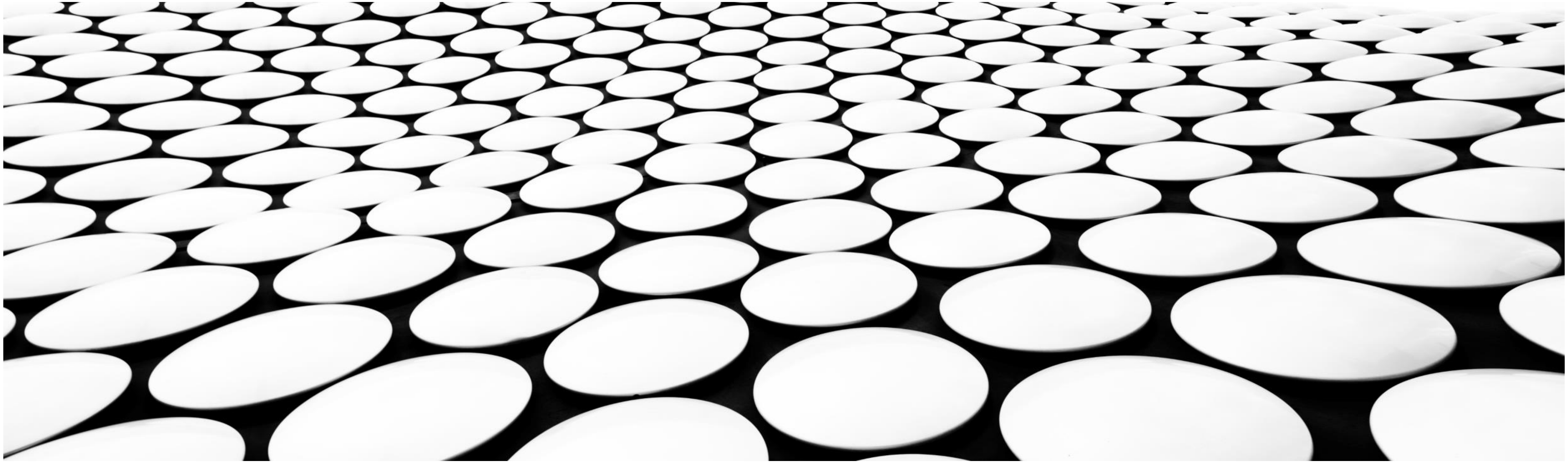
CYBERSECURITY ROLES AND SKILLS

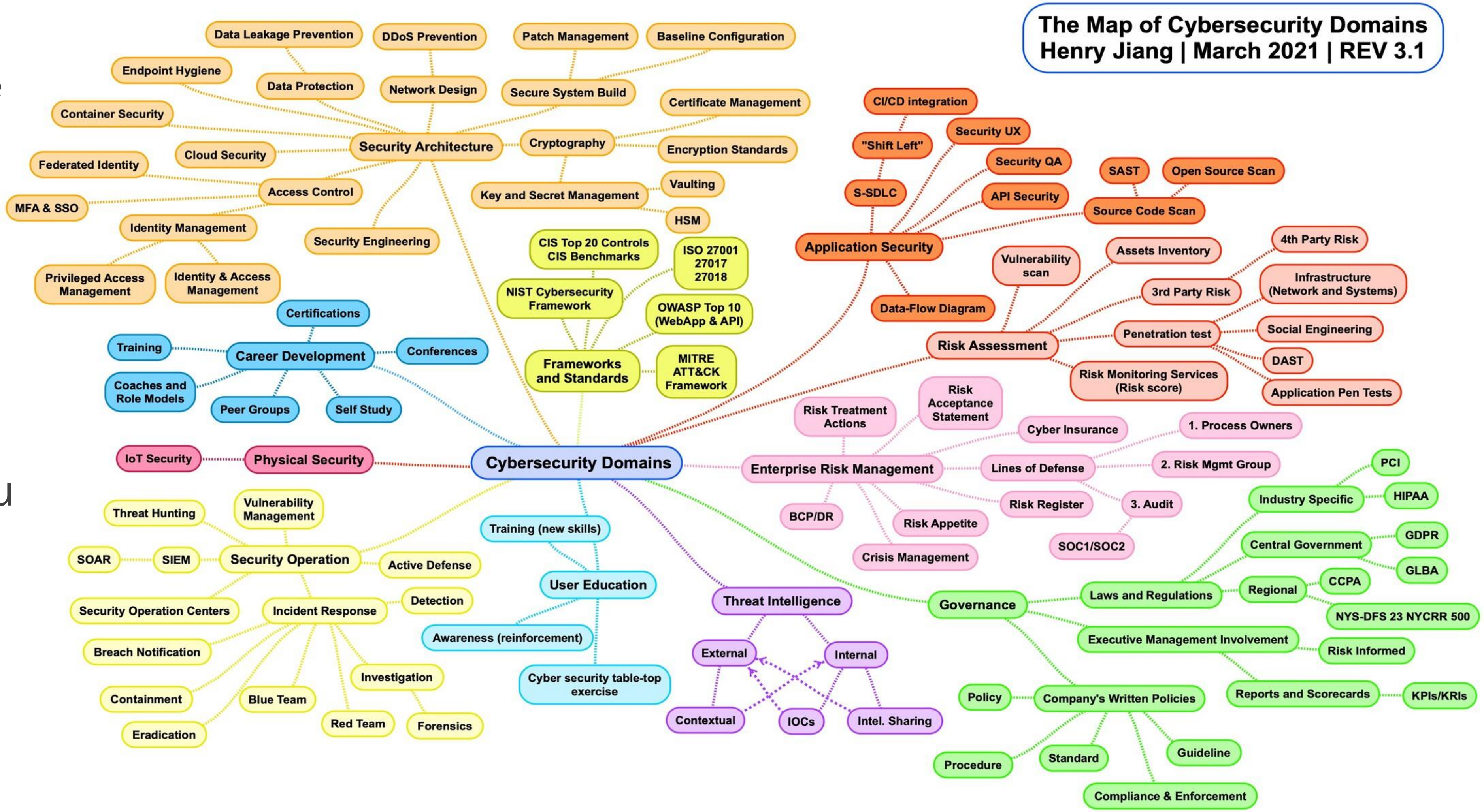
A GLIMPSE INTO THE POSSIBILITIES OF THE CYBERSECURITY FIELD



CYBERSECURITY – A DIVERSE FIELD

Cyber is too big for one person to do-it-all or know-it-all

- Identify the options and possibilities
- Diversify your skills and options
- Seek to do what you enjoy



CYBERSECURITY – THE PILLARS

- Security Operations – defenders, attackers, and specialized ops roles
- Architecture and Engineering – designing and creating security in systems, networks, apps, cloud
- Governance, Risk Management, and Compliance (GRC) – Risk managers, decision makers, business first approach geared towards ensuring the success of the company
- Product, Education, Awareness, Legal (PEAL) – the abnormal cybersecurity roles, focused on support, learning, other industries with a focus on the impacts of cybersecurity

SECURITY OPERATIONS TERMS/TOPICS

Threat Intelligence	TTPs
SIEM	APTs
IR	IOCs
Forensics	SOC
Malware/Vulnerabilities	EDR/XDR

ARCHITECTURE & ENGINEERING TERMS/TOPICS

Secure coding/SDLC	APIs
Static/Dynamic Code Analysis	Encryption
Cloud design	Key management
Application security	Container security
Scripting	SOAR
System Design	Web Application Development

