

Storytelling 4 Cybersecurity



in/rebeccaharness



@rebeccaharness

1

Becca's Backstory

- 1981 – First Commodore (VIC-20)
- 1991 – First PC (AMD 386 DX 40)
- Marketing & Communications Major
- 1997 – Landed in Information Technology
- 2010 – Transitioned to Cybersecurity
- 2019 – CISO: Saint Louis University & SLUCare

2



Audience Poll

3

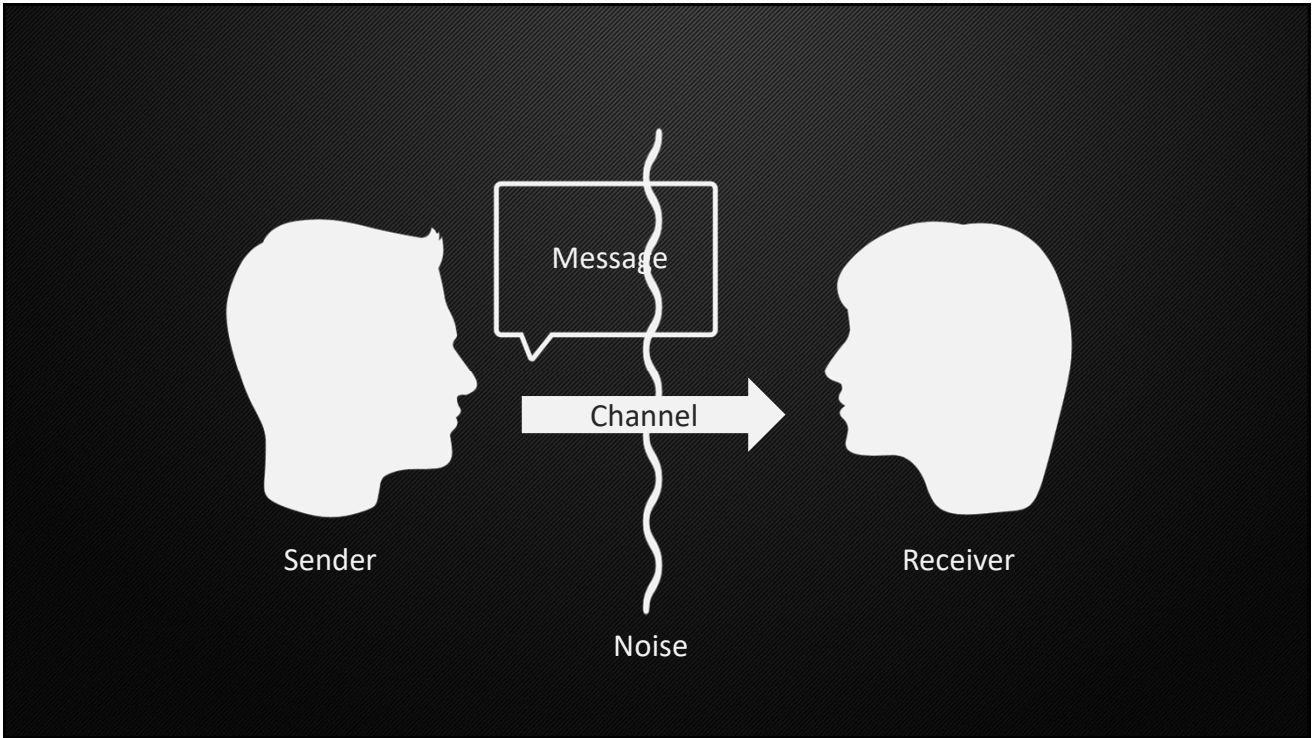


*It is critically important
for others to listen to my
cybersecurity concerns.*

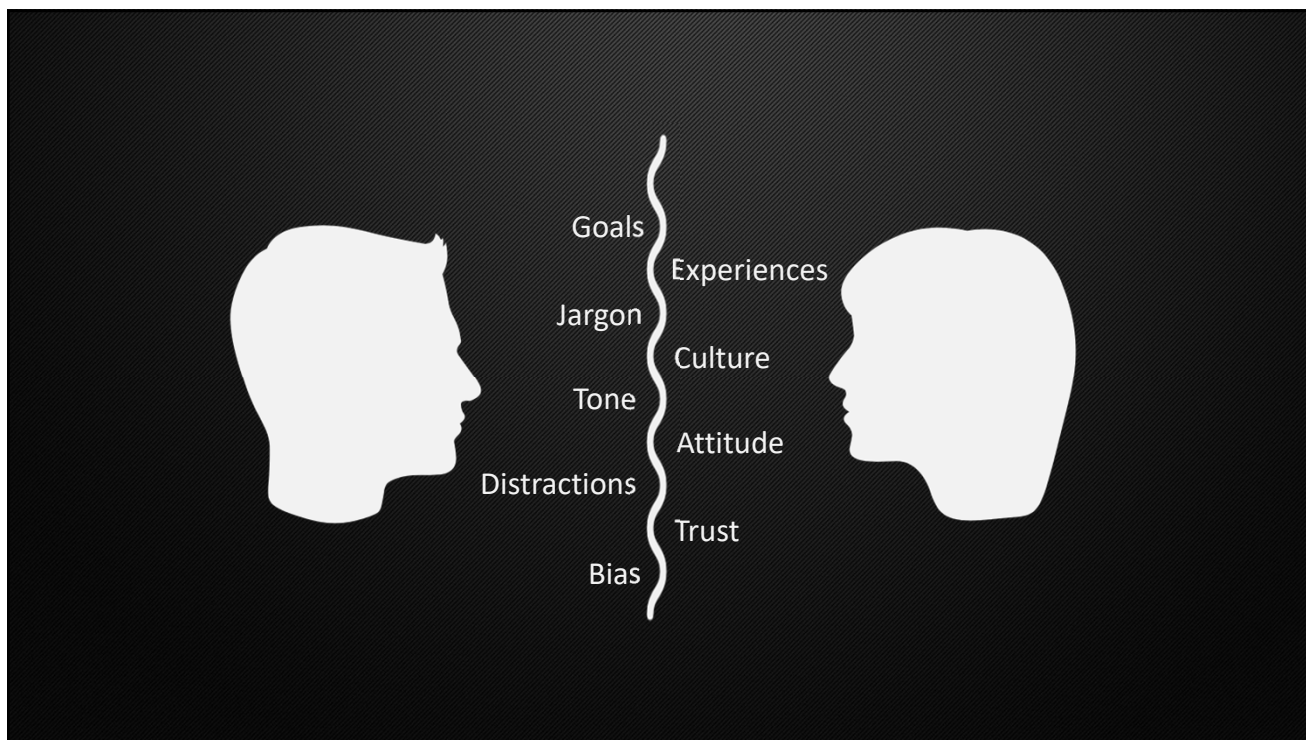
4

Noise.

