TESTING POSITIVE

Tricks of the “Transformation Trade"

CYBER SECURITY SUMMIT

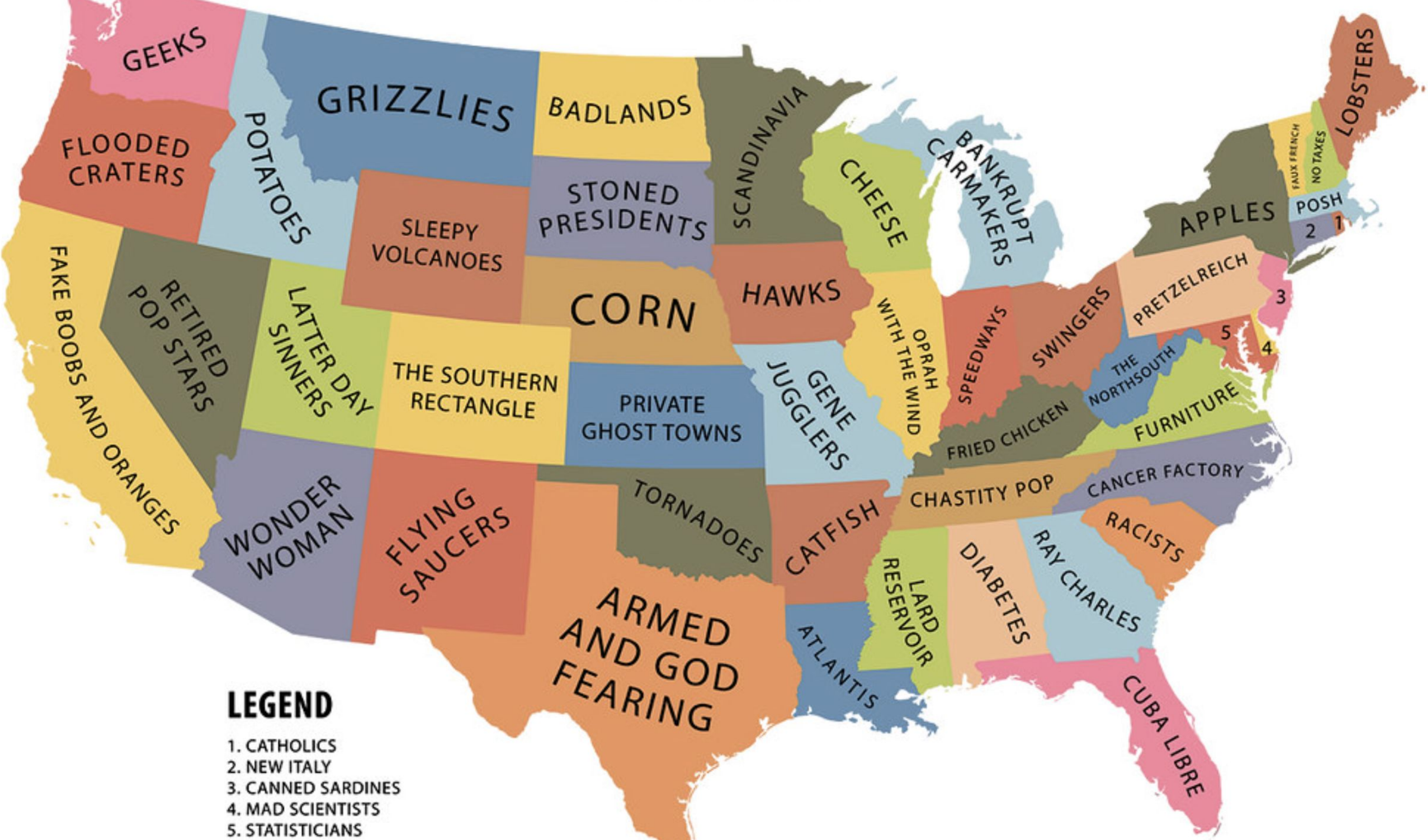
BOLSTERING YOUR SECURITY STRATEGY IN AN EVOLVING THREAT LANDSCAPE

THANK YOU!

HI, I’m Chris!

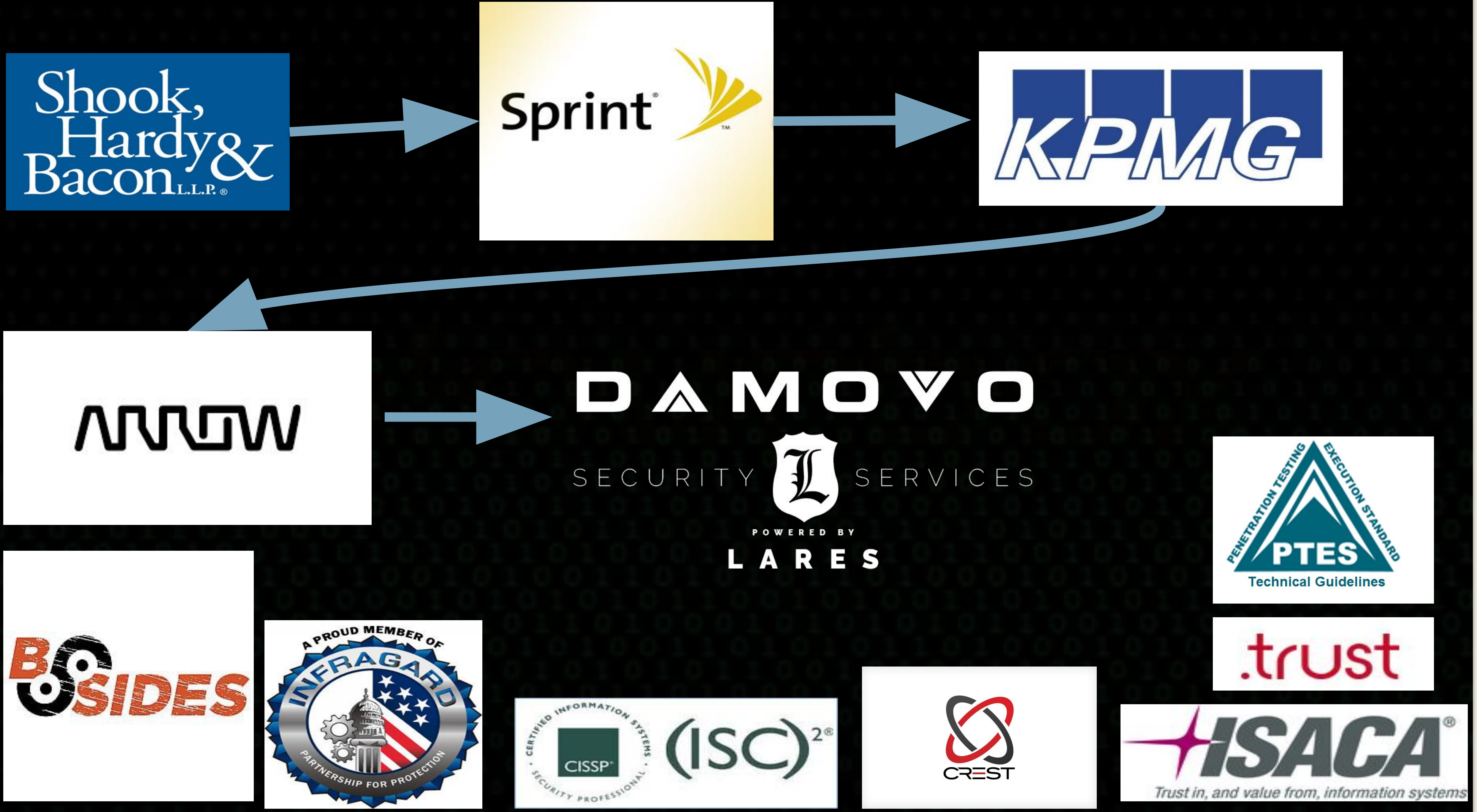
Those are my dogs Lord & Baron

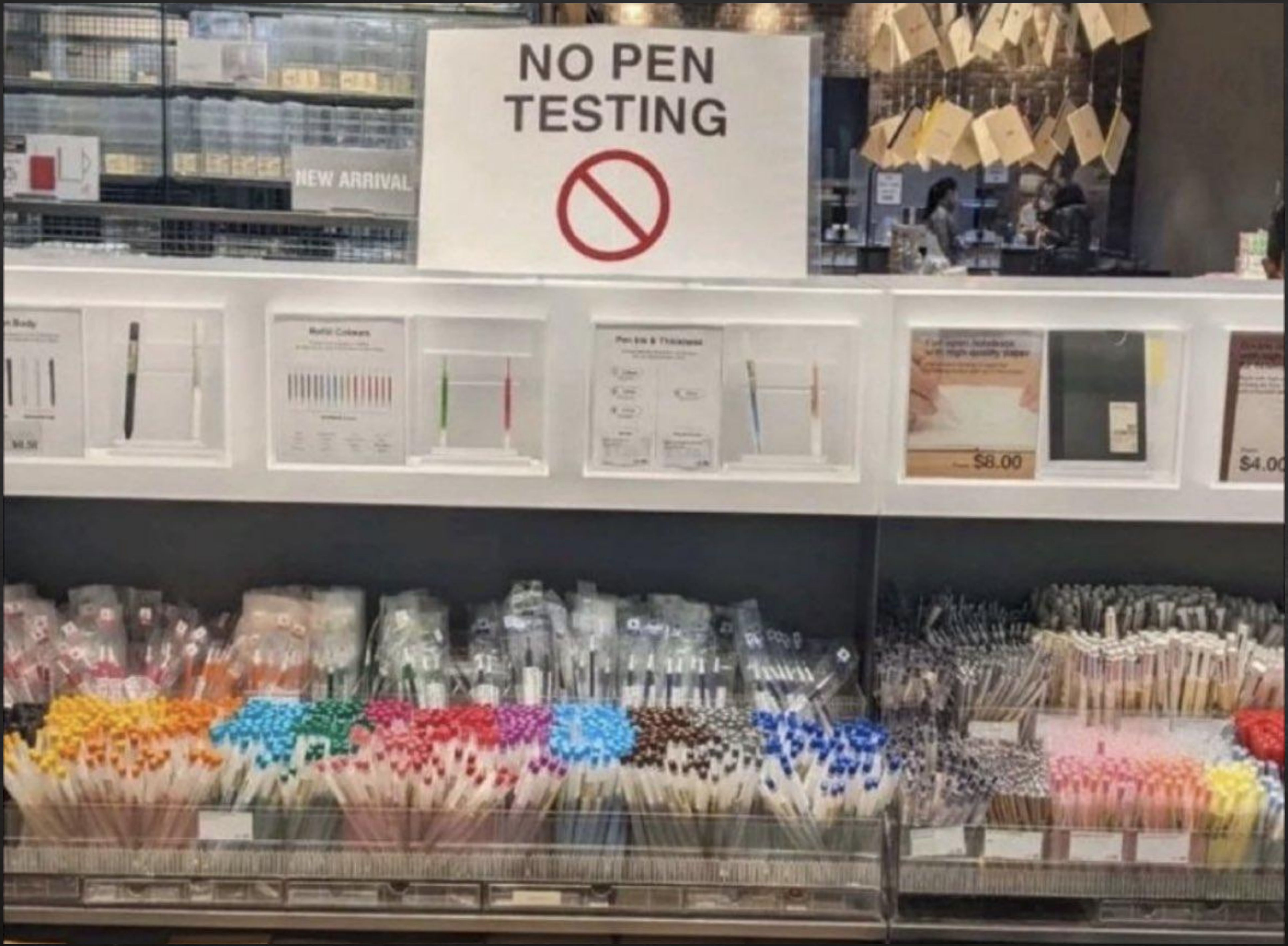
made by alphadesigner.com

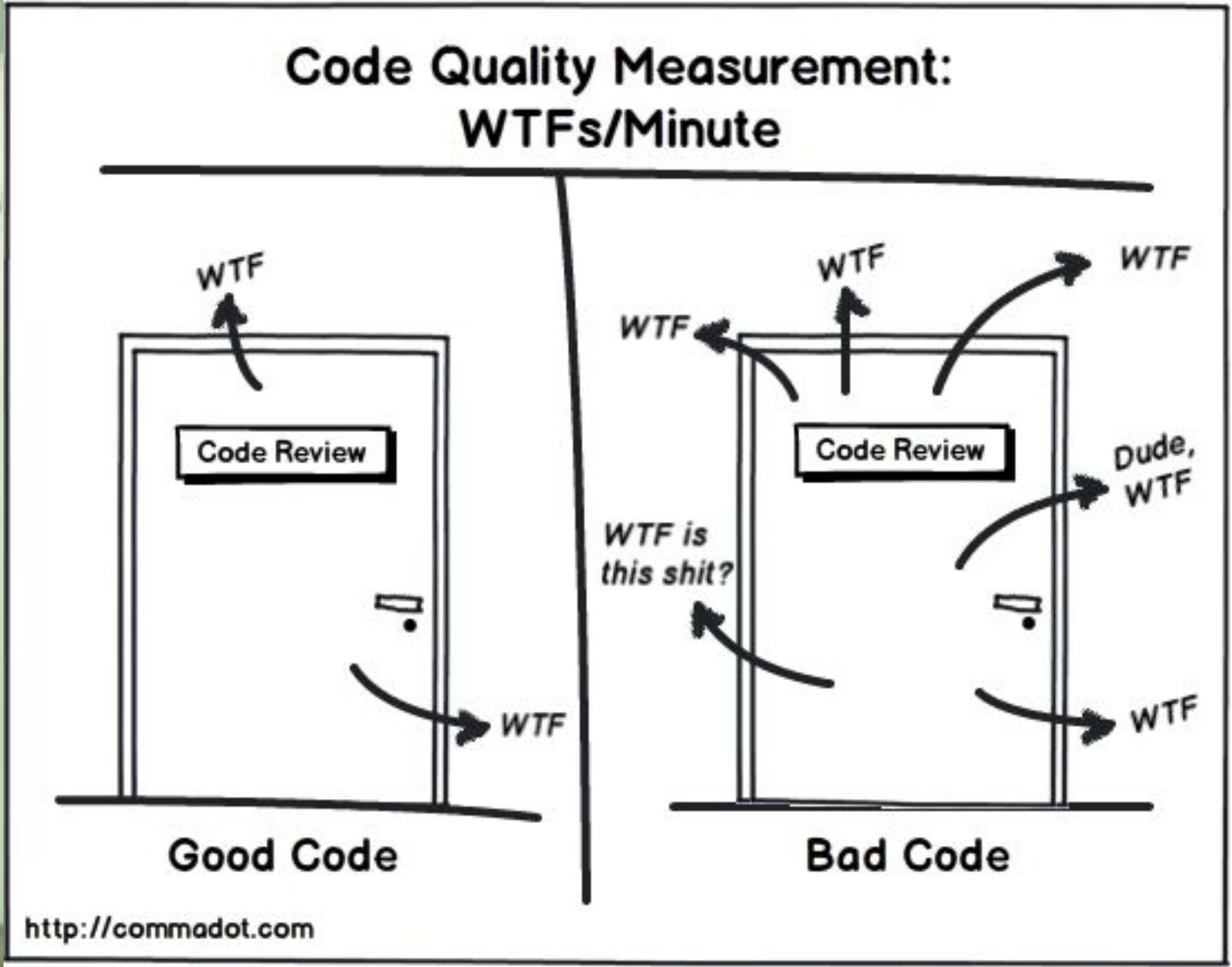


WARNING!!!

- I’m 25 yrs in and feel like we are going backwards
- I respect everyone in this room as a peer that can help solve the hard problems TOGETHER
- My opinion is my own, but I bet a few of you share it =)
- Status quo is unacceptable
- No matter what stupid example I use, its to make it light hearted and not INTENDED to offend
- My finger of blame points with one finger forward but 3 at myself
- If you disagree or want add something in **SPEAK UP**! I don’t bite.
- I don’t have all the answers, but I am trying to figure it out.
- I’ll work hard to not waste your time
- If I use language that is not “appropriate” it is likely because “im a dumb American” and have a limited vocabulary, opposed to my interest in offending you.


