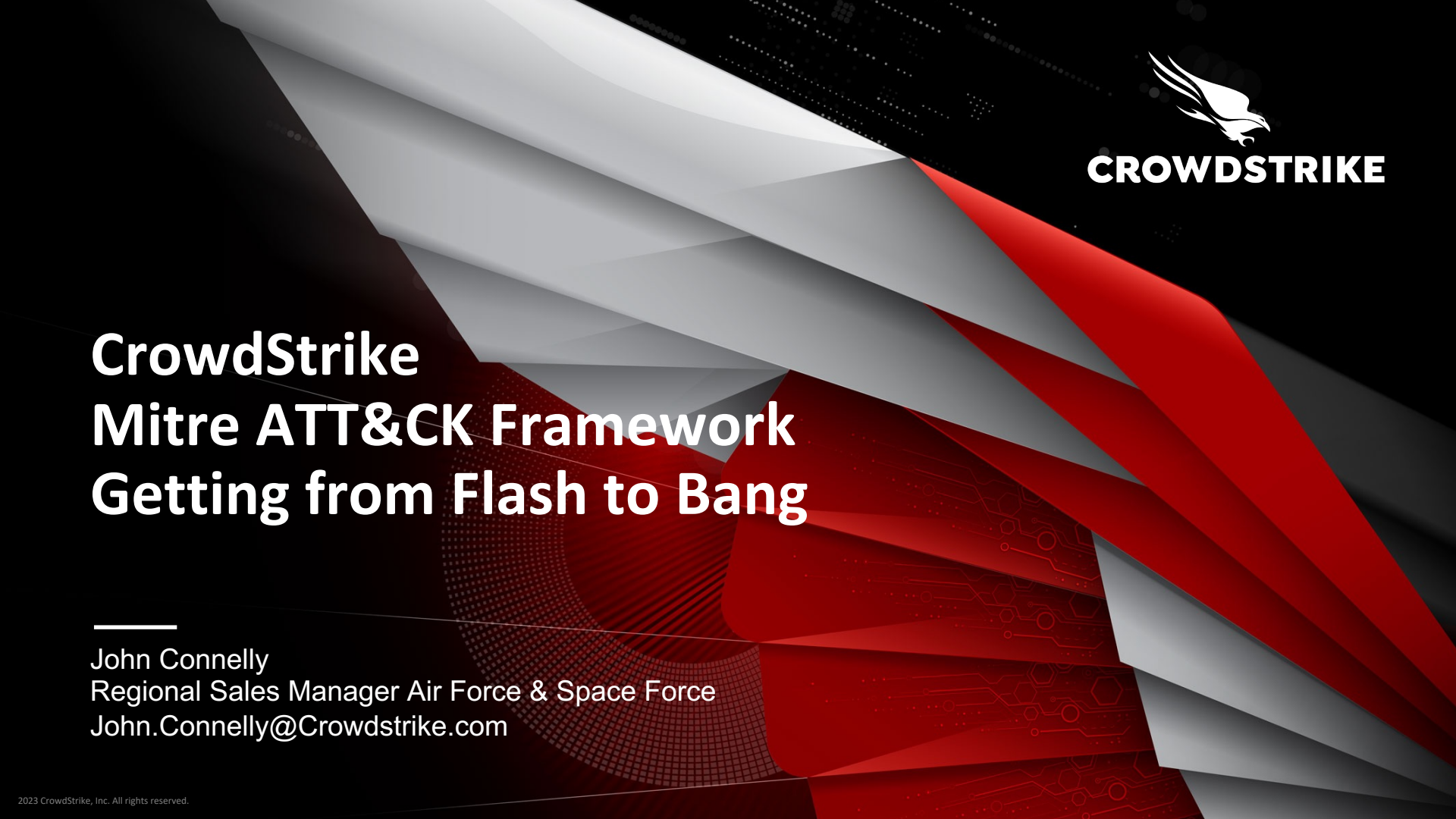


CrowdStrike
Mitre ATT&CK Framework
Getting from Flash to Bang

John Connelly
Regional Sales Manager Air Force & Space Force
John.Connelly@Crowdstrike.com

The Origin of Cannons

- Cannons first appeared in Battle in 12th Century China
- The ability to attack from a distance leaving an enemy with no way to defend themselves revolutionized warfare forever
- An early example of how technology could be employed to overpower an opposing force to tip the balance of power in an attacker's favor
- Opponents quickly learned that when you saw the 'Flash' of the cannon, what you did before you felt the 'Bang' could be the difference in life or death