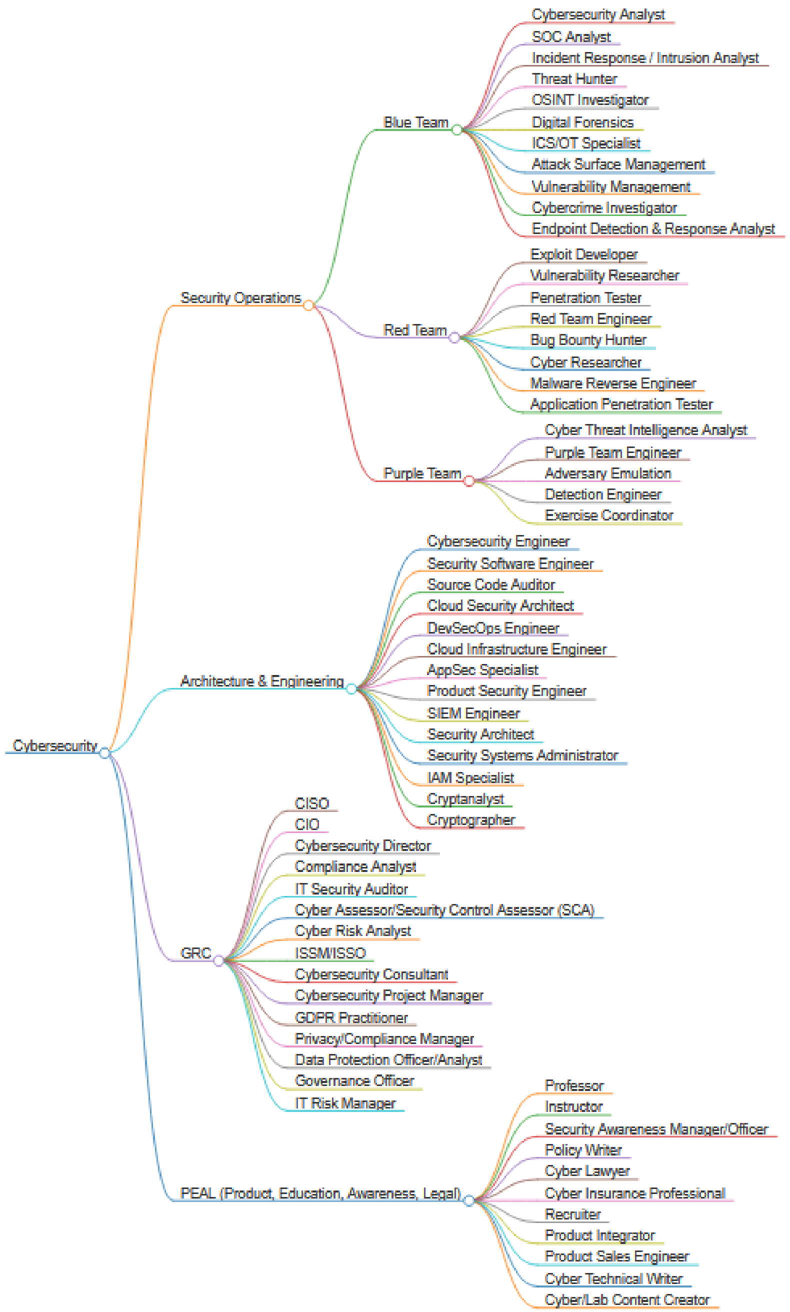
GRC TERMS/TOPICS

Frameworks	Policies
Risk Assessments	Standards
Audits	Security Controls
Business Continuity	Disaster Recovery
Laws/Regulations	PII

PEAL TERMS/TOPICS

Certifications	Security Awareness
Conferences	Security Training
Product Sales	Courses
Labs/CTFs	Degrees
Recruiting	Workforce Development
Law	Product Integration

ALL THE TITLES



- Cybersecurity
  - Security Operations
    - Blue Team
      - Cybersecurity Analyst
      - SOC Analyst
      - Incident Response / Intrusion Analyst
      - Threat Hunter
      - OSINT Investigator
      - Digital Forensics
      - ICS/OT Specialist
      - Attack Surface Management
      - Vulnerability Management
      - Cybercrime Investigator
      - Endpoint Detection & Response Analyst
    - Red Team
      - Exploit Developer
      - Vulnerability Researcher
      - Penetration Tester
      - Red Team Engineer
      - Bug Bounty Hunter
      - Cyber Researcher
      - Malware Reverse Engineer
      - Application Penetration Tester
    - Purple Team
      - Cyber Threat Intelligence Analyst
      - Purple Team Engineer
      - Adversary Emulation
      - Detection Engineer
      - Exercise Coordinator
  - Architecture & Engineering
    - Cybersecurity Engineer
    - Security Software Engineer
    - Source Code Auditor
    - Cloud Security Architect
    - DevSecOps Engineer
    - Cloud Infrastructure Engineer
    - AppSec Specialist
    - Product Security Engineer
    - SIEM Engineer
    - Security Architect
    - Security Systems Administrator
    - IAM Specialist
    - Cryptanalyst
    - Cryptographer
  - GRC
    - CISO
    - CIO
    - Cybersecurity Director
    - Compliance Analyst
    - IT Security Auditor
    - Cyber Assessor/Security Control Assessor (SCA)
    - Cyber Risk Analyst
    - ISSM/ISSO
    - Cybersecurity Consultant
    - Cybersecurity Project Manager
    - GDPR Practitioner
    - Privacy/Compliance Manager
    - Data Protection Officer/Analyst
    - Governance Officer
    - IT Risk Manager
  - PEAL (Product, Education, Awareness, Legal)
    - Professor
    - Instructor
    - Security Awareness Manager/Officer
    - Policy Writer
    - Cyber Lawyer
    - Cyber Insurance Professional
    - Recruiter
    - Product Integrator
    - Product Sales Engineer
    - Cyber Technical Writer
    - Cyber/Lab Content Creator

ABOUT ME

- 25 years old
- BS – Cybersecurity ‘20 (Regent)
- MS - Cybersecurity and Information Assurance ‘23 (WGU)
- Certs
  - CISSP, CC
  - CASP+, CySA+, PenTest+, Security+
  - CCSK
  - Splunk Cybersecurity Defense Analyst
  - BLT1
  - Microsoft SC-900, MS-900, AZ-900
  - CFR
  - INE ICCA, Cloud Fundamentals
  - ATT&CK – CTI, Threat Hunting and Detection Engineering, Adversary Emulation, SOC Assessment, Purple Teaming

US CYBER GAMES

TRAIN. COMPETE. WIN.

