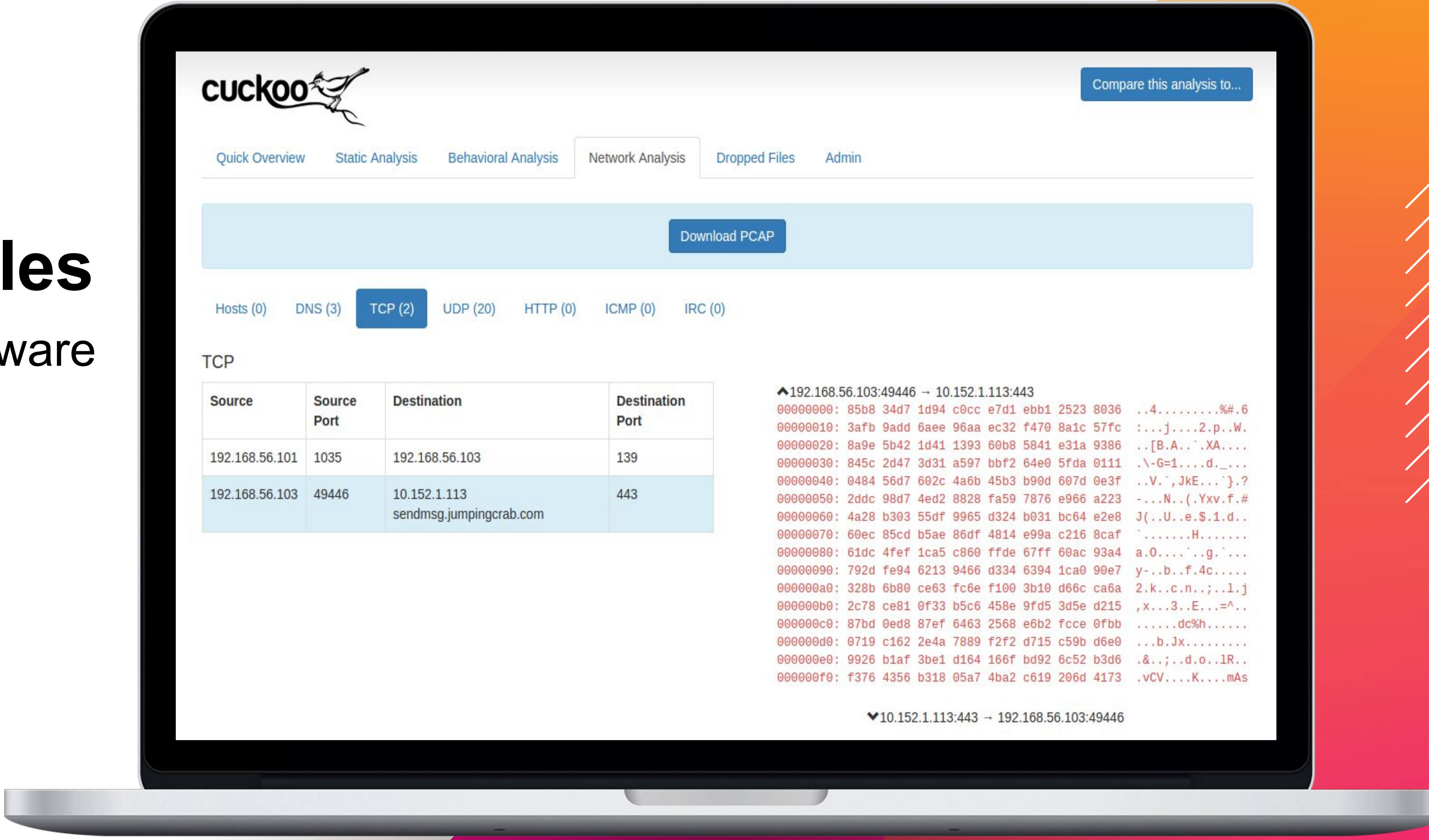
Accessibility | FirstGov.gov | Freedom of Information Act | Important Links | IRS Privacy Policy | U.S. Treasury
Treasury Inspector General for Tax Administration

splunk> turn data into doing

USE CASE: Process Employee-Submitted Phishing Emails

Step 3: Detonate Files

- Detonate samples in a malware sandbox (on Prem / Cloud)
- Review results



TCP

Source	Source Port	Destination	Destination Port
192.168.56.101	1035	192.168.56.103	139
192.168.56.103	49446	10.152.1.113 sendmsg.jumpingcrab.com	443

