Evolving Cyber Security Posture

One Financial Institution’s Strategy

Introduction

Tim Mielak
- VP of Enterprise Technology
- tim.mielak@msufcu.org

David Zuleski
- Chief Information Security Officer
- David.zuleski@msufcu.org

Our point of view …

Financial Sector

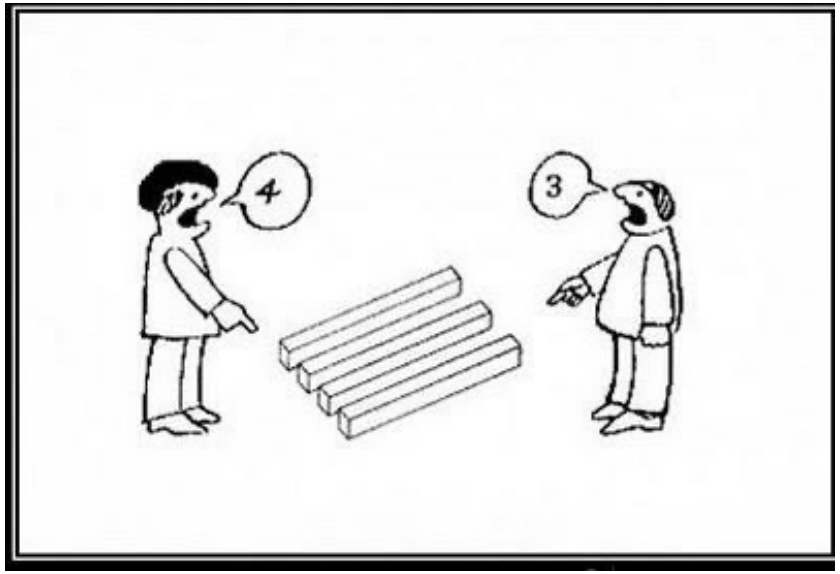
6.5 Billion in assets

Who provides regulatory governance?

- National Credit Union Administration (NCUA)
- Federal Financial Institutions Examination Council (FFIEC)

What constitutes sensitive data?

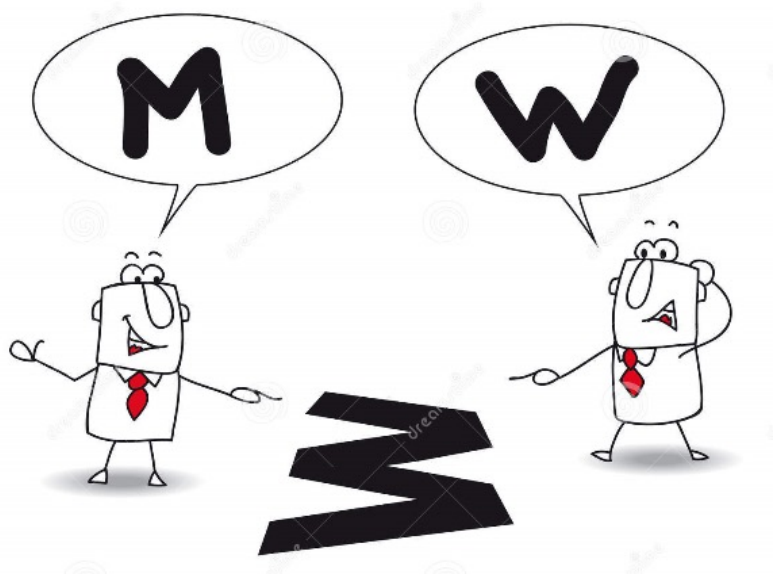
- Card (PAN, PIN, CVV)
- Personally Identifiable Financial Information (PIFI)



My point of view too …

How is money made, where is it, how does it move?

- Loans
- Card Interchange Fees
- Deposits
- Wire / ACH



What are some general characteristics of IT?

- Multiple datacenter facilities for redundancy
- Many satellite branches
- Remote and Hybrid workforce
- Many 3rd party network interfaces of various types
- Currently building out an Azure platform with a "*cloud smart*" adoption strategy

Objectives of a CU Cyber Security Program

- Part 748 Appendix A of NCUA Regulations
  - “These Guidelines provide guidance standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of member information.”
- Predict, Prevent, Detect, Respond
- Achieve Continuous Improvement and Maturity
- Don’t Interfere with or Interrupt the Business!

Controls (I.e. All the stuff we ***must*** have.)

