

RSA[®]Conference2022

San Francisco & Digital | June 6 – 9

SESSION ID: STR2-T01

Detect/Respond/Recover vs. Identify/Protect

Maturity Changes Everything...

Allan Alford

CISO/CTO @ TrustMAPP, Host of The Cyber Ranch Podcast
@AllanAlfordinTX

TRANSFORM



Disclaimer



#RSAC

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

©2022 RSA Conference LLC or its affiliates. The RSA Conference logo and other trademarks are proprietary. All rights reserved.

** Opinions expressed are mine, and not those of any past or present employers, sponsors, or companies in whom I hold equity or with whom I do business.*

We're Going to Turn NIST CSF Inside Out!

- Deconstruct NIST CSF using some real-world models
- Overlay program maturity on top of NIST CSF
- Analyze CSF from both a tech stack and GRC perspective
- Pivot which of the five functions we prioritize
- Employ a few stupid memes on the way
- But first, a quick bit of transparency...

Full Transparency: Past & Present Affiliations



Plus about a bazillion podcast sponsors...

Relax. This presentation is...

- Based on 20+ years of practitioner cybering.
- Influenced a bit by every vendor relationship and affiliation I have, and yet...
- Vendor-agnostic

Why are we here?



Why we are here:



So, we rely on frameworks like...

NIST CSF:

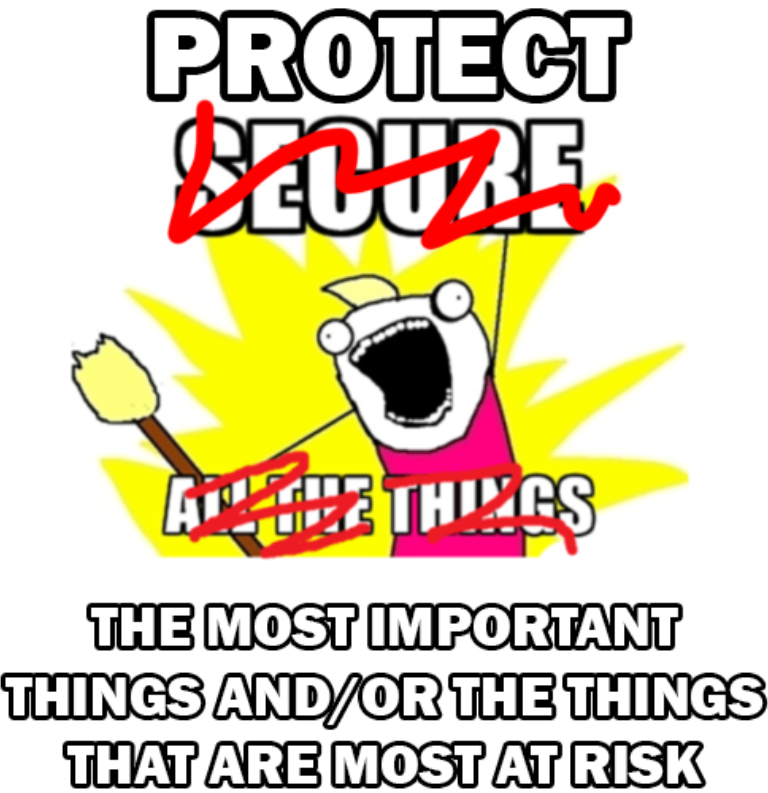
The most important things:

- Identify Hardware Assets (ID.AM-1)
- Identify Software Assets (ID.AM-2)

The things that are most at risk:

- Risk Management (ID.RM-1)

After we Identify, we Protect, right?