5



6

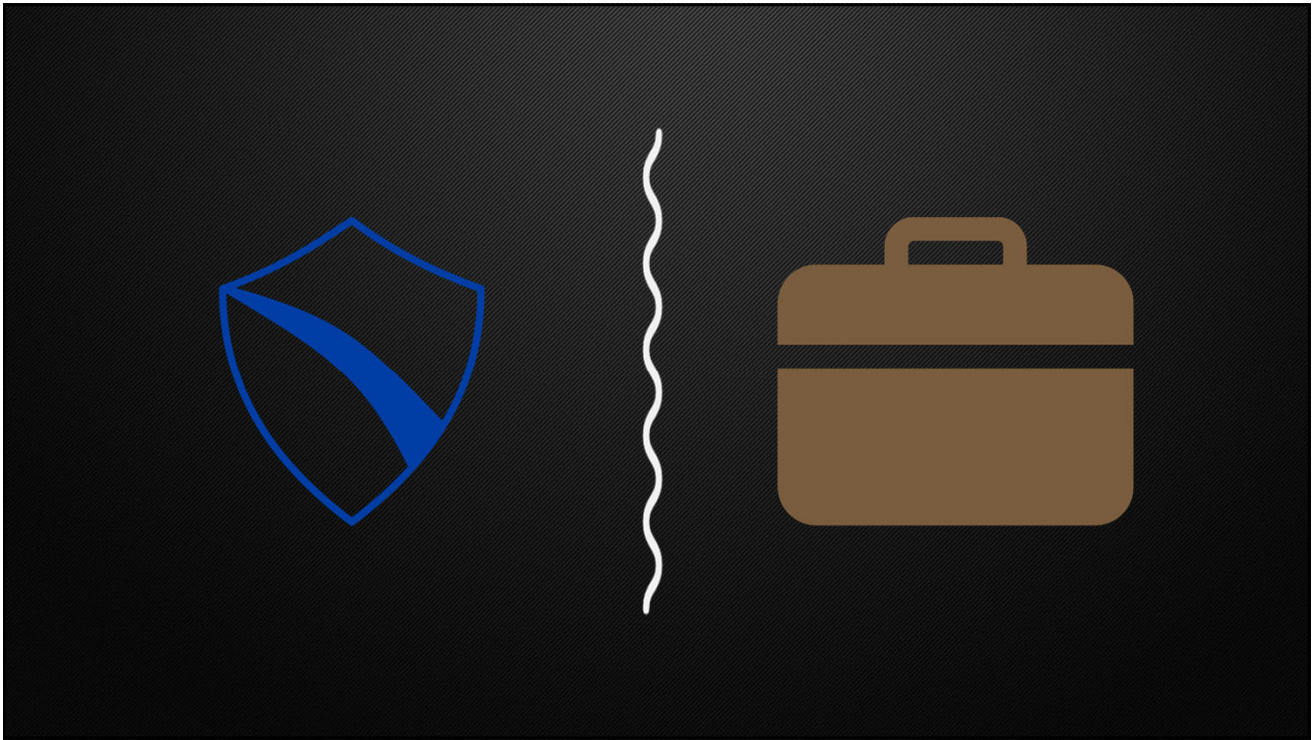


7

“The goal of all communication is understanding. Anything that interferes with this understanding is called noise.”

- Rosie Bunnow, University of Wisconsin

8



9

What's Our Noise?

10

Electrical grid, power plants, pipelines vulnerable to cyber attack, security expert says

Updated Oct 23; Posted Oct 23

Signal Desktop Leaves Message Decryption Key in Plain Sight

By Lawrence Abrams

October 23, 2018 10:39 AM

Cathay Pacific flags data breach affecting 9.4 million passengers

Missouri health department alerts of security breach

UPDATED 5:16 PM, OCTOBER 26, 2018, BY ASSOCIATED PRESS. UPDATED AT ORIGINAL OCTOBER 26, 2018

New ransomware can turn your computer into a hacker's tool

Virobot infects devices and then forces them to spread malware via email.

BY ALFRED NG | SEPTEMBER 21, 2018 6:11 AM PDT

UK Supermarket Morrisons Faces Payouts in Data Leak

By The Associated Press

Government Spyware Vendor Left Customer, Victim Data Online for Everyone to See

STATE OF SURVEILLANCE | By Lorenzo Franceschi-Bicchieri | Oct 24 2018, 10:04am

This is how cyber attackers stole £2.26m from Tesco Bank customers

11

CYBER SCOPE v2.7

Network & Infrastructure Security
 Advanced Threat Protection: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky, Avast, Avira, Bitdefender, ESET, Kaspersky, Avast, Avira, Bitdefender, ESET, Kaspersky.
 DNS Protection: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky.
 DNS Security: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky.

Web Security
 Cloud Managed Network: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky.
 Cloud Managed Network: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky.

Endpoint Security
 Endpoint Protection: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky.
 Endpoint Protection: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky.

Application Security
 WAF & Application Security: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky.
 WAF & Application Security: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky.

MSSP
 Traditional MSSP: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky.
 Traditional MSSP: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky.

Data Security
 Encryption: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky.
 Encryption: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky.

Mobile Security
 Mobile Security: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky.
 Mobile Security: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky.

Risk & Compliance
 Risk Assessment & Visibility: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky.
 Risk Assessment & Visibility: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky.

Security Operations & Incident Response
 SIEM: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky.
 SIEM: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky.