- Intrusion Detection and Prevention Systems (IDS / IPS)
- Endpoint Anti-Virus
- Data Loss Prevention
- Firewall
- Security Information and Event Management (SIEM)
- Internal Network Segmentation
- Network Flow Analysis and Classification
- Risk Assessment (Enterprise and System)
- Disaster Recovery / Business Continuity
- Threat Intelligence Monitoring
- Annual and Quarterly Board Reports on Risk
- Penetration Testing
- Web Proxy and Content Filtering
- Privileged Account Management (PAM)
- Helpdesk Ticket Escalation
- Vulnerability Management (Scanning)
- Configuration Management and Hardening Baselines
- DNS Reputation Filtering
- Email Anti-Virus
- Sandbox Detonation
- Email SPAM Filtering
- Behavioral Endpoint Protection
- Endpoint and Network Forensics
- Cyber Incident Response
- Security Policy & Procedure
- Security Education and Awareness Training
- Security Architecture Review (Communication Topology, Encryption)
- Change Management
- Security Exception Processing
- Regulatory and Internal Audit Responses
- Investigation and Security Data Analysis
- Vendor Management Security Reviews (SSAE 16 / SOC I, II)
- User and Active Directory Audits
- Password Cracking

CIS 18

With Limited Resources a Credit Union Security Organization Must:

- Achieve a Holistic Security Posture (Breadth of Coverage)
- Achieve Defense in Depth
  - Interlocking controls
  - Variety of controls
- Provide Incident Response
- Provide Business Continuity
- Provide Risk Analysis
- Evolve with an extremely fluid Threat-Scape

Sophistication Lifecycle

You want perfect security? Turn off the Internet and all system access.