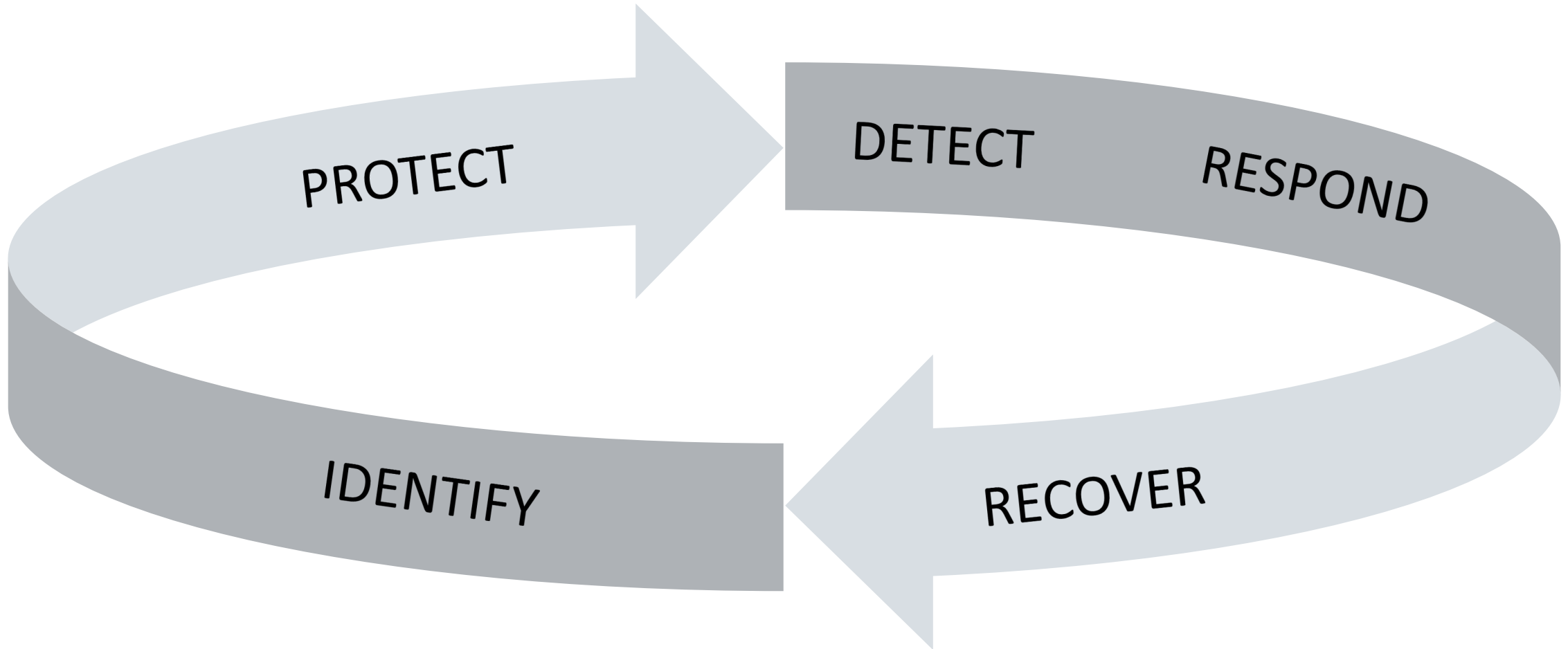
Meet Shiner the Sheepadoodle!



- He protec
- He attac
- But most importantly
- He doesn't secure anything!

The distinction I draw:

“SECURE”



Better yet, a real-world model:

You have to

Before you can

And then you can

“See it” → **“Manage it”** → **“Secure it”**

* Flagrantly stolen from Steve Williams over at NTT

Common Sense, Right?

“See it” → “Manage it” → “Secure it”

it's just common sense



RSA®Conference2022

The Tech Stack Perspective



Does I/P/D/R/R hold up in the real world?

Identify

Protect

Detect

Respond

Recover



“See it”

“Manage it”?



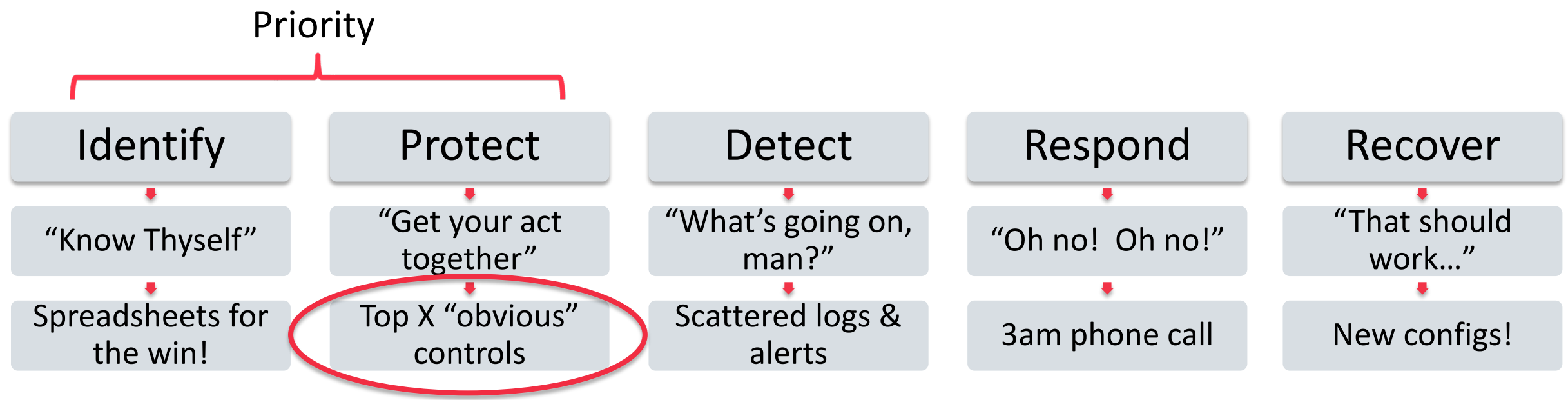
“Secure it”