- US Cyber Team SIII Pipeline Program and Tiger Team
- Blog – The Purple Van: https://purplevan.substack.com/
- Projects – TID Ecosystem: https://start.me/p/X25q7l/threat-informed-defense-ecosystem
- Speaker – SMD Symposium, DC3 TECH Exchange, National Cyber Summit (Sept 26)
  - (two largest cons in HSV)
- NCL Spring ‘24 Top 500

HOW I GOT HERE

- 2020
- BS Cybersecurity in 2020… :(
- Cert: Security+
- First FT job 11/20 – Cybersecurity Analyst (GRC)
- 2021
- Security clearance
- Certs: PenTest+, CySA+, INE Cloud Fundamentals, CMMC RP
- Join orgs – NDCA, SAME, HackerOne
- Built optimization tool, leading projects
- 2022
- Promoted 12/21 - Senior Cybersecurity Analyst/ISSM
- Join ISACA, InfraGard, ISC2
- Certs: CC, CISSP (associate), ATT&CK certs, MSFT certs, CFR, ICCA
- Speaker – SMD Symposium and DC3 Tech Ex
- 2023
- 5/23 - Move to new contract (flex)
- WGU MS Cybersecurity
- US Cyber Games Combine and Pipeline invite
- Certs: CCSK, Splunk Cyber Defense Analyst
- Start Writing Blog
- 2024
- US Cyber Games Pipeline and Tiger Team
- Certs: CASP+, CISSP
- NCL Top 500 (out of 8000+)
- Speaker – National Cyber Summit

MY ROLE AT H2L – APPLICATION ENGINEER

Day Role

- “Application Engineer” A diverse title, could encompass many roles
- My daily work involves aspects of:
  - Cybersecurity Engineer
  - Data Engineer
  - SIEM Engineer
  - Detection Engineer
  - Threat Hunting
  - Threat Intelligence
  - Incident Response(ish)

Journey

1. Cybersecurity Analyst – CMMC & RMF Consulting
2. Senior Cybersecurity Analyst – RMF (Sys Admin and ISSM)
3. Application Engineer – Security Data

EARLY CAREER TIPS

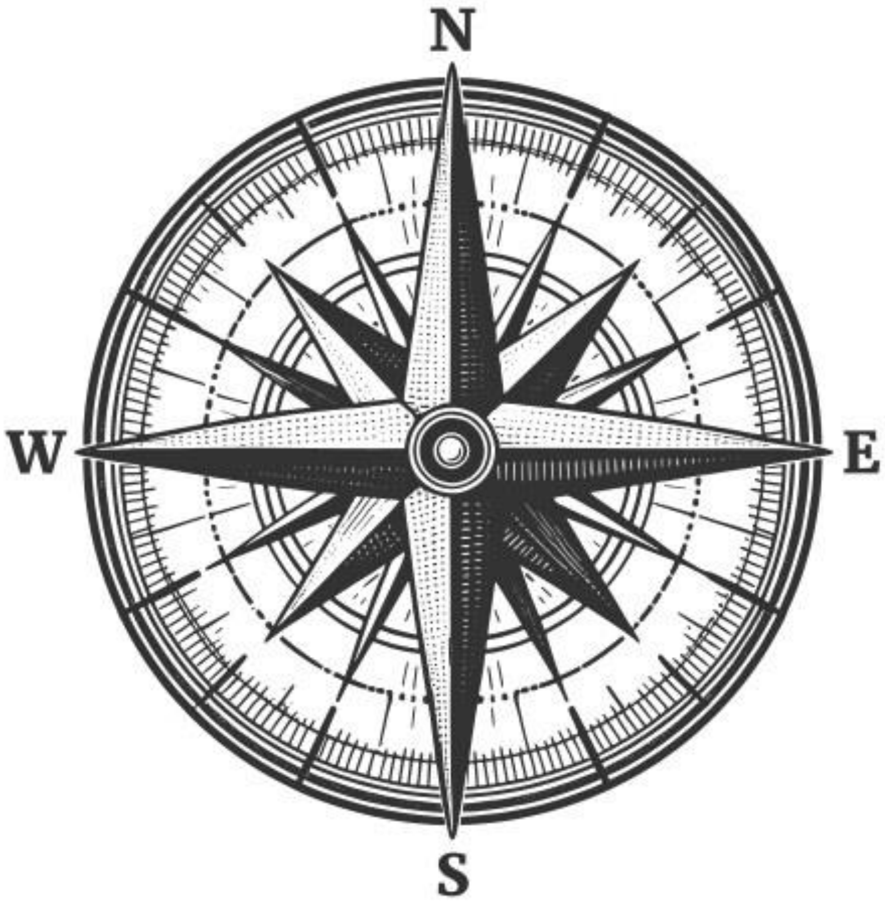
- Learn, Learn, Learn
- Set goals
- LinkedIn, network, conferences (remote options)
- Show passion - Projects, CTFs, VMs/labs
  - NCL, THM, HTB
- Utilize resources, student discounts, anything free
- Be patient and work hard

