Threat Hunting:

Lotta Ins,
Lotta Outs,
Lotta What Have Yous

SANS Threat Hunting & IR Summit 2021
Ashley Pearson | @onfvp

Hello, friends! I'm Ashley

- Professional foster failure
- Security Consultant @ TrustedSec
- Certified Nerd

- Socials:
  - Twitter: @onfvp
  - Website: blog.onfvp.com

Hunting Maturity

HMM0 Initial

- Relies primarily on automated alerting
- Little or no routine data collected

HMM1 Minimal

- Incorporates threat intelligence indicator searches
- Moderate or high level of routine data collections

HMM2 Procedural

- Follows data analysis procedures created by others
- High or very high level of routine data collection

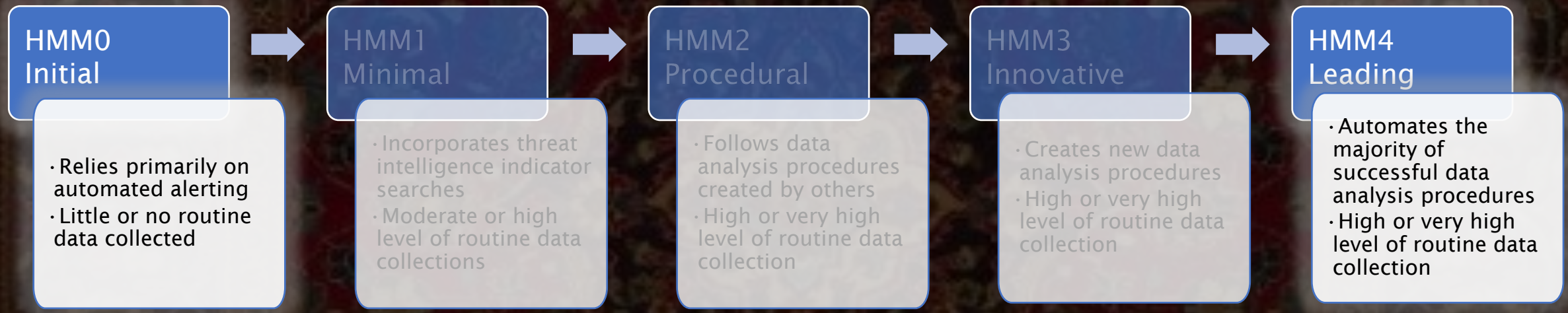
HMM3 Innovative

- Creates new data analysis procedures
- High or very high level of routine data collection

