Cybersecurity Overview

Alonzo Perry

Navigating fundamentals, learning, and collaborative growth.

Introduction

I’ve been in the industry for over 2 decades in various roles.

- Tech support, Network admin, Sys-admin, Web development, Infrastructure lead, DevOps engineer, Research & Development, Management, Compliance technical reviewer, Security engineering.
- Mostly for public sector but a fair amount of private sector roles as well.
- Currently working as a Principal Security Engineer for a large cloud service provider and software company.

Spent over a decade in the Air National Guard.

- Aircraft Avionics - Communications and Navigations systems for C-130s.
- Several deployments to various locations around the world.

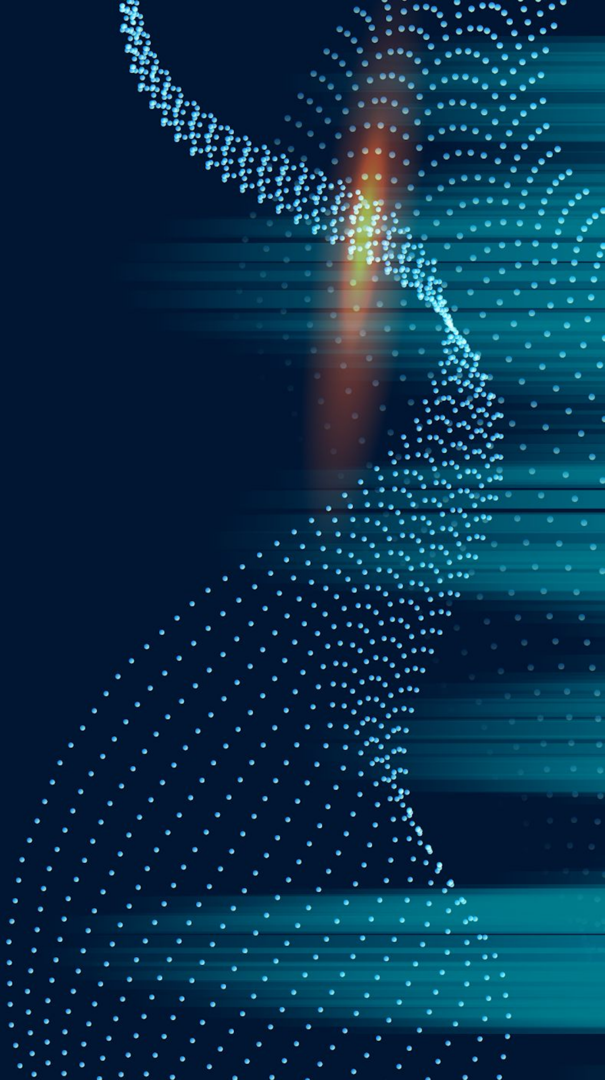
“Be like water making its way through cracks. Do not be assertive, but adjust to the object, and you shall find a way around or through it. If nothing within you stays rigid, outward things will disclose themselves.

Empty your mind, be formless. Shapeless, like water. If you put water into a cup, it becomes the cup. You put water into a bottle and it becomes the bottle. You put it in a teapot, it becomes the teapot. Now, water can flow or it can crash. Be water, my friend.”

— Bruce Lee

Topics covered

- Foundations
- Security Fundamentals
- Roles
- Frameworks
- Compliance
- AI/Machine Learning
- Continuous Learning
- Q&A