Threat Intelligence
 Threat Intelligence: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky.
 Threat Intelligence: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky.

IoT
 IoT Devices: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky.
 IoT Devices: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky.

Messaging Security
 Messaging Security: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky.
 Messaging Security: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky.

Identity & Access Management
 Authentication: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky.
 Authentication: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky.

Digital Risk Management
 Digital Risk Management: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky.
 Digital Risk Management: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky.

Security Consulting & Services
 Security Consulting & Services: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky.
 Security Consulting & Services: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky.

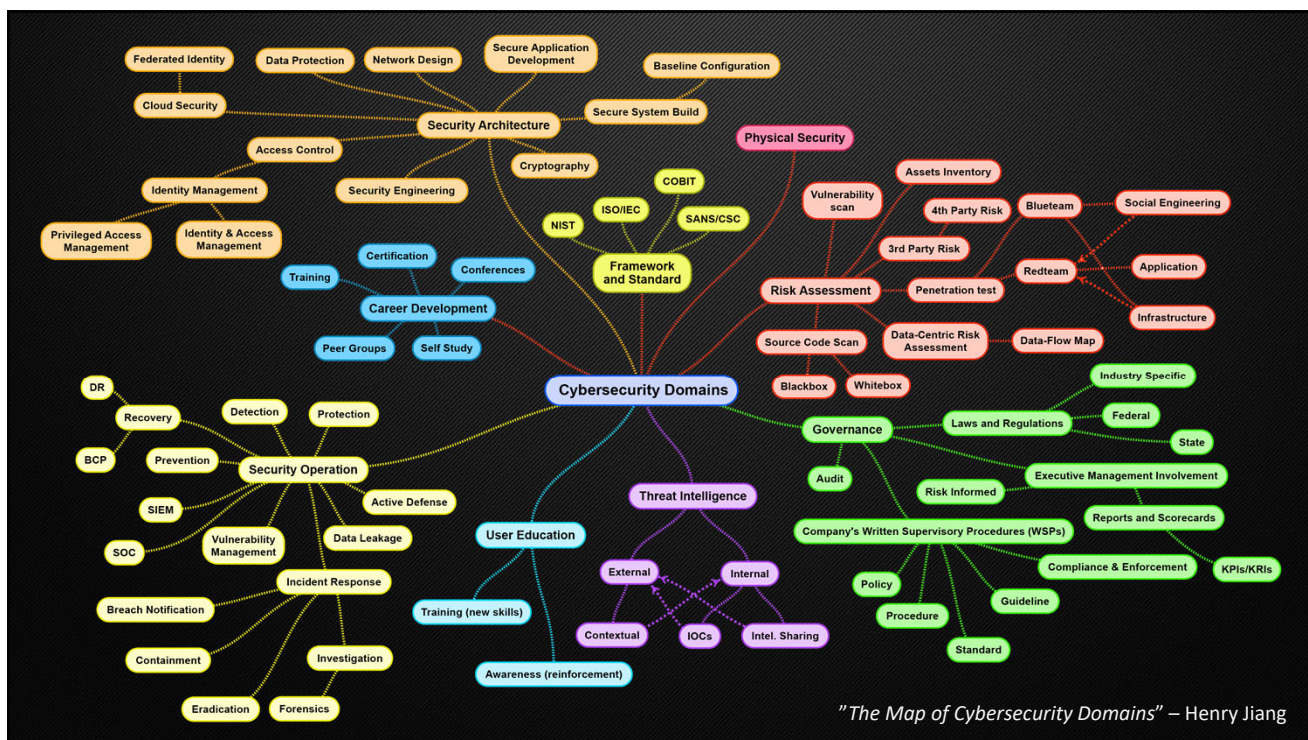
Cloud Security
 Cloud Security: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky.
 Cloud Security: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky.

CASB
 CASB: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky.
 CASB: Cisco, Palo Alto, Fortinet, Trend Micro, Symantec, McAfee, Sophos, Avast, Avira, Bitdefender, ESET, Kaspersky.