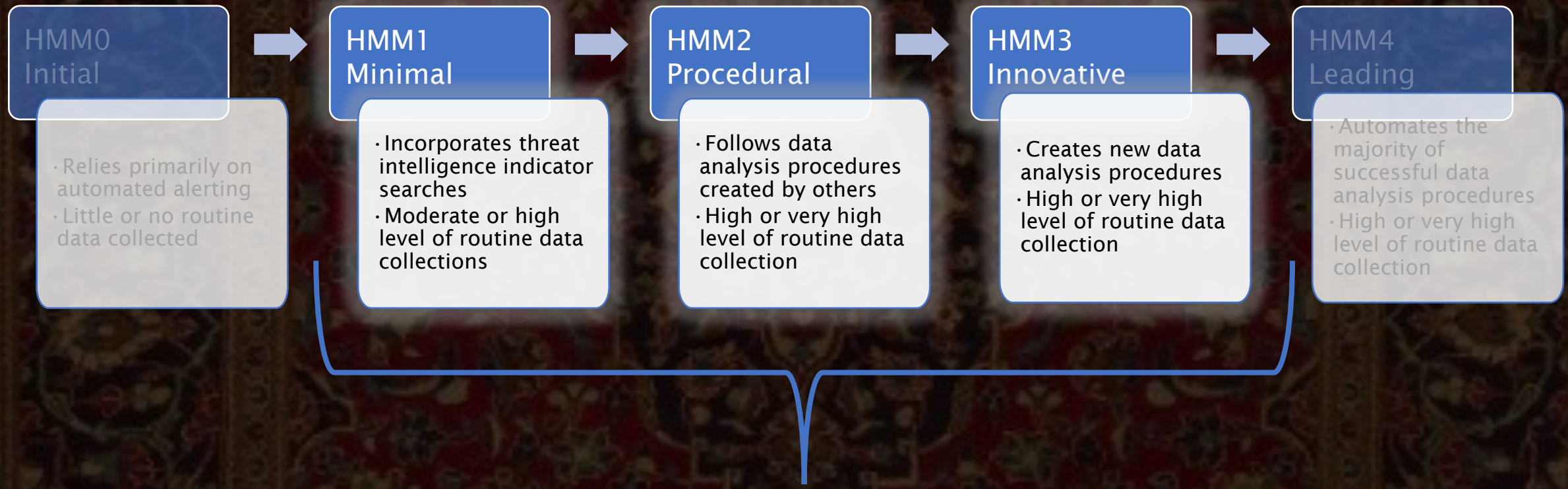
HMM4 Leading

- Automates the majority of successful data analysis procedures
- High or very high level of routine data collection

Hunting Maturity



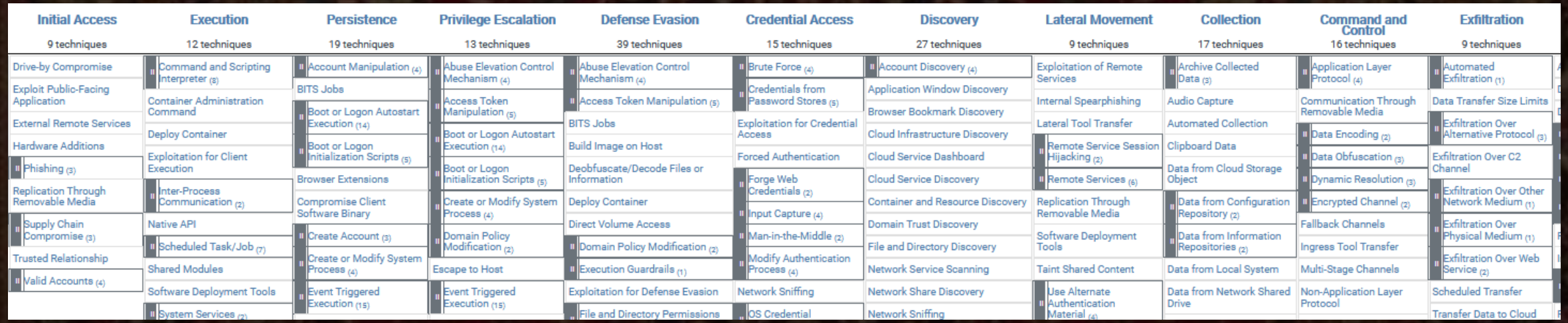
Hunting Maturity



The Ins

Framework-Based Hunts

MITRE ATT&CK



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
9 techniques	12 techniques	19 techniques	13 techniques	39 techniques	15 techniques	27 techniques	9 techniques	17 techniques	16 techniques	9 techniques
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)
Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (5)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits
External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)
Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel
Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Dashboard	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)
Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)
Supply Chain Compromise (3)	Scheduled Task/Job (7)	Create Account (3)	Escape to Host	Domain Policy Modification (2)	Man-in-the-Middle (2)	Container and Resource Discovery	Software Deployment Tools	Data from Information Repositories (2)	Fallback Channels	Exfiltration Over Web Service (2)
Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Event Triggered Execution (15)	Execution Guardrails (1)	Modify Authentication Process (4)	Domain Trust Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Scheduled Transfer
Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Exploitation for Defense Evasion	Network Sniffing	File and Directory Discovery	Use Alternate Authentication Material (4)	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud
	System Services (2)	File and Directory Permissions	OS Credential	Network Service Scanning	Network Share Discovery		Non-Application Layer Protocol	
				Network Sniffing				