Common Acronyms

CWE: Common Weakness Enumeration

CVE: Common Vulnerabilities and Exposures

NVD: National Vulnerability Database

IOC: Indicators of Compromise

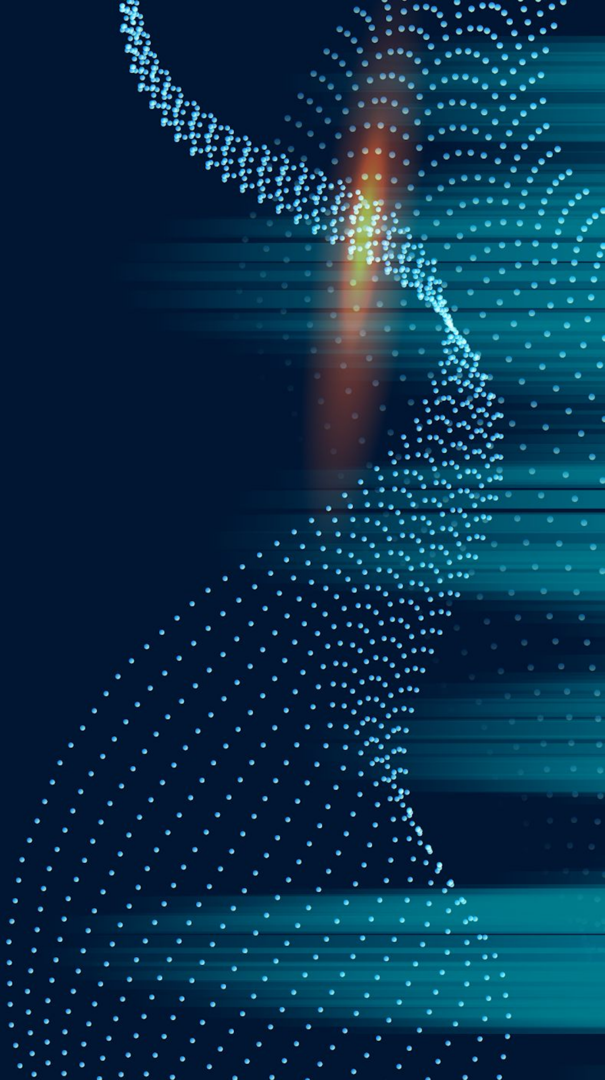
APT: Advanced Persistent Threat

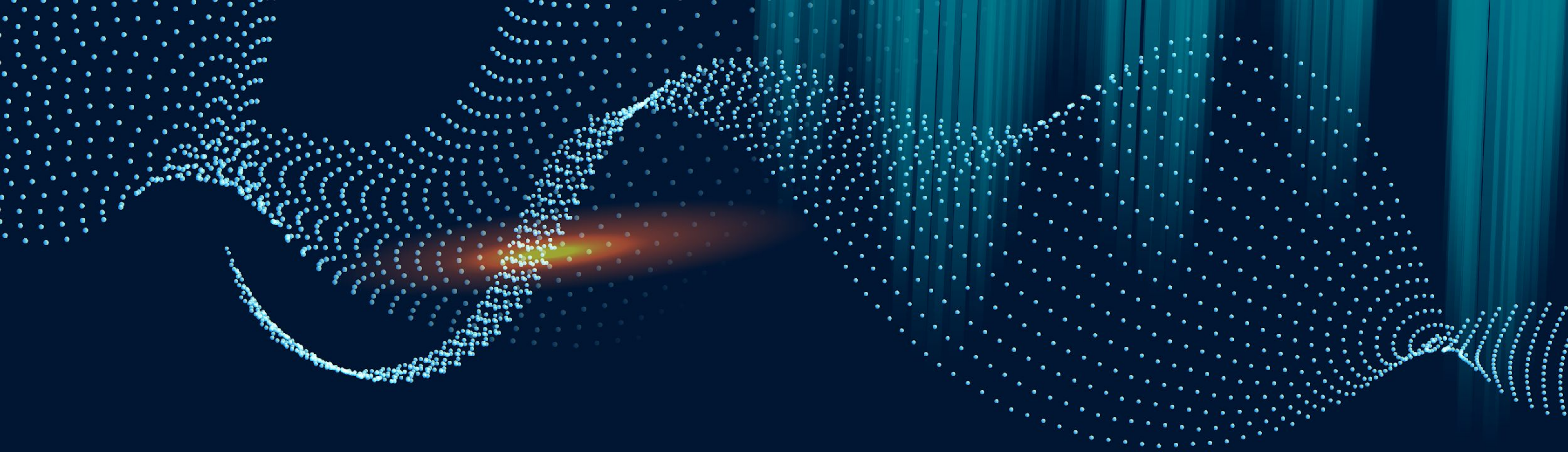
TTP: Tactics, Techniques & Procedures

SOC: Security Operations Center

PII: Personal Identifiable Information

IoT: Internet of Things





01

Foundations

Suggestions for helpful prerequisites

Tips - Securing your world - Passwords

Use Strong Passwords

- All passwords should be:
  - Long: At least 16 characters
  - Unique: Never reuse passwords
  - Random: Use a random string of mixed-case letters, numbers and symbols, like: Yuc8$RikA34%ZoPPao98t

Keep your passwords safe by using a password manager!

https://www.cisa.gov/sites/default/files/2024-09/Cybersecurity-Awareness-Month-2024-Posters.pdf

Tips - Securing your world - MFA

Turn on Multi Factor Authentication

Multifactor authentication provides an extra layer of security on your accounts and may include a biometric login or entering a code sent to your phone or email.

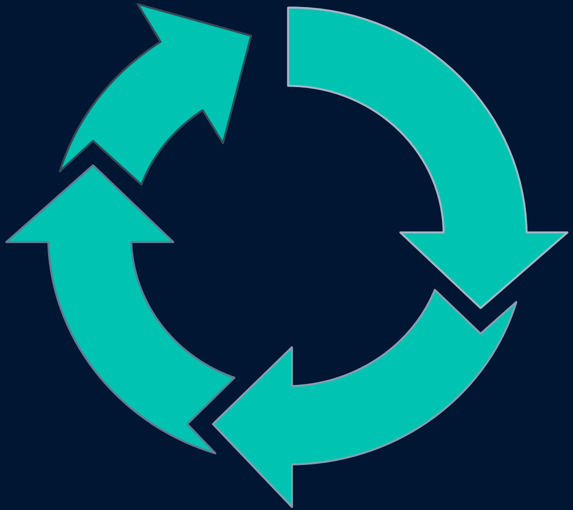
Note: When possible, download “bypass/backup” codes. This can be useful when all other authentication methods have been exhausted. Consider keeping them offline in written or printed format.

https://www.cisa.gov/sites/default/files/2024-09/Cybersecurity-Awareness-Month-2024-Posters.pdf

Tips - Securing your world - Updates

Update Software

Updating software and devices is the easiest way to stay protected from security threats. Perform updates as soon as they become available or set automatic updates.