The pictur

Observation

Today's Cyberattacks draw Parallels on the introduction of Cannon Warfare

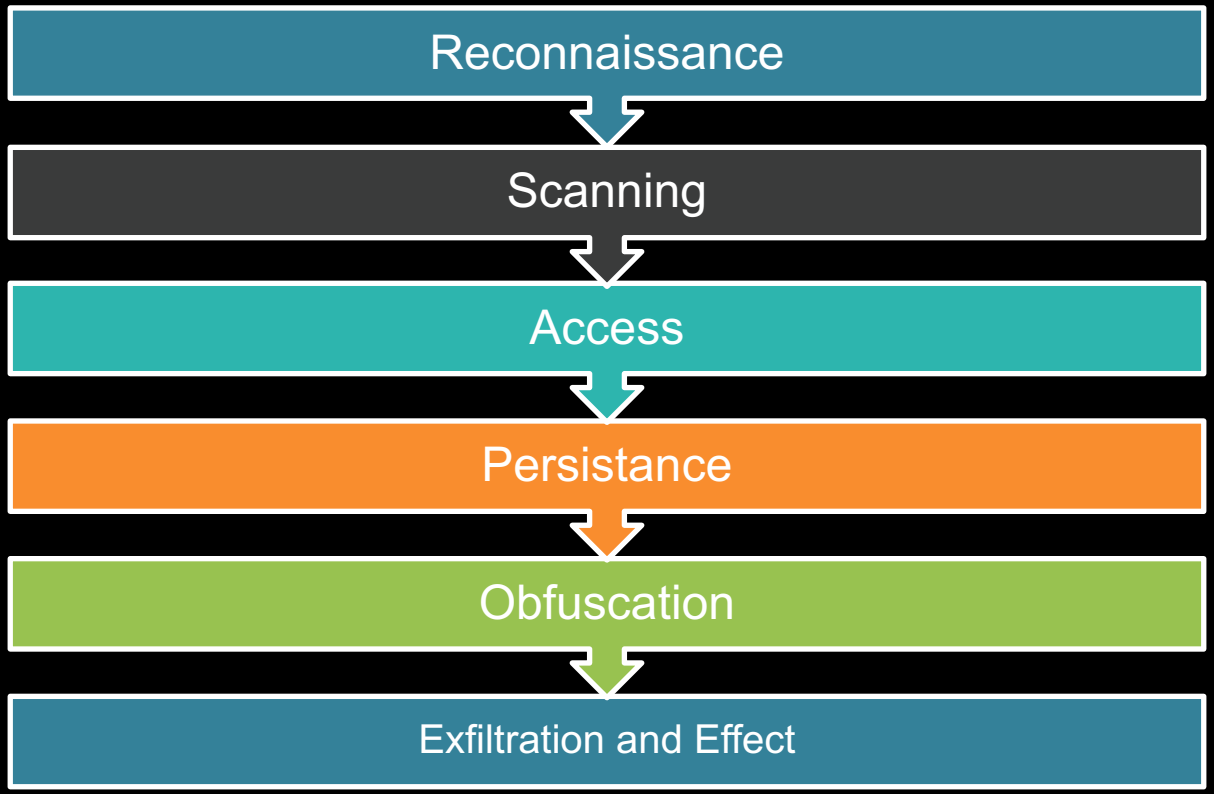
They are Launched from a Distance with Devastating Effect

