Prioritizing ATT&CK Informed Defenses

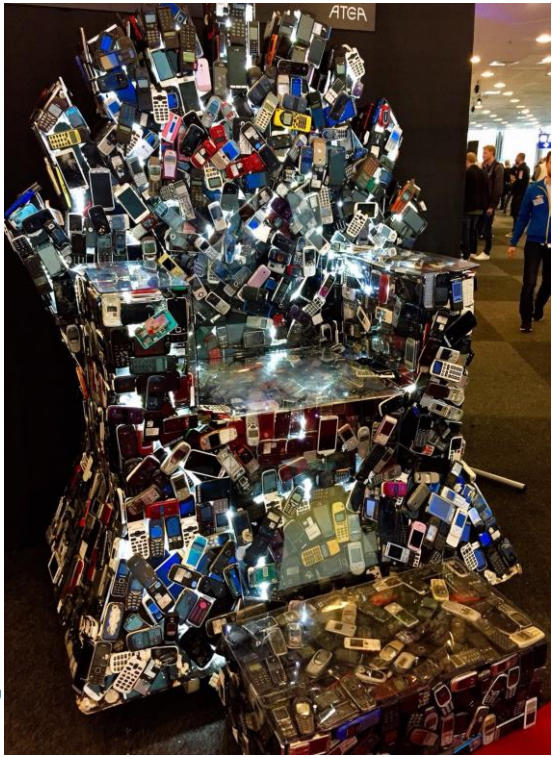
The CIS Way

Philippe Langlois
Senior Risk Analyst
Verizon DBIR

Joshua M Franklin
Senior Cybersecurity Engineer
Center for Internet Security

Joshua Franklin Background

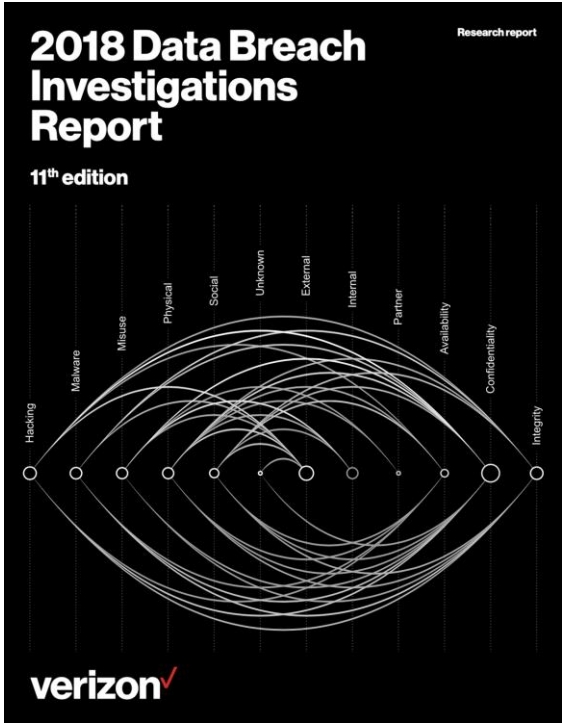
- Product owner of CIS Controls v7.1
- 10 years in the US government
  - NIST
  - Election Assistance Commission
- Telecommunications security, mobile security, mobile app vetting
  - Contributor to Mobile ATT&CK
- Election security
- Cybersecurity standards (e.g., NIST, CIS, IEEE, OASIS, 3GPP)



Game of Phones

Philippe Langlois Background

- Current:
  - Verizon DBIR Co-Author
- Former
  - Product Owner @ CIS
  - CIS Controls
  - Nationwide Cyber Security Review
  - Integrated Product Team Lead
- Focus on risk management and cyber security
- Can maybe code himself out of a paper bag