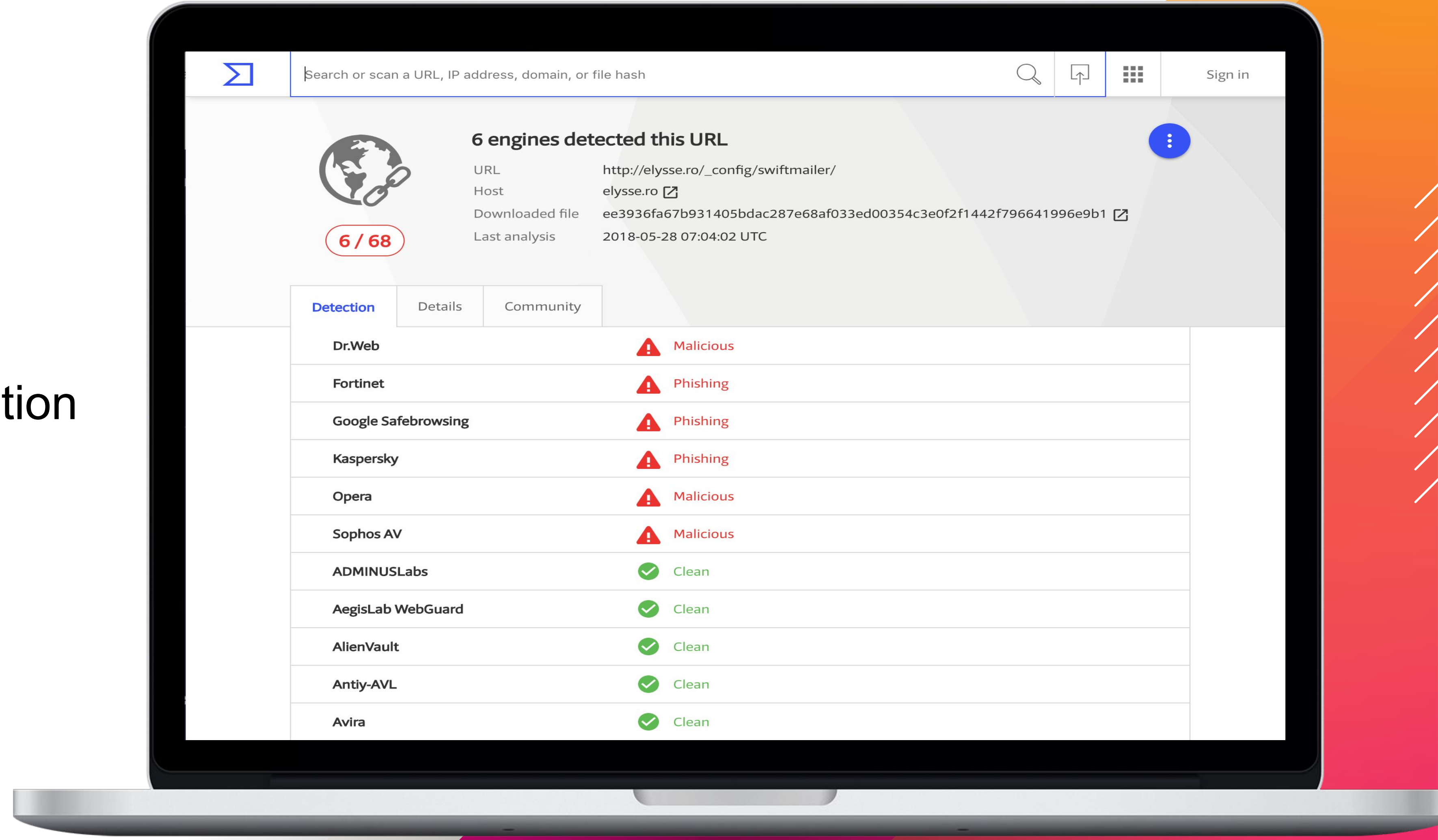
```
^192.168.56.103:49446 → 10.152.1.113:443
00000000: 85b8 34d7 1d94 c0cc e7d1 ebb1 2523 8036  ..4.........%#.6
00000010: 3afb 9add 6aee 96aa ec32 f470 8a1c 57fc  :...j....2.p..W.
00000020: 8a9e 5b42 1d41 1393 60b8 5841 e31a 9386  ..[B.A..`.XA....
00000030: 845c 2d47 3d31 a597 bbf2 64e0 5fda 0111  .\-G=1....d._...
00000040: 0484 56d7 602c 4a6b 45b3 b90d 607d 0e3f  ..V.`,JkE...`}.?
00000050: 2ddc 98d7 4ed2 8828 fa59 7876 e966 a223  -...N..(.Yxv.f.#
00000060: 4a28 b303 55df 9965 d324 b031 bc64 e2e8  J(..U..e.$.1.d..
00000070: 60ec 85cd b5ae 86df 4814 e99a c216 8caf  `.......H.......
00000080: 61dc 4fef 1ca5 c860 ffde 67ff 60ac 93a4  a.O....`..g.`...
00000090: 792d fe94 6213 9466 d334 6394 1ca0 90e7  y-..b..f.4c.....
000000a0: 328b 6b80 ce63 fc6e f100 3b10 d66c ca6a  2.k..c.n..;..l.j
000000b0: 2c78 ce81 0f33 b5c6 458e 9fd5 3d5e d215  ,x...3..E...=^..
000000c0: 87bd 0ed8 87ef 6463 2568 e6b2 fcce 0fbb  ......dc%h......
000000d0: 0719 c162 2e4a 7889 f2f2 d715 c59b d6e0  ...b.Jx.........
000000e0: 9926 b1af 3be1 d164 166f bd92 6c52 b3d6  .&..;..d.o..lR..
000000f0: f376 4356 b318 05a7 4ba2 c619 206d 4173  .vCV....K....mAs
```

˅10.152.1.113:443 → 192.168.56.103:49446

USE CASE: Process Employee-Submitted Phishing Emails

Step 4: Check URL Reputation

- Lookup each URL’s reputation
- Review results



6 engines detected this URL

6 / 68

URL	http://elysse.ro/_config/swiftmailer/
Host	elysse.ro
Downloaded file	ee3936fa67b931405bdac287e68af033ed00354c3e0f2f1442f796641996e9b1
Last analysis	2018-05-28 07:04:02 UTC

Dr.Web	Malicious
Fortinet	Phishing
Google Safebrowsing	Phishing
Kaspersky	Phishing
Opera	Malicious
Sophos AV	Malicious
ADMINUSLabs	Clean
AegisLab WebGuard	Clean
AlienVault	Clean
Antiy-AVL	Clean
Avira	Clean

