

Balancing the Scale of Just-Good-Enough

The Techniques vs. Procedures Debate
Why not both?

Ian Davila
Frank Duff



Who We Are

Frank Duff

CHIEF INNOVATION OFFICER, TIDAL
CYBER

Before that...

18 years at MITRE (Signal Processing,
Detection Engineering, Lead ATT&CK Evals)



Ian Davila

LEAD ADVERSARY EMULATOR, TIDAL
CYBER

Before that...

Computer Scientist, MITRE ATT&CK, ATT&CK Evals

Techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning (3) ▼	Acquire Infrastructure (6) ▼	Drive-by Compromise	Command and Scripting Interpreter (8) ▼	Account Manipulation (5) ▼	Abuse Elevation Control Mechanism (4) ▼	Abuse Elevation Control Mechanism (4) ▼	Adversary-in-the-Middle (3) ▼	Account Discovery (4) ▼	Exploitation of Remote Services	Adversary-in-the-Middle (3) ▼	Application Layer Protocol (4) ▼	Automated Exfiltration (1) ▼	Account Access Removal
Gather Victim Host Information (4) ▼	Compromise Accounts (2) ▼	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5) ▼	Access Token Manipulation (5) ▼	Brute Force (4) ▼	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3) ▼	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3) ▼	Compromise Infrastructure (6) ▼	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14) ▼	Boot or Logon Autostart Execution (14) ▼	BITS Jobs	Credentials from Password Stores (3) ▼	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2) ▼	Exfiltration Over Alternative Protocol (5) ▼	Data Encrypted for Impact
Gather Victim Network Information (6) ▼	Develop Capabilities (4) ▼	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Debugger Evasion	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (6) ▼	Automated Collection	Data Obfuscation (3) ▼	Exfiltration Over C2 Channel	Data Manipulation (3) ▼
Search Closed Sources (2) ▼	Establish Accounts (2) ▼	Phishing (3) ▼	Inter-Process Communication (3) ▼	Configure Client Software Binary	Domain Policy Modification (2) ▼	Domain Policy Modification (2) ▼	Input Capture (4) ▼	Cloud Service Discovery	Replication Through Removable Media	Browser Session Hijacking	Dynamic Resolution (3) ▼	Exfiltration Over Other Network Medium (1) ▼	Defacement (2) ▼
Search Open Technical Databases (5) ▼	Obtain Capabilities (6) ▼	Replication Through Removable Media	Native API	Create Account (3) ▼	Escape to Host	Escape to Host	Modify Authentication Process (5) ▼	Cloud Storage Object Discovery	Software Deployment Tools	Clipboard Data	Encrypted Channel (2) ▼	Exfiltration Over Physical Medium (1) ▼	Disk Wipe (2) ▼
Search Open Websites/Domains (2) ▼	Stage Capabilities (5) ▼	Supply Chain Compromise (3) ▼	Scheduled Task/job (5) ▼	Create or Modify System Process (4) ▼	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Multi-Factor Authentication Interception	Domain Trust Discovery	Replication Through Removable Media	Data from Cloud Storage Object	Failback Channels	Exfiltration Over Web Service (2) ▼	Endpoint Denial of Service (4) ▼
Search Victim-Owned Websites		Trusted Relationship	Shared Modules	Event Triggered Execution (15) ▼	Guardrails (1) ▼	Guardrails (1) ▼	File and Directory Permissions Modification (2) ▼	File and Directory Permissions Modification (2) ▼	Software Deployment Tools	Data from Configuration Repository (2) ▼	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
		Valid Accounts (4) ▼	System Services (2) ▼	External Remote Services	Hijack Execution Flow (12) ▼	Hijack Execution Flow (12) ▼	Network Sniffing	Group Policy Discovery	System Services (2) ▼	Data from Information Repositories (3) ▼	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
			User Execution (3) ▼	Hijack Execution Flow (12) ▼	Process Injection (12) ▼	Process Injection (12) ▼	OS Credential Dumping (8) ▼	File and Directory Permissions Modification (2) ▼	Software Deployment Tools	Data from Local System	Non-Application Layer Protocol		Network Denial of Service (2) ▼
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/job (5) ▼	Scheduled Task/job (5) ▼	Hide Artifacts (10) ▼	File and Directory Permissions Modification (2) ▼	Software Deployment Tools	Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
				Modify Authentication Process (5) ▼	Valid Accounts (4) ▼	Valid Accounts (4) ▼	Hijack Execution Flow (12) ▼	File and Directory Permissions Modification (2) ▼	Software Deployment Tools	Data from Removable Media	Proxy (4) ▼		Service Stop
				Office Application Startup (6) ▼			Impair Defenses (9) ▼	File and Directory Permissions Modification (2) ▼	Software Deployment Tools	Data Staged (2) ▼	Remote Access Software		System Shutdown/Reboot
				Pre-OS Boot (5) ▼			Indicator Removal on Host (6) ▼	File and Directory Permissions Modification (2) ▼	Software Deployment Tools	Email Collection (3) ▼	Traffic Signaling (1) ▼		
				Scheduled Task/job (5) ▼			Indirect Command Execution	File and Directory Permissions Modification (2) ▼	Software Deployment Tools	Input Capture (4) ▼	Web Service (5) ▼		
				Server Software Component (5) ▼			Masquerading (7) ▼	File and Directory Permissions Modification (2) ▼	Software Deployment Tools	Screen Capture			
				Traffic Signaling (1) ▼			Modify Authentication Process (5) ▼	File and Directory Permissions Modification (2) ▼	Software Deployment Tools	Video Capture			
				Valid Accounts (4) ▼			Modify Cloud Compute Infrastructure (4) ▼	File and Directory Permissions Modification (2) ▼	Software Deployment Tools				
							Modify Registry	File and Directory Permissions Modification (2) ▼	Software Deployment Tools				

