SOC ReLoad
#SOCReLoad21

TRACK 1 - LEADERS

How to Leverage a Threat-Centric Approach to Achieve Actionable Security Outcomes

Christiaan Beek
Lead Scientist,
Sr. Principal Engineer

Silvan Tschopp
Head of Product Marketing

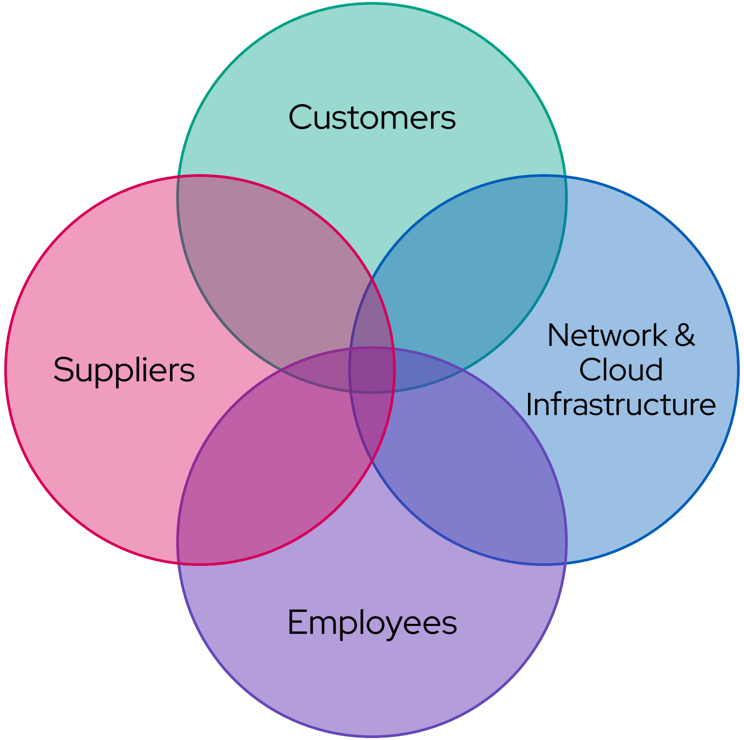
McAfee

PICUS

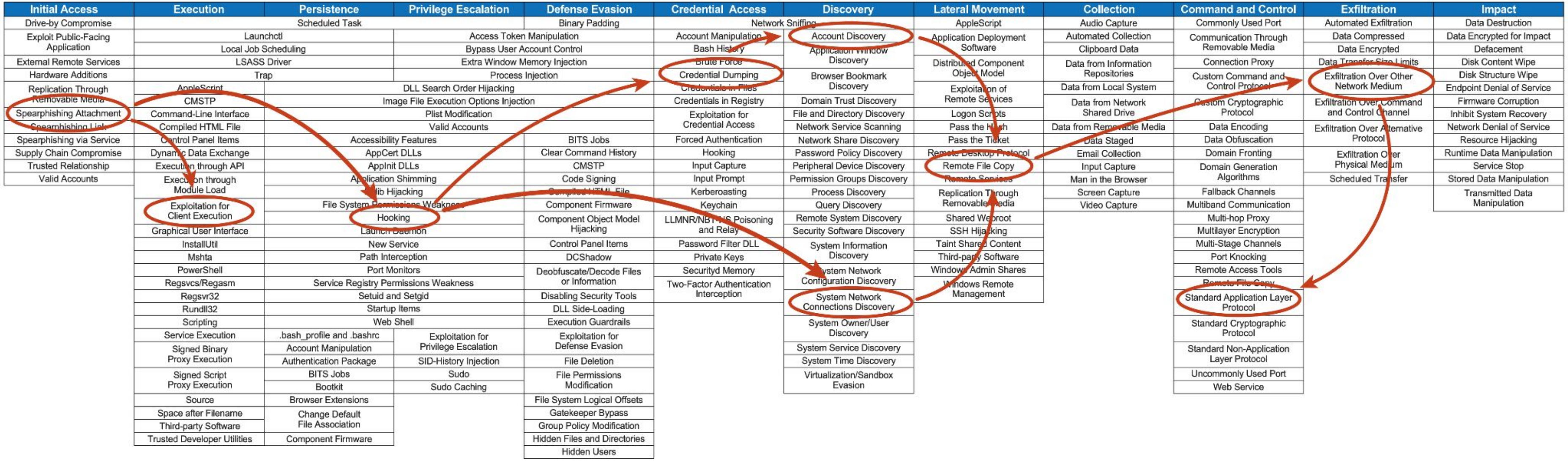
What does a “threat-centric approach to security” mean?