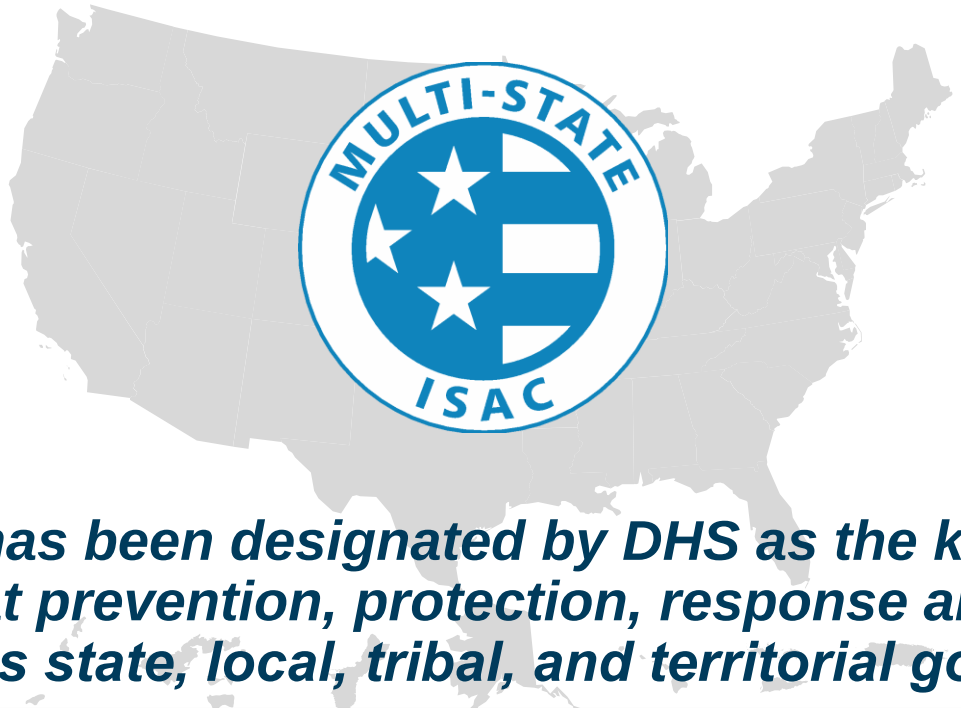
Defender's Dilemma

- What's the right thing to do, and how much do I need to do?
- How do I actually do it?
- And how can I demonstrate to others that I have done the right thing?

CIS Background

- US-based forward-thinking, non-profit entity that harnesses the power of a global IT community
- Goal of safeguarding private and public organizations against cyber threats
- CIS Vision: Leading the global community to secure our connected world
- CIS Mission:
  - Identify, develop, validate, promote, and sustain best practice solutions for cyber defense
  - Build and lead communities to enable an environment of trust in cyberspace

Multi-State Information Sharing and Analysis Center



The MS-ISAC has been designated by DHS as the key resource for cyber threat prevention, protection, response and recovery for the nation's state, local, tribal, and territorial governments

https://www.cisecurity.org/ms-isac/

TLP: WHITE

Security Best Practices

- CIS Benchmarks
  - Community developed security configuration guidance
  - Covers major applications and OS
  - Recognized by FISMA, FedRAMP, and PCI
  - Freely available in PDF Format
- CIS Controls
  - Internationally utilized standard
  - Making best practice, common practice

140+ benchmarks available

- RHEL 8,
- Microsoft Windows Server 2019, Kubernetes,
- Cloud Foundations for AWS,
- Azure,
- GCP,
- Ubuntu,
- CentOS

Get involved!
https://workbench.cisecurity.org

NSA/DoD Project

The Consensus Audit Guidelines (CSIS)

“The SANS Top 20” (the SANS Institute)

The Critical Security Controls (CCS/CIS)

CIS Controls™ V7.1

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

Implementation Groups

Implementation Group 3
A mature organization with significant resources and cybersecurity experience to allocate to Sub-Controls

Implementation Group 2
An organization with moderate resources and cybersecurity expertise to implement Sub-Controls

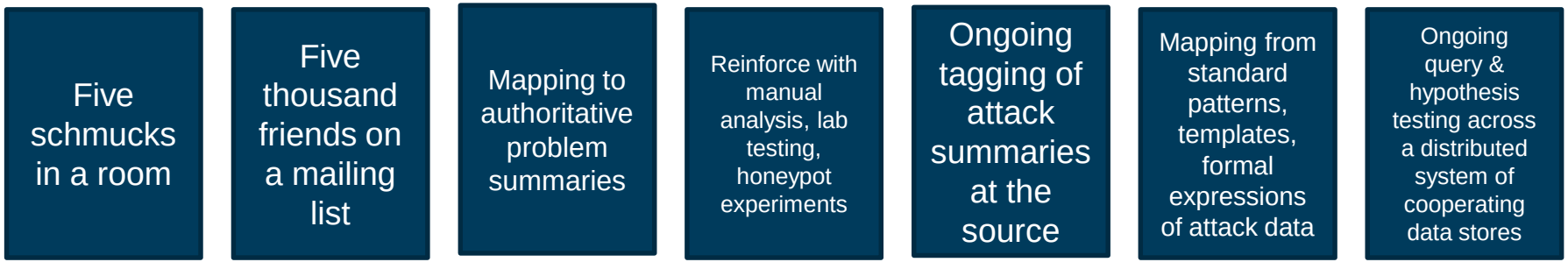
Implementation Group 1
An organization with limited resources and cybersecurity expertise available to implement Sub-Controls

Definitions	1	2	3
Implementation Group 1 CIS Sub-Controls for small, commercial off-the-shelf or home office software environments where sensitivity of the data is low will typically fall under IG1. Remember, any IG1 steps should also be followed by organizations in IG2 and IG3.	●		
Implementation Group 2 CIS Sub-Controls focused on helping security teams manage sensitive client or company information fall under IG2. IG2 steps should also be followed by organizations in IG3.	●	●	
Implementation Group 3 CIS Sub-Controls that reduce the impact of zero-day attacks and targeted attacks from sophisticated adversaries typically fall into IG3. IG1 and IG2 organizations may be unable to implement all IG3 Sub-Controls.	●	●	●

CIS defines Implementation Group 1 as Basic Cyber Hygiene

From Opinions to Data

Evolving the CIS Controls Selection Process



Lower Leverage, Scalability, Repeatability **Higher**

“Pre” ATT&CK

Community Attack Model v1.0

- CIS effort to analyze pertinent information relating to real-world attacks in the wild
- **Goal**: help enterprises make good choices about the most effective defensive actions they can take
- Released via Blackhat in 2016
- Leverages additional frameworks such as NIST CSF and Lockheed Martin Cyber Kill Chain

Why a Community Attack Model?