Note: This includes mobile and IOT devices as well. Common, smart household devices and network gear (routers, mesh gear) could open your home up to unwanted intruders.

https://www.cisa.gov/sites/default/files/2024-09/Cybersecurity-Awareness-Month-2024-Posters.pdf

Tips - Securing your world - Phishing

Recognize and Report Phishing

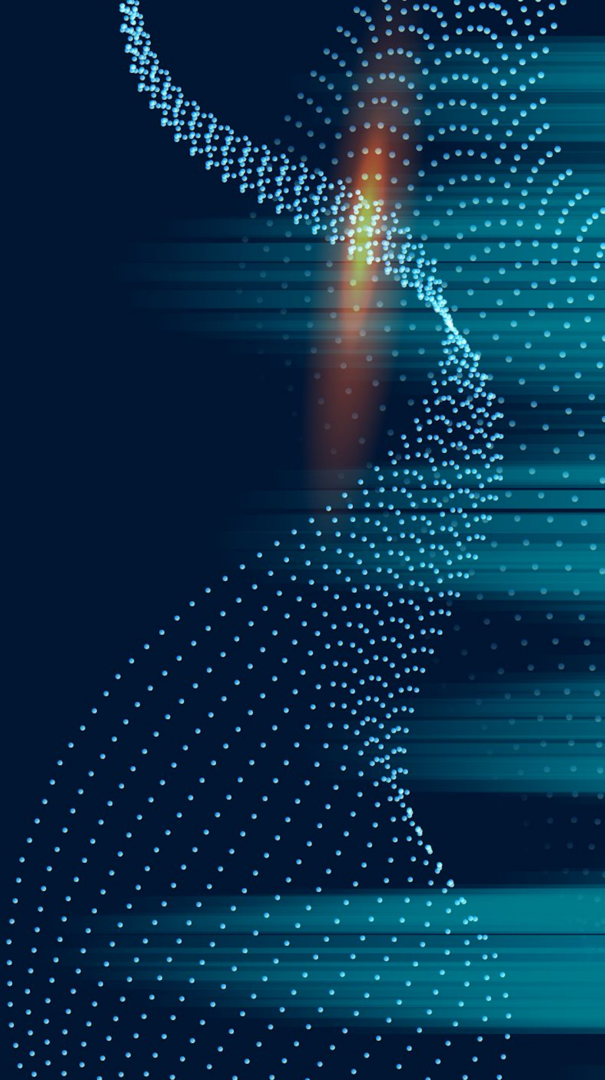
Keep an eye out for phishing and other scam attempts in your emails, texts, direct messages or phone calls. Always verify the sender before clicking links or downloading attachments. If you spot a scam, report it!

Note: This also applies to Deepfakes. AI generated video, audio, & images can also be used manipulate a target.

https://www.cisa.gov/sites/default/files/2024-09/Cybersecurity-Awareness-Month-2024-Posters.pdf