12



13

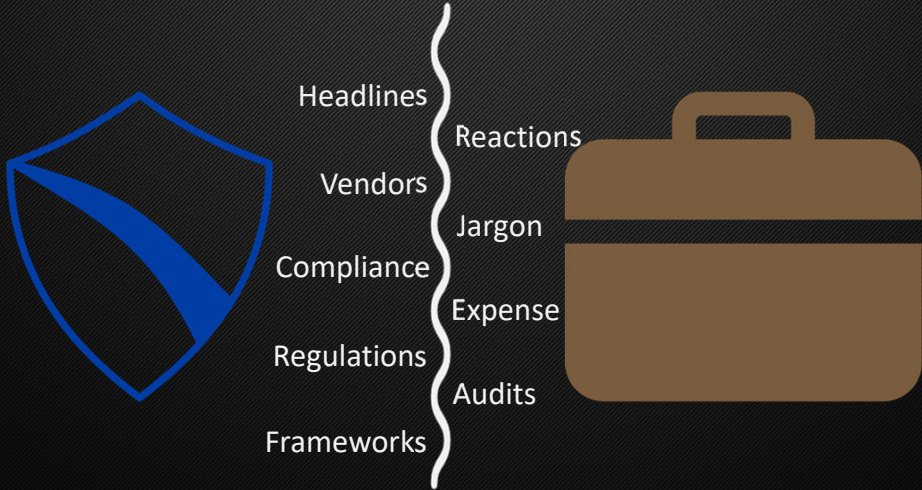


"The Map of Cybersecurity Domains" – Henry Jiang

14

Noise. Noise. Noise.

15



16

Noise
≠
Influence

17

“If you can’t explain something simply, you do not understand it well enough.”

- Albert Einstein (Maybe)

18



Other people listen to my cybersecurity concerns.

19



Perspective

20

“That’s not my job. My job is to make sure they know it’s their job.”

- Executive’s Cybersecurity Viewpoint

21

The Executive’s Playbook

- Deliver Faster
- Minimize Distraction
- Reduce Costs

22

Risk.

23

Threat x Vulnerability x Impact = Risk

24

The Executive's Risk Model

Threat

- Missed Deadline
- Service Failure
- Runaway Costs



Vulnerability

- Resource Utilization
- System Complexity
- Ability to Execute



Impact

- Market Position
- Opportunity Cost
- Loss of Revenue



25

*“Speak to your audience’s risk model...
Not your own.”*

26

Perspective
=
Reality

27



28

Storytelling

29

1. Automate

“Any security control that requires a human to make a decision will ultimately fail .”

30

2. Simplify

“Complexity breeds insecurity.”