Shook, Hardy & Bacon L.L.P.
Sprint
KPMG
ARROW
DAMOVO
SECURITY SERVICES
POWERED BY
LARES
PENETRATION TESTING EXECUTION STANDARD
PTES
Technical Guidelines
.trust
BSIDES
A PROUD MEMBER OF
INFRAGARD
PARTNERSHIP FOR PROTECTION
CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL
CISSP
(ISC)²
CREST
ISACA
Trust in, and value from, information systems

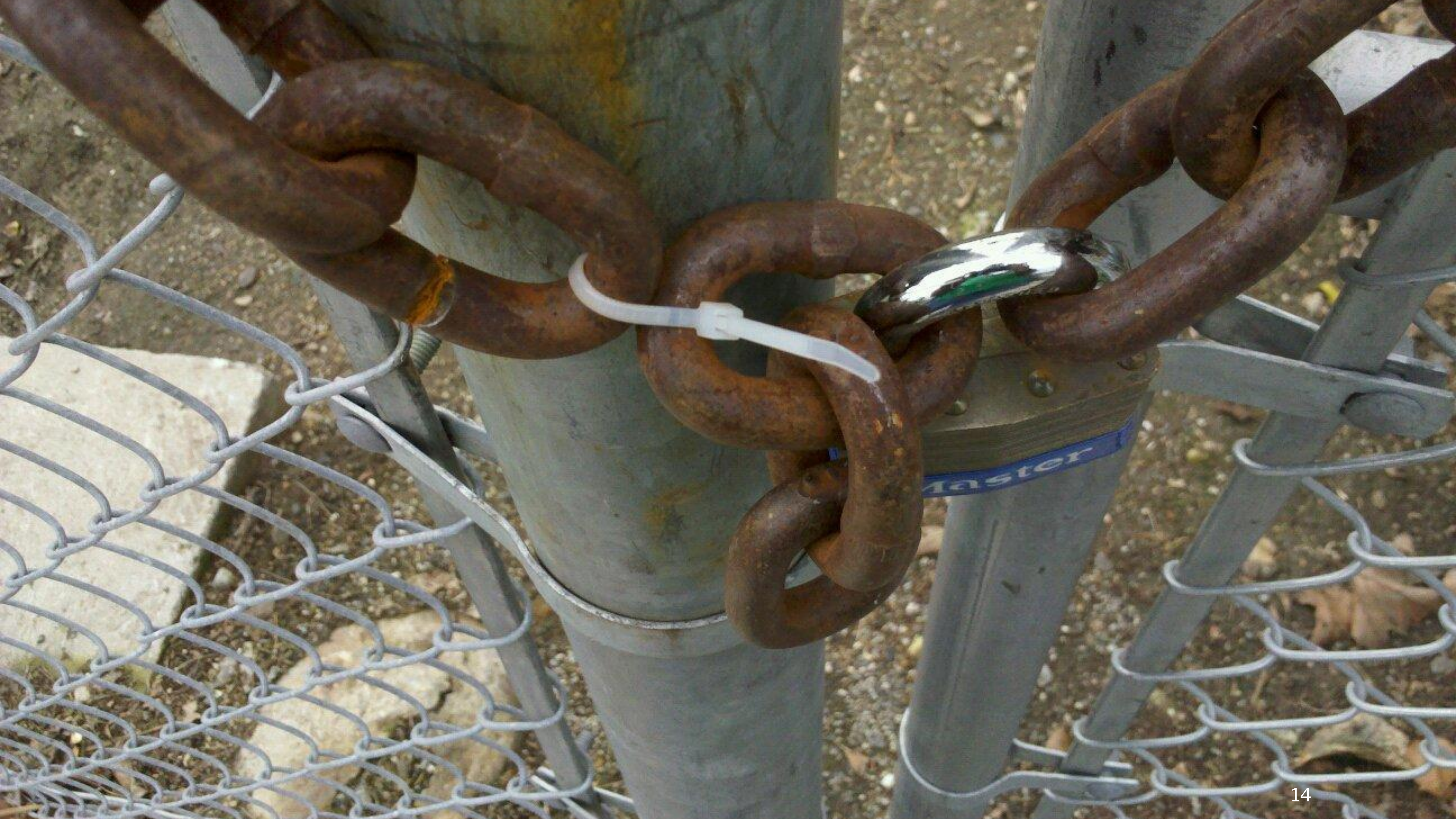

NO PEN
TESTING
NEW ARRIVAL
$8.00
$4.00

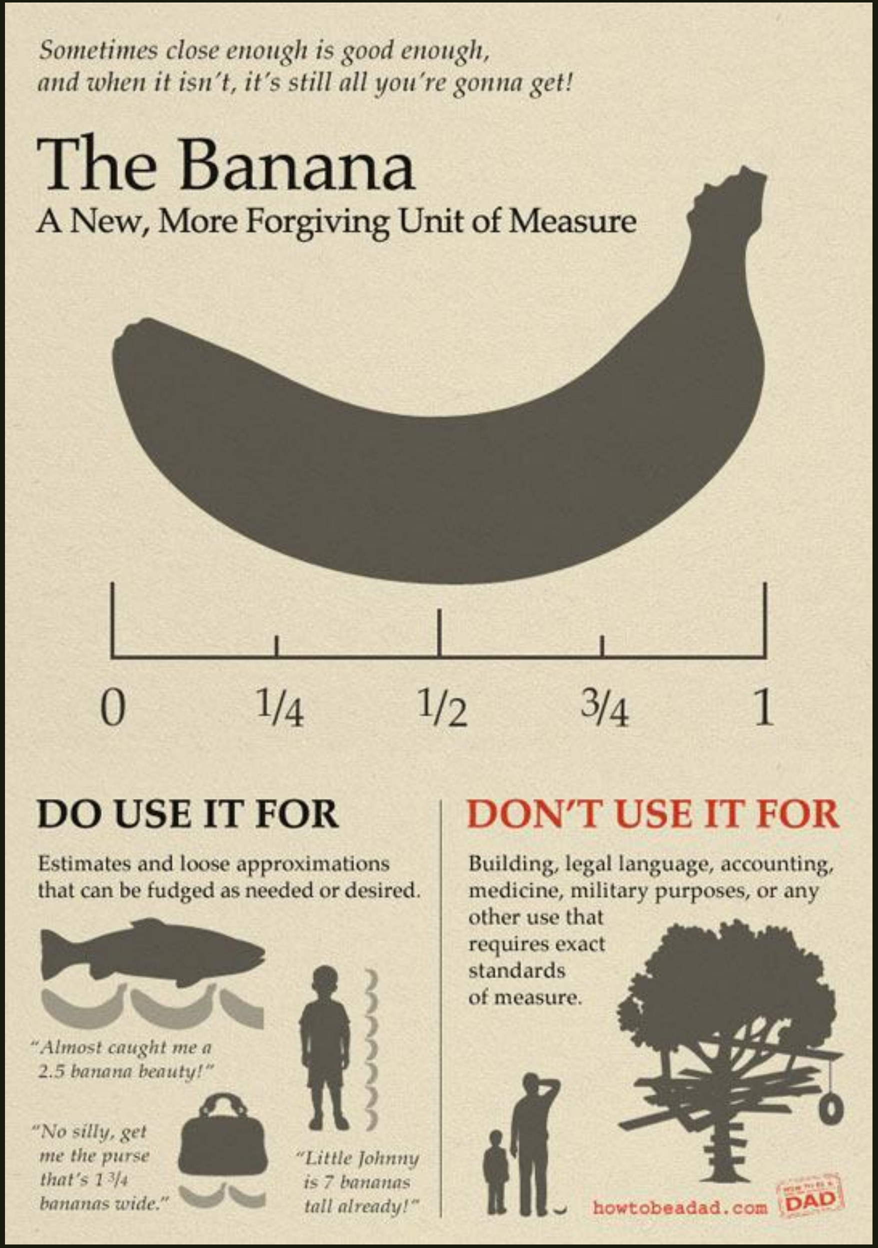

Code Quality Measurement:
WTFs/Minute
WTF
Code Review
WTF
Good Code
WTF
WTF
WTF
WTF
Code Review
Dude, WTF
WTF is this shit?
WTF
Bad Code
http://commadot.com

Marilyn Monroe Impersonation
Fail
ICANHASCHEEZBURGER.COM

Just
call us.

AQUAFINA


Master



Sometimes close enough is good enough,
and when it isn't, it's still all you're gonna get!

The Banana

A New, More Forgiving Unit of Measure

DO USE IT FOR

Estimates and loose approximations that can be fudged as needed or desired.

"Almost caught me a 2.5 banana beauty!"

"No silly, get me the purse that's 1 3/4 bananas wide."

"Little Johnny is 7 bananas tall already!"

DON'T USE IT FOR

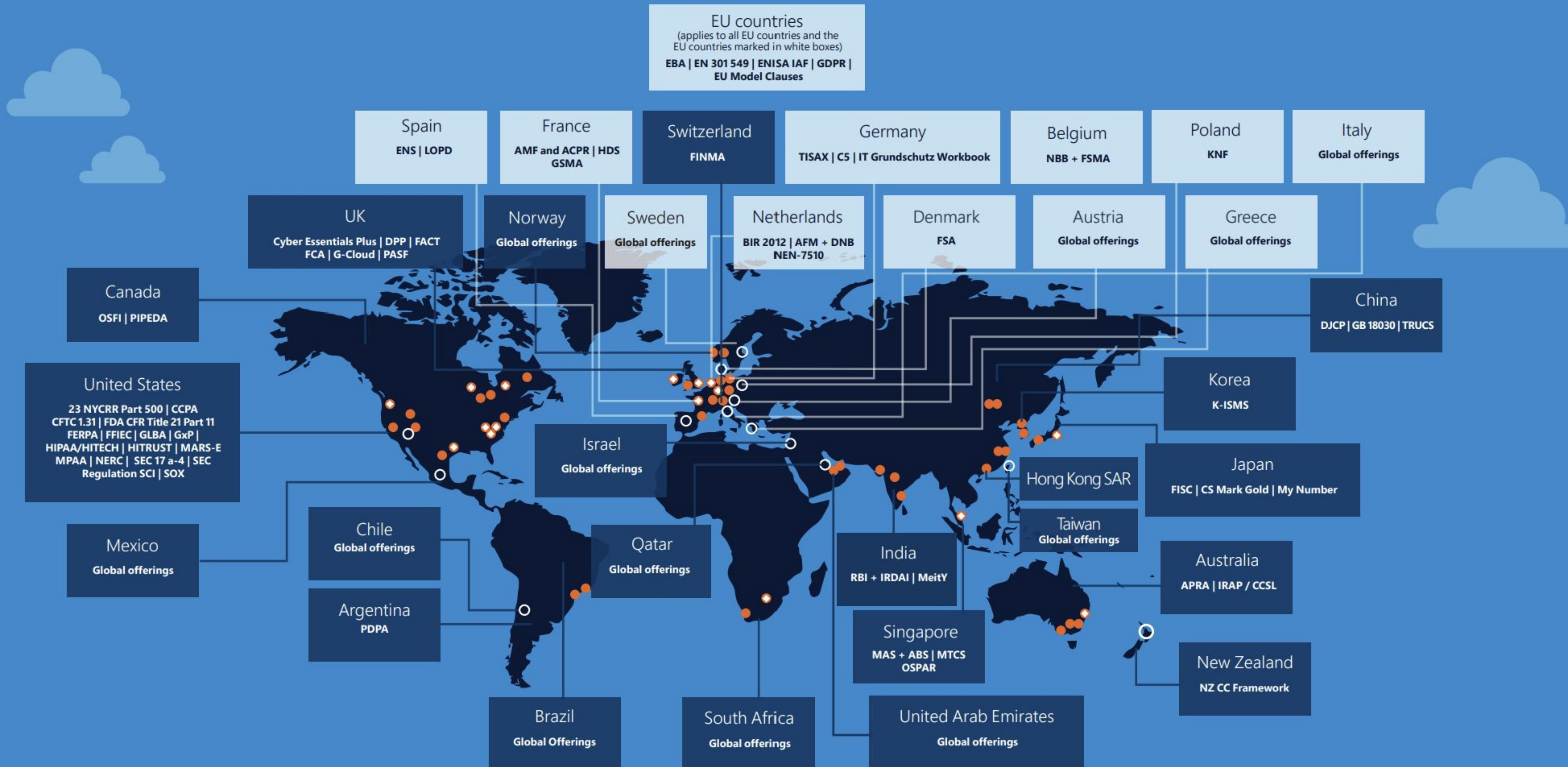
Building, legal language, accounting, medicine, military purposes, or any other use that requires exact standards of measure.

howtobeadad.com

OUR SCALES ARE BROKEN

So many negatives!!!!

ISO 20000-1:2011 | ISO 22301 | ISO 27001 | ISO 27017 | ISO 27018 | ISO 27701 | ISO 9001
PCI DSS | SOC | WCAG | CDSA | PCI DSS | Shared Assessments | TruSight



EU countries
(applies to all EU countries and the EU countries marked in white boxes)
EBA | EN 301 549 | ENISA IAF | GDPR | EU Model Clauses

Spain
ENS | LOPD

France
AMF and ACPR | HDS
GSMA

Switzerland
FINMA

Germany
TISAX | C5 | IT Grundschutz Workbook

Belgium
NBB + FSMA

Poland
KNF

Italy
Global offerings

UK
Cyber Essentials Plus | DPP | FACT
FCA | G-Cloud | PASF

Norway
Global offerings

Sweden
Global offerings

Netherlands
BIR 2012 | AFM + DNB
NEN-7510

Denmark
FSA

Austria
Global offerings

Greece
Global offerings

Canada
OSFI | PIPEDA

China
DJCP | GB 18030 | TRUCS

United States
23 NYCRR Part 500 | CCPA
CFTC 1.31 | FDA CFR Title 21 Part 11
FERPA | FFIEC | GLBA | GxP |
HIPAA/HITECH | HITRUST | MARS-E
MPAA | NERC | SEC 17 a-4 | SEC
Regulation SCI | SOX