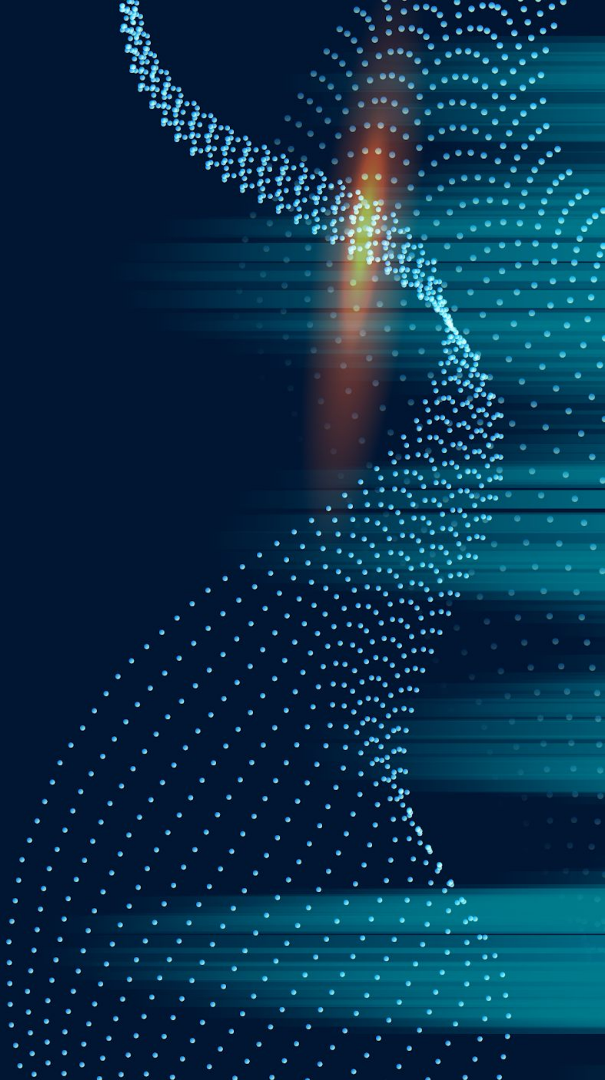
Foundational items

- Operating systems
  - Linux, Windows, MacOS, Unix variants, mobile
    - Common Linux flavors: Redhat/Centos, Oracle Linux, Debian/Ubuntu, Kali
    - Common BSD flavors: OpenBSD, FreeBSD, NetBSD
- Hardware basics (CPU, memory, storage, I/O cards (USB), network cards)
- Networking
- DNS
- Applications and services
  - Web apps, databases, system services, email, SSH, VPN, NTP



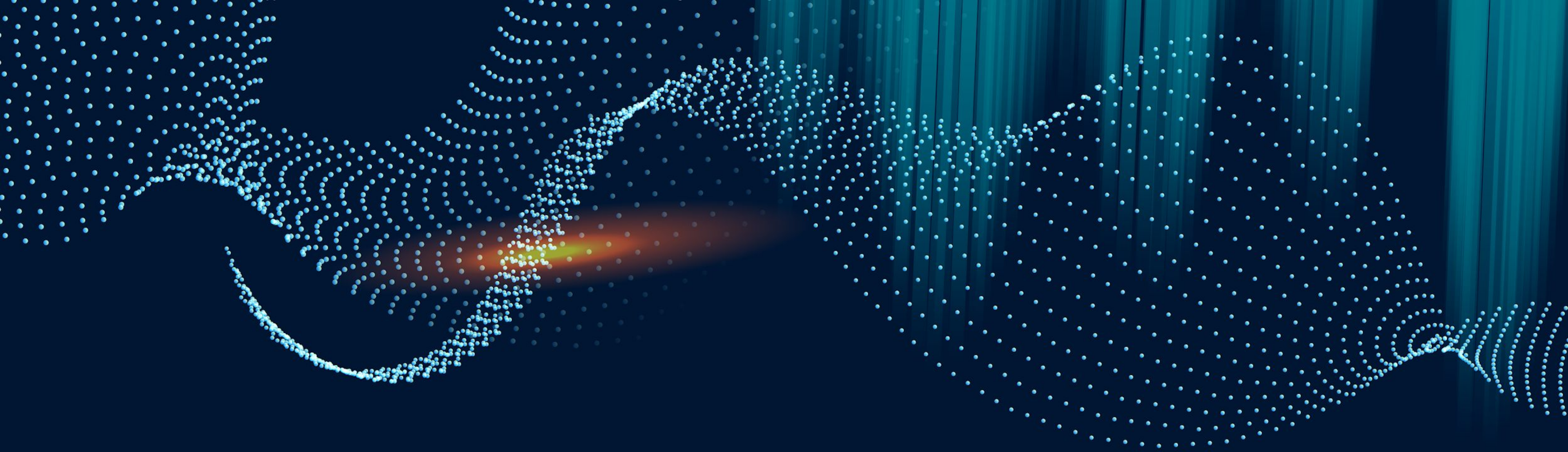
Foundational items - cont’d.

- IoT (Internet of Things)
- Virtualization
- Containers (Docker, Kubernetes etc..)
- Cloud infrastructure (services and connectivity)
- Coding
  - Bash, Python, Powershell, C++, Java etc..
  - IDE (Integrated development environment)
- CI/CD: Continuous Integration/Continuous Delivery or Deployment
- GIT (Source control)
  - Local and remote resources like GitHub
  - Bitbucket
- Logging



Foundational items - cont’d.