- Ensure offense informs defense
- Able to better prioritize defensive controls based on real-world techniques
- Communicate trade-offs
  - What techniques are likely to be successful if I don't put a control in place?
- Most enterprises can't go on their own
  - Or do it more than once

Community Attack Model v1.0

	Attack Stages								
CIS Controls (V6.0)	Initial Recon	Acquire/Develop Tools	Delivery	Initial Compromise	Misuse/Escalate Privilege	Internal Recon	Lateral Movement	Establish Persistence	Execute Mission Objectives
Identify		CSC 4		CSC 1, 2	CSC 5				
Protect	CSC 7, 9		CSC 7	CSC 3, 7, 8, 11, 15, 18	CSC 5, 14, 16	CSC 5	CSC 3, 5, 8, 14	CSC 8	CSC 13
Detect			CSC 17	CSC 4, 6, 8	CSC 16, 17	CSC 6	CSC 4, 8, 16	CSC 8	
Respond				CSC 4	CSC 6		CSC 4, 6		CSC 19
Recover									CSC 10

Literature Review

- Verizon Data Breach Investigations Report
- FireEye M-Trends Report
- ESET Cybersecurity Trends
- Symantec Internet Security Threat Report
- Arbor Networks Worldwide Security Report
- IBM X-Force Threat Intelligence Index
- Microsoft Security Intelligence Report
- Akamai [State of the internet]
- …

Before

After

Harnessing the Literature

- If you want data, it's available
- But…
  - Reviewing is time intensive
  - Inconsistent language
  - Vendor biases
  - Sometimes Marketing focused
  - Often difficult to get underlying data and check their work

More concisely:

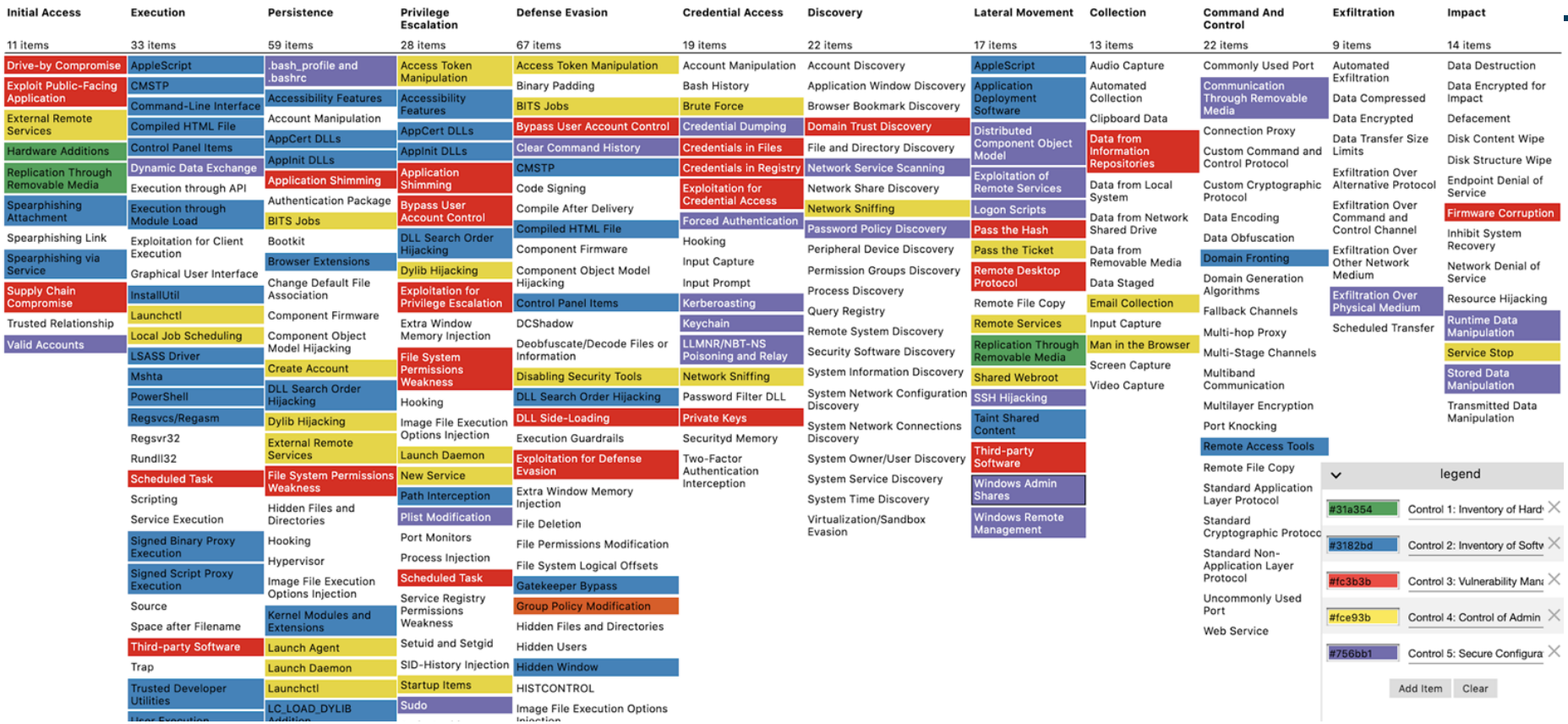
1. *How do we compare reports?*
2. *How can we use them?*