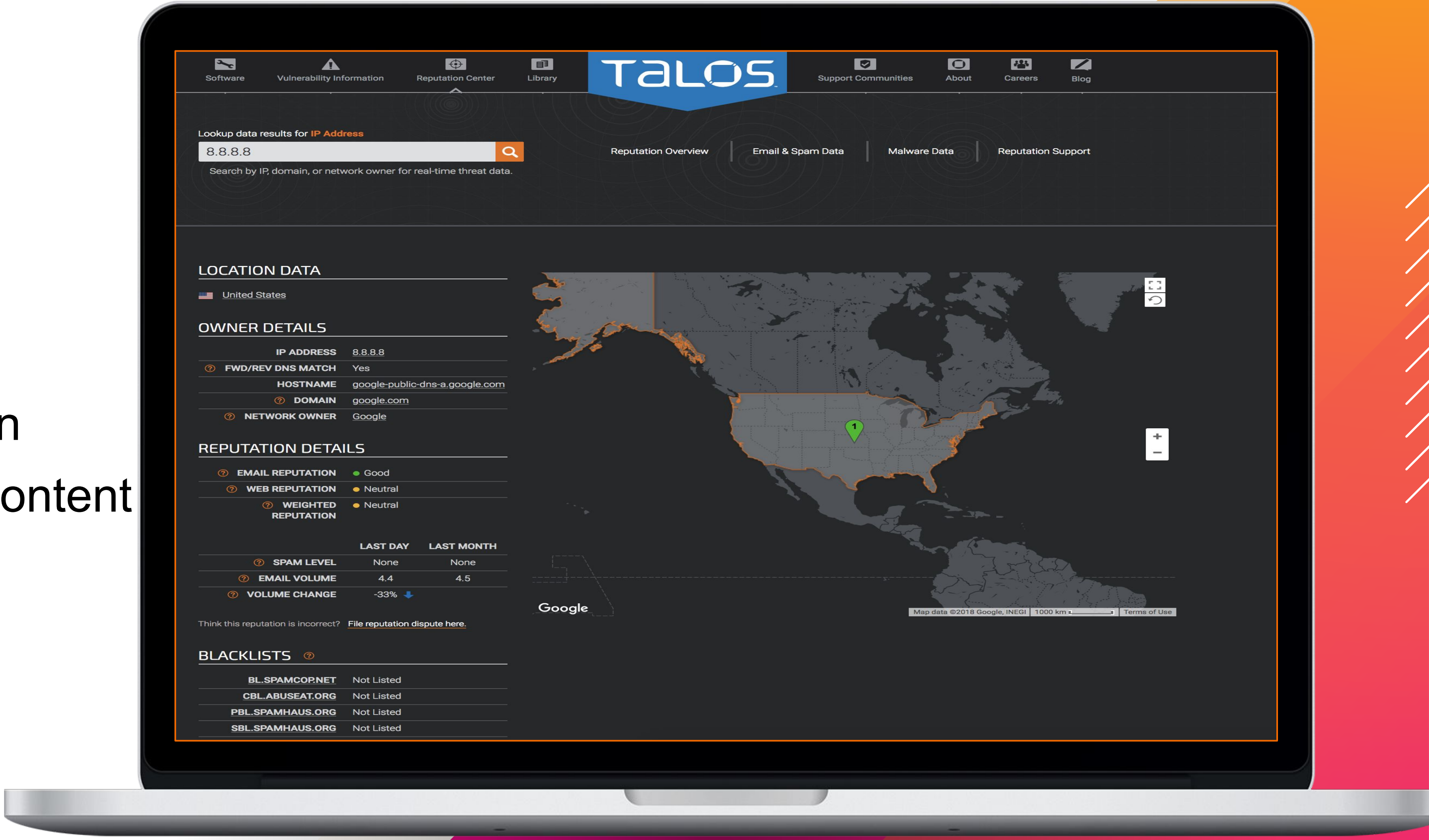
VirusTotal

splunk> turn data into doing

USE CASE: Process Employee-Submitted Phishing Emails

Step 5: Check IP Reputation

- Lookup each IP’s reputation
- Sender / MTA / Message Content
- Review results



Lookup data results for IP Address

8.8.8.8

Search by IP, domain, or network owner for real-time threat data.

LOCATION DATA

United States

OWNER DETAILS

IP ADDRESS	8.8.8.8
FWD/REV DNS MATCH	Yes
HOSTNAME	google-public-dns-a.google.com
DOMAIN	google.com
NETWORK OWNER	Google

REPUTATION DETAILS

EMAIL REPUTATION	● Good
WEB REPUTATION	● Neutral
WEIGHTED REPUTATION	● Neutral

	LAST DAY	LAST MONTH
SPAM LEVEL	None	None
EMAIL VOLUME	4.4	4.5
VOLUME CHANGE	-33% ↓	

Think this reputation is incorrect? File reputation dispute here.