Yes and no...

The early days of maturity – technology-based



The early days of maturity – technology-based



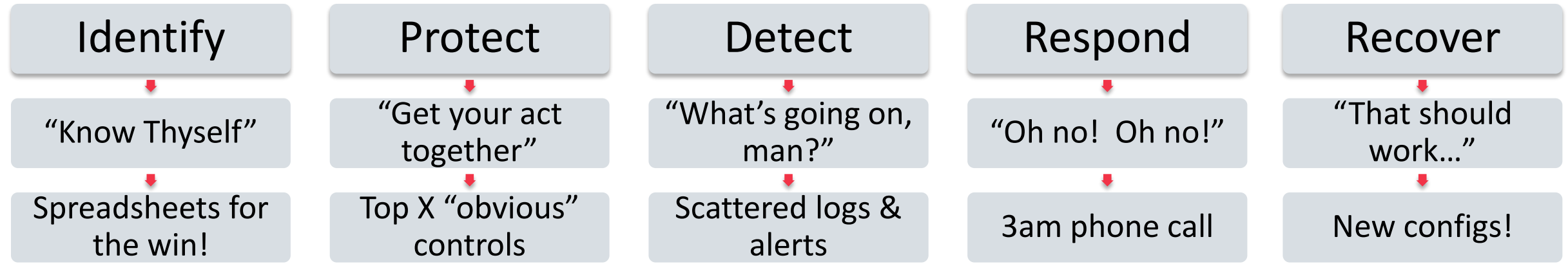
MVS
now!
ask me
how

Minimum Viable Security – A Brief Aside

- We are always supposed to implement controls based on known risk and the value of known assets, and yet...
 - How many of you need email protection?
 - How many of you need endpoint protection?
 - How many of you need MFA?
 - Etc...



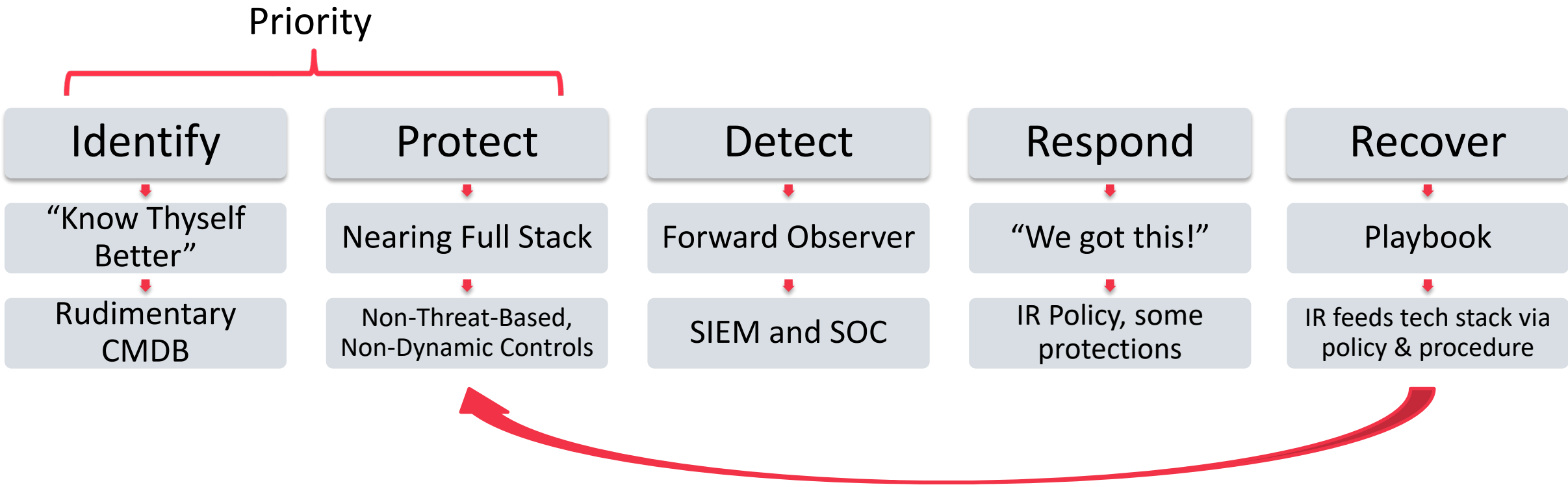
There is also immaturity to process: linearity...