- Communications (oral/written)
- Other soft skills
  - Networking with people
  - Mentors/Mentees
  - Public speaking (Toastmasters)
  - Collaboration & team oriented approaches
  - Conflict management
  - Flexibility and adaptability
  - Time management
- Anxiety management
- Imposter syndrome
- Positive attitude



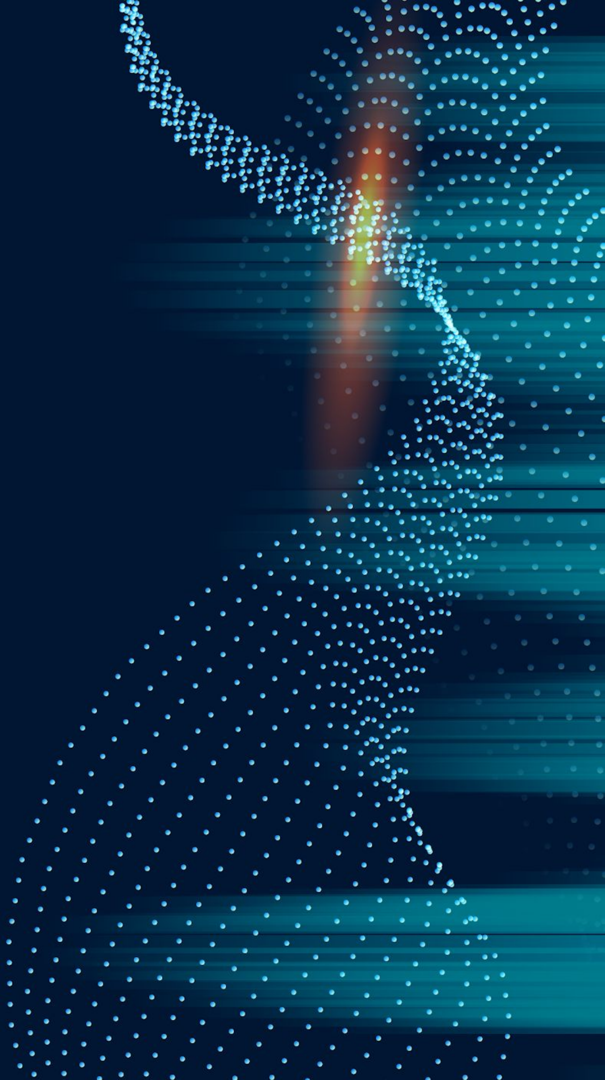
02

Security Fundamentals

An overview of key areas of interest

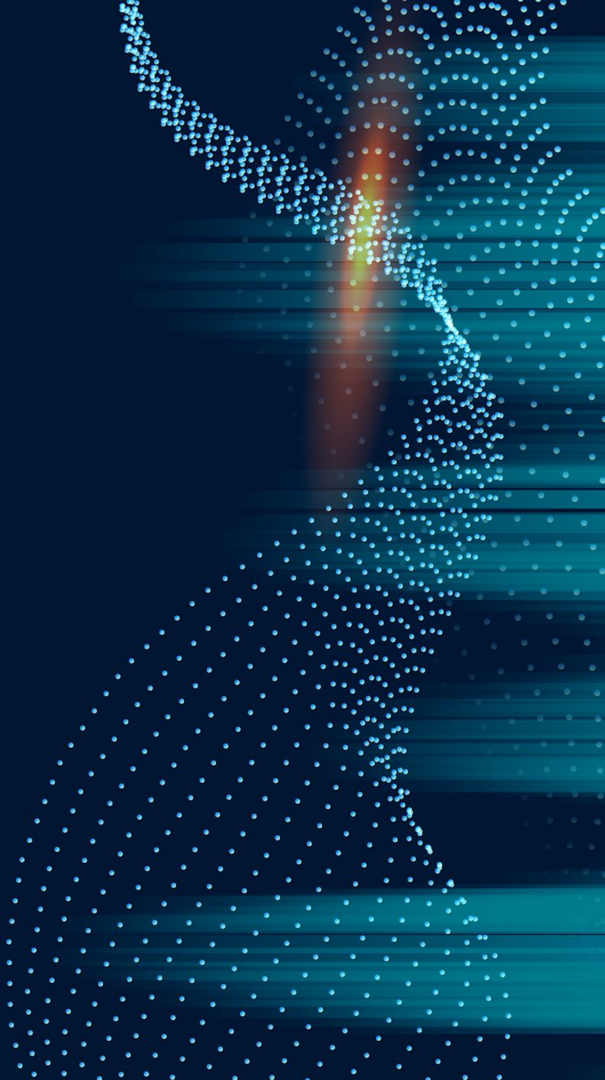
Security items

- Firewalls and proxies
- Intrusion detection, Intrusion prevention
- Malware detection
- EDR (Endpoint detection and response)
- XDR (Extended detection and response)
- Access controls
  - LDAP/AD
  - Passwords, MFA
- Cryptography
  - PKI
  - TLS/SSL
  - Hashing (files etc)
  - Wi-Fi (WPA2, WPA3)
- VPNs, SSH, SCP
- Nmap