To work in Gov:

- Get degree (or self learn) and a Sec+ (90 days after job otherwise)
- Identify options and align with abilities, but be willing to take something to get in the door
- Get job
- Get clearance (might be in reverse order to the job)

WHAT YOU CAN DO NOW

- Identify your target role – start with pillar, move towards more specific
- Create Your Roadmap – goals, skills, knowledge, certs
- Stay the Course – don’t fall for “new shiny cert/course” syndrome
- Quality Over Quantity – focus on useful learning items that support the target
- Measure Progress – check in, how is it going, stay on track

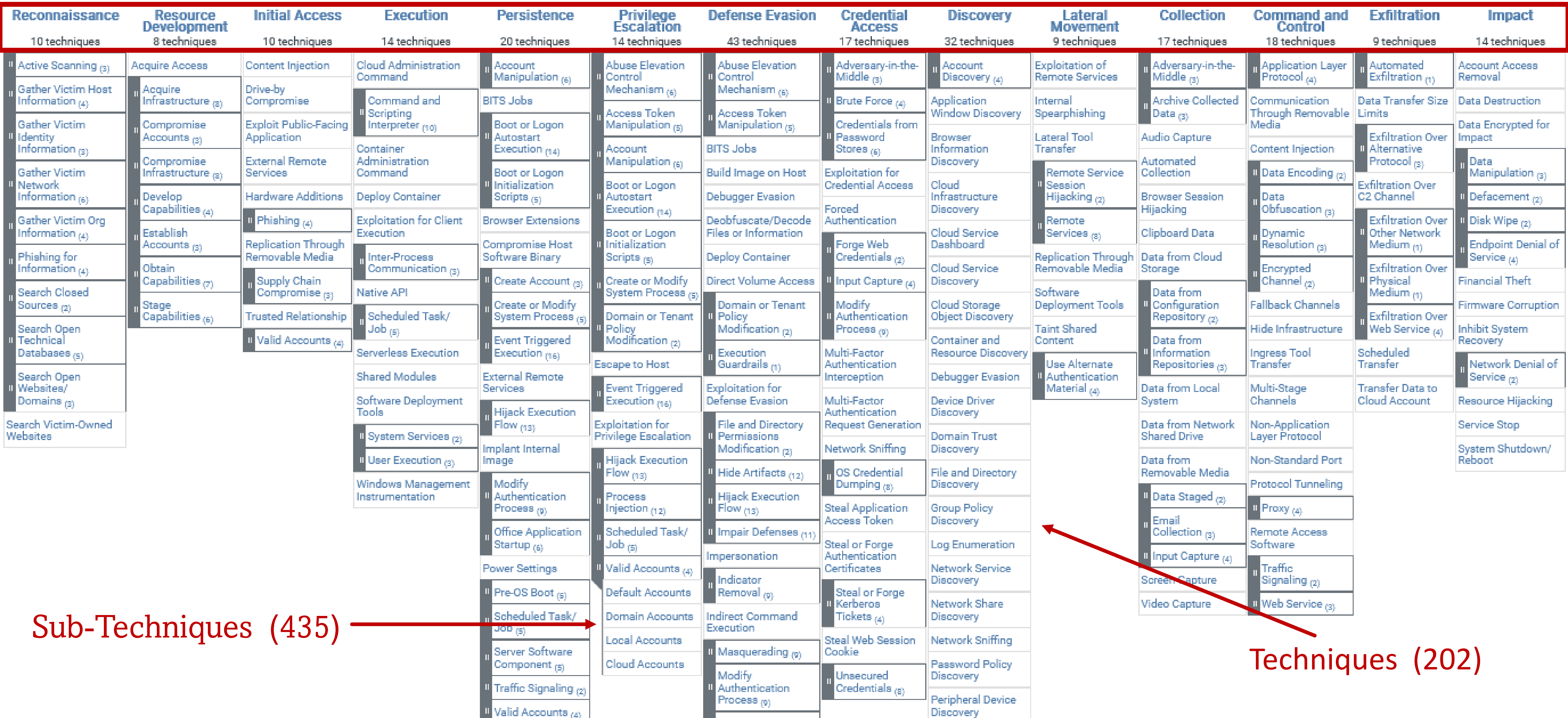


EXAMPLE – SECURITY OPERATIONS

- Identify your target role – Security Operations, SOC / Incident Response
- Create Your Roadmap – SIEM, Threat hunting, cyber kill chain, MITRE ATT&CK, EDR, network/host forensics
  - CTFs/Labs - hands on learning
  - Certs – CC, Sec+, CySA+/BLT1
- Stay the Course – Only doing school work and learning the above items in regards to cyber
- Quality Over Quantity – THM, HTB, AttackIQ Academy, Let’s Defend, NCL, Huntress CTF
- Measure Progress – quarterly