People understand it and it's still tractable

- MITRE ATT&CK® has become a de facto standard on the threat techniques at its core
- 576 (Sub-)Techniques is still tractable

Procedures



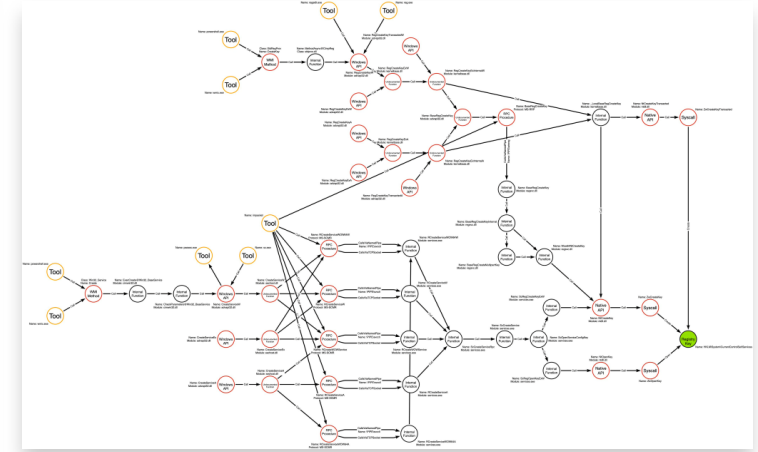
Credit: Jamie Williams, MITRE

Dissecting a Detection: An Analysis of ATT&CK Evaluations Data (Sources)



- Procedures give you the how to drive
- Credit: Tim Schulz, Scythe

Devil in the Details: Why Legacy Breach and Attack Simulation (BAS) Falls Short, SecureWorld



Credit: Jared Atkinson

<https://twitter.com/jaredcatkinson/status/1512067698863198215>

Techniques? Procedures?

TECHNIQUES???



Technique “coverage” is an overgeneralization

What it takes to cover a technique is misunderstood or abused, leading to misplaced confidence

PROCEDURES???



Procedure “coverage” drives complexity and costs up

Procedure variance requires you to develop and run multiple test scenarios. Skills, money, time all become an issue.