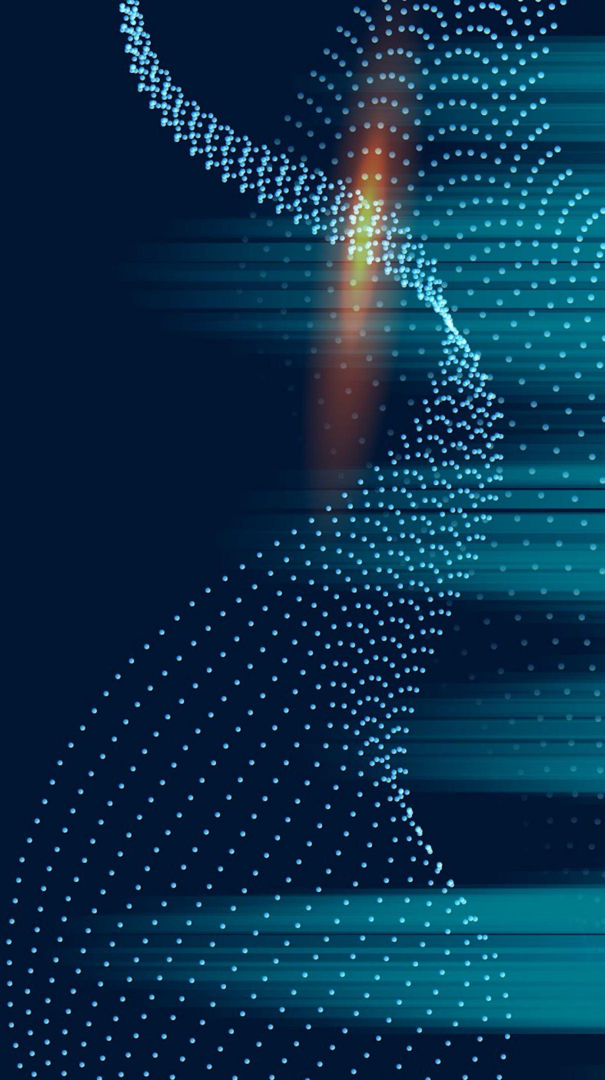
Security items - cont’d

- Configuration management
  - Chef, Puppet, Ansible
  - Microsoft GPO (Group Policy)
  - Microsoft Intune
- Patching
  - OS, Applications, Firmware
- Backups
- Documentation
  - SOPs (Standard operating procedures)
  - Runbooks
  - Vendor documentation
  - Local “help” documentation