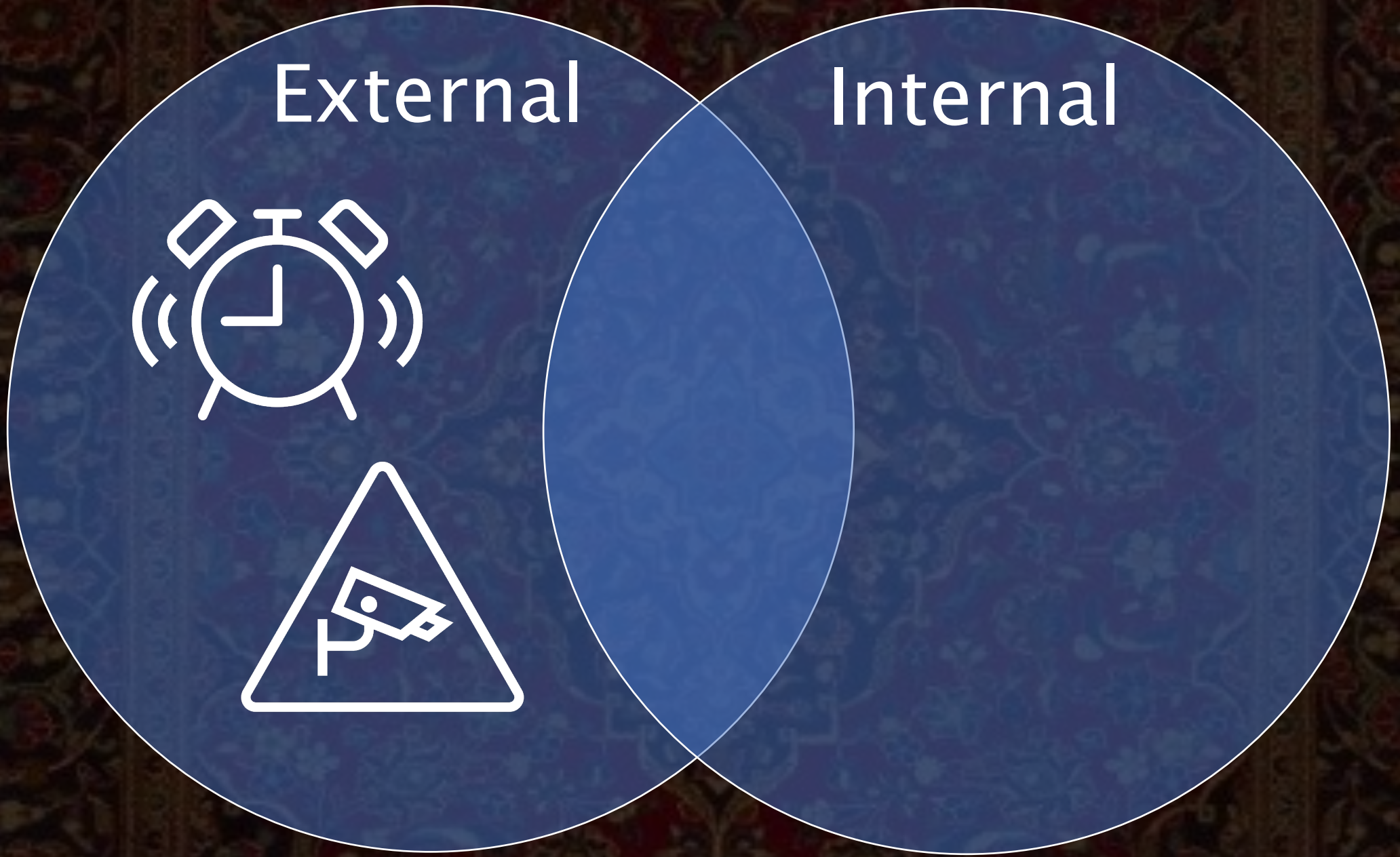
Intel-Based Hunts

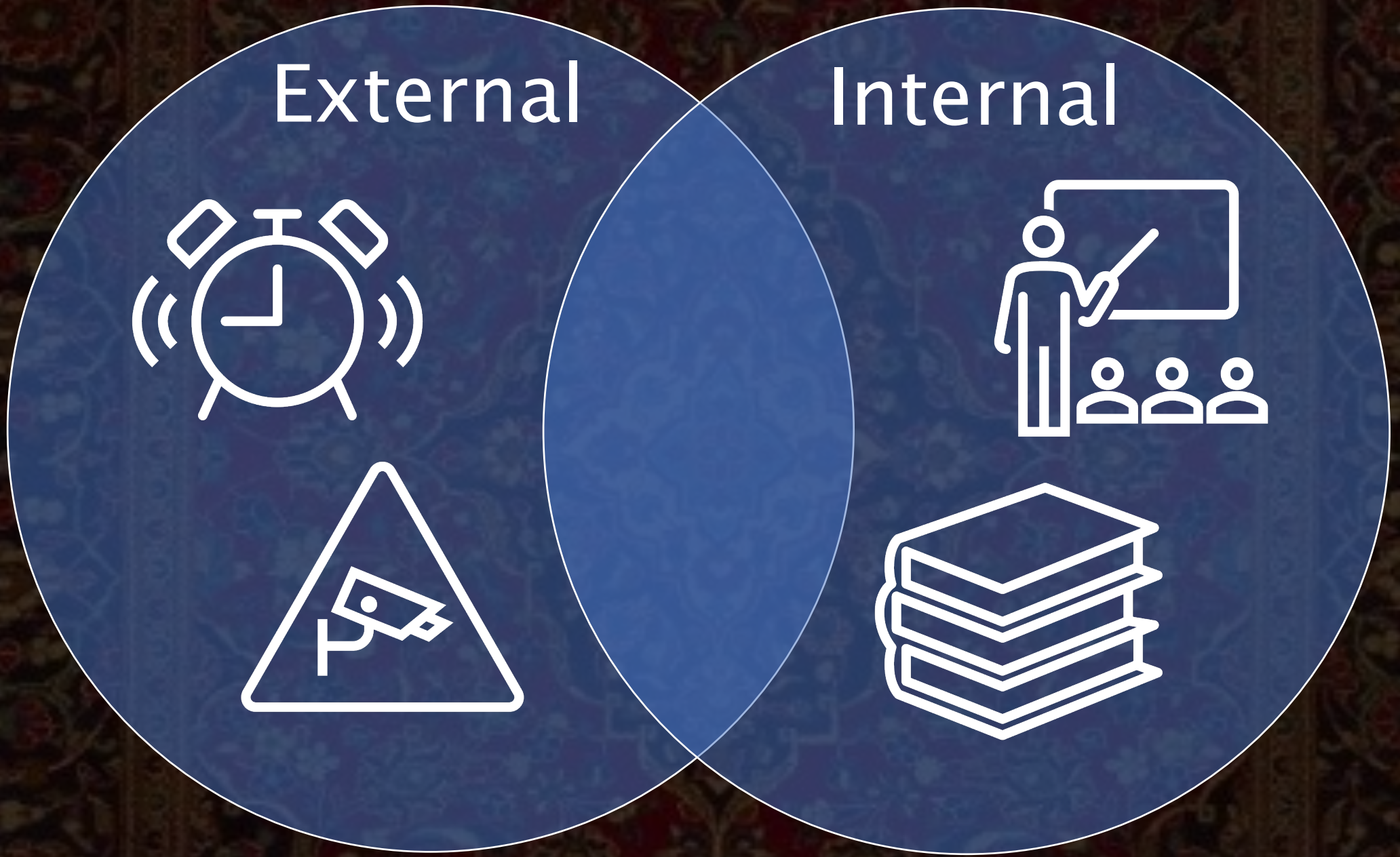
- Combination of *reactive* and *proactive*
- Third-party reporting
  - CISA or 3 letter agencies
  - Law enforcement
- IOC sweeps
  - Identify behavior that may not be retroactively alerted on