50ccs of ATT&CK

Towards Standardization

- We can engineer a solution to some of these problems
  - Specifically, the use of standard language
- MITRE ATT&CK can be used as a *lingua franca*
- Mitigations were added as an object (huzzah!)
- Working to map the CIS Controls to MITRE ATT&CK

Controls to Mitigations to Techniques v0.1

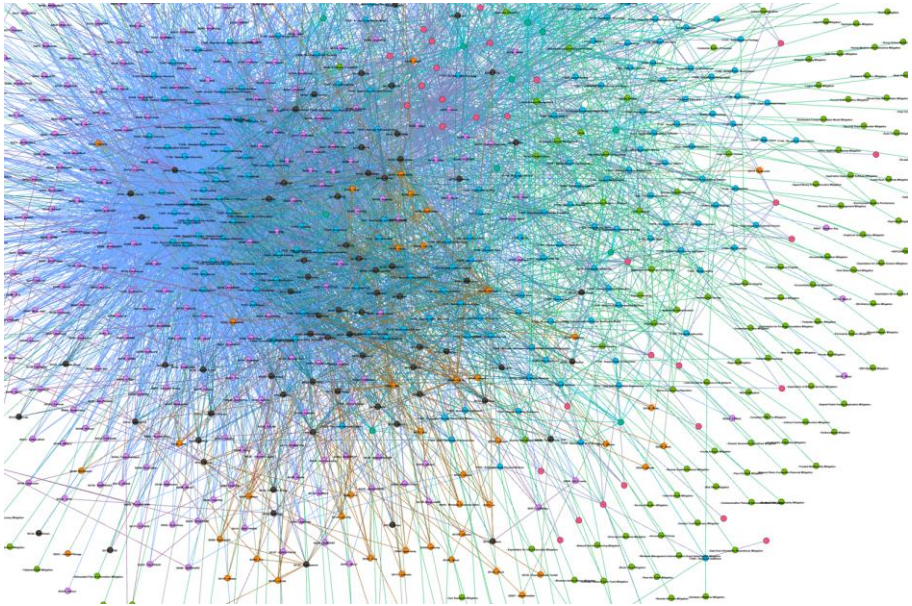


Community Attack Model v2

- Revamp of the Model
- Tie to a standard method of expression
- General methodology:
  - Analyze data sources
  - Identify key attack paths
  - Identify mitigations for key attacks
  - Map mitigations to CIS Controls
- Output:
  - Mapping of the CIS Controls to MITRE ATT&CK
  - Mapping of the CIS Controls to MITRE ATT&CK Mitigations
  - Data-backed attack patterns that the CIS Controls defend against

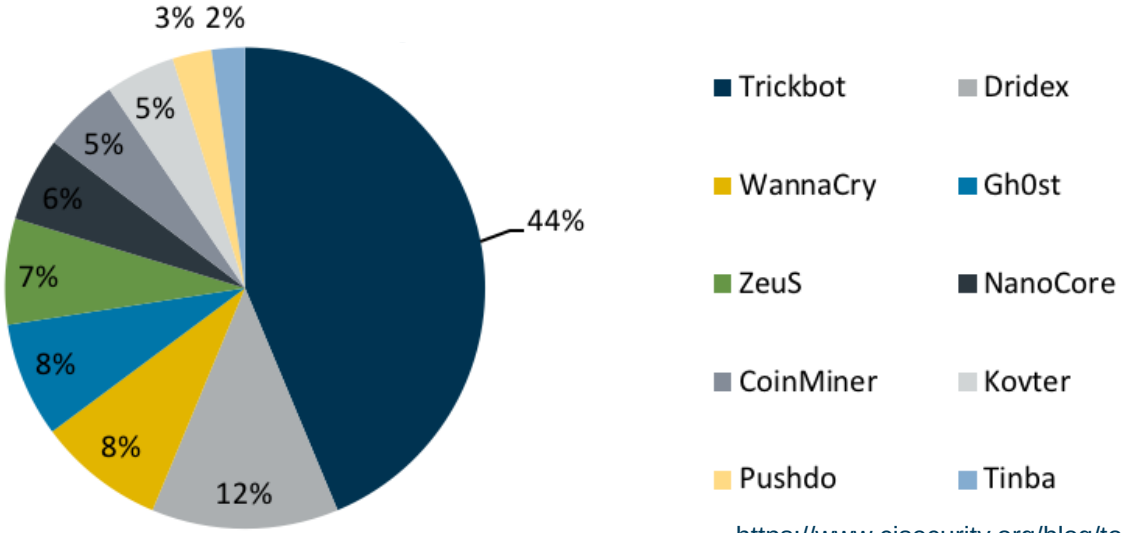
How to Prioritize ATT&CK

- …let's make a network
  - What are central points for Adversaries
  - What are the central points for Software
- Caveats
  - This just tells us what is commonly found in ATT&CK, NOT what is found out there in the wild
  - Focused largely on APT