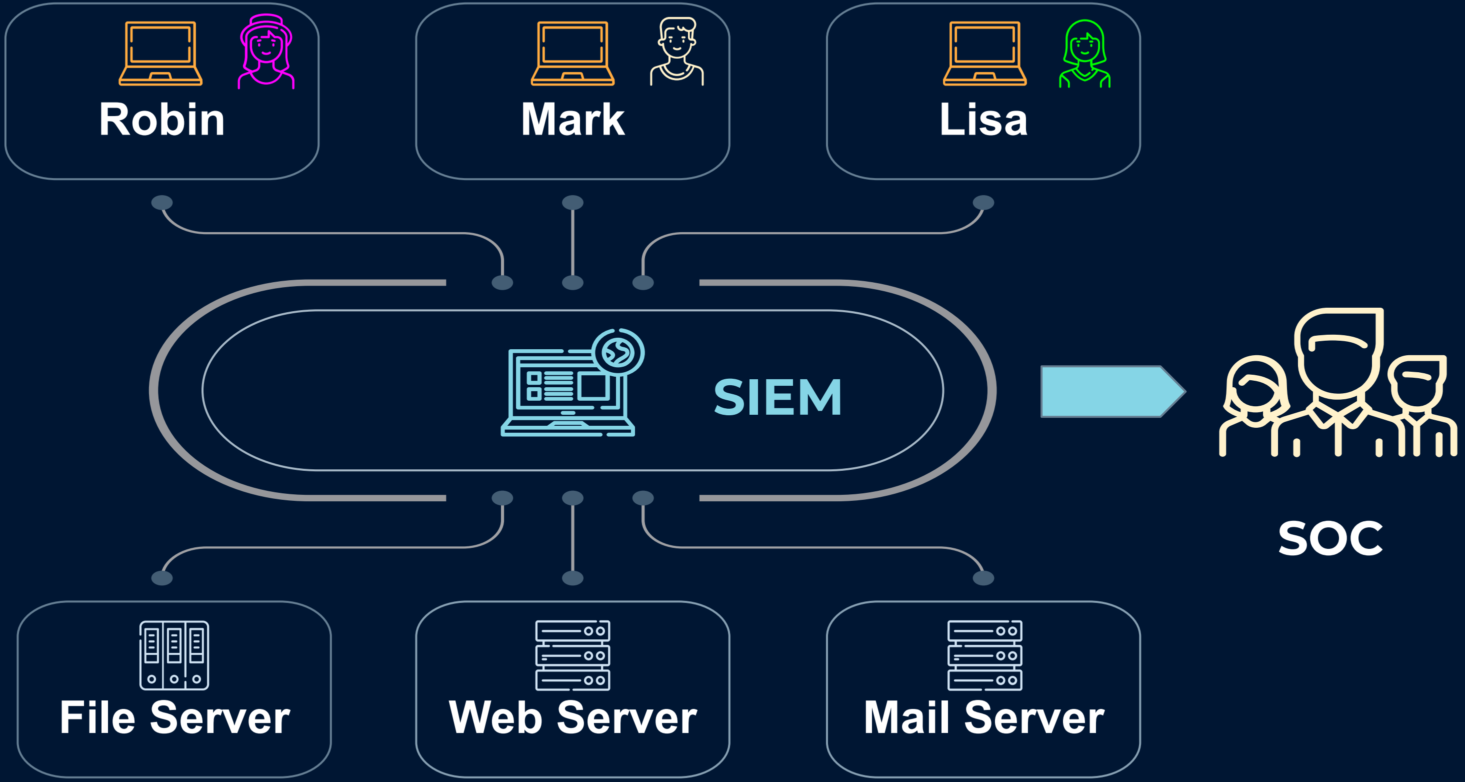


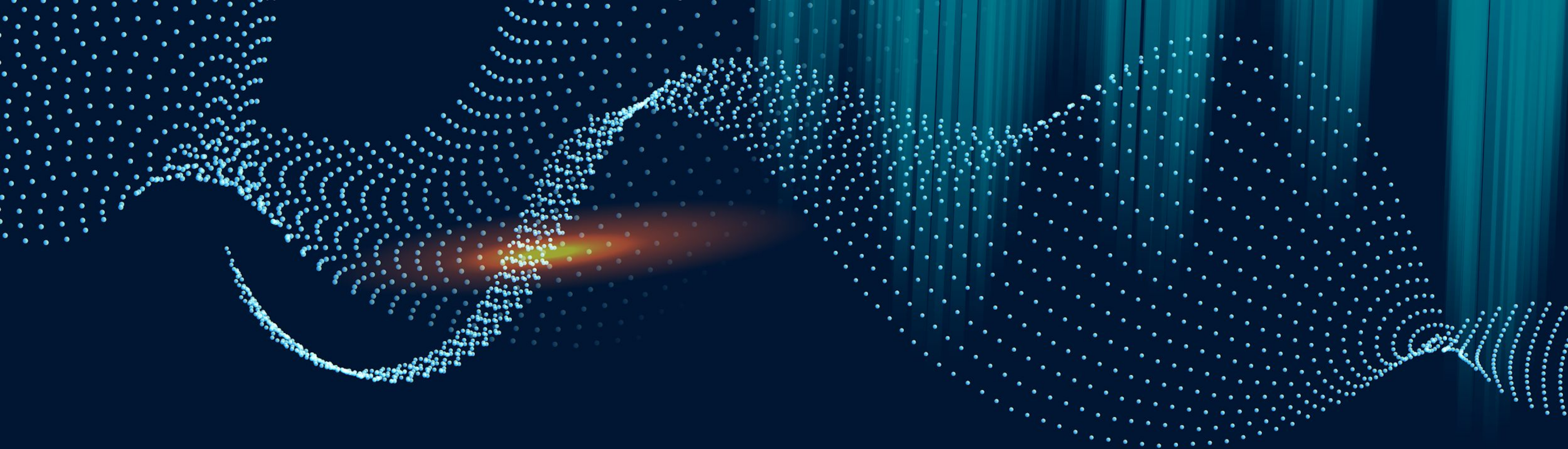
Security items - cont’d

- XSOAR (Extended Security Orchestration, Automation, and Response)
- UBA/RBA (User/Risk based analytics)
- Zero Trust security
- Insider Threat training
- Employee training (Social Engineering, Phishing, standard annual security training)
- SIEM (Security Information and Event Management)
    - Log analysis, alerting, reporting & auditing, threat hunting



SIEM (Security Information and Event Management)





03

Roles

One team, one fight

Roles: Red vs Blue (& Purple)