ATT&CK ENTERPRISE MATRIX

Tactics (14)



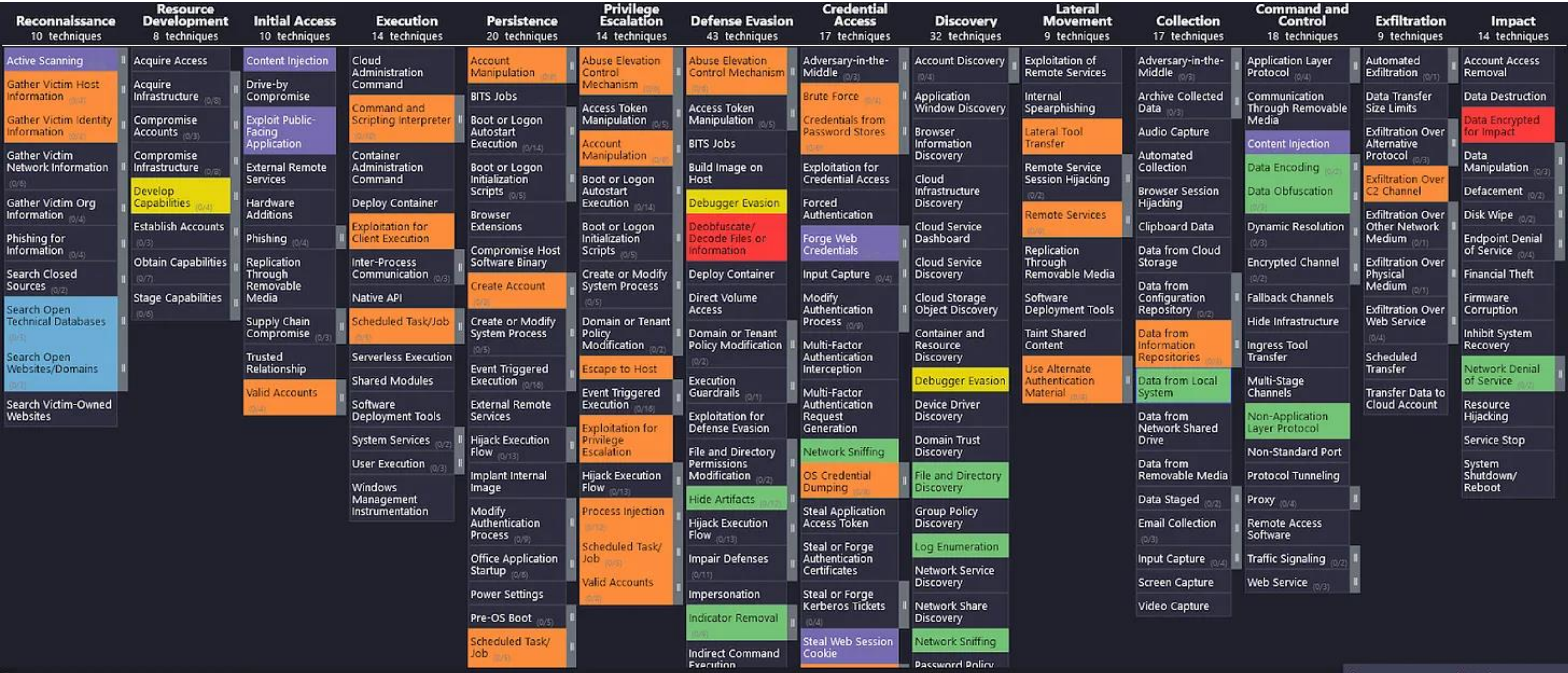
Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 14 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	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)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (10)	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 Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Host Software Binary	Create or Modify System Process (5)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Native API	Create Account (3)	Domain or Tenant Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (5)	Escape to Host	Direct Volume Access	Modify Authentication Process (9)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Scheduled Transfer	Financial Theft
Search Open Websites/Domains (3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (16)	Event Triggered Execution (16)	Domain or Tenant Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Hide Infrastructure	Transfer Data to Cloud Account	Firmware Corruption
Search Victim-Owned Websites		Valid Accounts (4)	Shared Modules	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails (1)	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Ingress Tool Transfer		Inhibit System Recovery
			Software Deployment Tools	Hijack Execution Flow (13)	Hijack Execution Flow (13)	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Multi-Stage Channels		Network Denial of Service (2)
			System Services (2)	Implant Internal Image	Process Injection (12)	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	File and Directory Discovery		Data from Removable Media	Non-Application Layer Protocol		Resource Hijacking
			User Execution (3)	Modify Authentication Process (9)	Scheduled Task/Job (5)	Hide Artifacts (12)	Steal Application Access Token	Group Policy Discovery		Data Staged (2)	Non-Standard Port		Service Stop
			Windows Management Instrumentation	Office Application Startup (6)	Valid Accounts (4)	Hijack Execution Flow (13)	Steal or Forge Authentication Certificates	Log Enumeration		Email Collection (3)	Protocol Tunneling		System Shutdown/Reboot
				Power Settings	Default Accounts	Impair Defenses (11)	Steal or Forge Kerberos Tickets (4)	Network Service Discovery		Input Capture (4)	Proxy (4)		
				Pre-OS Boot (5)	Domain Accounts	Impersonation	Steal Web Session Cookie	Network Share Discovery		Screen Capture	Remote Access Software		
				Scheduled Task/Job (5)	Local Accounts	Indicator Removal (9)	Unsecured Credentials (8)	Network Sniffing		Video Capture	Traffic Signaling (2)		
				Server Software Component (5)	Cloud Accounts	Indirect Command Execution		Password Policy Discovery			Web Service (3)		
				Traffic Signaling (2)		Masquerading (9)		Peripheral Device Discovery					
				Valid Accounts (4)		Modify Authentication Process (9)							