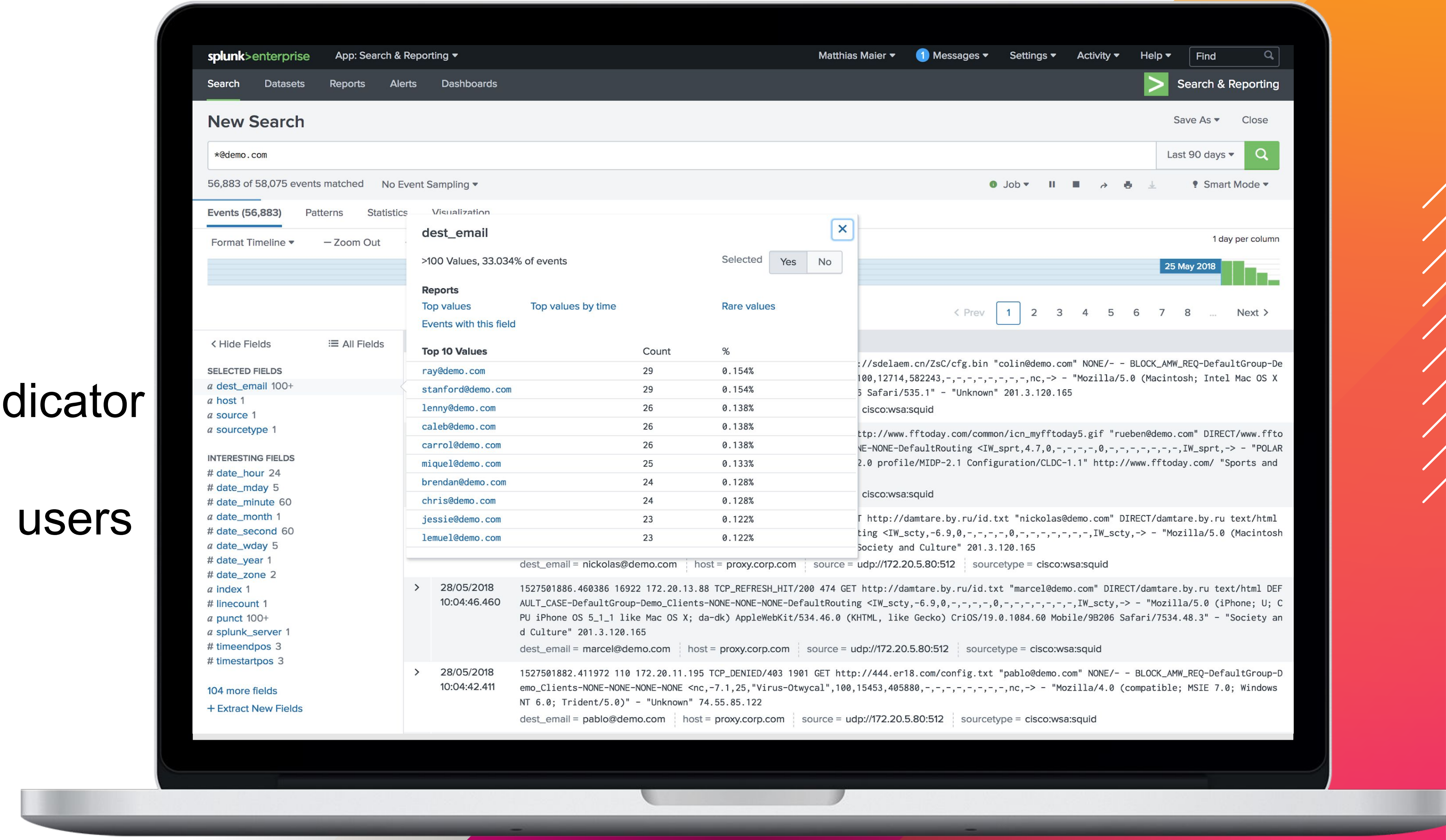
BLACKLISTS

BL.SPAMCOP.NET	Not Listed
CBL.ABUSEAT.ORG	Not Listed
PBL.SPAMHAUS.ORG	Not Listed
SBL.SPAMHAUS.ORG	Not Listed

USE CASE: Process Employee-Submitted Phishing Emails

Step 6: Hunt for Indicators

- Search security data for indicator matches
- Identify affected hosts and users
- Document findings



New Search

`*@demo.com`

56,883 of 58,075 events matched   No Event Sampling

SELECTED FIELDS
- a dest_email 100+
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS
- # date_hour 24
- # date_mday 5
- # date_minute 60
- a date_month 1
- # date_second 60
- a date_wday 5
- # date_year 1
- # date_zone 2
- a index 1
- # linecount 1
- a punct 100+
- a splunk_server 1
- # timeendpos 3
- # timestartpos 3

dest_email

>100 Values, 33.034% of events   Selected: Yes | No

Reports

Top values   Top values by time   Rare values

Events with this field

Top 10 Values	Count	%
ray@demo.com	29	0.154%
stanford@demo.com	29	0.154%
lenny@demo.com	26	0.138%
caleb@demo.com	26	0.138%
carrol@demo.com	26	0.138%
miquel@demo.com	25	0.133%
brendan@demo.com	24	0.128%
chris@demo.com	24	0.128%
jessie@demo.com	23	0.122%
lemuel@demo.com	23	0.122%

```
://sdelaem.cn/ZsC/cfg.bin "colin@demo.com" NONE/- - BLOCK_AMW_REQ-DefaultGroup-De
100,12714,582243,-,-,-,-,-,-,-,-,nc,-> - "Mozilla/5.0 (Macintosh; Intel Mac OS X
5 Safari/535.1" - "Unknown" 201.3.120.165
cisco:wsa:squid

ttp://www.fftoday.com/common/icn_myfftoday5.gif "rueben@demo.com" DIRECT/www.ffto
NE-NONE-DefaultRouting <IW_sprt,4.7,0,-,-,-,-,0,-,-,-,-,-,-,-,IW_sprt,-> - "POLAR
2.0 profile/MIDP-2.1 Configuration/CLDC-1.1" http://www.fftoday.com/ "Sports and
cisco:wsa:squid

T http://damtare.by.ru/id.txt "nickolas@demo.com" DIRECT/damtare.by.ru text/html
ting <IW_scty,-6.9,0,-,-,-,-,0,-,-,-,-,-,-,-,IW_scty,-> - "Mozilla/5.0 (Macintosh
Society and Culture" 201.3.120.165
dest_email = nickolas@demo.com | host = proxy.corp.com | source = udp://172.20.5.80:512 | sourcetype = cisco:wsa:squid

> 28/05/2018    1527501886.460386 16922 172.20.13.88 TCP_REFRESH_HIT/200 474 GET http://damtare.by.ru/id.txt "marcel@demo.com" DIRECT/damtare.by.ru text/html DEF
  10:04:46.460  AULT_CASE-DefaultGroup-Demo_Clients-NONE-NONE-NONE-DefaultRouting <IW_scty,-6.9,0,-,-,-,-,0,-,-,-,-,-,-,-,IW_scty,-> - "Mozilla/5.0 (iPhone; U; C
                PU iPhone OS 5_1_1 like Mac OS X; da-dk) AppleWebKit/534.46.0 (KHTML, like Gecko) CriOS/19.0.1084.60 Mobile/9B206 Safari/7534.48.3" - "Society an
                d Culture" 201.3.120.165
                dest_email = marcel@demo.com | host = proxy.corp.com | source = udp://172.20.5.80:512 | sourcetype = cisco:wsa:squid

> 28/05/2018    1527501882.411972 110 172.20.11.195 TCP_DENIED/403 1901 GET http://444.er18.com/config.txt "pablo@demo.com" NONE/- - BLOCK_AMW_REQ-DefaultGroup-D
  10:04:42.411  emo_Clients-NONE-NONE-NONE-NONE <nc,-7.1,25,"Virus-Otwycal",100,15453,405880,-,-,-,-,-,-,-,-,nc,-> - "Mozilla/4.0 (compatible; MSIE 7.0; Windows
                NT 6.0; Trident/5.0)" - "Unknown" 74.55.85.122
                dest_email = pablo@demo.com | host = proxy.corp.com | source = udp://172.20.5.80:512 | sourcetype = cisco:wsa:squid
```