There are limits on what can be done to Defend against attacks

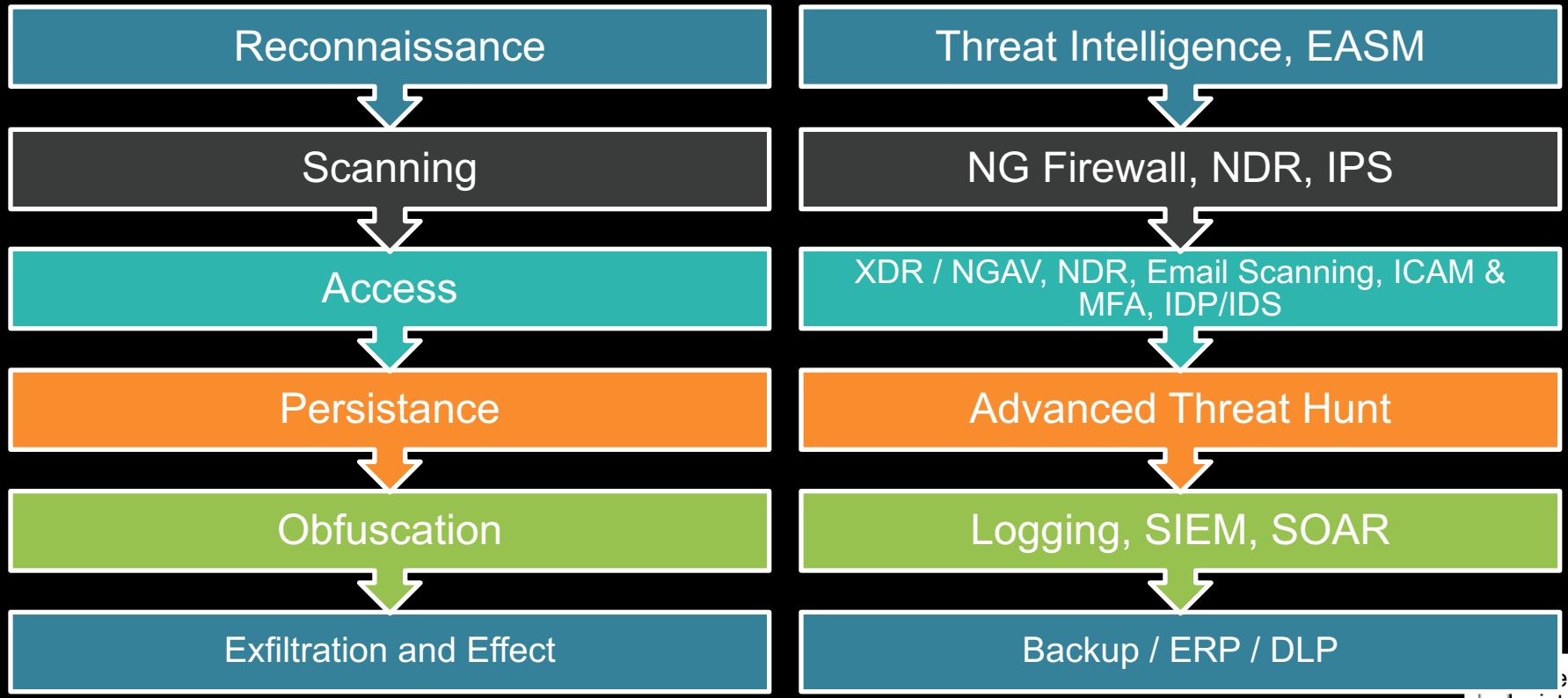
This is Changing Warfare Forever

The Biggest Challenge is NOT the Bang, it is Recognizing the Flash

Anatomy of a Cyber Attack



Anatomy of a Cyber Attack



Reconnaissance

Threat

- Attacker is gathering information from multiple OSINT sources
  - TCP/IP Address Space / Open Ports
  - DNS
  - Network Equipment Type
  - Server Hardware
  - Cloud Resources
  - Employee PII
  - Social Media Information

Response

- Attack Surface Monitoring
  - Third party service that performs similar surveillance as an attacker would to highlight potential weaknesses in your digital surface
- Threat Intelligence
  - Understanding an adversary's methods and TTP's will put you ahead of them when they shift from commercial to targeting the DoD.

Scanning

Threat

- Attacker is using techniques to actively scan for vulnerabilities in your defemses
  - Network scans for open ports
  - Scans for misconfigured applications
  - Common UID/Password Combos
  - Brute Force Password attacks
  - Vulnerability mapping of discovered resources

Response

- Nextgen Firewall / IPS
  - Uses DPI to inspect packets and makes intelligent decisions on how to respond.
  - Blocks or ignores packets that are identified as malicious

Access*

Threat

- Attacker is now actively attempting to gain access to your enterprise
  - Malware, Virus, Phishing, Smishing, Salting, Wardriving, Etc.
  - Modern adversaries are much more likely to gain access through unpatched vulnerabilities or misconfigurations in OS

Response

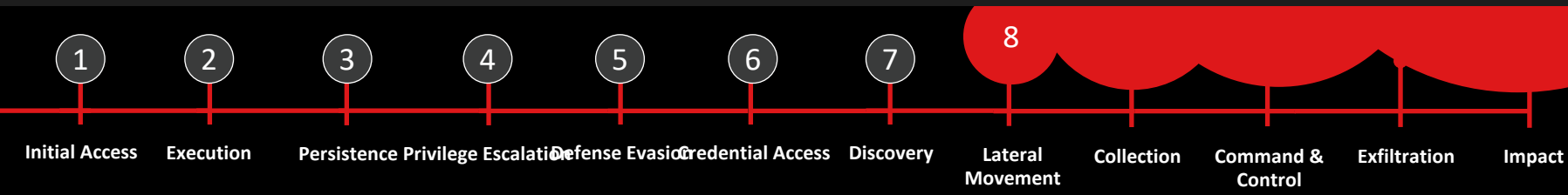
- Here is where the bulk of your defensive capability is concentrated.
  - EDR/XDR/MDR on Endpoint
  - Email Scanning
  - USB Device Management
  - Identity Management and Multifactor Authentication
  - Mobile Device Management & Security
  - Cloud Native Application Security
  - Container Security
  - Patch, Patch, Patch!!!
  - Etc……

* This is traditionally where ‘Flash’ occurs

SURVIVAL OF THE FASTEST

TO STAY AHEAD YOU MUST:

DETECT IN	INVESTIGATE IN	RESPOND IN
1min	**10min**	**60min**



MITRE ATT&CK PHASE

The pictur

Persistance

Threat

- Attacker has access to your network and his software is beaconing back to the Attacker
- Now the Attacker is looking for a way to ‘Persist in your environment’. That way if the server or endpoint they have established themselves on is rebooted or power cycled, the software will relaunch either on that same device or on another.
- The Enemy is in your environment and it is encumbant upon you to find them. Even if you don’t know they are there.