Korea
K-ISMS

Israel
Global offerings

Hong Kong SAR

Japan
FISC | CS Mark Gold | My Number

Taiwan
Global offerings

Mexico
Global offerings

Chile
Global offerings

Qatar
Global offerings

India
RBI + IRDAI | MeitY

Australia
APRA | IRAP / CCSL

Argentina
PDPA

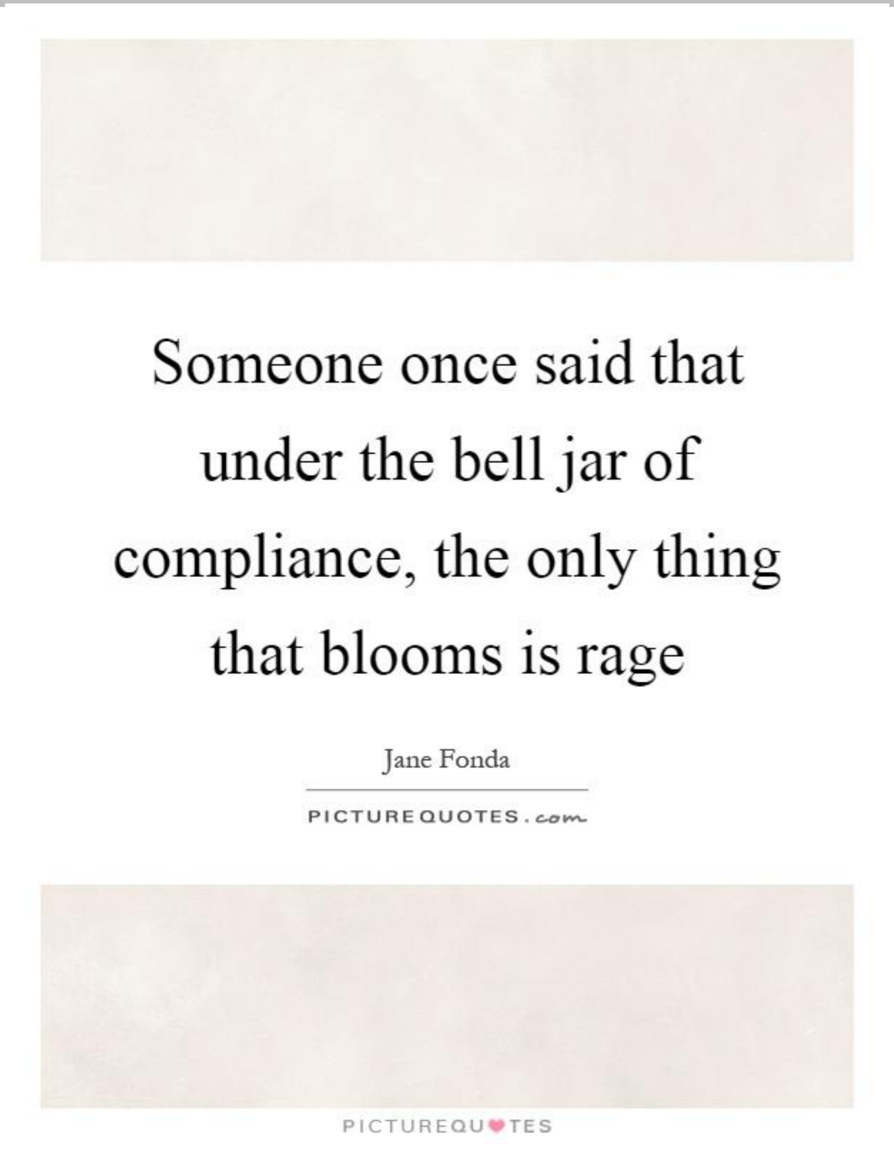
Singapore
MAS + ABS | MTCS
OSPAR

New Zealand
NZ CC Framework

Brazil
Global Offerings

South Africa
Global offerings

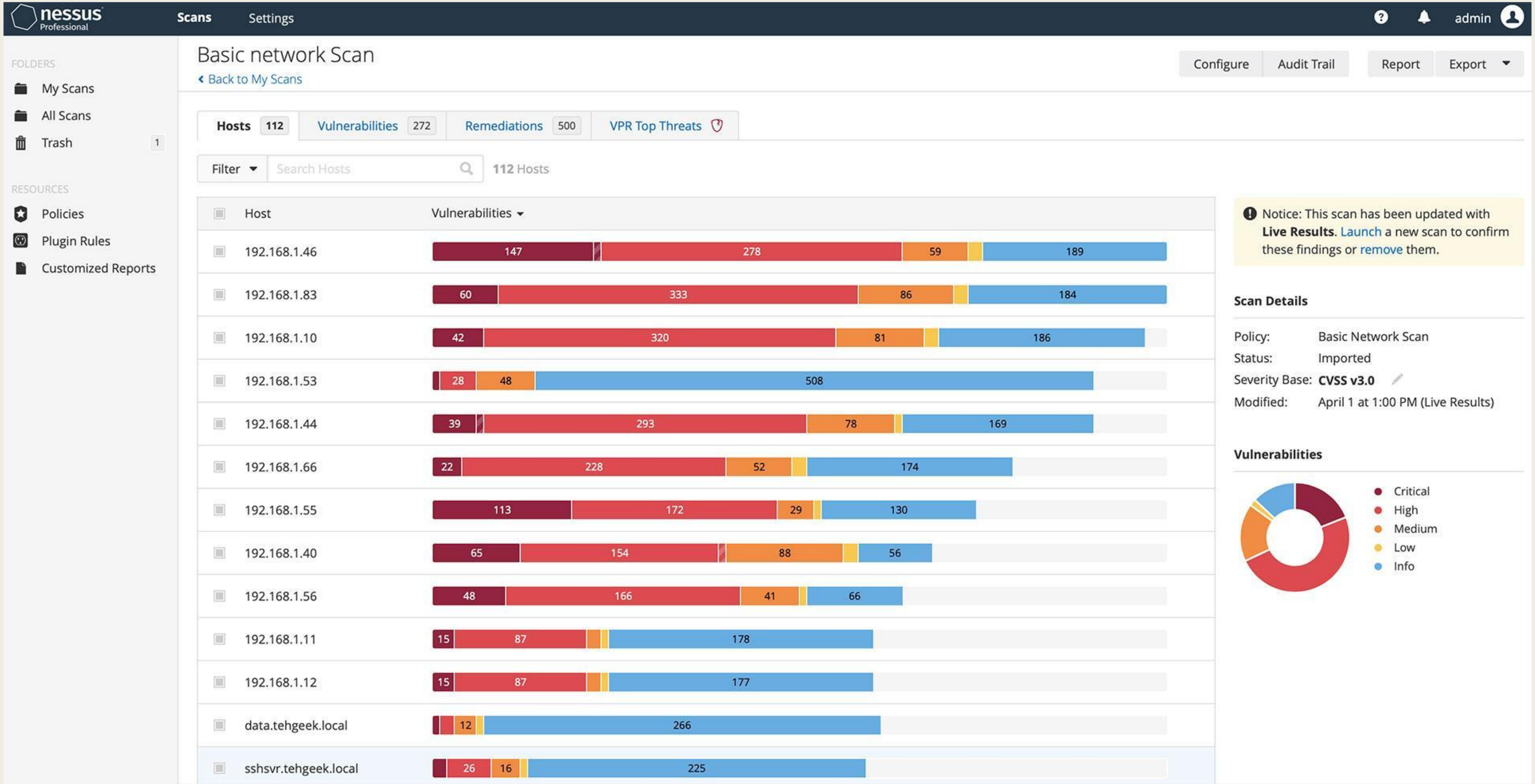
United Arab Emirates
Global offerings



Someone once said that under the bell jar of compliance, the only thing that blooms is rage

Jane Fonda

Hrm, Looks bad?



Basic network Scan

‹ Back to My Scans

Hosts 112 | Vulnerabilities 272 | Remediations 500 | VPR Top Threats

112 Hosts

Host	Vulnerabilities
192.168.1.46	147 278 59 189
192.168.1.83	60 333 86 184
192.168.1.10	42 320 81 186
192.168.1.53	28 48 508
192.168.1.44	39 293 78 169
192.168.1.66	22 228 52 174
192.168.1.55	113 172 29 130
192.168.1.40	65 154 88 56
192.168.1.56	48 166 41 66
192.168.1.11	15 87 178
192.168.1.12	15 87 177
data.tehgeek.local	12 266
sshsvr.tehgeek.local	26 16 225

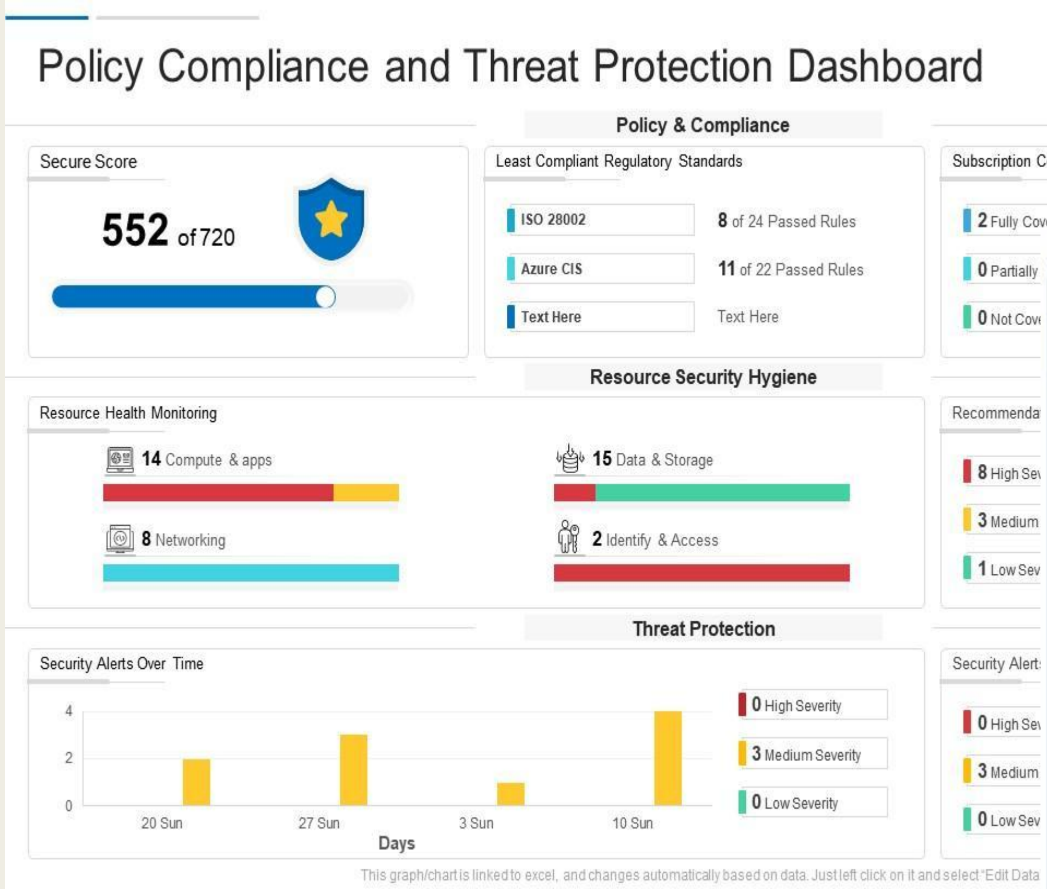
Notice: This scan has been updated with **Live Results**. Launch a new scan to confirm these findings or remove them.

Scan Details

Policy: Basic Network Scan
Status: Imported
Severity Base: **CVSS v3.0**
Modified: April 1 at 1:00 PM (Live Results)

Vulnerabilities

What do these graphs tell me?



Policy Compliance and Threat Protection Dashboard

Policy & Compliance

Secure Score

552 of 720

Least Compliant Regulatory Standards

ISO 28002	8 of 24 Passed Rules
Azure CIS	11 of 22 Passed Rules
Text Here	Text Here

Subscription Coverage

- 2 Fully Covered
- 0 Partially
- 0 Not Cov

Resource Security Hygiene

Resource Health Monitoring

- 14 Compute & apps
- 15 Data & Storage
- 8 Networking
- 2 Identify & Access

Recommenda

- 8 High Se
- 3 Medium
- 1 Low Sev

Threat Protection

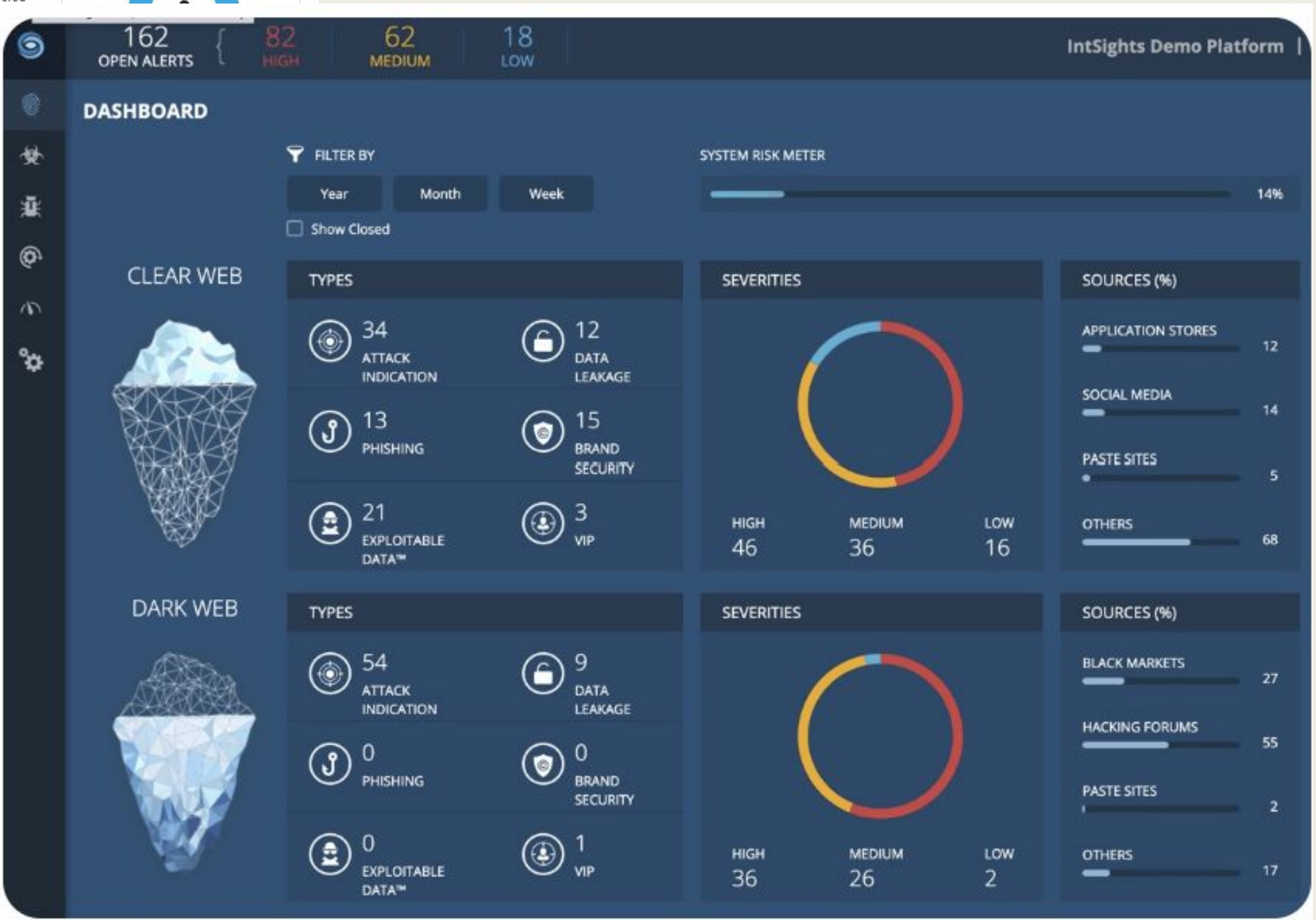
Security Alerts Over Time

- 0 High Severity
- 3 Medium Severity
- 0 Low Severity

Security Alert

- 0 High Se
- 3 Medium
- 0 Low Sev

This graph/chart is linked to excel, and changes automatically based on data. Just left click on it and select "Edit Data



162	82	62	18
OPEN ALERTS	HIGH	MEDIUM	LOW

IntSights Demo Platform

DASHBOARD

FILTER BY: Year | Month | Week

□ Show Closed

SYSTEM RISK METER 14%

CLEAR WEB

TYPES

34 ATTACK INDICATION	12 DATA LEAKAGE
13 PHISHING	15 BRAND SECURITY
21 EXPLOITABLE DATA™	3 VIP

SEVERITIES

HIGH	MEDIUM	LOW
46	36	16

SOURCES (%)