Sub-Techniques (435)

Techniques (202)

50 TOP TTPS IN CTFS: HTTPS://GITHUB.COM/PURPLEVAN/ATTACK_CTF_LAYER/TREE/MAIN

COLOR KEY: ORANGE=PWN, YELLOW=RE, BLUE=OSINT, GREEN=FORENSICS, PURPLE=WEB, RED=CRYPTO



Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 14 techniques
🟪 Active Scanning	Acquire Access	🟪 Content Injection	Cloud Administration Command	🟧 Account Manipulation (0/6)	🟧 Abuse Elevation Control Mechanism (0/6)	🟧 Abuse Elevation Control Mechanism (0/6)	Adversary-in-the-Middle (0/3)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
🟧 Gather Victim Host Information (0/4)	Acquire Infrastructure (0/8)	Drive-by Compromise	🟧 Command and Scripting Interpreter (0/12)	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	🟧 Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
🟧 Gather Victim Identity Information (0/3)	Compromise Accounts (0/3)	🟪 Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (0/14)	🟧 Account Manipulation (0/6)	BITS Jobs	🟧 Credentials from Password Stores (0/6)	Browser Information Discovery	🟧 Lateral Tool Transfer	Audio Capture	🟪 Content Injection	Exfiltration Over Alternative Protocol (0/3)	🟥 Data Encrypted for Impact
Gather Victim Network Information (0/6)	Compromise Infrastructure (0/8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Autostart Execution (0/14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection	🟩 Data Encoding (0/2)	🟧 Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	🟨 Develop Capabilities (0/4)	Hardware Additions	🟧 Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (0/5)	🟨 Debugger Evasion	Forced Authentication	Cloud Service Dashboard	🟧 Remote Services (0/8)	Browser Session Hijacking	🟩 Data Obfuscation (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing for Information (0/4)	Establish Accounts (0/3)	Phishing (0/4)	Inter-Process Communication (0/3)	Compromise Host Software Binary	Create or Modify System Process (0/5)	🟥 Deobfuscate/ Decode Files or Information	🟪 Forge Web Credentials	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (0/3)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Search Closed Sources (0/2)	Obtain Capabilities (0/7)	Replication Through Removable Media	Native API	🟧 Create Account (0/3)	Domain or Tenant Policy Modification (0/2)	Deploy Container	Input Capture (0/4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (0/2)	Exfiltration Over Web Service (0/4)	Endpoint Denial of Service (0/4)
🟦 Search Open Technical Databases (0/5)	Stage Capabilities (0/6)	Supply Chain Compromise (0/3)	🟧 Scheduled Task/Job (0/5)	Create or Modify System Process (0/5)	🟧 Escape to Host	Direct Volume Access	Modify Authentication Process (0/9)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (0/2)	Fallback Channels	Scheduled Transfer	Financial Theft
🟦 Search Open Websites/Domains (0/3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (0/16)	Event Triggered Execution (0/16)	Domain or Tenant Policy Modification (0/2)	Multi-Factor Authentication Interception	🟨 Debugger Evasion	🟧 Use Alternate Authentication Material (0/4)	🟧 Data from Information Repositories (0/5)	Hide Infrastructure	Transfer Data to Cloud Account	Firmware Corruption
Search Victim-Owned Websites		🟧 Valid Accounts (0/4)	Shared Modules	External Remote Services	🟧 Exploitation for Privilege Escalation	Execution Guardrails (0/1)	Multi-Factor Authentication Request Generation	Device Driver Discovery		🟩 Data from Local System	Ingress Tool Transfer		Inhibit System Recovery
			Software Deployment Tools	Hijack Execution Flow (0/13)	Hijack Execution Flow (0/13)	Exploitation for Defense Evasion	🟩 Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Multi-Stage Channels		🟩 Network Denial of Service (0/2)
			System Services (0/2)	Implant Internal Image	🟧 Process Injection (0/12)	File and Directory Permissions Modification (0/2)	🟧 OS Credential Dumping (0/8)	🟩 File and Directory Discovery		Data from Removable Media	🟩 Non-Application Layer Protocol		Resource Hijacking
			User Execution (0/3)	Modify Authentication Process (0/9)	🟧 Scheduled Task/ Job (0/5)	🟩 Hide Artifacts (0/12)	Steal Application Access Token	Group Policy Discovery		Data Staged (0/2)	Non-Standard Port		Service Stop
			Windows Management Instrumentation	Office Application Startup (0/6)	🟧 Valid Accounts (0/4)	Hijack Execution Flow (0/13)	Steal or Forge Authentication Certificates	🟩 Log Enumeration		Email Collection (0/3)	Protocol Tunneling		System Shutdown/ Reboot
				Power Settings		Impair Defenses (0/11)	Steal or Forge Kerberos Tickets (0/4)	Network Service Discovery		Input Capture (0/4)	Proxy (0/4)		
				Pre-OS Boot (0/5)		Impersonation	🟪 Steal Web Session Cookie	Network Share Discovery		Screen Capture	Remote Access Software		
				🟧 Scheduled Task/ Job (0/5)		🟩 Indicator Removal (0/9)		🟩 Network Sniffing		Video Capture	Traffic Signaling (0/2)		
						Indirect Command Execution		Password Policy			Web Service (0/3)		