Response

- Advanced Threat Hunting is the act of searching for an exploited system when no indication has been given that it has been compromised.
- A variety of tools are necessary for ATH to be effective.
- The more difficult issue is not the tools, but the talent and training of an effective Threat hunting force

SKILLS SHORTAGE

TASKS REQUIRED	RESOURCES NEEDED
KEEPING SIGNATURES UP TO DATE	
IMPLEMENTING, CONFIGURING AND TUNING	
SUPPORTING, MANAGING AND MAINTAINING	
TRIAGING ALERTS	
RESPONDING TO INCIDENTS	
REMEDIATING	

The pictur

Obfuscation

Threat

- Your Adversary now has a foothold in your environment and is doing their best to hide
  - Masquerading as a valid executable
  - Going low & slow to avoid being detected by security applications
  - Modifying or even deleting log files that would have recorded it activity
  - Might be a fileless attack and is hiding in a valid code source like GIT

Response

- Logging platforms are critical, log as much system and security data as you possibly can.
- Use tools like SIEM to analyze the log data and raise security events on anomalous behavior.
- Use SOAR to Automate the handling of the Obfuscation activity.

Obfuscation

Threat

- At this phase, your Adversary has accomplished everything they have set out to achieve and are wrapping up their mission. The endgame may be to make off with classified data, to deny access to resources by encrypting data so the warfighter cannot access it, and possibly to render the system unusable by deleting OS System files necessary for the system to boot.

Response

- All of your options at this point are exhausted but the fight must continue.
- All Mission Critical applications and data MUST be backed up in a secure location. Restoral Plans must be a part of the Mission Continuity plan and should be rehearsed Regularly. Hardware resources should also be planned for as some modern malware can cause physical damage to systems.

THE MITRE ATT&CK MATRIX

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Command-Line Interface	AppCert DLLs	Accessibility Features	BITS Jobs	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Control Panel Items	AppInit DLLs	AppCert DLLs	Binary Padding	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	AppInit DLLs	Bypass User Account Control	Credentials in Files	File and Directory Discovery	Logon Scripts	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Execution through API	Authentication Package	Application Shimming	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryp-tographic Protocol
Spearphishing Link	Execution through Module Load	BITS Jobs	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Exploitation for Client Execution	Bootkit	DLL Search Order Hijacking	Component Firmware	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Peripheral Device Discovery	Remote File Copy	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Permission Groups Discovery	Remote Services	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	LSASS Driver	Component Firmware	File System Permis-sions Weakness	DCShadow	Kerberoasting	Process Discovery	Replication Through Removable Media	Input Capture		Multi-Stage Channels
	Mshta	Component Object Model Hijacking	Hooking	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning	Query Registry	Shared Webroot	Man in the Browser		Multi-hop Proxy
	PowerShell	Create Account	Image File Execution Options Injection	DLL Side-Loading	Network Sniffing	Remote System Discovery	Taint Shared Content	Screen Capture		Multiband Communication
	Regsvcs/Regasm	DLL Search Order Hijacking	New Service	Deobfuscate/ Decode Files or Information	Password Filter DLL	Security Software Discovery	Third-party Software	Video Capture		Multilayer Encryption
	Regsvr32	External Remote Services	Path Interception	Disabling Security Tools	Private Keys	System Information Discovery	Windows Admin Shares			Remote Access Tools
	Rundll32	File System Permissions Weakness	Port Monitors	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Network Configuration Discovery	Windows Remote Management			Remote File Copy
	Scheduled Task	Hidden Files and Directories	Process Injection	Extra Window Memory Injection		System Network Connections Discovery				Standard Application Layer Protocol
				Network Share Connection Removal						
				Obfuscated Files or Information						
				Plist Modification						
				Port Knocking						
				Process Doppelgänging						
				Process Hollowing						
				Process Injection						
				Redundant Access						
				Regsvcs/Regasm						
				Regsvr32						
				Rootkit						
				Rundll32						
				SIP and Trust Provider Hijacking						

Recent studies of cyber attacks confirm that 85% of successful cyber attacks were perpetrated with valid credentials

The pictur