splunk> turn data into doing

USE CASE: Process Employee-Submitted Phishing Emails

Step 7: Escalate to Incident Responder

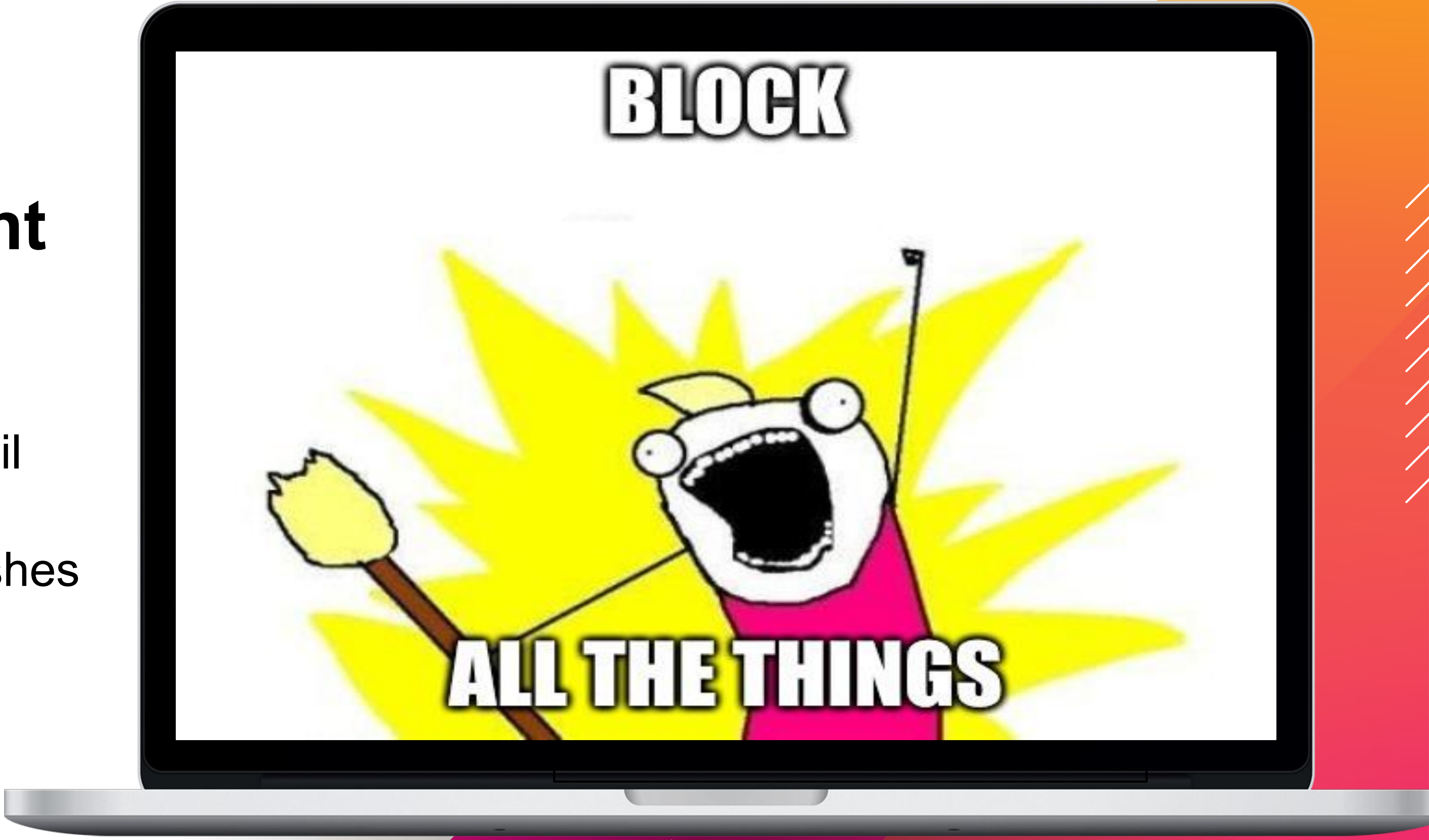
- Create ticket for escalation
- Document all findings

splunk> turn data into doing

USE CASE: Process Employee-Submitted Phishing Emails

Step 8: Containment

- Block IP (Firewall)
- Block URL (Web Proxy)
- Block E-Mail Domain (Email Security)
- Block URLs / IPs / File Hashes (Endpoints)