Find the Balance



**Techniques are
the heart**

ATT&CK enhances understandability

**Procedures are the
feather of truth**

Procedures enhance confidence

How do we balance the scales?

- CTI, Offensive, Defensive considerations
- Easier to build technique flow than procedure flow, start there
- Sub-techniques are more specific than techniques
- For each (sub-)technique... many procedures
- Do we have all the necessary information to emulate procedures?

CTI Considerations

Closing Gaps

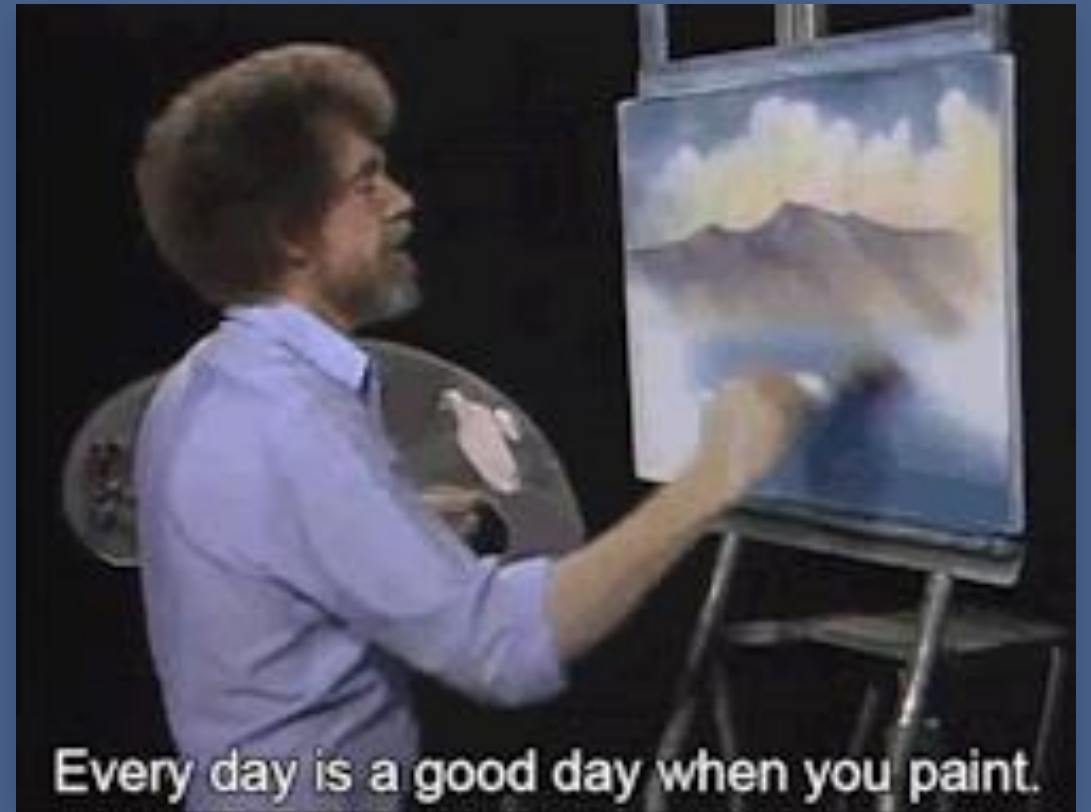
Goal is to be as close as possible to real threat

Sometimes you must be an artist

* shoutout to Cat Self

Close gaps in procedures

- Lack of intel
- Inferred intel
 - Not enough information but can infer from known