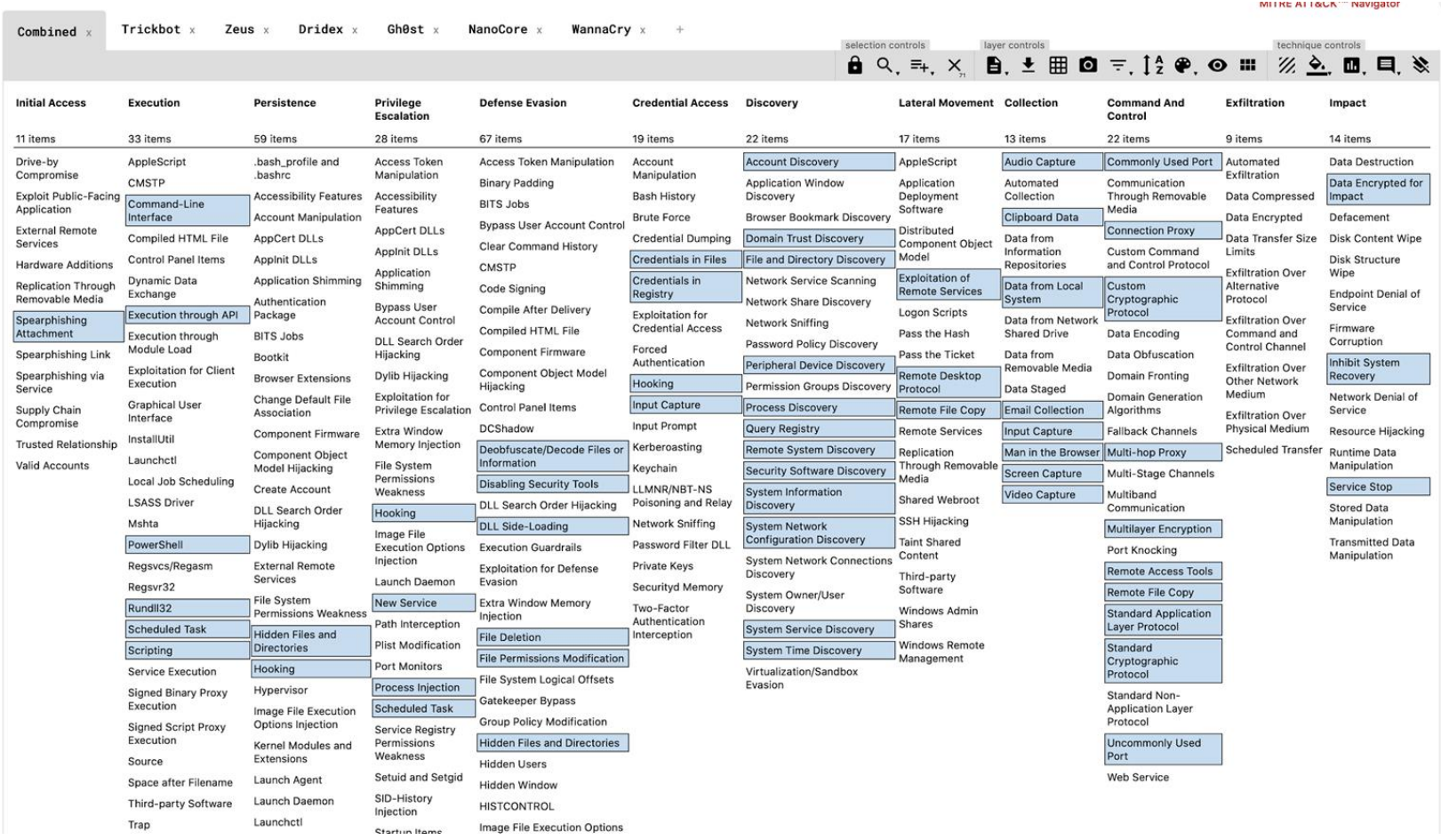
We Need Real Data

- MS-ISAC + EI-ISAC to the rescue
- 100+ network sensors,
- 100+ forensic reports a year