- Unemployed IT Professional

Federal Financial Institutions Examination Council

The FFIEC CAT Maturity Model

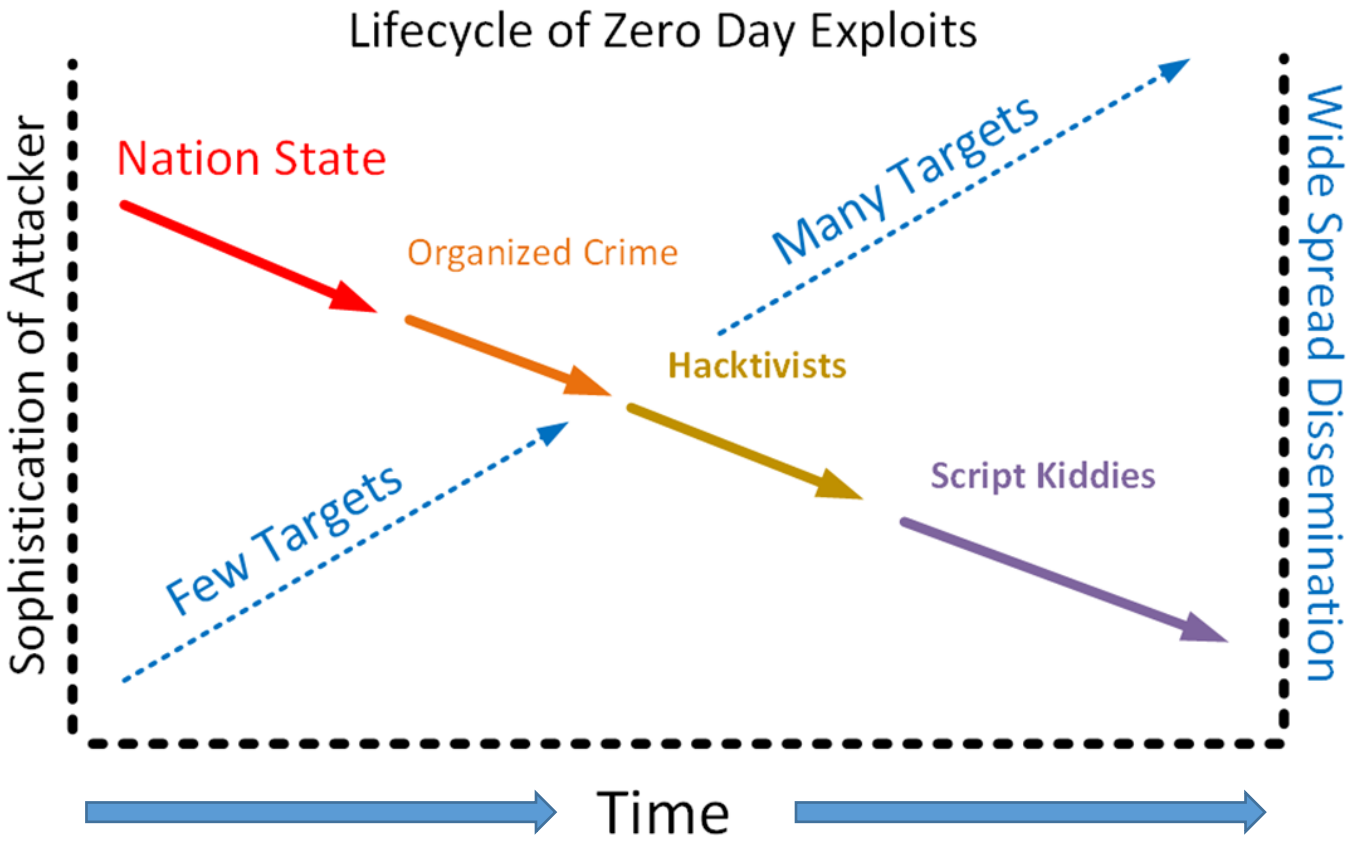
Cyber Assessment Tool

495 Binary Declarative Statements

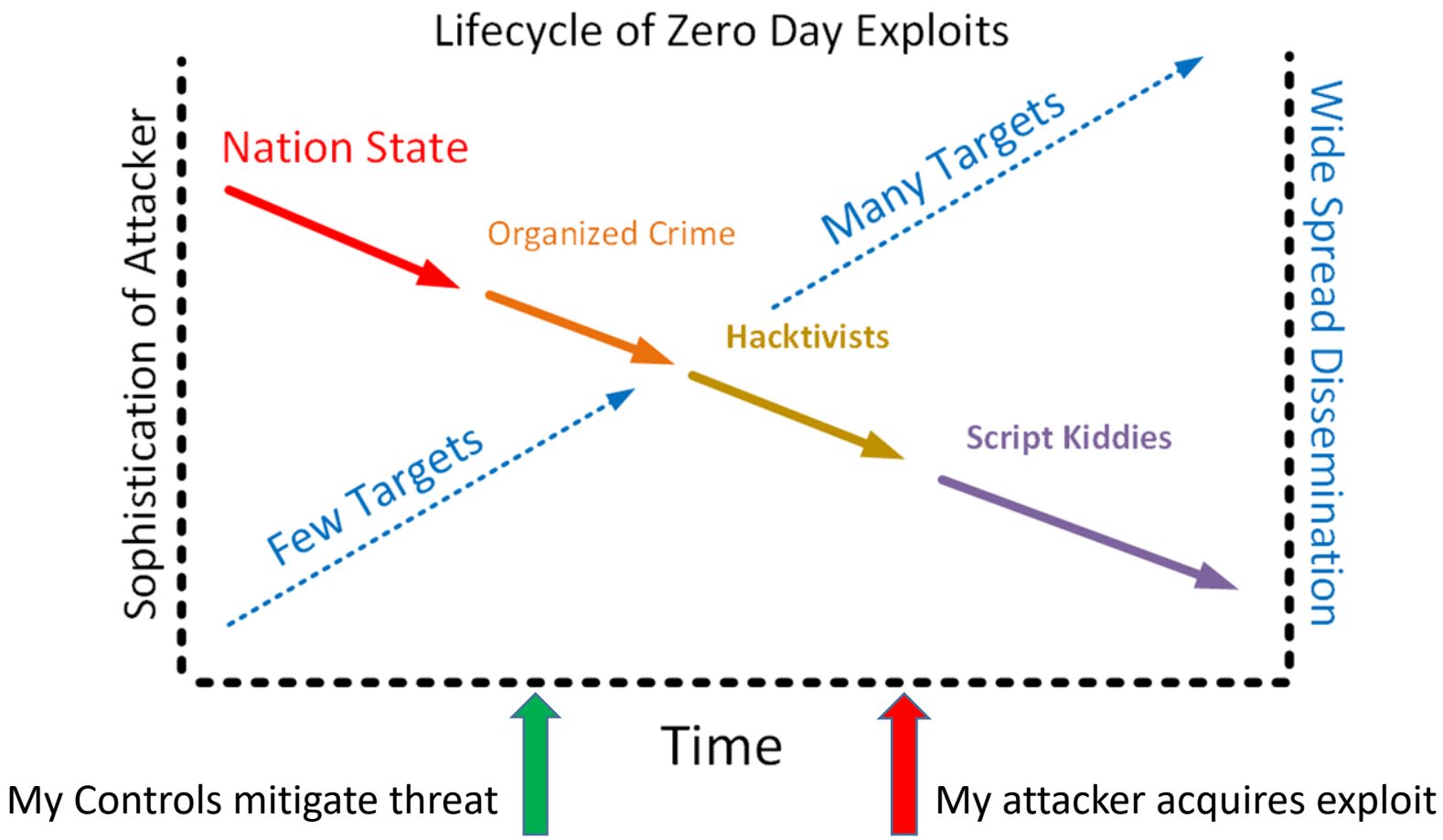
Domain	Domain Maturity	Assessment Factor	Assessment Factor Maturity	Component	Baseline	Evolving	Intermediate	Advanced	Innovative	Assessed Maturity Level
1: Cyber Risk Management & Oversight	Evolving	1: Governance	Evolving	1:Oversight	100%	100%	63%	100%	100%	Evolving
				2: Strategy / Policies	100%	100%	40%	20%	100%	Evolving
				3: IT Asset Management	100%	100%	0%	50%	100%	Evolving
		2: Risk Management	Evolving	1: Risk Management Program	100%	100%	80%	80%	100%	Evolving
				2: Risk Assessment	100%	100%	100%	0%	100%	Intermediate
				3: Audit	100%	100%	50%	100%	100%	Evolving
		3: Resources	Evolving	1: Staffing	100%	100%	0%	100%	100%	Evolving
		4: Training & Culture	Intermediate	1: Training	100%	100%	100%	100%	100%	Innovative
				2: Culture	100%	100%	100%	0%	100%	Intermediate
2: Threat Intelligence & Collaboration	Intermediate	1: Threat Intelligence	Innovative	1: Threat Intelligence and Information	100%	100%	100%	100%	100%	Innovative
		2: Monitoring & Analyzing	Intermediate	1: Monitoring and Analyzing	100%	100%	100%	60%	100%	Intermediate
		3: Information Sharing	Intermediate	1: Information Sharing	100%	100%	100%	33%	100%	Intermediate