31

3. Inform

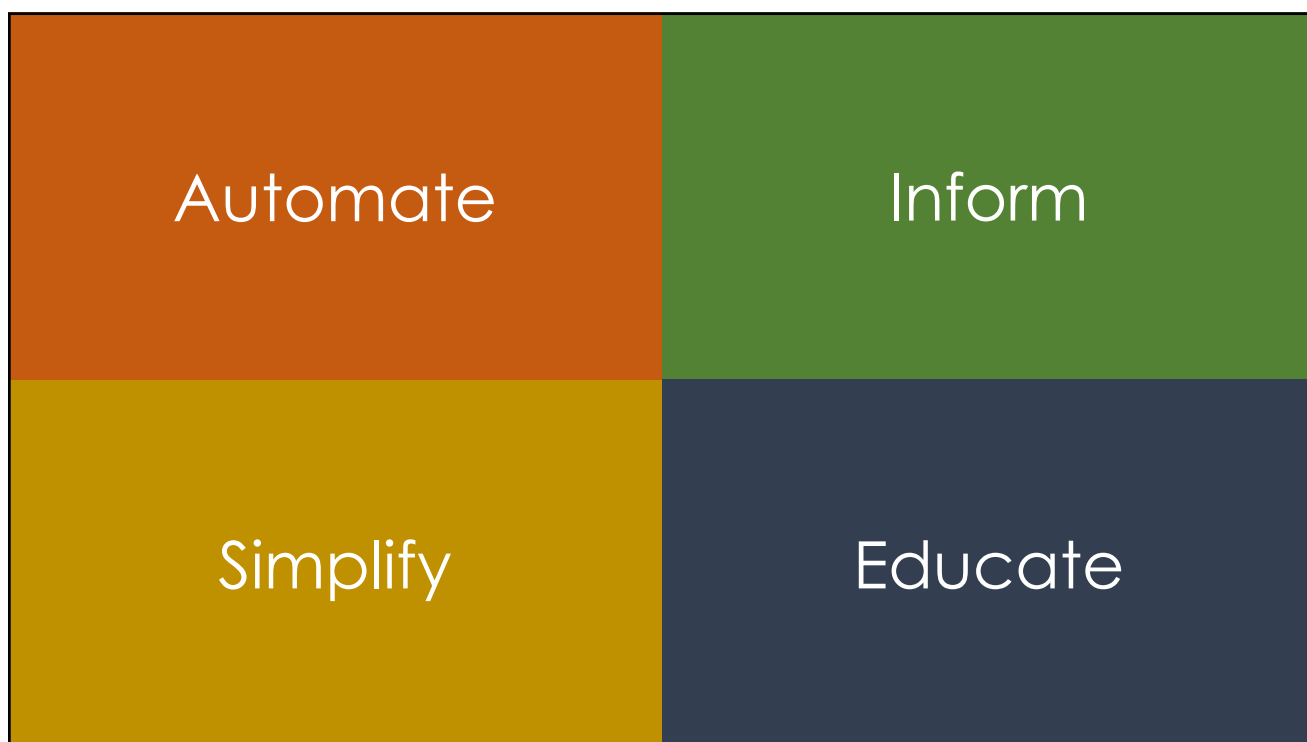
“The timely collection and analysis of information is foundational to security.”