https://www.cisecurity.org/blog/top-10-malware-june-2019

Top 6 Malware Techniques to Controls



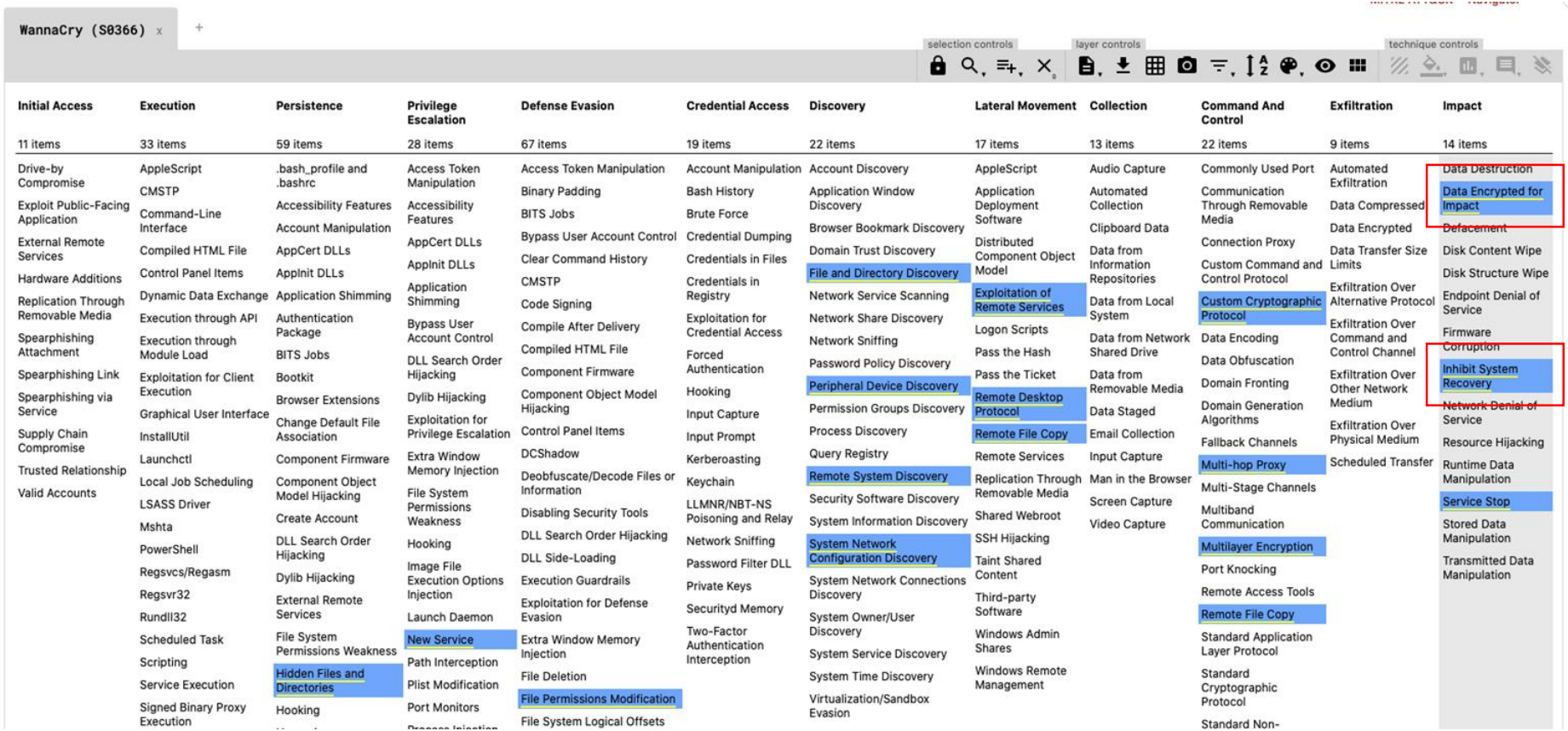
Attack Paths

- Logical ordering of events and techniques that occur
  - Conditions have to be right for the attack to be successful
- We “control” the environment and circumstances that they have to operate in
- What are the conditions and preconditions required for certain techniques?
  - Are certain techniques more commonly used with conditions that we can more easily influence