3: Cybersecurity Controls	Evolving	1: Preventative Controls	Evolving	1: Infrastructure Management	100%	100%	50%	0%	50%	Evolving
				2: Access and Data Management	100%	100%	0%	50%	0%	Evolving
				3: Device / End-Point Security	100%	100%	100%	100%	0%	Advanced
				4: Secure Coding	100%	100%	75%	100%	0%	Evolving
		2: Detective Controls	Evolving	1: Threat and Vulnerability Detection	100%	100%	0%	33%	0%	Evolving
				2: Anomalous Activity Detection	100%	100%	50%	0%	0%	Evolving
				3: Event Detection	100%	100%	100%	50%	0%	Intermediate
		3: Corrective Controls	Evolving	1: Patch Management	100%	100%	100%	100%	0%	Advanced
				2: Remediation	100%	100%	50%	0%	0%	Evolving
4: External Dependency Management	Evolving	1: Connections	Intermediate	1: Connections	100%	100%	100%	0%	0%	Intermediate
		2: Relationship Management	Evolving	1: Due Diligence	100%	100%	50%	0%	0%	Evolving
				2: Contracts	100%	100%	0%	50%	0%	Evolving
				3: Ongoing Monitoring	100%	100%	0%	0%	0%	Evolving
5: Cyber Incident Management and Resilience	Baseline	1: Incident Resilience Planning and Strategy	Evolving	1: Planning	100%	100%	100%	33%	0%	Intermediate
				2: Testing	100%	100%	0%	40%	0%	Evolving
		2: Detection, Response, and Mitigation	Baseline	1: Detection	100%	100%	100%	50%	0%	Intermediate
				2: Response and Mitigation	100%	88%	50%	67%	0%	Baseline
		3: Escalation and Reporting	Intermediate	1: Escalation and Reporting	100%	100%	100%	0%	0%	Intermediate

This data is synthetic and does not represent the CAT results of MSUFCU.