Bodiam Castle East Sussex, UK by WyrdLight.com, CC BY-SA 3.0

Understand where attacks may be coming from



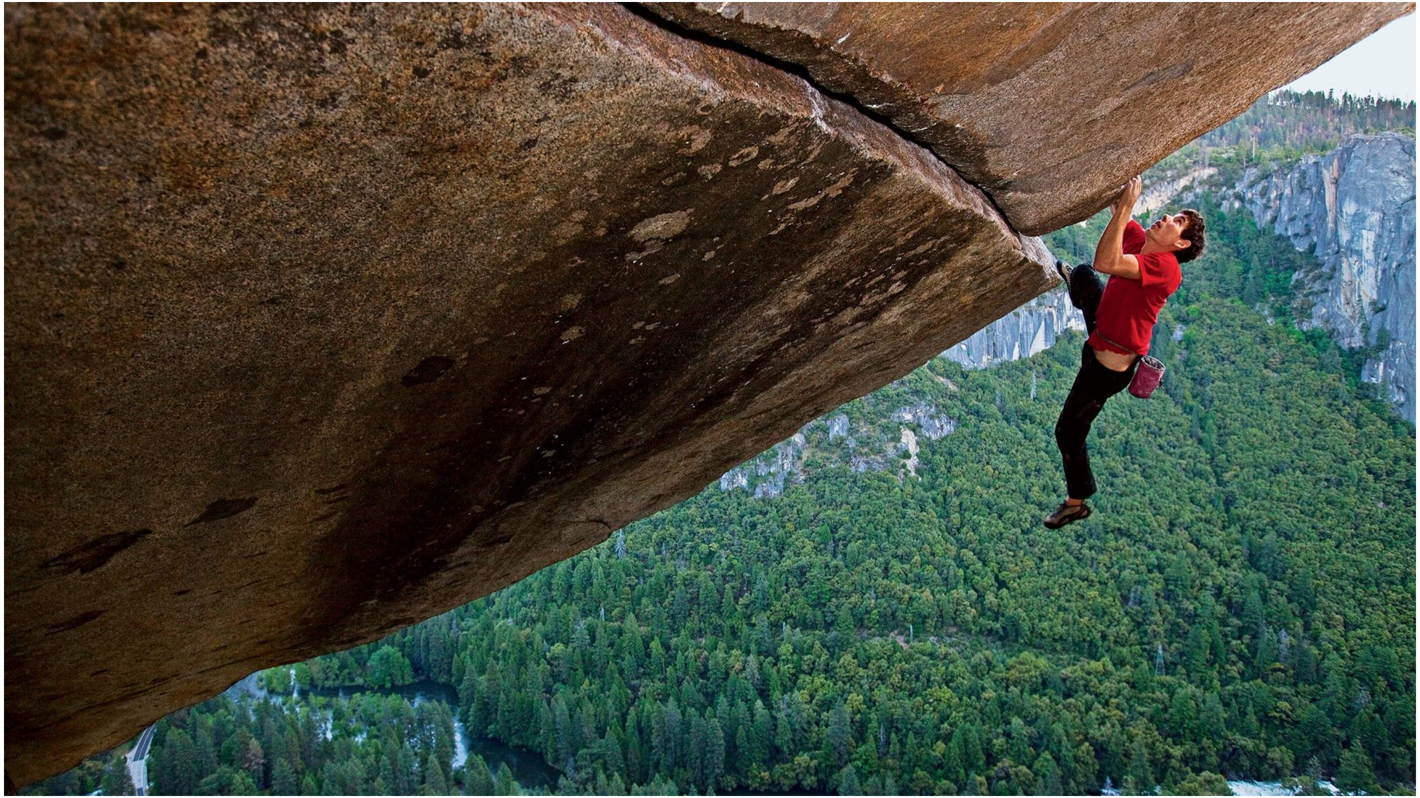
Visualise attack paths to align your defenses