Over and over and over and over...

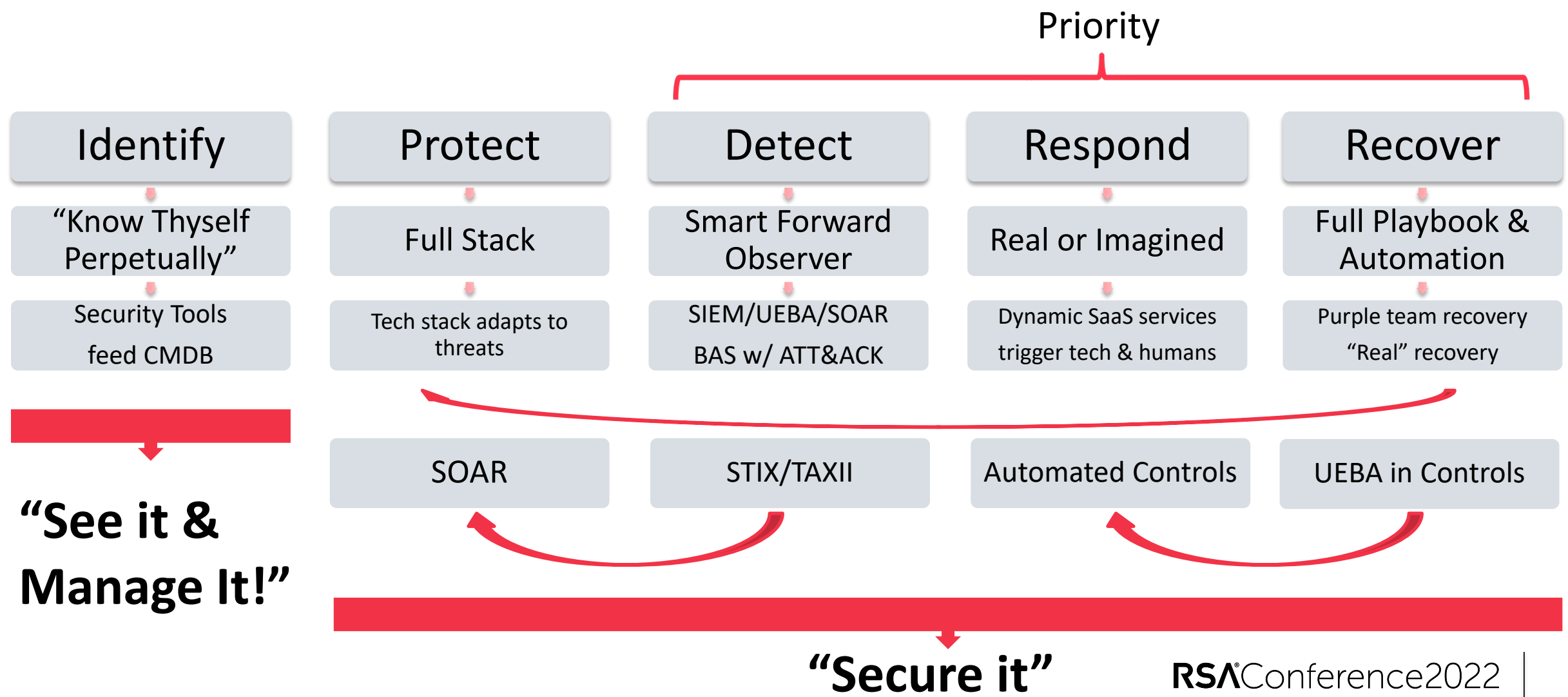


Apply Better Methods: Mid-Tier Maturity



Linearity starts to become a cycle

Apply Better Methods: Full Maturity



(Challenges with the model):

- Limited tools available that: perform endpoint health checks, push patches and configs, and populate CMDB.
- UEBA -> Controls = Proprietary (& Change Management?)
- STIX/TAXII limited & not supported everywhere.
- SOAR not supported everywhere, provides little protection
- ATT&CK framework never 100% complete or current
- Purple Team & BAS must rotate through the estate

Despite All That...