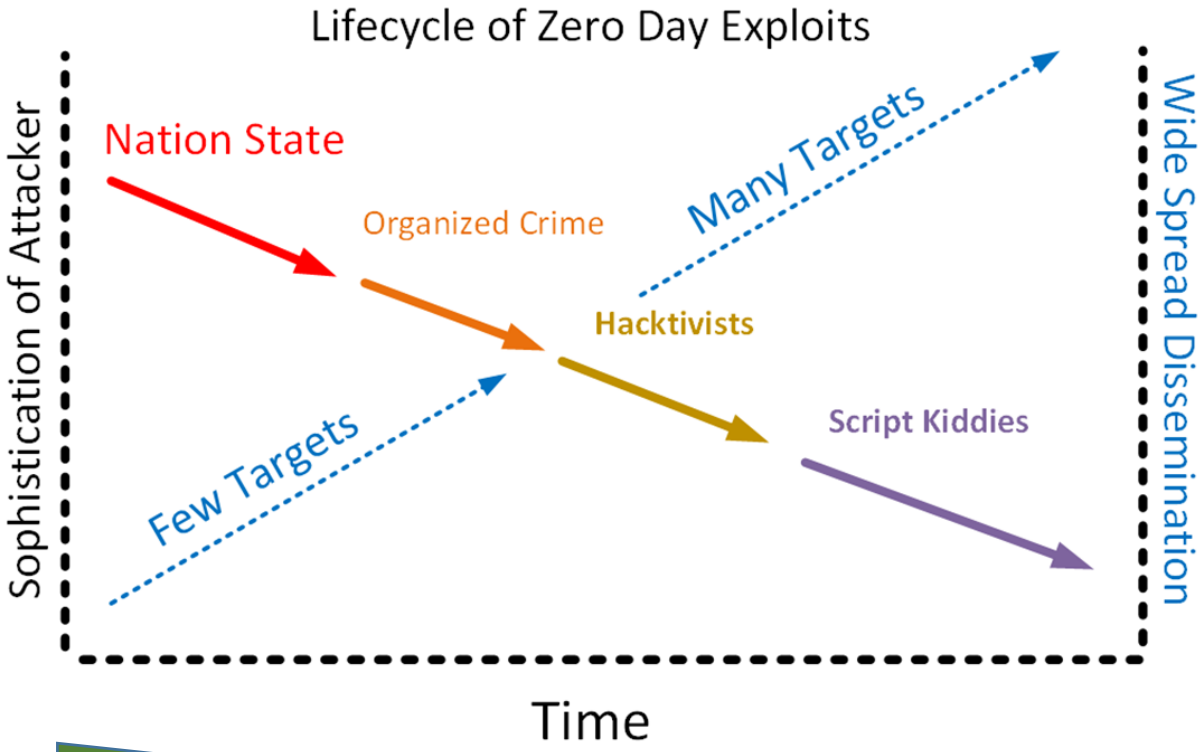
Sophistication Lifecycle

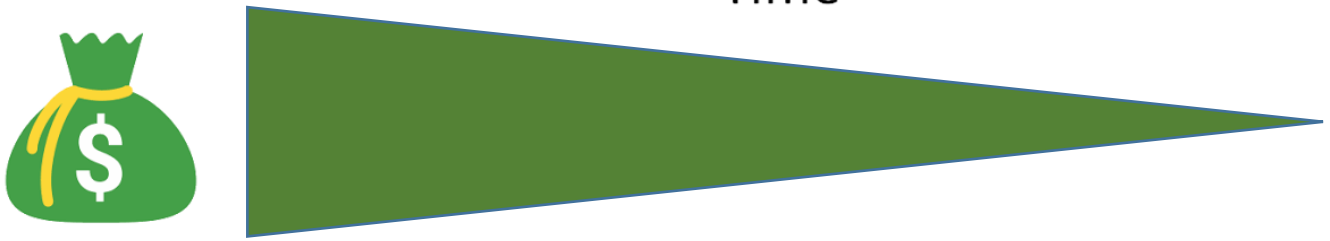


When does my control set (including patching) become effective?
When does my attacker get the exploit?



What can my company afford?



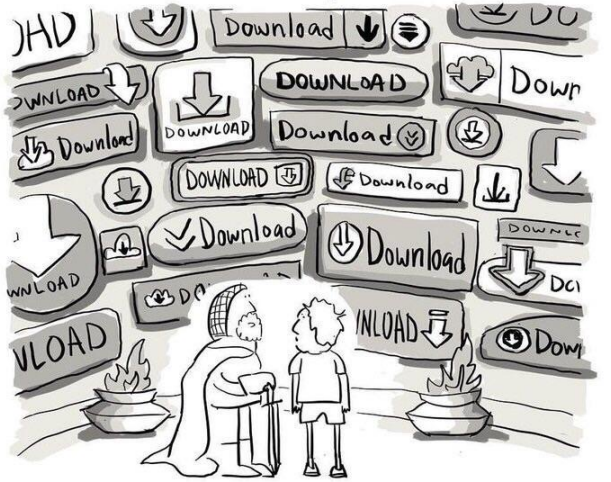


Cost

Sophistication and Risk

Why does this matter?