32

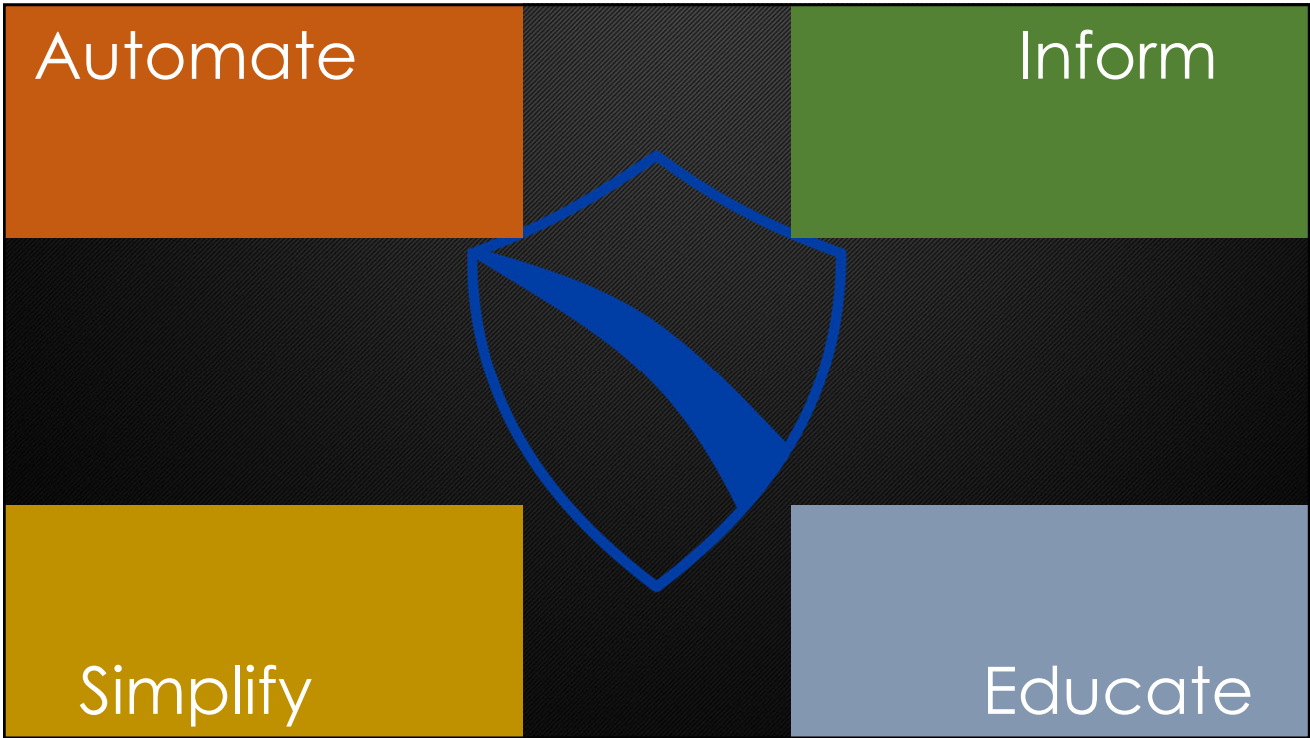
4. Educate

“Transform security from something they have to learn about to something they want to learn about.”

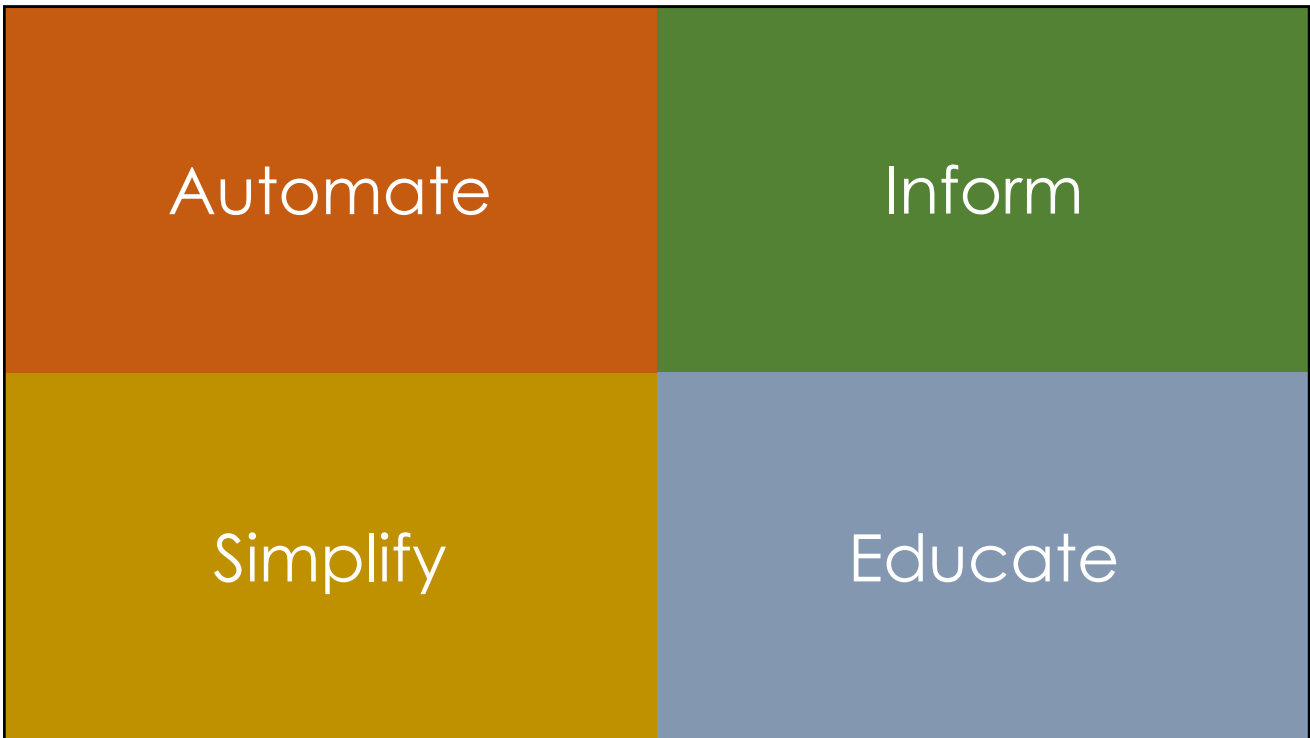
33



34



35



36

Questions?



[in/rebeccaharness](https://www.linkedin.com/in/rebeccaharness)



[@rebeccaharness](https://twitter.com/rebeccaharness)