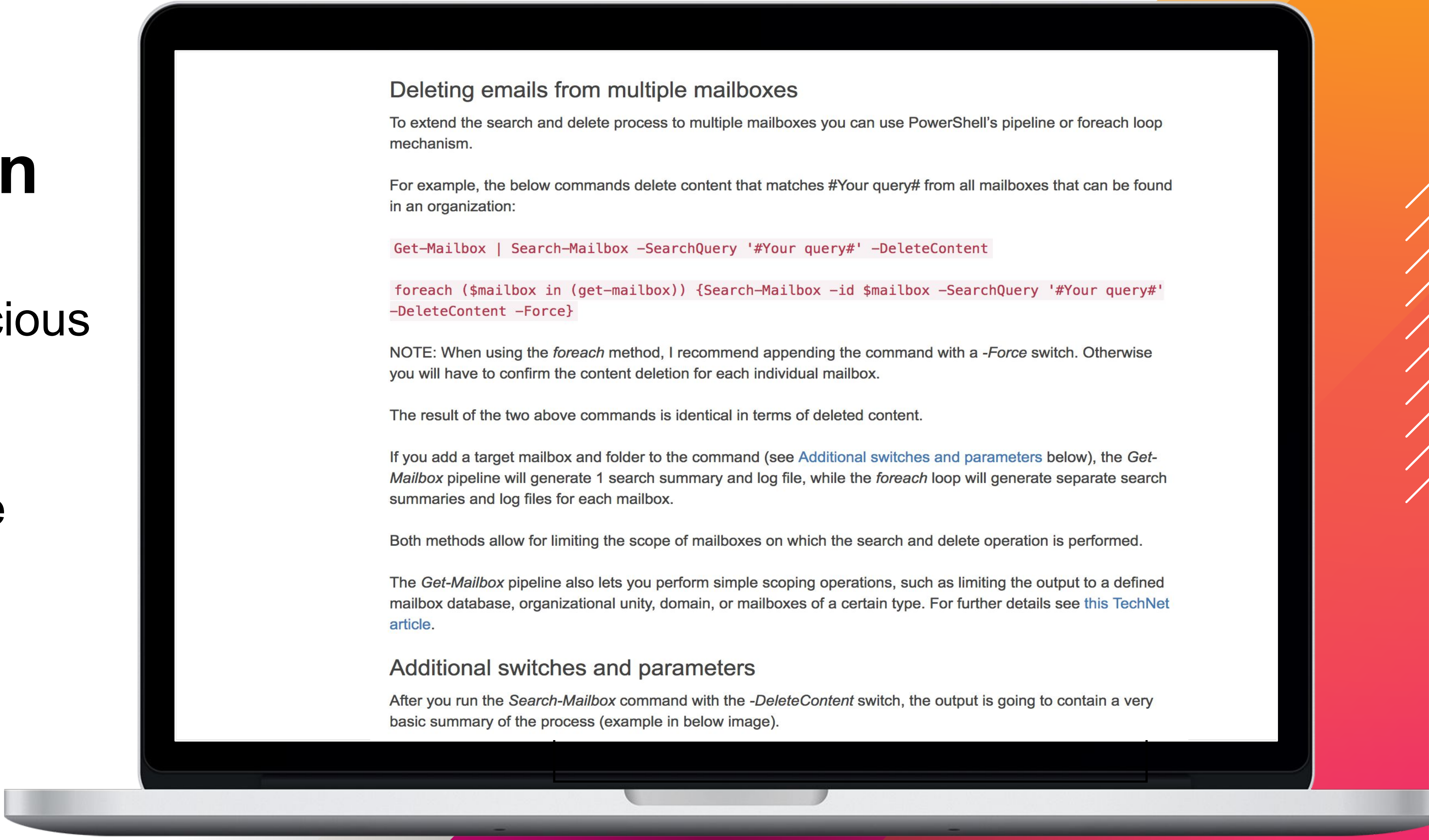
paloalto NETWORKS CISCO Symantec

splunk> turn data into doing

USE CASE: Process Employee-Submitted Phishing Emails

Step 9: Remediation (Email Server)

- Search mailboxes for malicious emails
- Validate emails returned
- Delete emails from multiple mailboxes
- Create tickets for work as necessary



Deleting emails from multiple mailboxes

To extend the search and delete process to multiple mailboxes you can use PowerShell's pipeline or foreach loop mechanism.

For example, the below commands delete content that matches #Your query# from all mailboxes that can be found in an organization:

```
Get-Mailbox | Search-Mailbox -SearchQuery '#Your query#' -DeleteContent
```

```
foreach ($mailbox in (get-mailbox)) {Search-Mailbox -id $mailbox -SearchQuery '#Your query#'
-DeleteContent -Force}
```

NOTE: When using the *foreach* method, I recommend appending the command with a *-Force* switch. Otherwise you will have to confirm the content deletion for each individual mailbox.

The result of the two above commands is identical in terms of deleted content.

If you add a target mailbox and folder to the command (see Additional switches and parameters below), the *Get-Mailbox* pipeline will generate 1 search summary and log file, while the *foreach* loop will generate separate search summaries and log files for each mailbox.

Both methods allow for limiting the scope of mailboxes on which the search and delete operation is performed.

The *Get-Mailbox* pipeline also lets you perform simple scoping operations, such as limiting the output to a defined mailbox database, organizational unity, domain, or mailboxes of a certain type. For further details see this TechNet article.

Additional switches and parameters

After you run the *Search-Mailbox* command with the *-DeleteContent* switch, the output is going to contain a very basic summary of the process (example in below image).