APPLICATION STORES	12
SOCIAL MEDIA	14
PASTE SITES	5
OTHERS	68

DARK WEB

TYPES

54 ATTACK INDICATION	9 DATA LEAKAGE
0 PHISHING	0 BRAND SECURITY
0 EXPLOITABLE DATA™	1 VIP

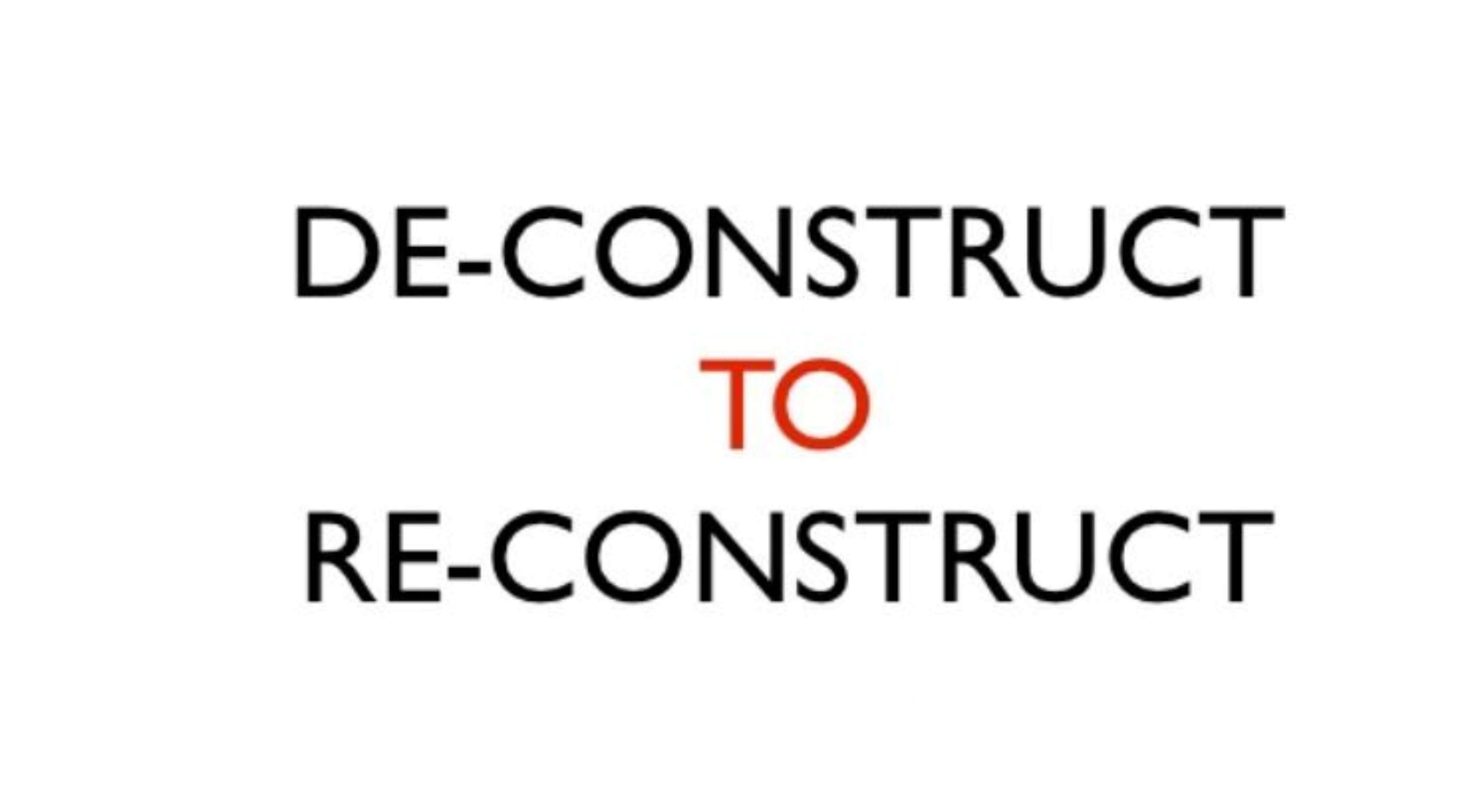
SEVERITIES

HIGH	MEDIUM	LOW
36	26	2

SOURCES (%)

BLACK MARKETS	27
HACKING FORUMS	55
PASTE SITES	2
OTHERS	17

Balbix
1st year in InfoSec
10 years in InfoSec

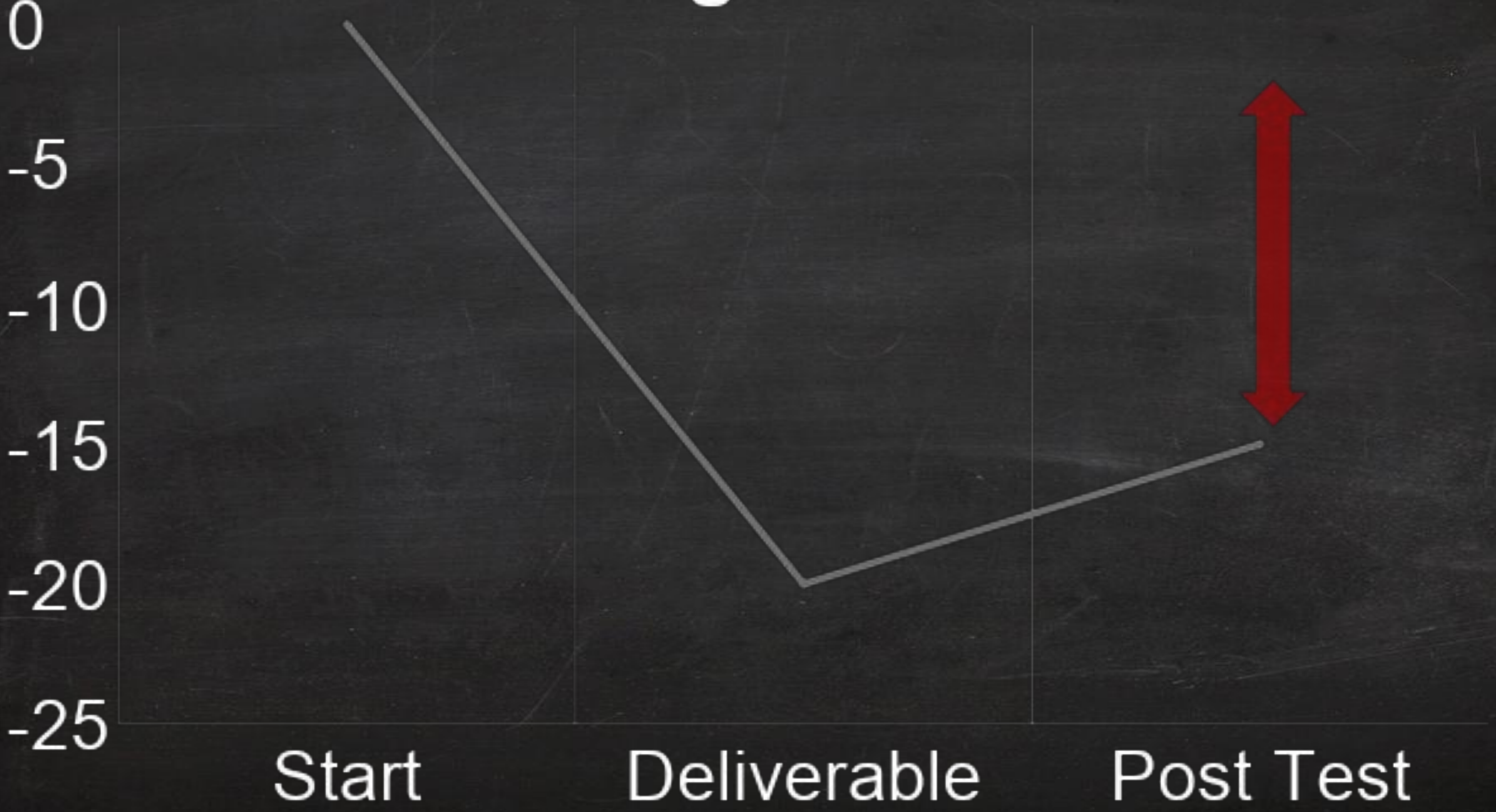


DE-CONSTRUCT

TO

RE-CONSTRUCT

Testing Metrics



Traditional Results

- Blame and Shame for Vulnerabilities
- Limited metrics
- Limited repeatability
- Nonstandard terminology
- Success of one team is determined by the failure of another
- Limited to no collaboration
- Limited to no OWNERSHIP of the debt created by the test
- Emotionally toxic
- Tests of design NOT Effectiveness

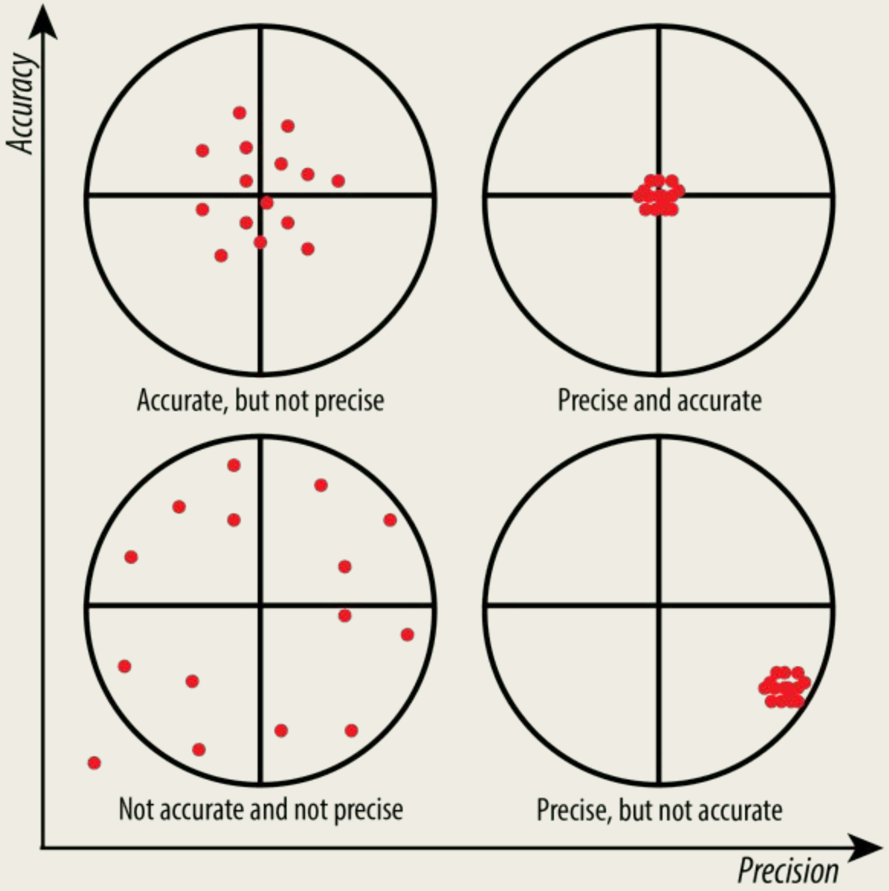
FIRST, WE MUST BUILD POSITIVE RELATIONSHIPS

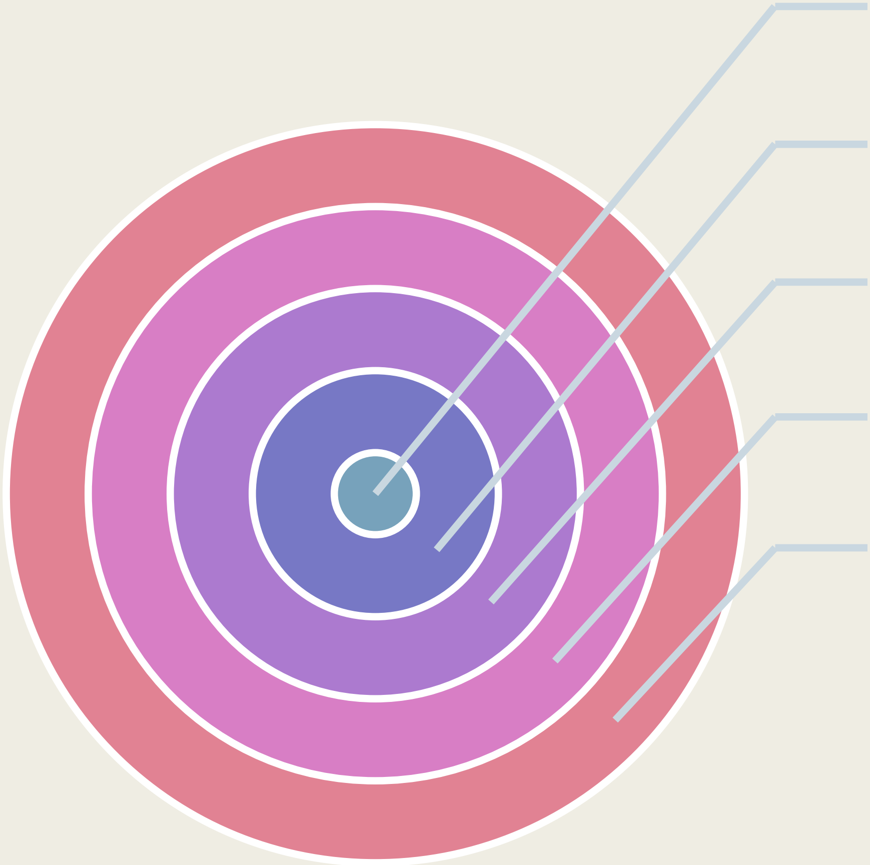
Shame and Blame do not BUILD a program.

Starting with positive intentions

- Reduce the amount of testing debt
- Create team collaboration
- Define suitable boundaries for all parties involved
- Measure everything
- Learn through experience
- Prove that we IMPROVE
- Remove the legacy scale so we can SCALE
- Transition to a proactive security program
- Remove Fear, Uncertainty, and Doubt to be replaced with data to make more informed decisions.
- Build confidence
- ELIMINATE shame / blame
- Leverage cognitive and neuro diversity (360 views)

Precision vs Accuracy


Accuracy
Accurate, but not precise
Precise and accurate
Not accurate and not precise
Precise, but not accurate
Precision



Funded innovation

Tactics

Vulnerabilitie
s

Compliance

Best Practice

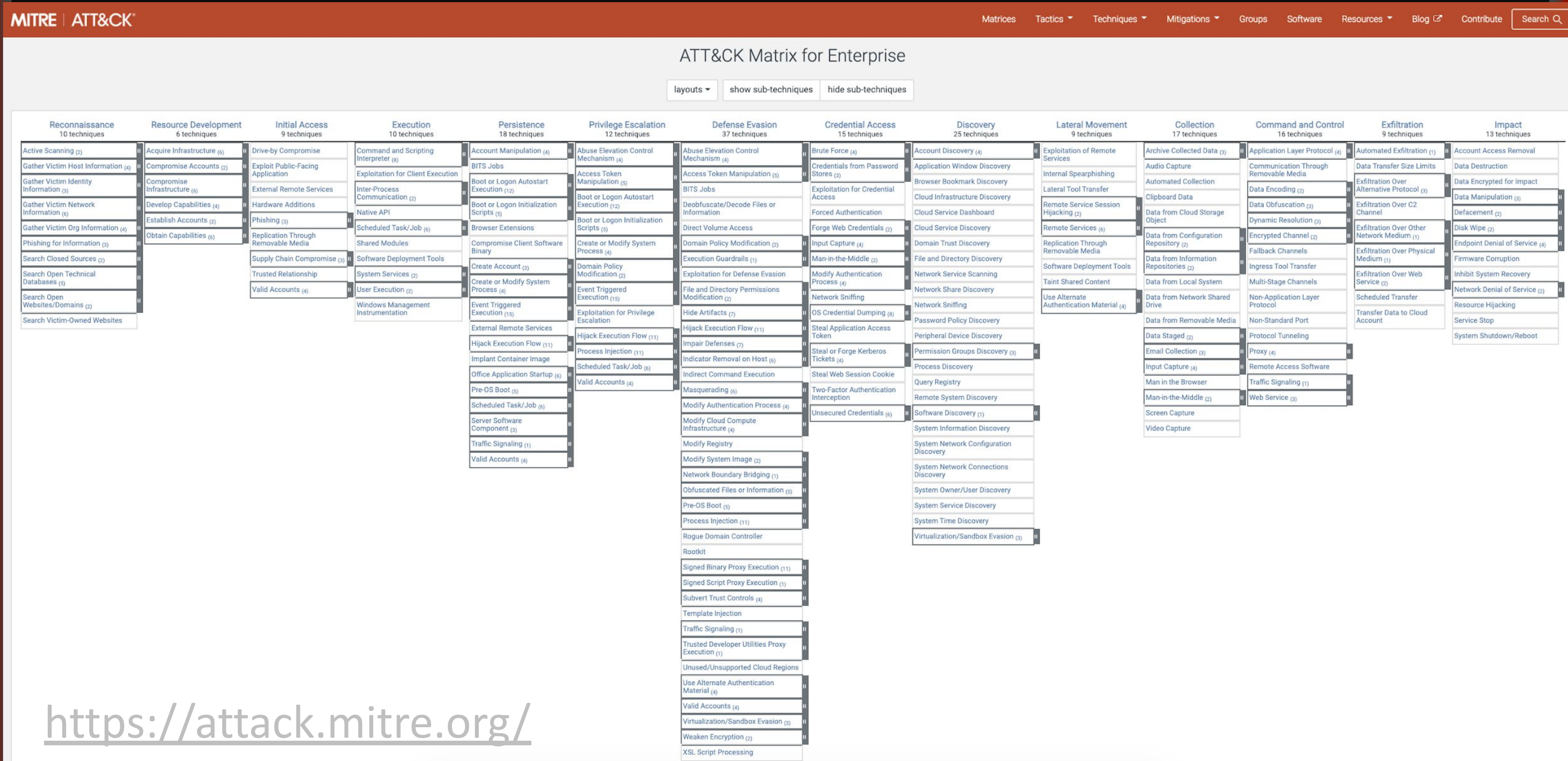
WHAT IS A TTP?