- You have to choose the level of sophistication you intend to defend against
- Each decision is specific to a particular aspect of a particular point in the kill chain
- If you choose not to decide, you still have made a choice!



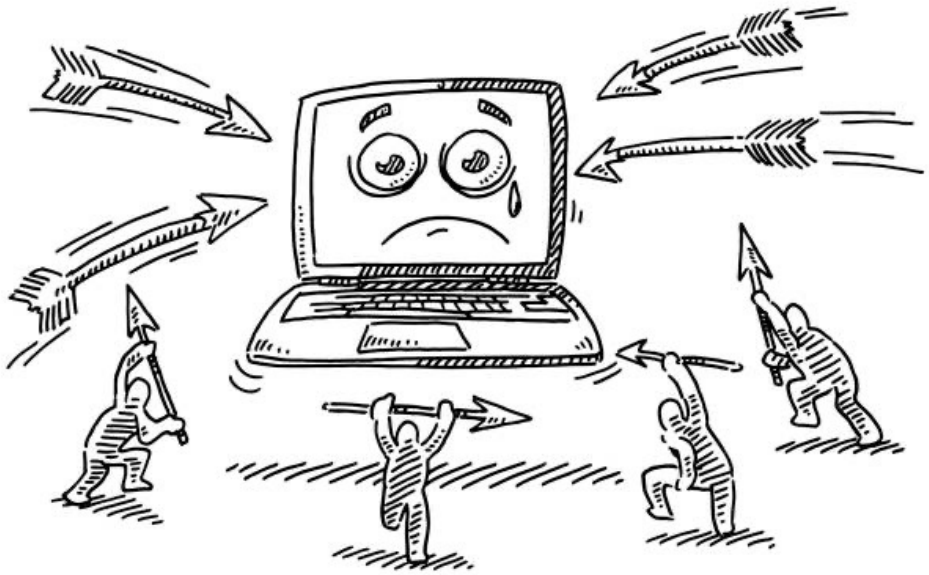
"You must click, but click wisely. For as the true button will bring you a pirated movie, the false button will melt your face off."