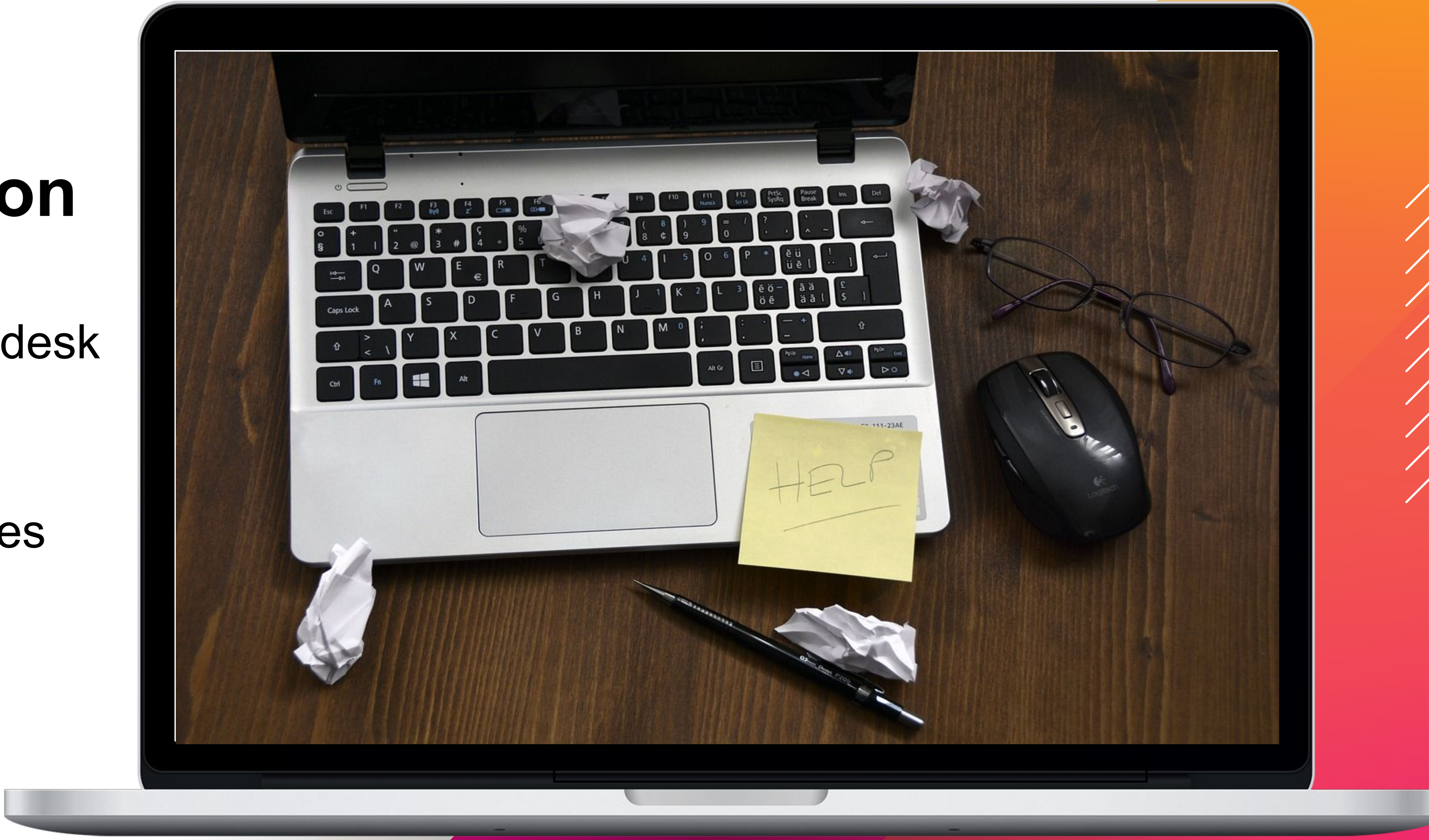
Exchange

splunk> turn data into doing

USE CASE: Process Employee-Submitted Phishing Emails

Step 10: Remediation (Endpoints)

- Create ticket for IT service desk
- Service desk cleans (or reimages) host
- Incident Responder validates cleanup was effective
- Ticket closed



Carbon Black. JIRA

splunk> turn data into doing

USE CASE: Process Employee-Submitted Phishing Emails

Systems involved

- Malware sandbox
- Mail server / email security
- Threat intelligence services
- SIEM
- Network firewall
- Proxy server
- Endpoint security
- Ticketing system
- Paper notes / local system

Can you investigate this phishing mail?
APPs
Uh, yeah... Give me a minute...
VM_123
VM_046
VM_215