Tactics, Techniques, and Procedures (TTPs) is a key concept in cybersecurity and threat intelligence. The purpose is to identify patterns of behavior which can be used to defend against specific strategies and threat vectors used by malicious actors

Efficiency is doing the thing right. Effectiveness is doing the right thing.

Peter F. Drucker

How attackers work

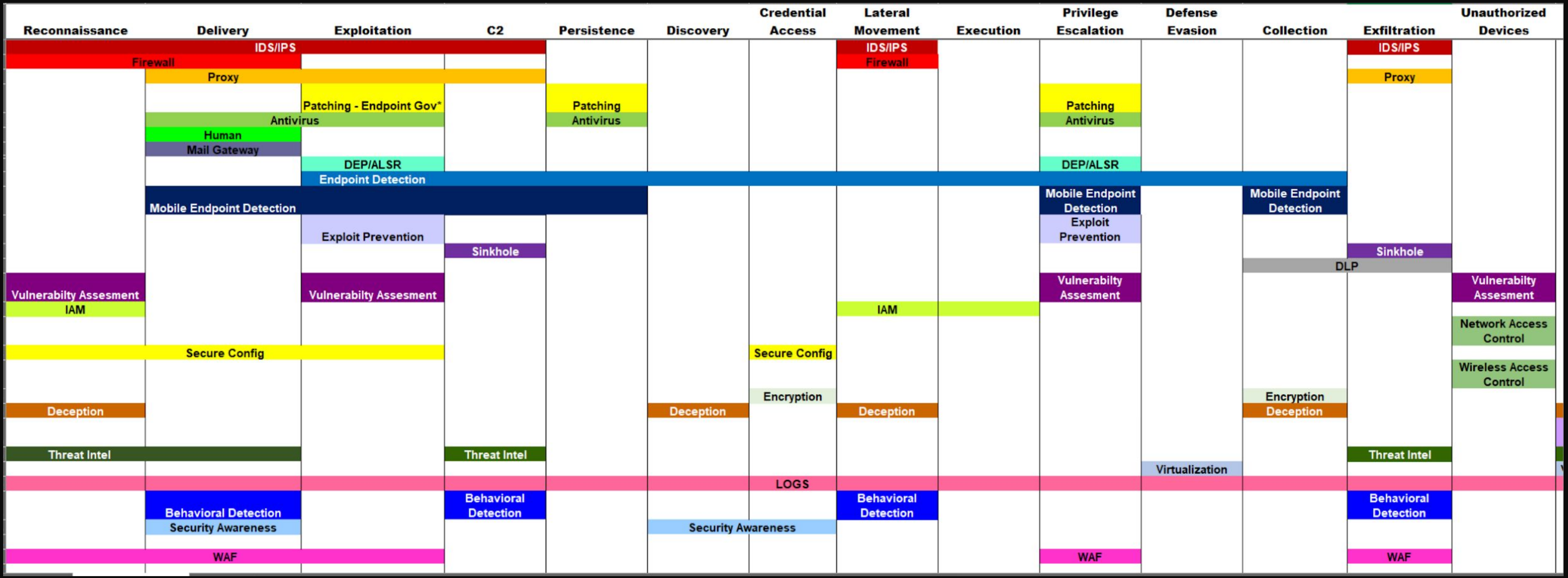


ATT&CK Matrix for Enterprise

Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 15 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (12)	Boot or Logon Autostart Execution (12)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Scheduled Task/Job (6)	Browser Extensions	Create or Modify System Process (4)	Direct Volume Access	Forge Web Credentials (2)	Cloud Service Dashboard	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Domain Policy Modification (2)	Domain Policy Modification (2)	Input Capture (4)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)		Supply Chain Compromise (3)	Software Deployment Tools	Create Account (3)	Event Triggered Execution (15)	Execution Guardrails (1)	Man-in-the-Middle (2)	Domain Trust Discovery	Software Deployment Tools	Data from Information Repositories (2)	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	System Services (2)	Create or Modify System Process (4)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process (4)	File and Directory Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (2)		Valid Accounts (4)	User Execution (2)	Event Triggered Execution (15)	Hijack Execution Flow (11)	File and Directory Permissions Modification (2)	Network Sniffing	Network Service Scanning	Use Alternate Authentication Material (4)	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			Windows Management Instrumentation	External Remote Services	Process Injection (11)	Hide Artifacts (7)	OS Credential Dumping (8)	Network Share Discovery		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service (2)
				Hijack Execution Flow (11)	Scheduled Task/Job (6)	Hijack Execution Flow (11)	Steal Application Access Token	Network Sniffing		Data Staged (2)	Non-Standard Port		Resource Hijacking
				Implant Container Image	Valid Accounts (4)	Impair Defenses (7)	Steal or Forge Kerberos Tickets (4)	Password Policy Discovery		Email Collection (3)	Protocol Tunneling		Service Stop
				Office Application Startup (6)		Indicator Removal on Host (6)	Steal Web Session Cookie	Peripheral Device Discovery		Input Capture (4)	Proxy (4)		System Shutdown/Reboot
				Pre-OS Boot (5)		Indirect Command Execution	Two-Factor Authentication Interception	Permission Groups Discovery (3)		Man in the Browser	Remote Access Software		
				Scheduled Task/Job (6)		Masquerading (6)	Unsecured Credentials (6)	Process Discovery		Man-in-the-Middle (2)	Traffic Signaling (1)		
				Server Software Component (3)		Modify Authentication Process (4)		Query Registry		Screen Capture	Web Service (3)		
				Traffic Signaling (1)		Modify Cloud Compute Infrastructure (4)		Remote System Discovery		Video Capture			
				Valid Accounts (4)		Modify Registry		Software Discovery (1)					
						Modify System Image (2)		System Information Discovery					
						Network Boundary Bridging (1)		System Network Configuration Discovery					
						Obfuscated Files or Information (5)		System Network Connections Discovery					
						Pre-OS Boot (5)		System Owner/User Discovery					
						Process Injection (11)		System Service Discovery					
						Rogue Domain Controller		System Time Discovery					
						Rootkit		Virtualization/Sandbox Evasion (3)					
						Signed Binary Proxy Execution (11)							
						Signed Script Proxy Execution (1)							
						Subvert Trust Controls (4)							
						Template Injection							
						Traffic Signaling (1)							
						Trusted Developer Utilities Proxy Execution (1)							
						Unused/Unsupported Cloud Regions							
						Use Alternate Authentication Material (4)							
						Valid Accounts (4)							
						Virtualization/Sandbox Evasion (3)							
						Weaken Encryption (2)							
						XSL Script Processing							

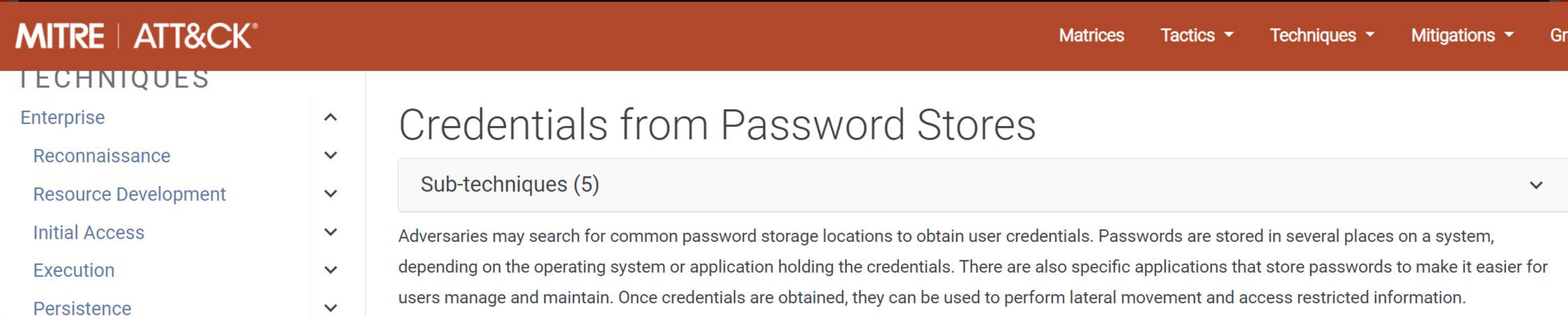
https://attack.mitre.org/

How & Where do our controls meet attackers



Reconnaissance	Delivery	Exploitation	C2	Persistence	Discovery	Credential Access	Lateral Movement	Execution	Privilege Escalation	Defense Evasion	Collection	Exfiltration	Unauthorized Devices
IDS/IPS	IDS/IPS	IDS/IPS	IDS/IPS				IDS/IPS					IDS/IPS	
Firewall	Firewall						Firewall						
	Proxy	Proxy	Proxy									Proxy	
		Patching - Endpoint Gov*		Patching					Patching				
	Antivirus	Antivirus		Antivirus					Antivirus				
	Human												
	Mail Gateway												
		DEP/ALSR							DEP/ALSR				
		Endpoint Detection	Endpoint Detection	Endpoint Detection	Endpoint Detection	Endpoint Detection	Endpoint Detection	Endpoint Detection	Endpoint Detection	Endpoint Detection	Endpoint Detection		
	Mobile Endpoint Detection	Mobile Endpoint Detection	Mobile Endpoint Detection	Mobile Endpoint Detection					Mobile Endpoint Detection		Mobile Endpoint Detection		
		Exploit Prevention							Exploit Prevention				
			Sinkhole									Sinkhole	
											DLP	DLP	
Vulnerabilty Assesment		Vulnerabilty Assesment							Vulnerabilty Assesment				Vulnerabilty Assesment
IAM							IAM	IAM					
													Network Access Control
Secure Config	Secure Config	Secure Config				Secure Config							
													Wireless Access Control
						Encryption					Encryption		
Deception					Deception		Deception				Deception		
Threat Intel	Threat Intel		Threat Intel									Threat Intel	
										Virtualization			
LOGS	LOGS	LOGS	LOGS	LOGS	LOGS	LOGS	LOGS	LOGS	LOGS	LOGS	LOGS	LOGS	LOGS
	Behavioral Detection		Behavioral Detection				Behavioral Detection					Behavioral Detection	
	Security Awareness				Security Awareness	Security Awareness							
WAF	WAF	WAF							WAF			WAF	

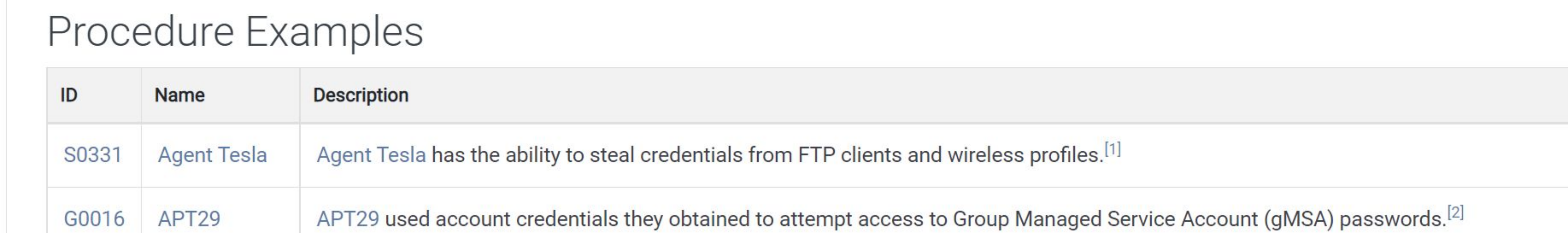
Understanding an attack



Credentials from Password Stores

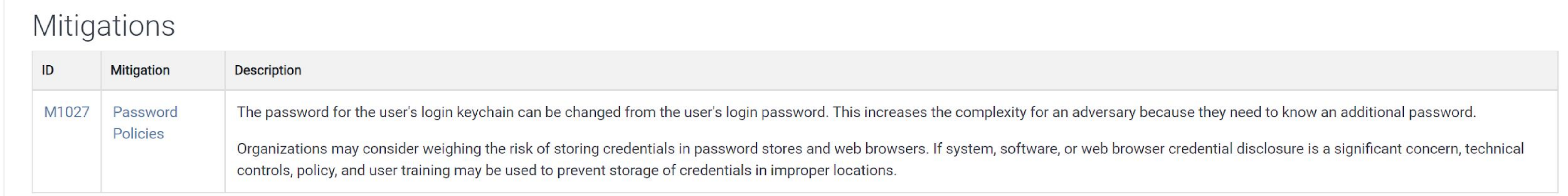
Sub-techniques (5)

Adversaries may search for common password storage locations to obtain user credentials. Passwords are stored in several places on a system, depending on the operating system or application holding the credentials. There are also specific applications that store passwords to make it easier for users manage and maintain. Once credentials are obtained, they can be used to perform lateral movement and access restricted information.