Simple Security Strategy for a Complex World

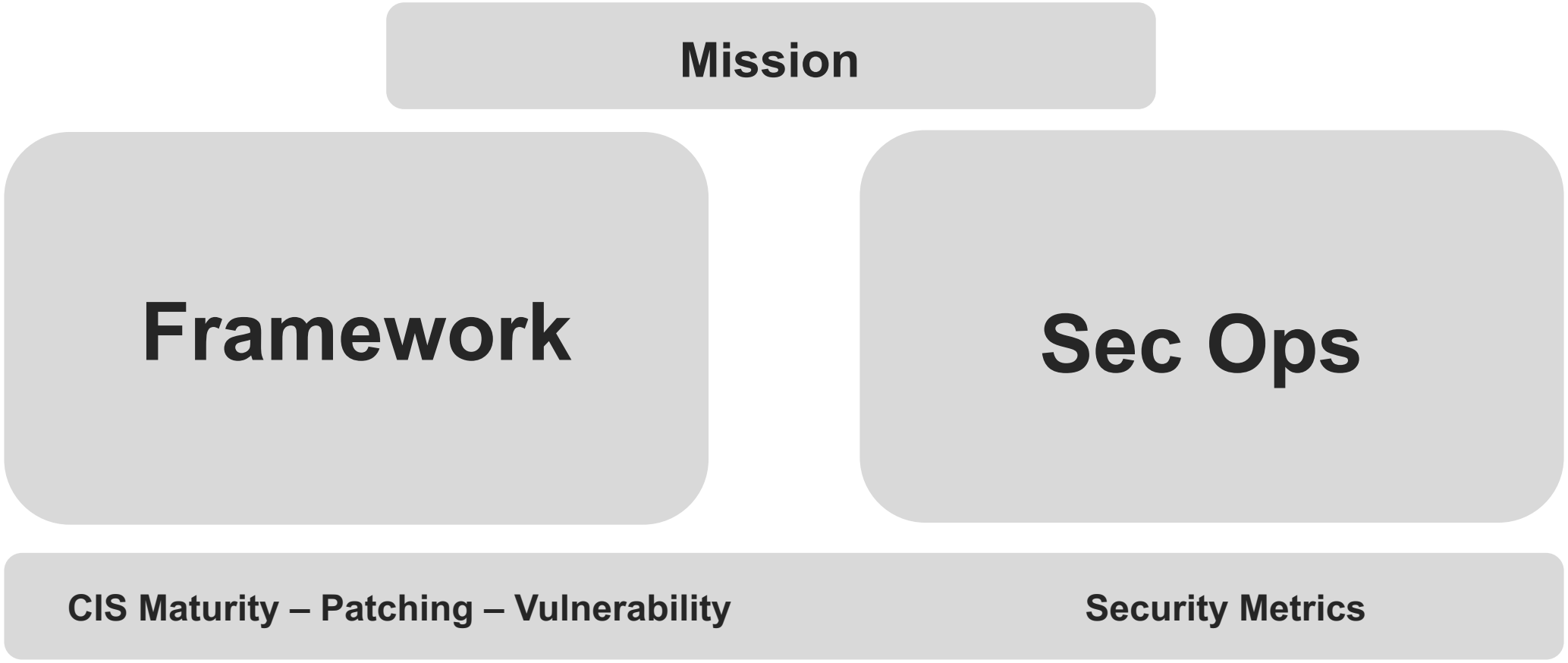
That’s not that simple

What we are up against …

- Nation State and highly organized
- Ransomware/Wipers
- Remote Access Trojans
- Exfiltration or data loss
- Denial of service
- Theft/fraud – inappropriate access
- Lateral movement – Island hopping

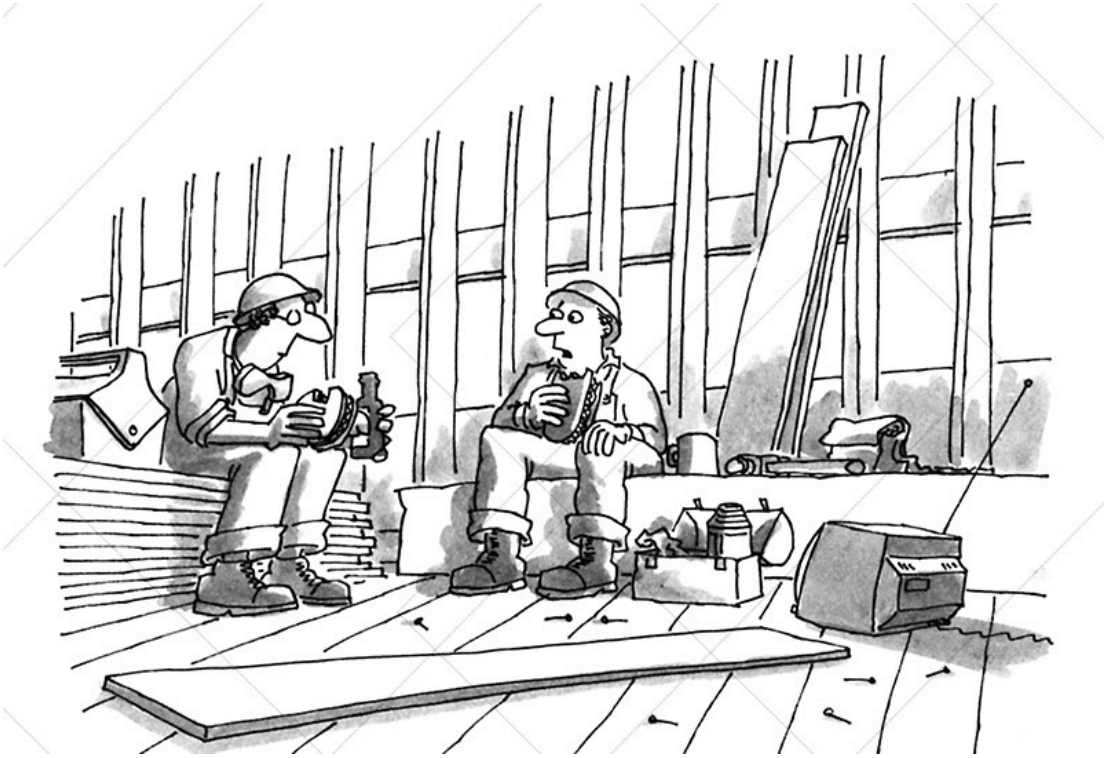


A simple strategy?