USE CASE: Process Employee-Submitted Phishing Emails

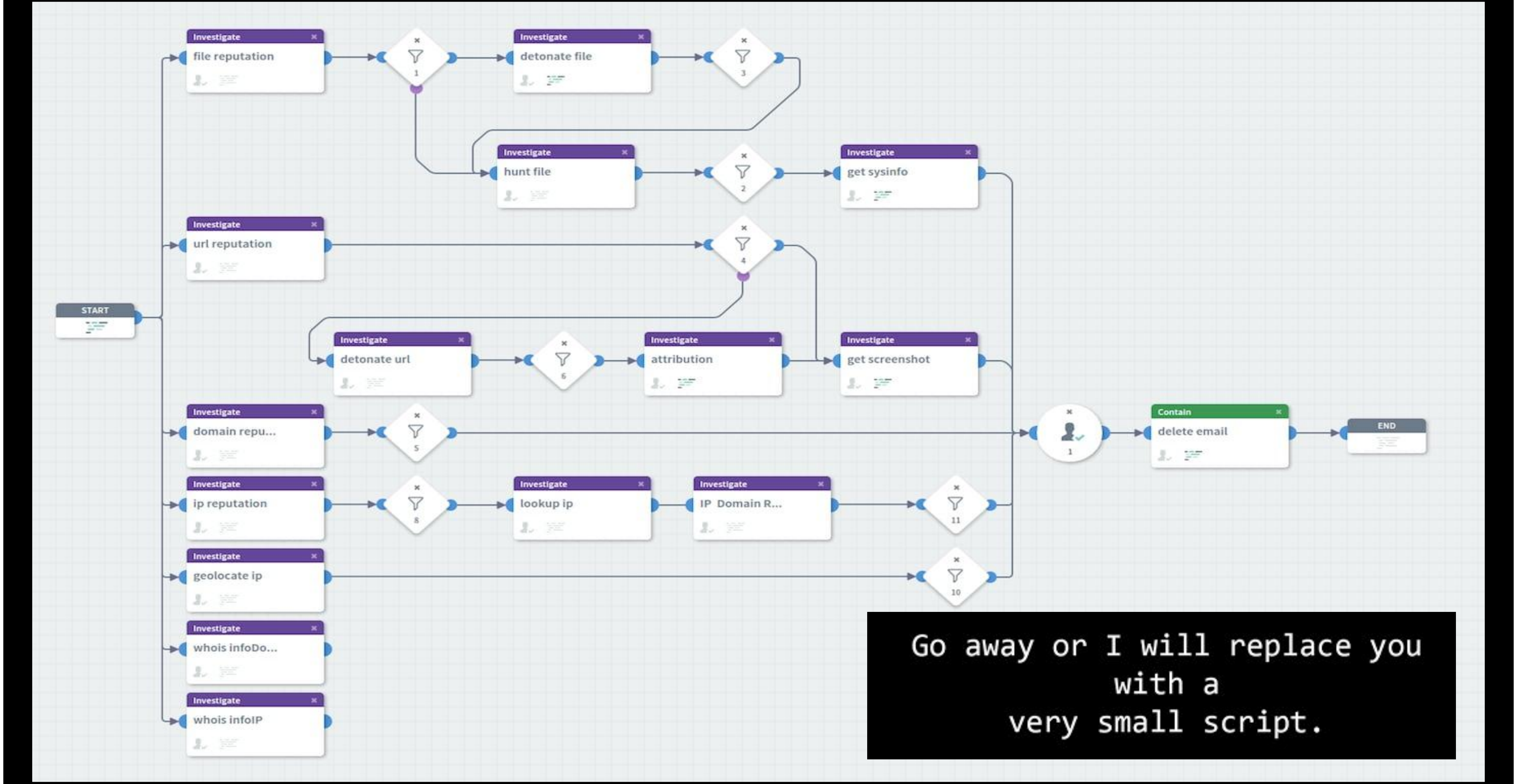
TIME SPENT

45m

JOB SATISFACTION OF SECURITY ANALYST

☹

can we automate phishing email response?



Go away or I will replace you
with a
very small script.

But Wait, THERE'S MORE!
™

posture via people

splunk> turn data into doing™

the strongest link

ecosystem

leverage SMEs

partnerships

public/private sector collaborations that increase cyber posture

community growth

build the next generation of defenders

culture not compliance

- annual training solves nothing
- name/shame creates divide
- interactive training builds community

CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY

MULTI-STATE CIS ISAC

Center for Internet Security®

Creating Confidence in the Connected World.™

SURGe

by Splunk

splunk> turn data into doing™

splunk> .conf21

SURGe: Blue Collar for the Blue Team

#splunkconf21

splunk> turn data into doing

#coffeetalkwithSURGe

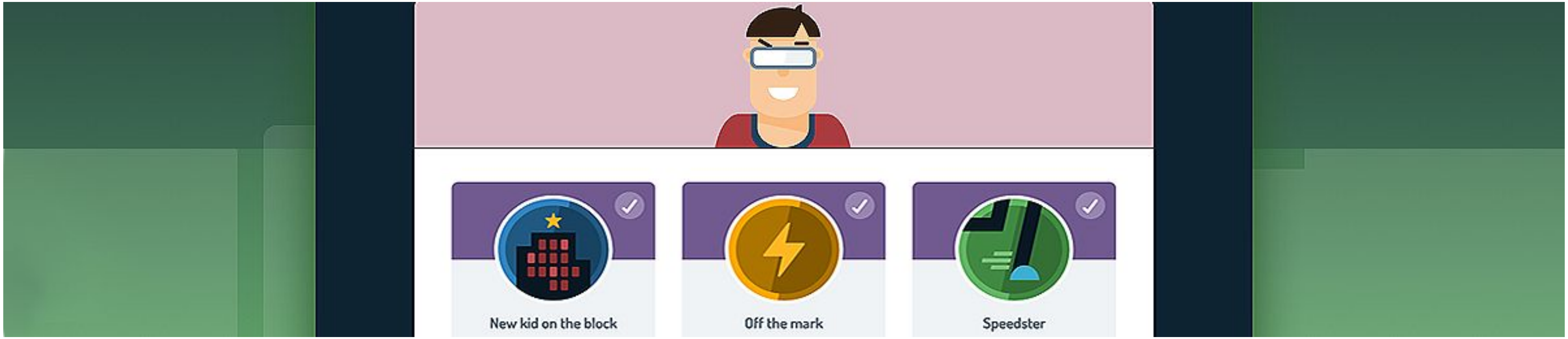
- wombat facts
- trusted security information
- practical security research

1mo •

Coffee Talk with the Splunk Security Gang

Join Ryan Kovar and Mick Baccio for another Splunk security gang ...see more

Previously live



New kid on the block

Off the mark

Speedster

CyberStart America 2021

splunk> turn data into doing™

Delaware DigiGirlz Day VIRTUAL

May 4, 2021

Bsides Delaware
Keeping with the Virtual – November 12-13, 2021
FE.
AN TOO.

be nice.

splunk> turn data into doing™

take home

- it will not get easier
- eat your cyber vegetables
- leverage technology
- people are the strongest link

Thank You

splunk> turn data into doing™