Offensive Considerations

Testing



Development Costs

Offensive Considerations

Testing



Authenticity



**Development
Costs**

Offensive Considerations

Testing



Defensive Considerations

Not all detections are created equal

Graph based detections

- Hard
- Expensive
- Data Sources/Components
- More than one procedure

It is easier to detect at the procedure level

- Process creates + arguments

Chained detections



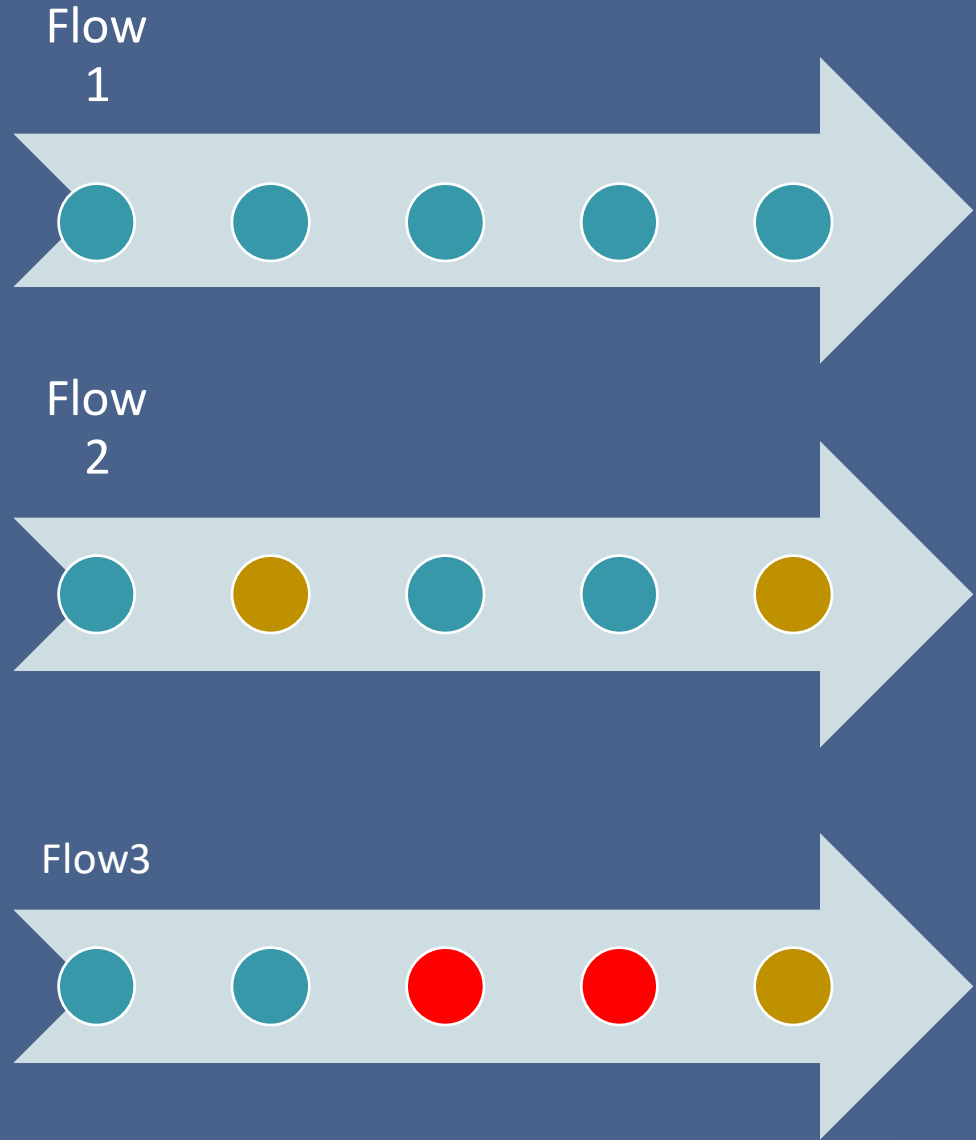
Our Approach

Flows that align to specific threats we care about

- Potential targeting of user
- User says they care about them
- Bang for the buck

We want procedural variance to test defenses

Execute flows – chained detections



Final Statements

- 1 test or 1 detection isn't "Coverage"
- Look at procedure coverage through the lens of technique coverage
- Understand what you detect and what you test (and why!)
- Don't let perfect be the enemy of the good



Thank you!

Frank.duff@tidalcyber.com

Ian.Davila@tidalcyber.com