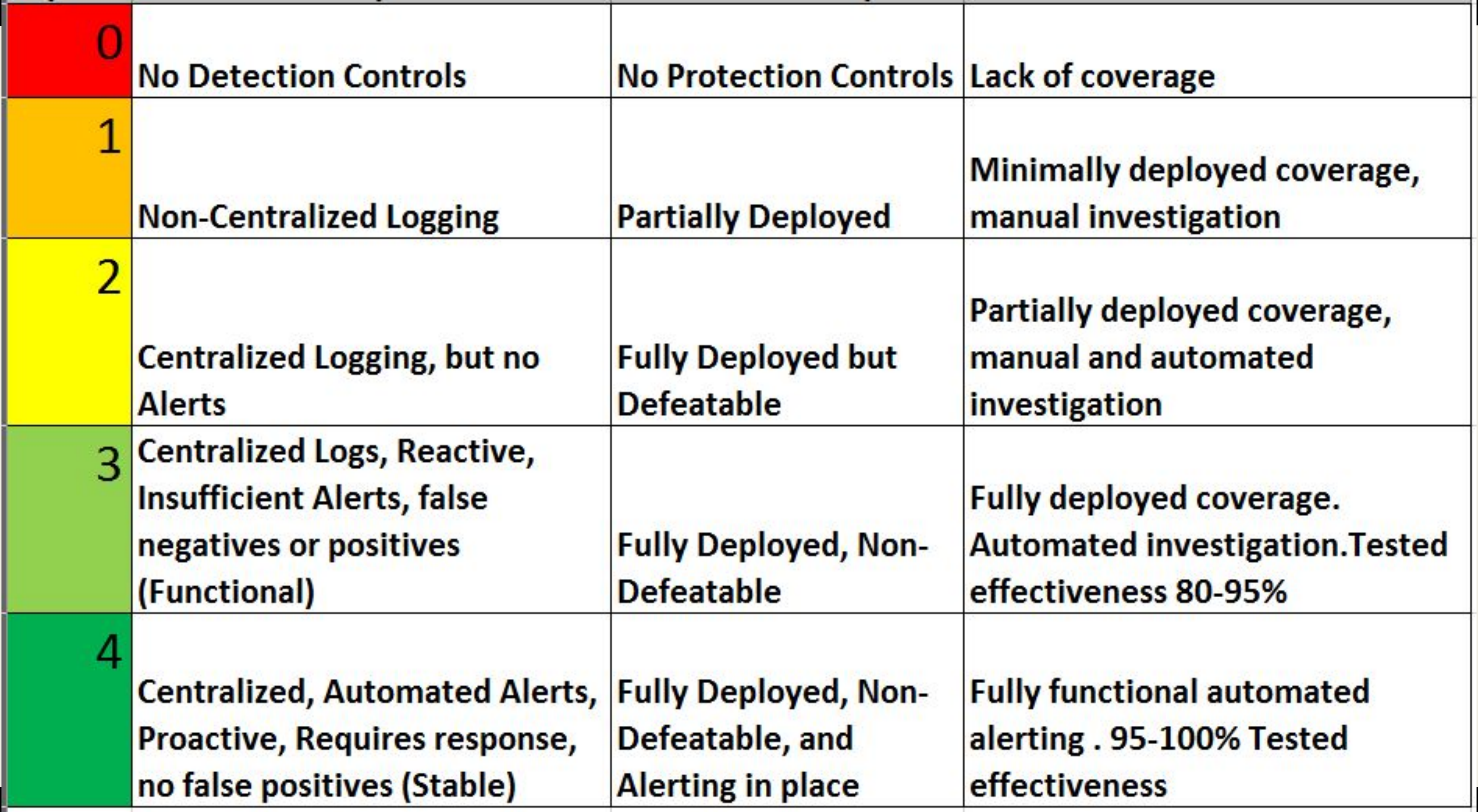
Procedure Examples

ID	Name	Description
S0331	Agent Tesla	Agent Tesla has the ability to steal credentials from FTP clients and wireless profiles.[1]
G0016	APT29	APT29 used account credentials they obtained to attempt access to Group Managed Service Account (gMSA) passwords.[2]



Mitigations

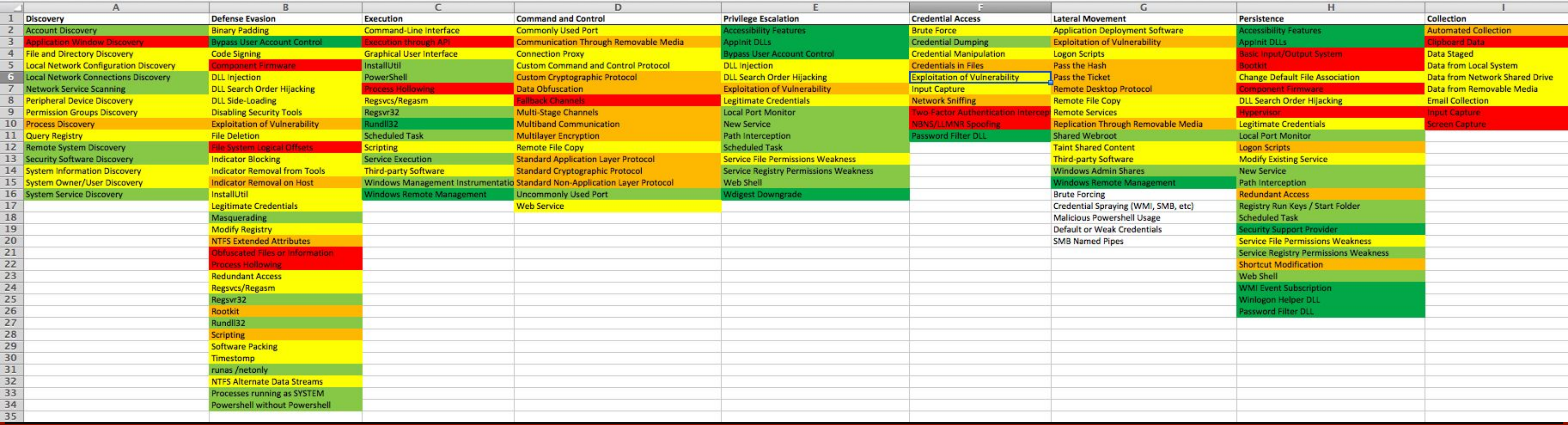
ID	Mitigation	Description
M1027	Password Policies	The password for the user's login keychain can be changed from the user's login password. This increases the complexity for an adversary because they need to know an additional password. Organizations may consider weighing the risk of storing credentials in password stores and web browsers. If system, software, or web browser credential disclosure is a significant concern, technical controls, policy, and user training may be used to prevent storage of credentials in improper locations.



0	No Detection Controls	No Protection Controls	Lack of coverage
1	Non-Centralized Logging	Partially Deployed	Minimally deployed coverage, manual investigation
2	Centralized Logging, but no Alerts	Fully Deployed but Defeatable	Partially deployed coverage, manual and automated investigation
3	Centralized Logs, Reactive, Insufficient Alerts, false negatives or positives (Functional)	Fully Deployed, Non-Defeatable	Fully deployed coverage. Automated investigation.Tested effectiveness 80-95%
4	Centralized, Automated Alerts, Proactive, Requires response, no false positives (Stable)	Fully Deployed, Non-Defeatable, and Alerting in place	Fully functional automated alerting . 95-100% Tested effectiveness

Score yourself against each technique and analyze results.

- Ability to Protect
- Ability to detect
- Quality of detection
- Coverage
- Root Cause Analysis of score

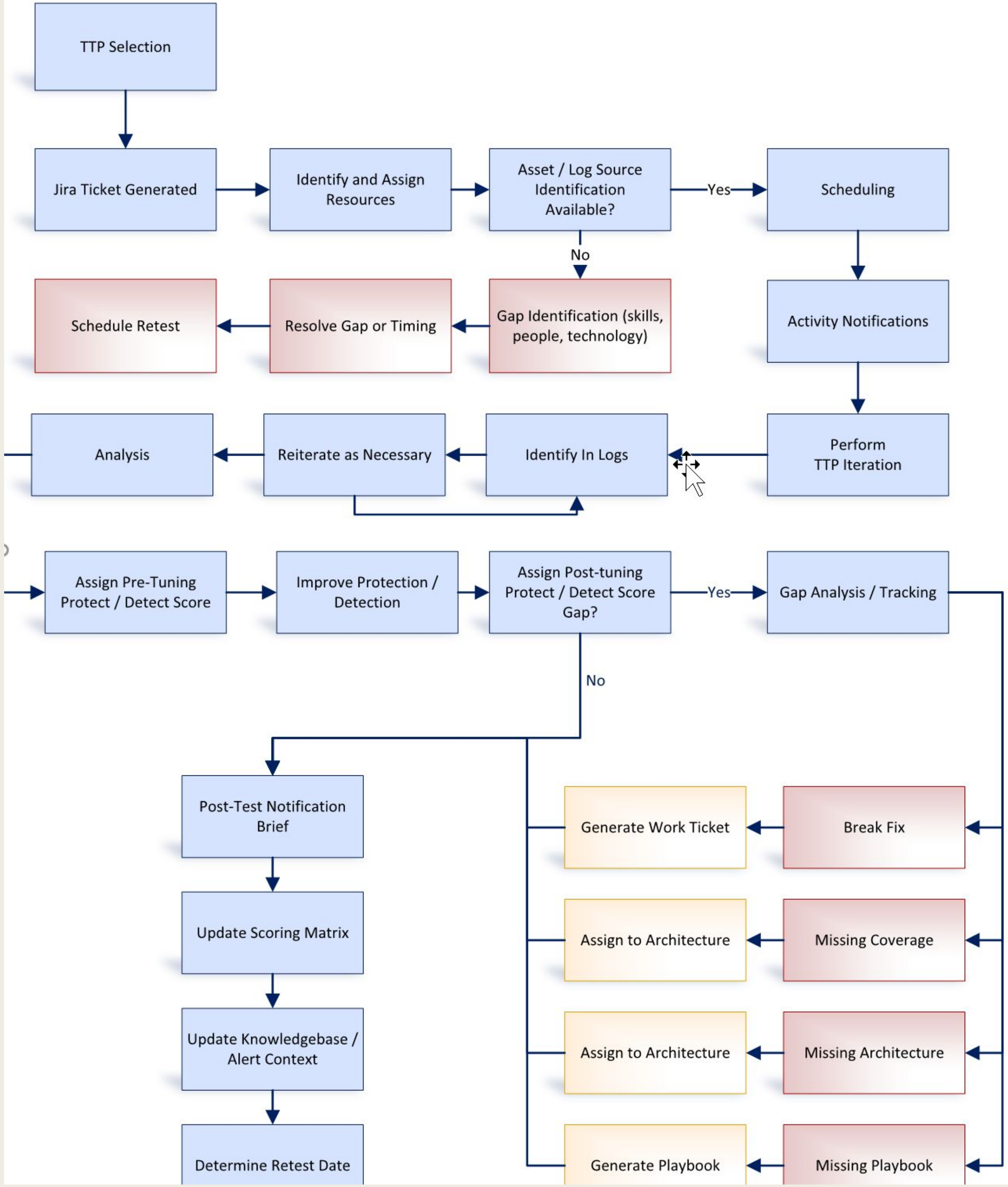


	A	B	C	D	E	F	G	H	I
1	**Discovery**	**Defense Evasion**	**Execution**	**Command and Control**	**Privilege Escalation**	**Credential Access**	**Lateral Movement**	**Persistence**	**Collection**
2	Account Discovery	Binary Padding	Command-Line Interface	Commonly Used Port	Accessibility Features	Brute Force	Application Deployment Software	Accessibility Features	Automated Collection
3	Application Window Discovery	Bypass User Account Control	Execution through API	Communication Through Removable Media	AppInit DLLs	Credential Dumping	Exploitation of Vulnerability	AppInit DLLs	Clipboard Data
4	File and Directory Discovery	Code Signing	Graphical User Interface	Connection Proxy	Bypass User Account Control	Credential Manipulation	Logon Scripts	Basic Input/Output System	Data Staged
5	Local Network Configuration Discovery	Component Firmware	InstallUtil	Custom Command and Control Protocol	DLL Injection	Credentials in Files	Pass the Hash	Bootkit	Data from Local System
6	Local Network Connections Discovery	DLL Injection	PowerShell	Custom Cryptographic Protocol	DLL Search Order Hijacking	Exploitation of Vulnerability	Pass the Ticket	Change Default File Association	Data from Network Shared Drive
7	Network Service Scanning	DLL Search Order Hijacking	Process Hollowing	Data Obfuscation	Exploitation of Vulnerability	Input Capture	Remote Desktop Protocol	Component Firmware	Data from Removable Media
8	Peripheral Device Discovery	DLL Side-Loading	Regsvcs/Regasm	Fallback Channels	Legitimate Credentials	Network Sniffing	Remote File Copy	DLL Search Order Hijacking	Email Collection
9	Permission Groups Discovery	Disabling Security Tools	Regsvr32	Multi-Stage Channels	Local Port Monitor	Two Factor Authentication Intercep	Remote Services	Hypervisor	Input Capture
10	Process Discovery	Exploitation of Vulnerability	Rundll32	Multiband Communication	New Service	NBNS/LLMNR Spoofing	Replication Through Removable Media	Legitimate Credentials	Screen Capture
11	Query Registry	File Deletion	Scheduled Task	Multilayer Encryption	Path Interception	Password Filter DLL	Shared Webroot	Local Port Monitor	
12	Remote System Discovery	File System Logical Offsets	Scripting	Remote File Copy	Scheduled Task		Taint Shared Content	Logon Scripts	
13	Security Software Discovery	Indicator Blocking	Service Execution	Standard Application Layer Protocol	Service File Permissions Weakness		Third-party Software	Modify Existing Service	
14	System Information Discovery	Indicator Removal from Tools	Third-party Software	Standard Cryptographic Protocol	Service Registry Permissions Weakness		Windows Admin Shares	New Service	
15	System Owner/User Discovery	Indicator Removal on Host	Windows Management Instrumentatio	Standard Non-Application Layer Protocol	Web Shell		Windows Remote Management	Path Interception	
16	System Service Discovery	InstallUtil	Windows Remote Management	Uncommonly Used Port	Wdigest Downgrade		Brute Forcing	Redundant Access	
17		Legitimate Credentials		Web Service			Credential Spraying (WMI, SMB, etc)	Registry Run Keys / Start Folder	
18		Masquerading					Malicious Powershell Usage	Scheduled Task	
19		Modify Registry					Default or Weak Credentials	Security Support Provider	
20		NTFS Extended Attributes					SMB Named Pipes	Service File Permissions Weakness	
21		Obfuscated Files or Information						Service Registry Permissions Weakness	
22		Process Hollowing						Shortcut Modification	
23		Redundant Access						Web Shell	
24		Regsvcs/Regasm						WMI Event Subscription	
25		Regsvr32						Winlogon Helper DLL	
26		Rootkit						Password Filter DLL	
27		Rundll32							
28		Scripting							
29		Software Packing							
30		Timestomp							
31		runas /netonly							
32		NTFS Alternate Data Streams							
33		Processes running as SYSTEM							
34		Powershell without Powershell							
35									

Technique	Function	Methods for detection	Methods for protection	Sophistication	Detection	End Maturity	Timing	Protection	Begin Maturity	Confidence	Last Test Date
LSASS password/ hash recovery	Local Security Authority Subsystem Service (LSASS) is a process in Microsoft Windows operating systems that is responsible for enforcing the security policy on the system. It verifies users logging on to a Windows computer or server, handles password changes, and creates access tokens. (from Wikipedia) For the purposes of Single Sign On (SSO) in Windows environments, lsass also stores the NT hash and sometimes, in the case of wdigest, the cleartext credentials of users who have logged into the system. These can be recovered by dumping the contents of the process in memory through use tools such as procdump and mimikatz.	The most optimal way to detect this is to identify processes that are crossproc'd into lsass. The signal to noise ratio here is high, due to the nature of lsass' function. Typically meterpreter uses rundll32 to run, so identifying rundll32 into lsass along with processes injected into winlogon that cross process into lsass will reliably identify malicious activity	An automated password management tool such as CyberArk can be used to randomize passwords and change them after every use, thus decreasing the efficacy of mimikatz as any recovered credential will likely be expired. Further, on all windows 8/2012+ desktops and servers, wdigest should be disabled in accordance with the following KB article from Microsoft: https://support.microsoft.com/en-us/kb/2871997 Enforcing the principle of Least User Access will also help mitigate the effectiveness of mimikatz as it will limit the access provided by the compromised credentials. Lastly, adding some form of Two Factor Authentication, such as smart cards, can further limit the usefulness of the recovered credentials.	2	Rules written in carbon black to detect cross process activity from rundll32 into lsass Rule written to identify PowerShell crossproc into lsass. Additional rule written to detect an injected process into winlogon with cross process activity into lsass	3	00:00:18	2FA (user-land only), some CyberArk usage, some credentials flushed every 24 hours	1	1	

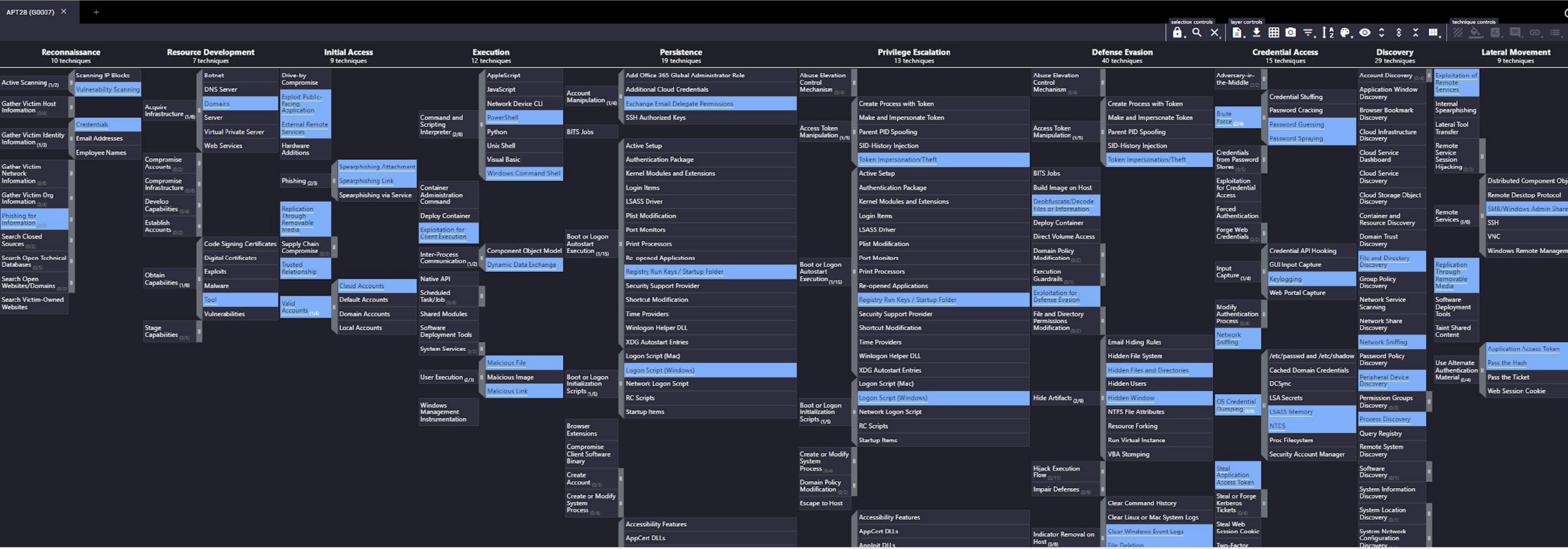
Create repeatable process to measure the capabilities of your defensive controls.