EXPLAIN WHAT YOU LEARNED

- Why it would be beneficial to learn cybersecurity through CTF challenges within the context of ATT&CK TTPs:
  - Relate to real-world cyber-attack TTPs
  - Understand how to better communicate the skills and knowledge gained in CTFs
  - Better preparation for industry terms and understanding of how to categorize cyber attacks
  - Develop a ‘purple team’ mentality by identifying attack and defense measures
- It is one thing for a student to be able to say “I found the flag” or…
- Explain how they utilized Active Scanning, Gather Victim Host Information, Search Open Websites/Domains, Valid Accounts, Command and Scripting Interpreter, Exploitation for Privilege Escalation, to identify the hidden flag.
- Create a better knowledge grasp of industry terminology while enjoying the fun nature of a CTF

SKILLS TO GROW

- “Future-proof” yourself - top cybersecurity skills to possess in *2024*

1. Scripting - This is what allows you to provide value. Automation is king.
2. Research/Intel collection - OSINT, threat intel, Google wizardry, whatever you call it. The ability to find desired information is crucial.
3. System admin - So this one encompasses a lot and probably should be broken into 3 separate points… but the knowledge of how a system fundamentally works, how networking can happen, why the cloud isn’t some magical fairy land, is important. Cloud makes a lot more sense when you know how it operates. Also, this helps you weed out the bs from AI product vendors.
4. Critical analysis - Each environment is different; nothing can be standardized to fit everything. You need to know how a vuln impacts your environment, how changes will impact security, where the greatest weaknesses lie, which threats pose the greatest risk, etc. If you can’t make recommendations based on effective analysis, you won’t get far.
5. Ability to adjust - It’s hard to describe this one in words, but the ability to switch and adapt to what products are used, what controls are in place, deal with the changes from tech refreshes, moving to or out of the cloud, etc. If you can’t effectively learn new, you’ll be stuck in the past.

- Anything worthwhile is hard

RESOURCES FROM SLIDES

- NCL: https://nationalcyberleague.org/
- TryHackMe: https://tryhackme.com/
- HackTheBox (look into Academy, $8 a month): https://www.hackthebox.com/
- ISC2 Certified in Cybersecurity (Free): https://www.isc2.org/Certifications/CC
- US Cyber Team: https://www.uscybergames.com/
- Purple Van Blog - How to Learn Cybersecurity for (Almost) Free: https://open.substack.com/pub/purplevan/p/how-to-learn-cybersecurity-for-almost
- ATT&CK CTF layer: https://github.com/purplevan/attack_ctf_layer/tree/main
- MITRE ATT&CK: https://attack.mitre.org/
- Cyber Domain Map: https://www.linkedin.com/pulse/cybersecurity-domain-map-ver-30-henry-jiang/
- AttackIQ Academy: https://www.academy.attackiq.com/
- Let’s Defend: https://letsdefend.io/