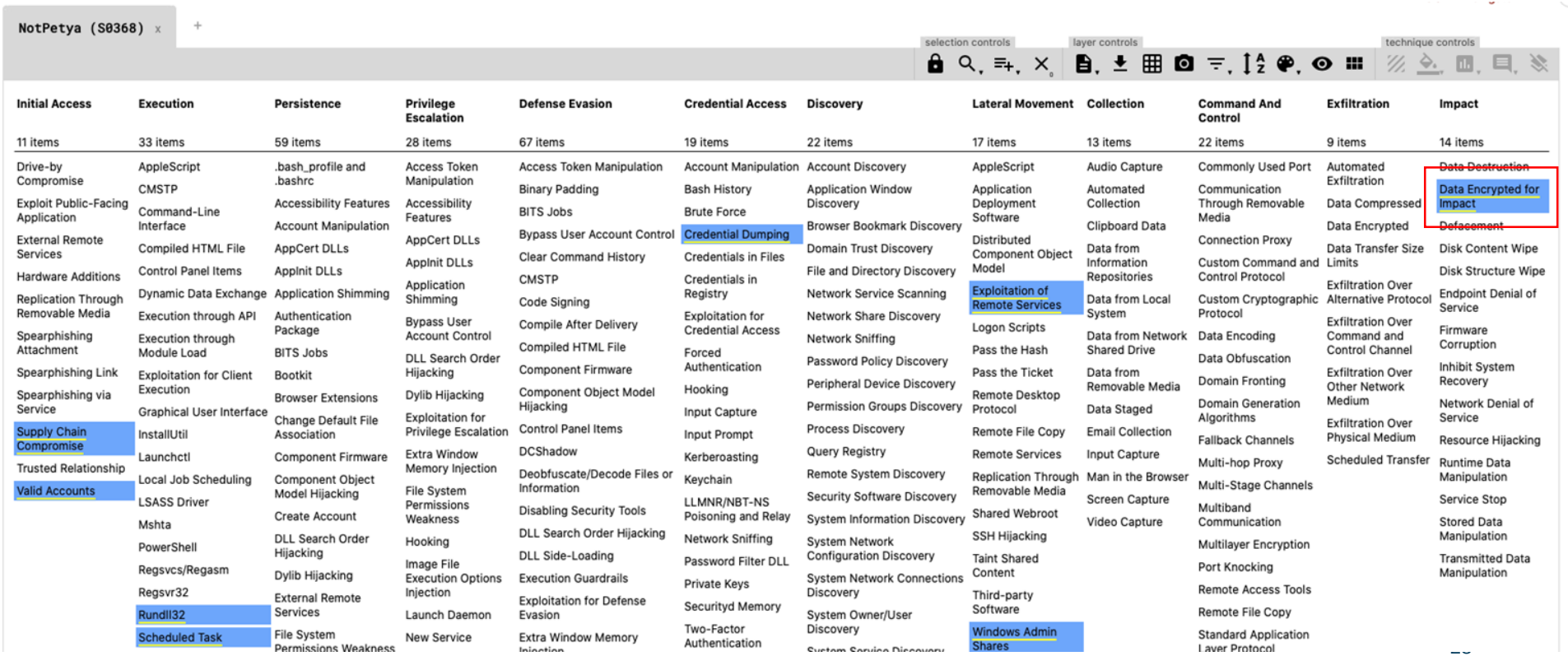
How to Identify Attack Patterns of Note

- Identifying relevant attack paths is difficult
- How to define relevance:
  - Number of breaches attributed?
  - Criticality of affected assets?
  - Financial impact of breaches?
  - Number of times we're forced to read a security blog about the topic?
- Verizon says 28% of all breaches can be attributed to malware
- Verizon also states that 30% of those incidents can be attributed to ransomware
  - Let's explore the attack path and mapping to CIS Controls