There is ALWAYS room



INVISIBLE MEASURING TAPE

But will we be effective against



Reconnaissance
10 techniques

- Active Scanning (1/2)
  - Scanning IP Blocks
  - Vulnerability Scanning
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (1/3)
  - Credentials
  - Email Addresses
  - Employee Names
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (0/3)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/2)
- Search Victim-Owned Websites

Resource Development
7 techniques

- Acquire Infrastructure (1/6)
  - Botnet
  - DNS Server
  - Domains
  - Server
  - Virtual Private Server
  - Web Services
- Compromise Accounts (0/2)
- Compromise Infrastructure (0/6)
- Develop Capabilities (0/4)
- Establish Accounts (0/2)
- Obtain Capabilities (1/6)
  - Code Signing Certificates
  - Digital Certificates
  - Exploits
  - Malware
  - Tool
  - Vulnerabilities
- Stage Capabilities (0/5)

Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (2/3)
  - Spearphishing Attachment
  - Spearphishing Link
  - Spearphishing via Service
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (1/4)
  - Cloud Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts

Execution
12 techniques

- Command and Scripting Interpreter (2/8)
  - AppleScript
  - JavaScript
  - Network Device CLI
  - PowerShell
  - Python
  - Unix Shell
  - Visual Basic
  - Windows Command Shell
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (1/2)
  - Component Object Model
  - Dynamic Data Exchange
- Native API
- Scheduled Task/Job (0/6)
- Shared Modules
- Software Deployment Tools
- System Services (0/2)
- User Execution (2/3)
  - Malicious File
  - Malicious Image
  - Malicious Link
- Windows Management Instrumentation

Persistence
19 techniques

- Account Manipulation (1/4)
  - Add Office 365 Global Administrator Role
  - Additional Cloud Credentials
  - Exchange Email Delegate Permissions
  - SSH Authorized Keys
- BITS Jobs
- Boot or Logon Autostart Execution (1/15)
  - Active Setup
  - Authentication Package
  - Kernel Modules and Extensions
  - Login Items
  - LSASS Driver
  - Plist Modification
  - Port Monitors
  - Print Processors
  - Re-opened Applications
  - Registry Run Keys / Startup Folder
  - Security Support Provider
  - Shortcut Modification
  - Time Providers
  - Winlogon Helper DLL
  - XDG Autostart Entries
- Boot or Logon Initialization Scripts (1/5)
  - Logon Script (Mac)
  - Logon Script (Windows)
  - Network Logon Script
  - RC Scripts
  - Startup Items
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/3)
- Create or Modify System Process (0/4)
  - Accessibility Features
  - AppCert DLLs

Privilege Escalation
13 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (1/5)
  - Create Process with Token
  - Make and Impersonate Token
  - Parent PID Spoofing
  - SID-History Injection
  - Token Impersonation/Theft
- Boot or Logon Autostart Execution (1/15)
  - Active Setup
  - Authentication Package
  - Kernel Modules and Extensions
  - Login Items
  - LSASS Driver
  - Plist Modification
  - Port Monitors
  - Print Processors
  - Re-opened Applications
  - Registry Run Keys / Startup Folder
  - Security Support Provider
  - Shortcut Modification
  - Time Providers
  - Winlogon Helper DLL
  - XDG Autostart Entries
- Boot or Logon Initialization Scripts (1/5)
  - Logon Script (Mac)
  - Logon Script (Windows)
  - Network Logon Script
  - RC Scripts
  - Startup Items
- Create or Modify System Process (0/4)
- Domain Policy Modification (0/2)
- Escape to Host
  - Accessibility Features
  - AppCert DLLs
  - AppInit DLLs

Defense Evasion
40 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (1/5)
  - Create Process with Token
  - Make and Impersonate Token
  - Parent PID Spoofing
  - SID-History Injection
  - Token Impersonation/Theft
- BITS Jobs
- Build Image on Host
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (0/2)
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Hide Artifacts (2/9)
  - Email Hiding Rules
  - Hidden File System
  - Hidden Files and Directories
  - Hidden Users
  - Hidden Window
  - NTFS File Attributes
  - Resource Forking
  - Run Virtual Instance
  - VBA Stomping
- Hijack Execution Flow (0/11)
- Impair Defenses (0/9)
- Indicator Removal on Host (3/6)
  - Clear Command History
  - Clear Linux or Mac System Logs
  - Clear Windows Event Logs
  - File Deletion

Credential Access
15 techniques

- Adversary-in-the-Middle (0/2)
- Brute Force (2/4)
  - Credential Stuffing
  - Password Cracking
  - Password Guessing
  - Password Spraying
- Credentials from Password Stores (0/5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (0/2)
- Input Capture (1/4)
  - Credential API Hooking
  - GUI Input Capture
  - Keylogging
  - Web Portal Capture
- Modify Authentication Process (0/4)
- Network Sniffing
- OS Credential Dumping (2/8)
  - /etc/passwd and /etc/shadow
  - Cached Domain Credentials
  - DCSync
  - LSA Secrets
  - LSASS Memory
  - NTDS
  - Proc Filesystem
  - Security Account Manager
- Steal Application Access Token
- Steal or Forge Kerberos Tickets (0/4)
- Steal Web Session Cookie
- Two-Factor

Discovery
29 techniques

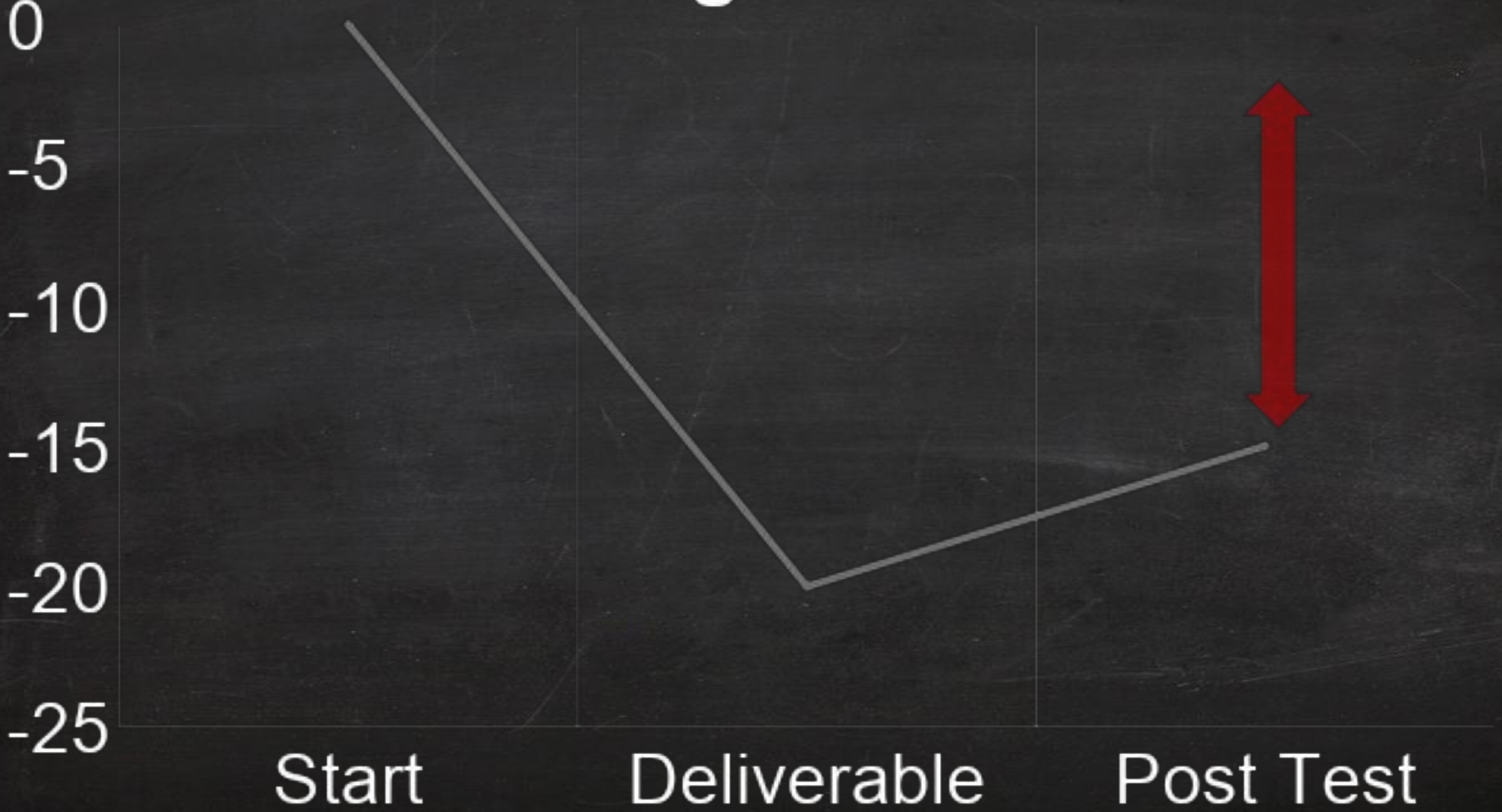
- Account Discovery (0/4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (0/3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (0/1)
- System Information Discovery
- System Location Discovery (0/1)
- System Network Configuration Discovery

Lateral Movement
9 techniques

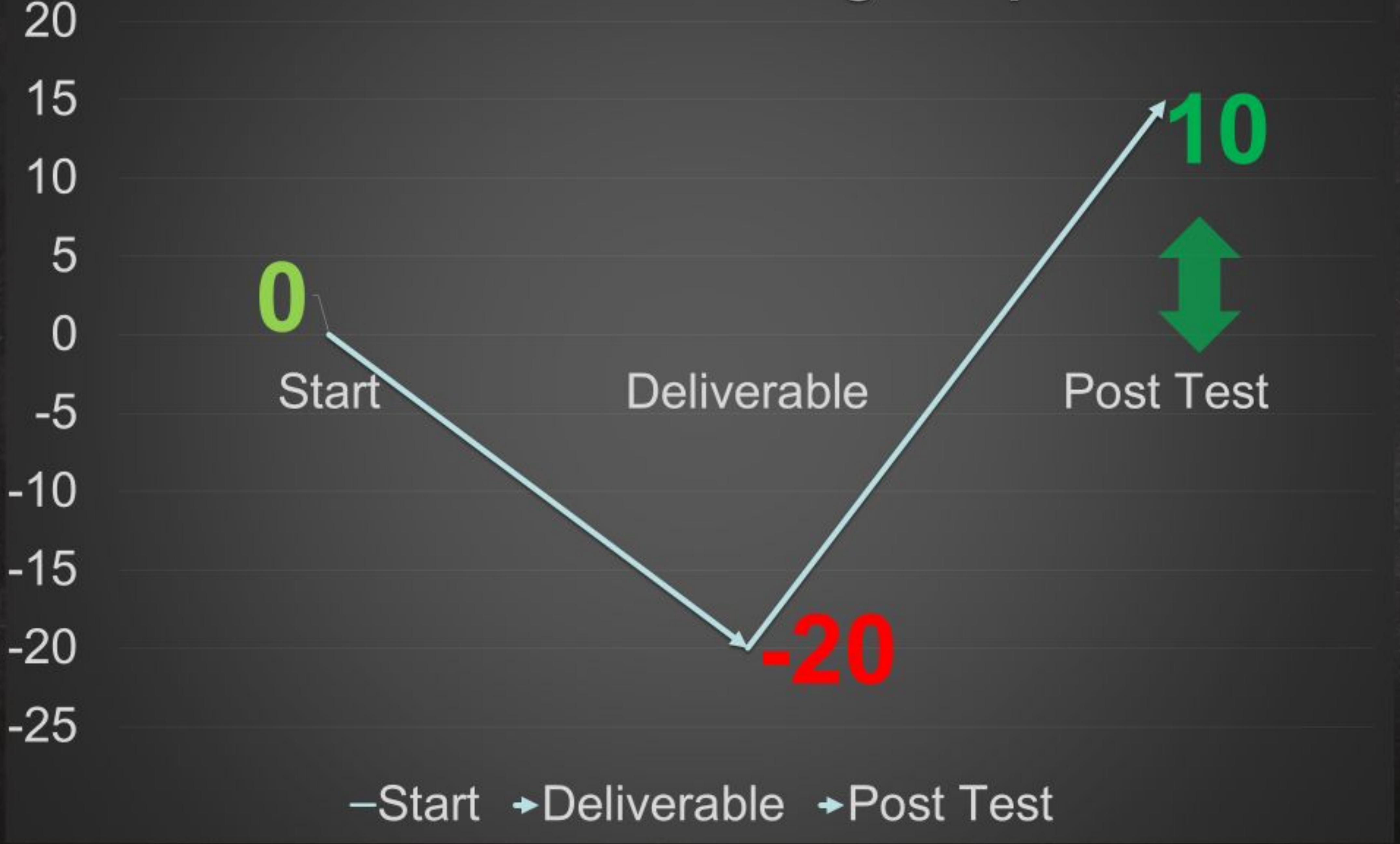
- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (1/6)
  - Distributed Component Obj
  - Remote Desktop Protocol
  - SMB/Windows Admin Share
  - SSH
  - VNC
  - Windows Remote Managem
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (2/4)
  - Application Access Token
  - Pass the Hash
  - Pass the Ticket
  - Web Session Cookie

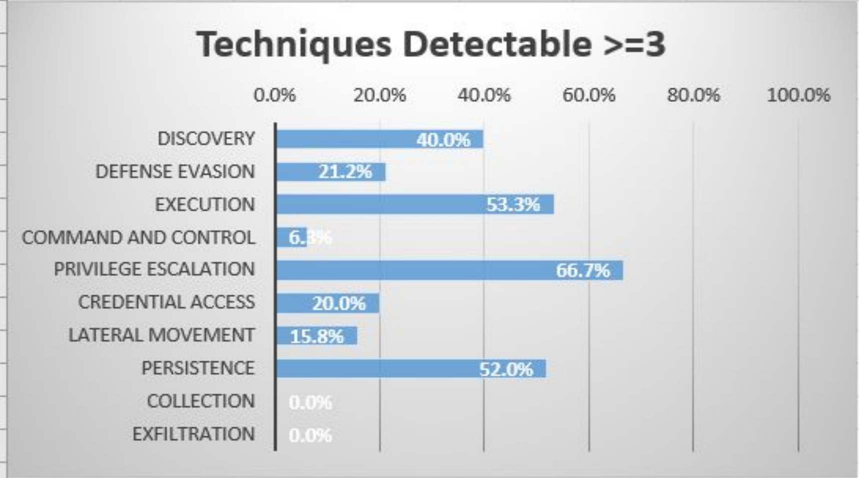
https://mitre-attack.github.io/attack-navigator//#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0007%2FG0007-enterprise-layer.json