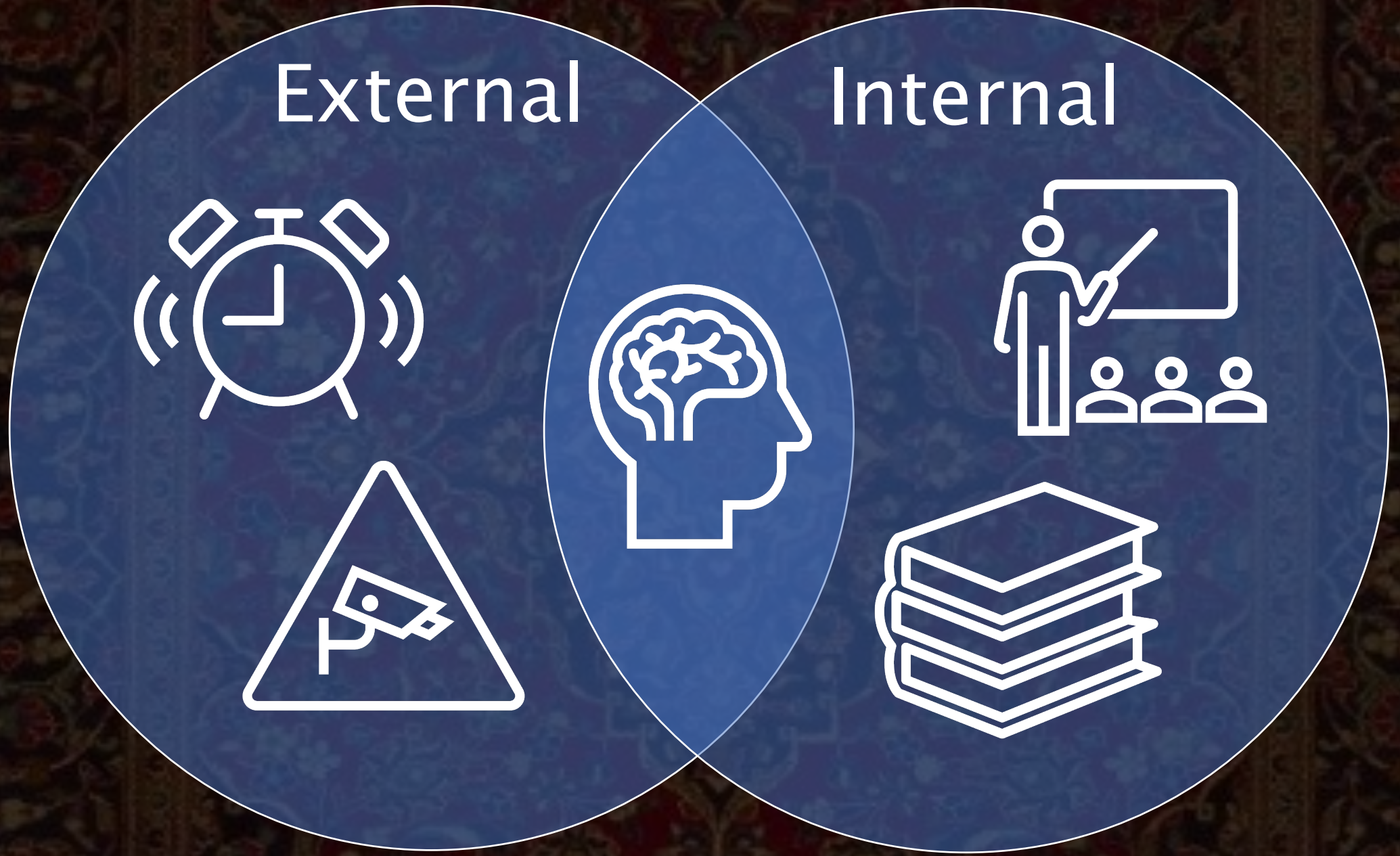
Internally-Generated Hunts

- Open-source intelligence
  - Proof of concepts (Twitter, Github, Reddit)
  - Socials (Discord, Slack)
  - Shodan
- Crown Jewels
- Pattern-based anomaly detection
  - Least frequency and longtail analysis
  - Deviations from expected user and endpoint behavior

The Outs


External
Internal


External
Internal


External
Internal

That’s just, like, your opinion, man

Questions?