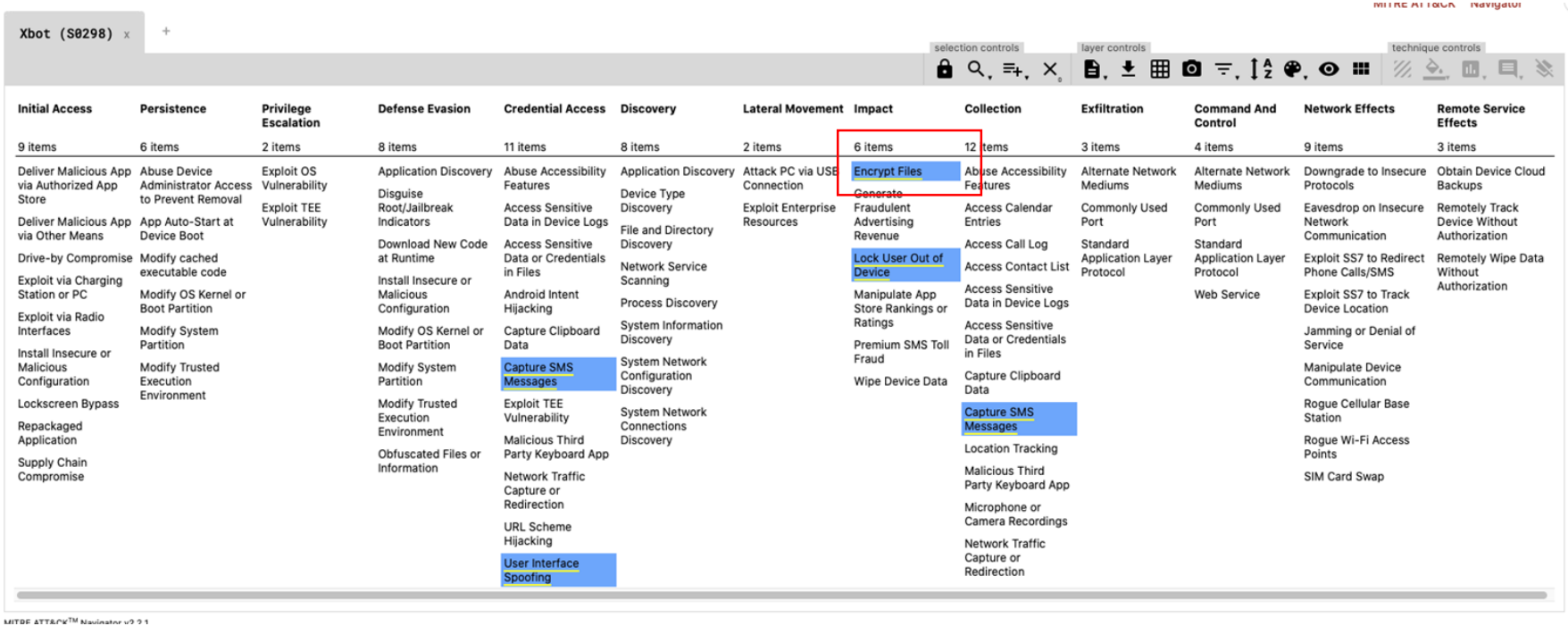
WannaCry Ransomware



NotPetya Ransomware



Xbot Android Malware



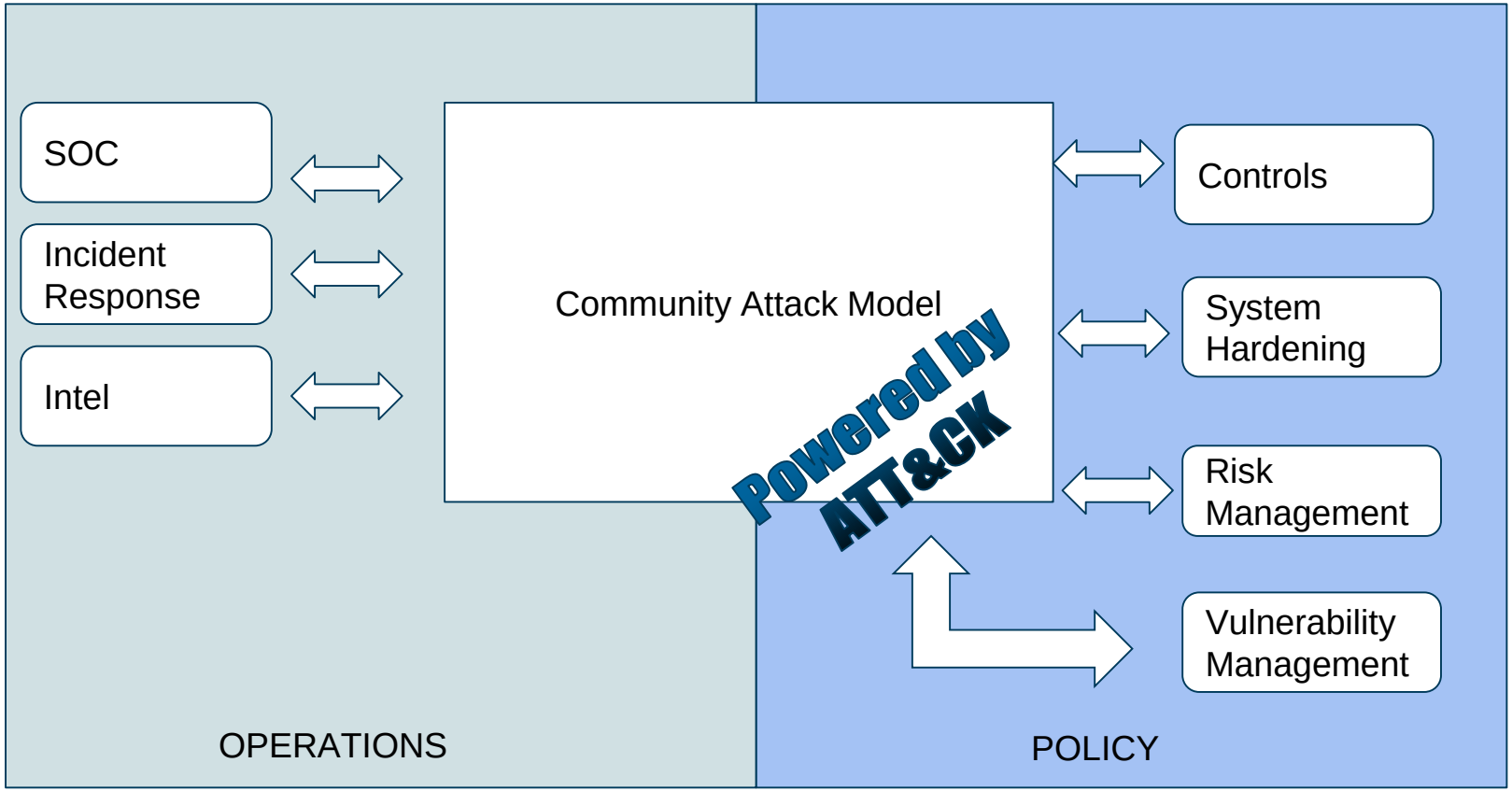
… of course it's not shared in Mobile ATT&CK!

Attack Paths

- Ransomware contains the *Data Encrypted for Impact* technique
- MITRE maps *Data Encrypted for Impact* to *Data Backup*
- Data Backup can be mapped to CIS Controls 10.1 and 10.5

10	10.1	Ensure Regular Automated BackUps	Ensure that all system data is automatically backed up on a regular basis.
10	10.2	Perform Complete System Backups	Ensure that all of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.
10	10.3	Test Data on Backup Media	Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.
10	10.4	Ensure Protection of Backups	Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.
10	10.5	Ensure Backups Have At least One Non-Continuously Addressable Destination	Ensure that all backups have at least one backup destination that is not continuously addressable through operating system calls.

Pipe Dream


SOC
Incident Response
Intel
Community Attack Model
Powered by ATT&CK
Controls
System Hardening
Risk Management
Vulnerability Management
OPERATIONS
POLICY

Next Steps

- Continue developing the CIS Community Attack Model
- Help vet the Controls mapping to MITRE ATT&CK and ATT&CK Mitigations
- Use Community Attack Model to improve Controls v8 and the Implementation Groups
- Reach out to: controlsinfo@cisecurity.org
- Join the Community: https://workbench.cisecurity.org

Thank You

Philippe Langlois
philippe.langlois@verizon.com
@langlois925

Joshua M Franklin
josh.franklin@cisecurity.org
@thejoshpit