Pick a framework any framework

- Pick one and follow it
- Don’t make your own version
- Do all of it
- Measure and show progress
  - Maturity
  - Gap
- It never ends!



Sec Ops

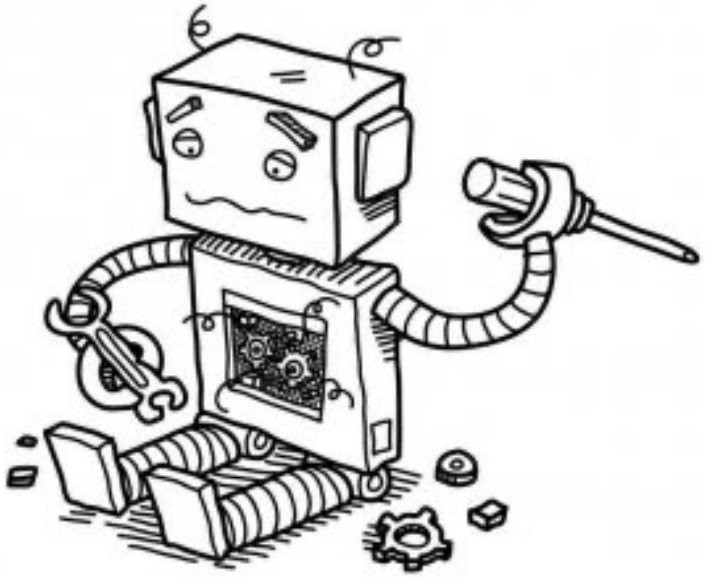
- What about a world we can not control?
- Rapid detection and response is key
- Need some way to log and correlate
- Need a way to take action(s)

Know your gaps – you need logs but…

- Build use cases and collect what is needed to solve for those
- Don’t collect everything “just because”
- MITRE(https://attack.mitre.org/) is your friend
  - View from the attackers perspective
  - Helps identify gaps
  - Do hunts and Purple Team exercises

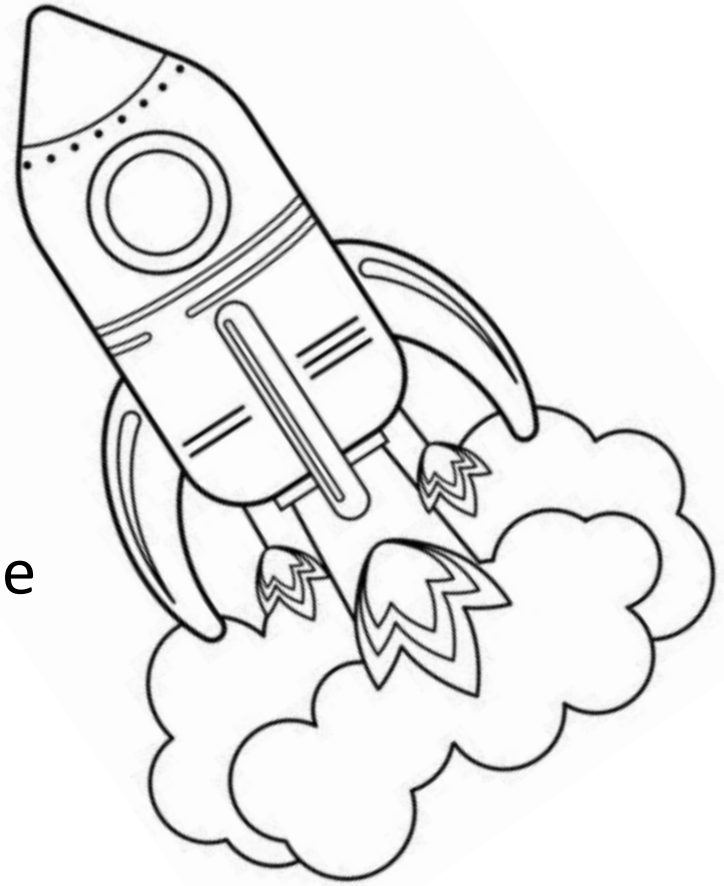
Automate – Automate – Automate

- Robots work 24x7 365
- Can handle volume
- Robots are fast
- Help you sleep



Some examples

- “Is this you?” kind of alerts
- Auto machine isolations
- Files and hashes
- URLS from phishing emails
- Additional challenges/account blocks
- You know your pain, build use cases around those
- Build safety valves
  - you may break things, its probably ok..



Questions?