Testing Metrics

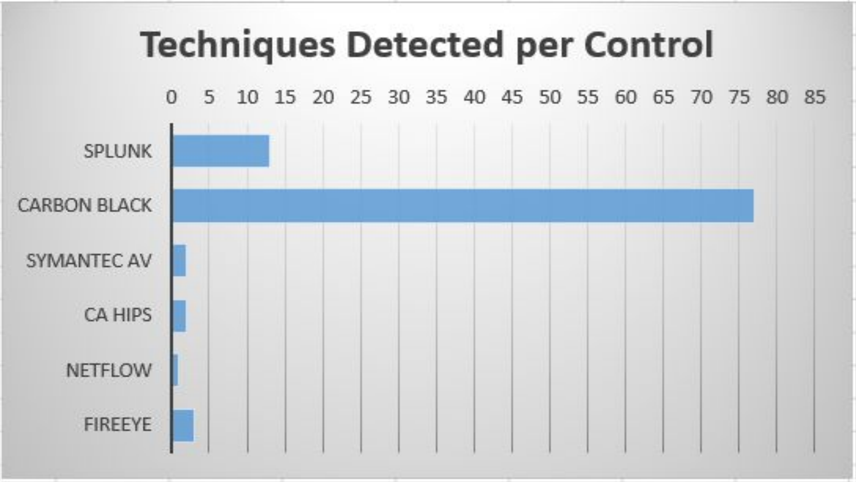


Simulated Testing Loop

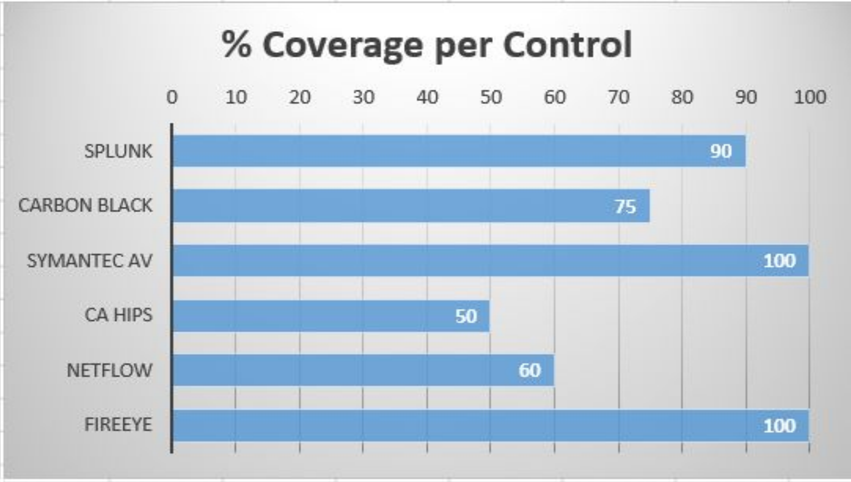




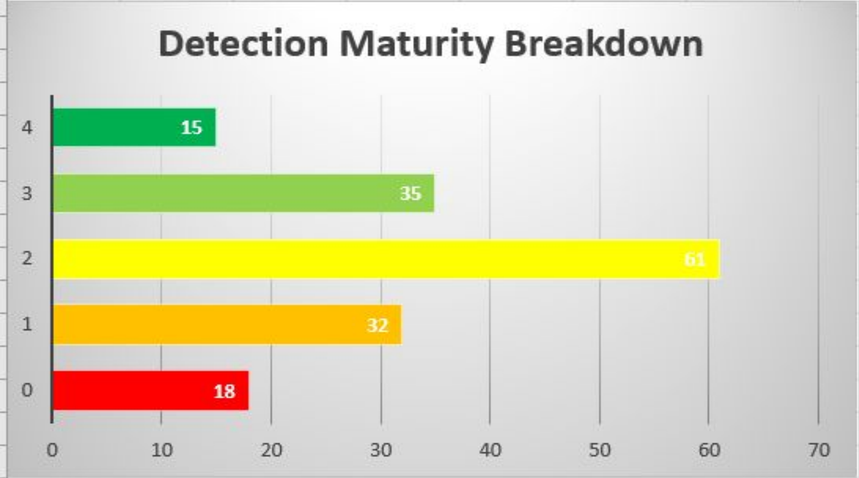
Techniques Detectable >=3



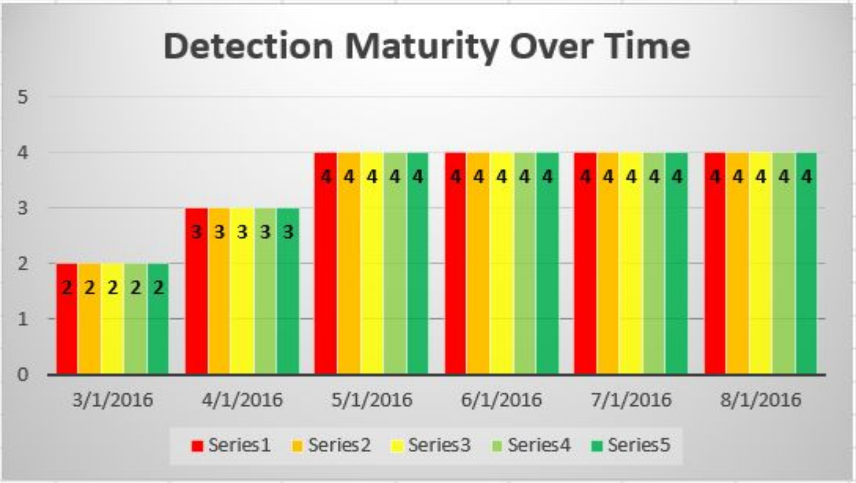
Techniques Detected per Control



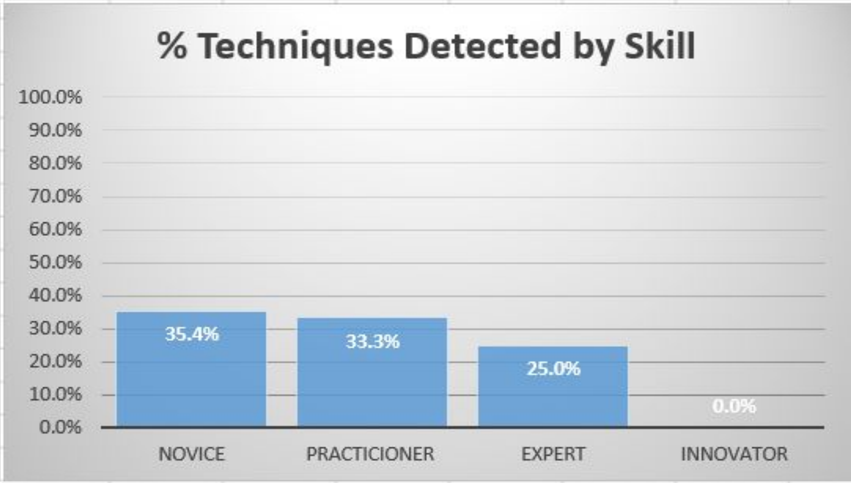
% Coverage per Control



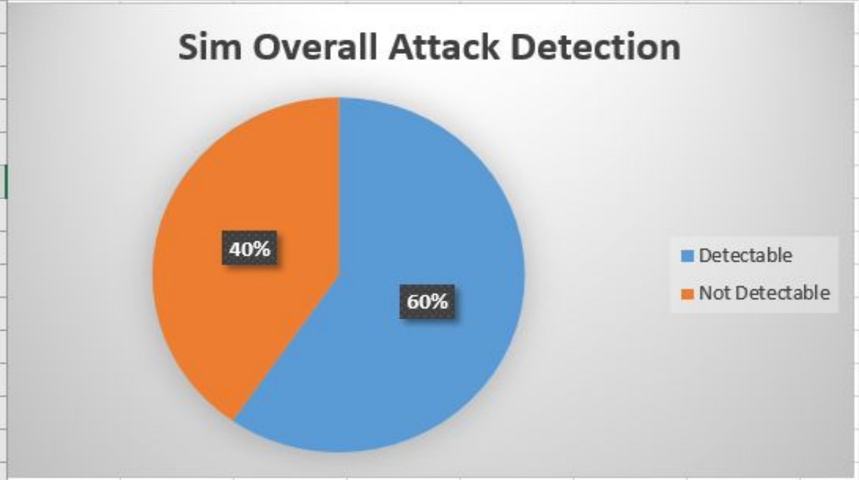
Detection Maturity Breakdown



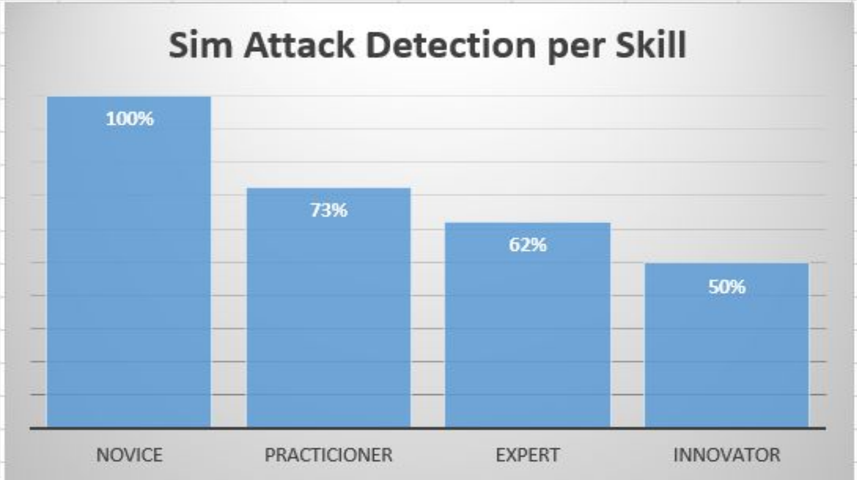
Detection Maturity Over Time



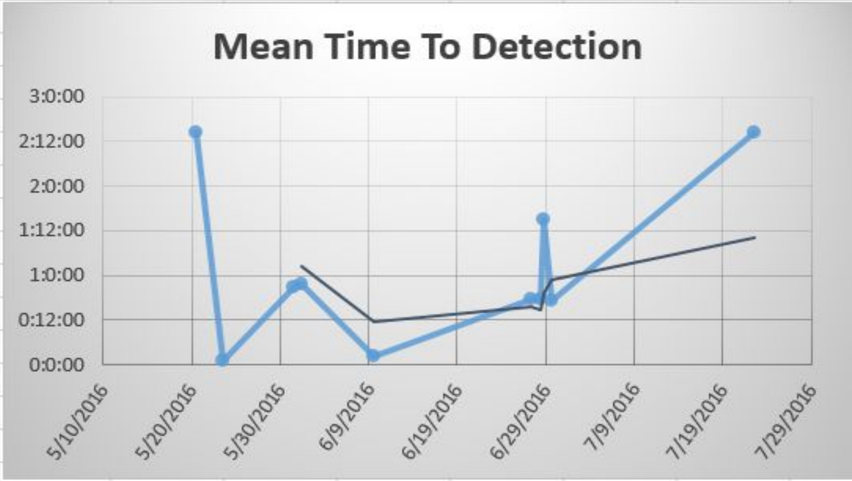
% Techniques Detected by Skill



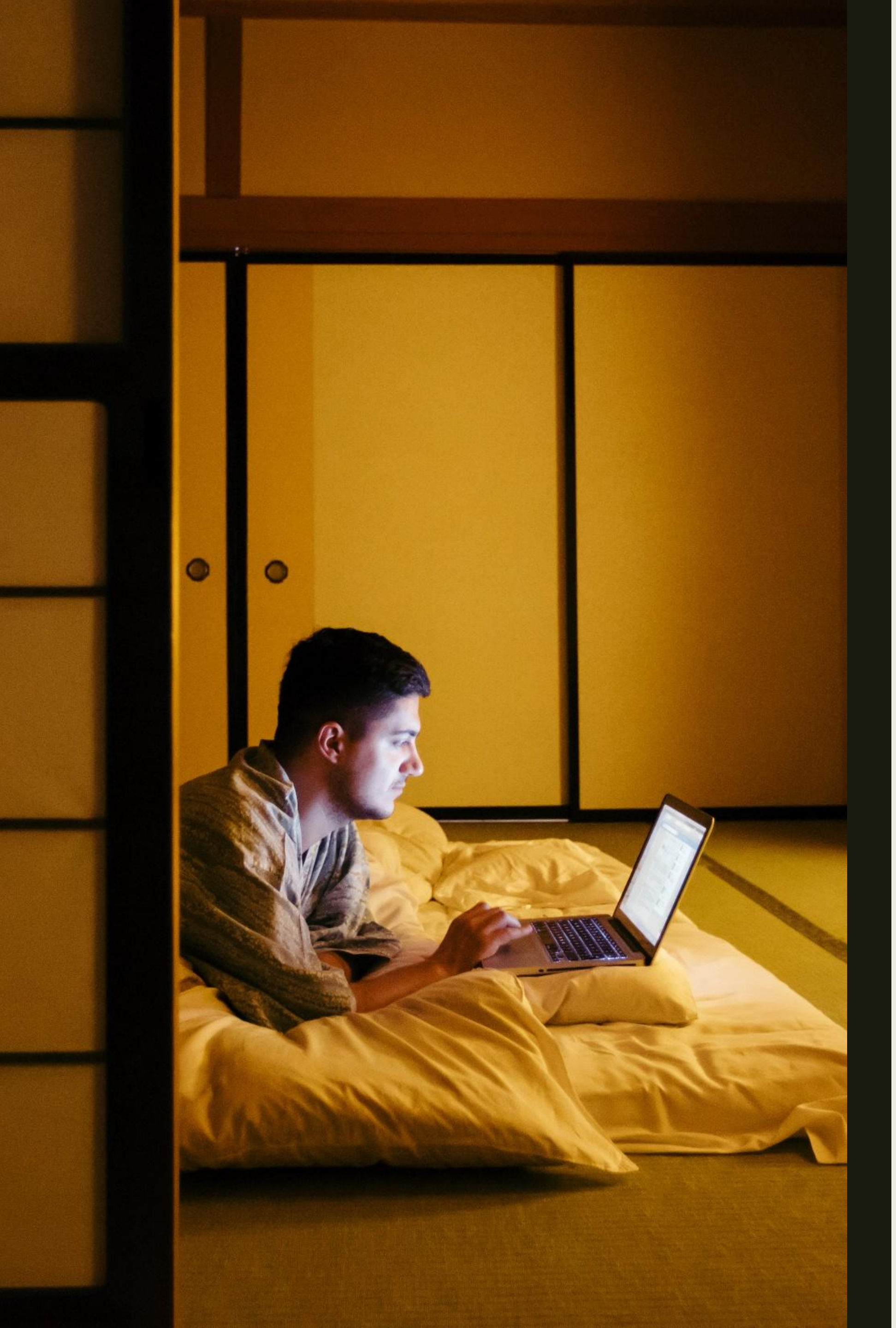
Sim Overall Attack Detection



Sim Attack Detection per Skill



Mean Time To Detection



Create positive Addiction

- Reduce Vulnerability Paralysis
- Measure your capabilities
- Show continual defensive improvement

TBDL (Too boring didn’t listen)

- Always set your intentions on positive results
- Focus on team accountability
- One team One goal
- Eliminate Vulnerability Paralysis
- Bad Metrics = Bad Decisions
- Molon Labe mentality
- Build each other up, don’t tear each other down
- Measure everything
- Always be improving
- Create addiction to POSITIVE results
- Educate don’t Adjudicate
- Diversity trumps Adversity when Adversity isn’t Diverse

Thank You

Chris Nickerson, @indi303

Chris.nickerson@damovo.com

www.Damovo.com
www.lares.com