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	Scheduled Task	Scheduled Task	Scheduled Task	Binary Padding	Network Sniffing	Network Sniffing	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Launchctl	Launchctl	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Local Job Scheduling	Local Job Scheduling	Bypass User Account Control	Bypass User Account Control	Bash History	Application Window Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	LSASS Driver	LSASS Driver	Extra Window Memory Injection	Extra Window Memory Injection	Brute Force	Browser Bookmark Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Trap	Trap	Process Injection	Process Injection	Credential Dumping	Domain Trust Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Other Network Medium	Disk Structure Wipe
Spearphishing Attachment	AppleScript	DLL Search Order Hijacking	DLL Search Order Hijacking	DLL Search Order Hijacking	Credentials in Files	File and Directory Discovery	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	CMSTP	Image File Execution Options Injection	Image File Execution Options Injection	Image File Execution Options Injection	Credentials in Registry	Network Service Scanning	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Alternative Protocol	Firmware Corruption
Spearphishing via Service	Command-Line Interface	Plist Modification	Plist Modification	Plist Modification	Exploitation for Credential Access	Network Share Discovery	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Compiled HTML File	Valid Accounts	Valid Accounts	Valid Accounts	Forced Authentication	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Control Panel Items	Accessibility Features	Accessibility Features	BITS Jobs	Hooking	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	Dynamic Data Exchange	AppCert DLLs	AppCert DLLs	Clear Command History	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multiband Communication		Runtime Data Manipulation
	Execution through API	AppInit DLLs	AppInit DLLs	CMSTP	Input Prompt	Process Discovery	Shared Webroot	Screen Capture	Multi-hop Proxy		Service Stop
	Execution through Module Load	Application Shimming	Application Shimming	Code Signing	Kerberoasting	Query Discovery	SSH Hijacking	Video Capture	Multilayer Encryption		Stored Data Manipulation
	Exploitation for Client Execution	Dylib Hijacking	Dylib Hijacking	Compiled HTML File	Keychain	Remote System Discovery	Taint Shared Content		Multi-Stage Channels		Transmitted Data Manipulation
	Graphical User Interface	File System Permissions Weakness	File System Permissions Weakness	Component Firmware	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Third-party Software		Port Knocking		
	InstallUtil	Hooking	Hooking	Component Object Model Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Mshta	Launch Daemon	Launch Daemon	Control Panel Items	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	PowerShell	New Service	New Service	DCShadow	Securityd Memory	System Network Connections Discovery			Standard Application Layer Protocol		
	Regsvcs/Regasm	Path Interception	Path Interception	Deobfuscate/Decode Files or Information	Two-Factor Authentication Interception	System Owner/User Discovery			Standard Cryptographic Protocol		
	Regsvr32	Port Monitors	Port Monitors	Disabling Security Tools		System Service Discovery			Standard Non-Application Layer Protocol		
	Rundll32	Service Registry Permissions Weakness	Service Registry Permissions Weakness	DLL Side-Loading		System Time Discovery			Uncommonly Used Port		
	Scripting	Setuid and Setgid	Setuid and Setgid	Execution Guardrails		Virtualization/Sandbox Evasion			Web Service		
	Service Execution	Startup Items	Startup Items	Exploitation for Defense Evasion							
	Signed Binary Proxy Execution	Web Shell	Web Shell	File Deletion							
	Signed Script Proxy Execution	.bash_profile and .bashrc	Exploitation for Privilege Escalation	File Permissions Modification							
	Source	Account Manipulation	SID-History Injection	File System Logical Offsets							
	Space after Filename	Authentication Package	Sudo	Gatekeeper Bypass							
	Third-party Software	BITS Jobs	Sudo Caching	Group Policy Modification							
	Trusted Developer Utilities	Bootkit		Hidden Files and Directories							
		Browser Extensions		Hidden Users							
		Change Default File Association									
		Component Firmware									

ATT&CK folding map, mitre.org

Understand your risk profile to take informed decisions



Alex Honnold on El Capitan, USA by Jimmy Chin

THANK YOU!