RSA[®]Conference2022

The GRC Perspective



You May Not Have Known:

NIST CSF

MAPS TO

NIST 800-53

MAPS TO

MITRE ATT&CK

MAPS TO

CVEs

Which Also Means:

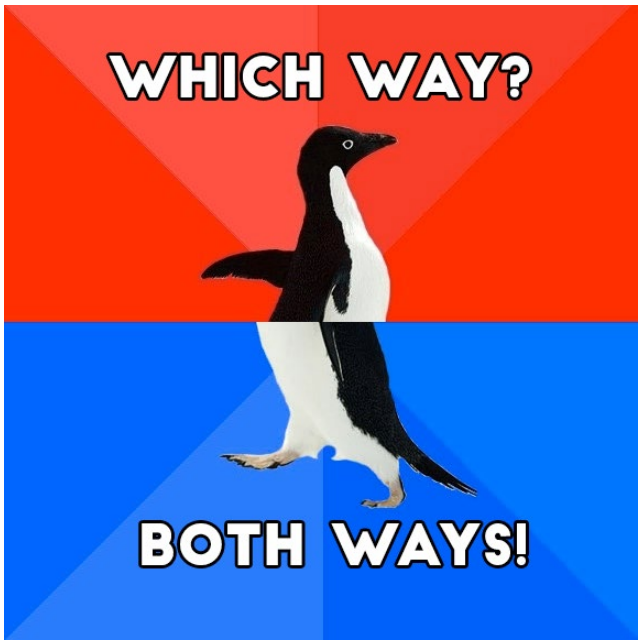
CVEs



Red Teaming or Blue Teaming?



It's Bi-Directional! Start Anywhere!



Early Maturity: Protection before Attacks...

Assess...Prioritize...Prescriptive Controls...Threat-Informed Controls...Measure



NIST
CSF

NIST SP
800-53

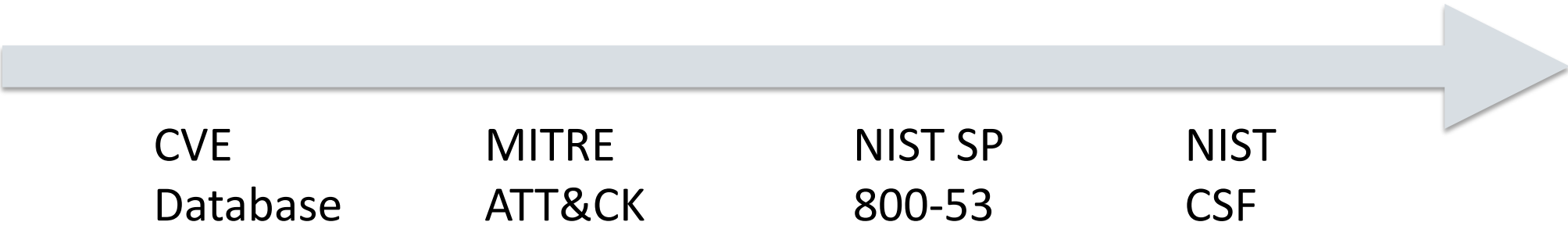
MITRE
ATT&CK

CVE
Database

Later Maturity: Attack-Driven Protection!



Scan...Self-Attack...Prescriptive Controls...Framework Population...Report



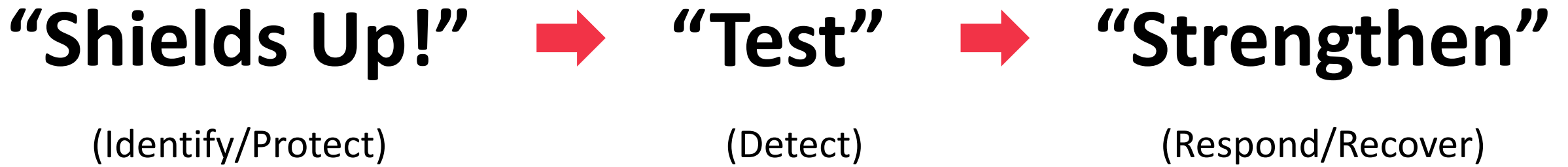
Key Takeaways – GRC:

- Start with NIST CSF and Focus on Identify-Protect
 - Detect/Respond/Recover will be more reactionary
- Once you have most of your estate in-hand, map to NIST SP 800-53 to get more prescriptive around your controls, start focusing more now D/R/R.
- Map to MITRE ATT&CK as you invert your program, starting with a known threat, working into Detection and Response, and using Recover to feed into Protect. Identify should not come up much, and the line between Protect and Recover should blur. GRC team has bridged with technical team by this time, and frameworks are populated based on real attack scenarios.
- Map to CVEs to close the loop, proactively applying ATT&CK to identified vulnerabilities for a D/R/R + I/P strategy.

Key Takeaways – Tech Stack:

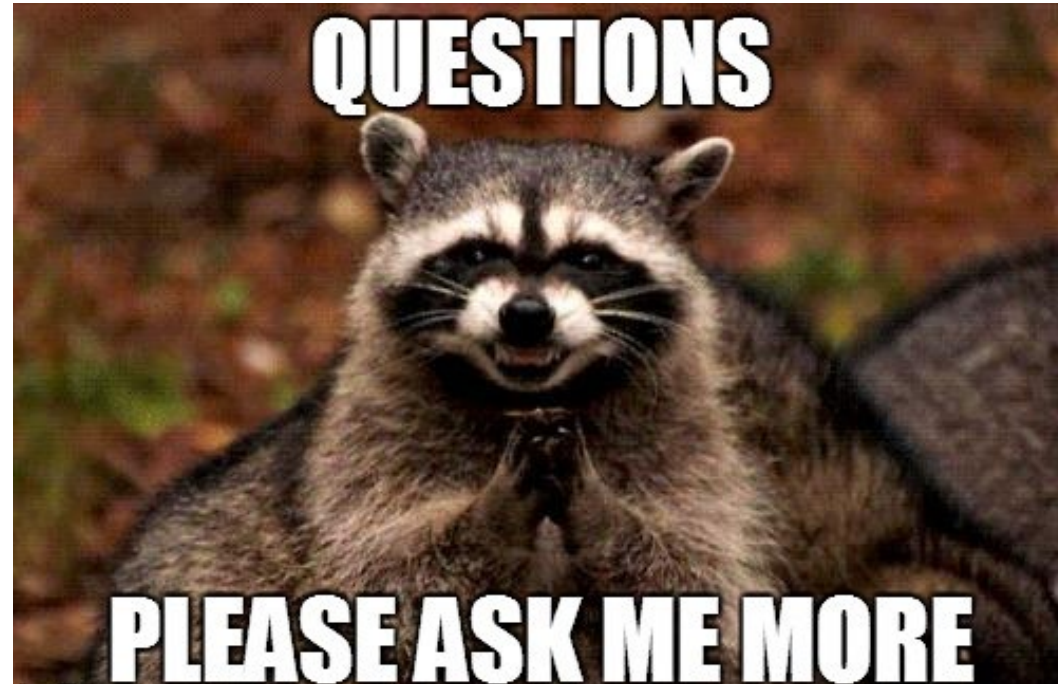
- Get a **CMDB** in place and get **Minimum Viable Security** in place (“MVS”):
 - IA&M, Secure endpoint management, EDR, SASE w/CASB, Email Protection
 - IR consists of **rudimentary playbook** leveraging these tools
- Feed this into a SIEM with UEBA, add DLP, Insider Threat Protection, etc. as desired.
 - IR is more robust and prescriptive, **centered around SIEM/SOC**.
- SOAR drives SOC & your controls where possible, **BAS w/ ATT&CK**, STIX/TAXII, **UEBA drives Controls** where possible, **IR automated** where possible
- Purple team, purple team, purple team...

Key Takeaways: It's Really This Simple:



Common sense, right?

Thank You



And good luck with all your cyber stuffs!



Oh, and please listen to my show!
<https://hackervalley.com/show/cyber ranch>

OR

Wherever you get your podcasts...