Blue Team

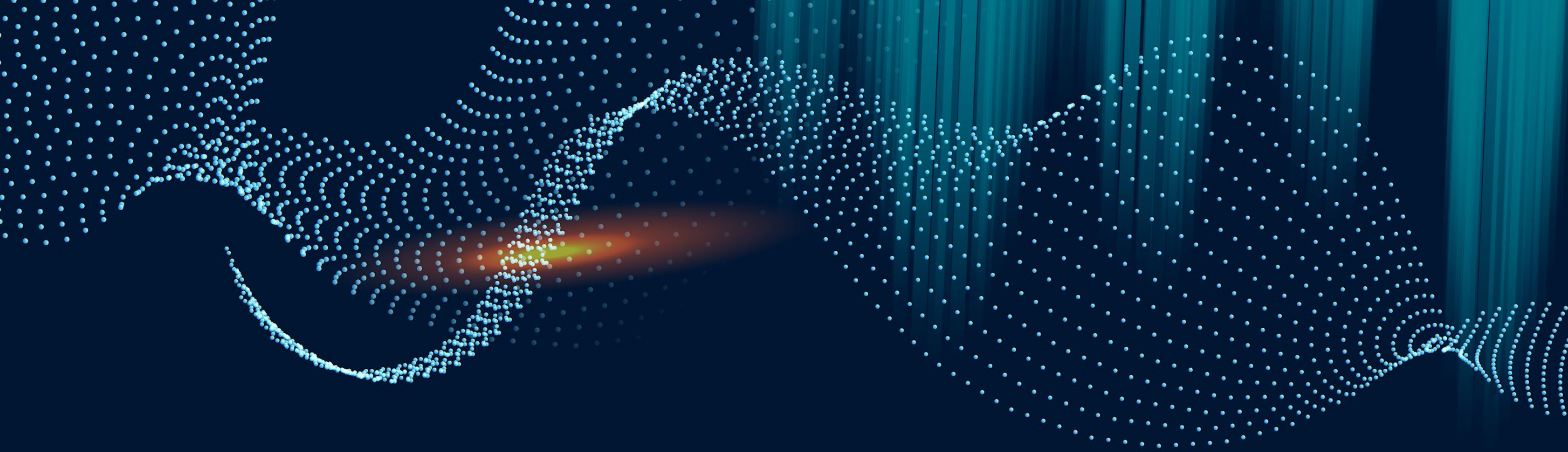
- SOC (Security Operations Center)
- Threat Hunting
- Incident Response
- Forensics
- Threat Intelligence
- Security Engineering
- Auditing

Red Team

- Pentesting
- Adversary Emulation
- Security Research
- Security Assessments
- Auditing

Roles: Incident Response

- Coordinates the response effort between stakeholders
- Gathers evidence
    - Often works directly with other Blue team members for threat hunts
- Incident remediation
- Documentation and AARs (after action reports)
- Conducts periodic TTX with other shareholders (tabletop exercises)

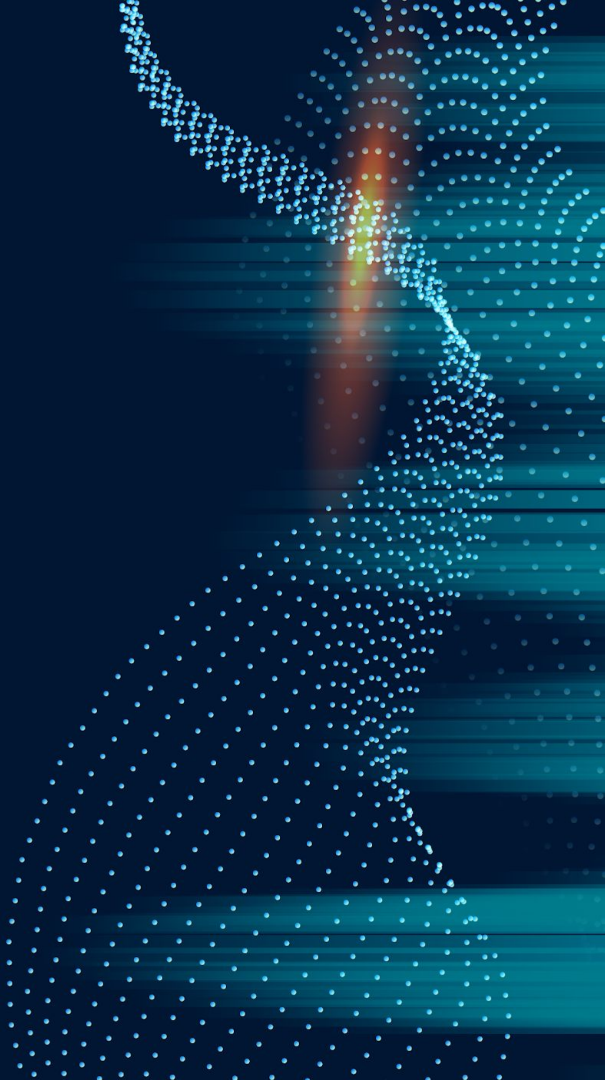


04 Frameworks

Guidelines and best practices

Frameworks & Best Practices

- MITRE ATT&CK
- MITRE ATLAS
- NIST 800.53 rev 5
- OWASP Top Ten
- NIST Risk Management Framework
- NIST NICE Framework
- NIST AI RMF (Risk Management Framework)
- NIST Cybersecurity Framework
- MITRE CWE



OWASP Top Ten

https://owasp.org/www-project-top-ten/

A01:2021-Broken Access Control

A02:2021-Cryptographic Failures

A03:2021-Injection

A04:2021-Insecure Design

A05:2021-Security Misconfiguration

A06:2021-Vulnerable and Outdated Components

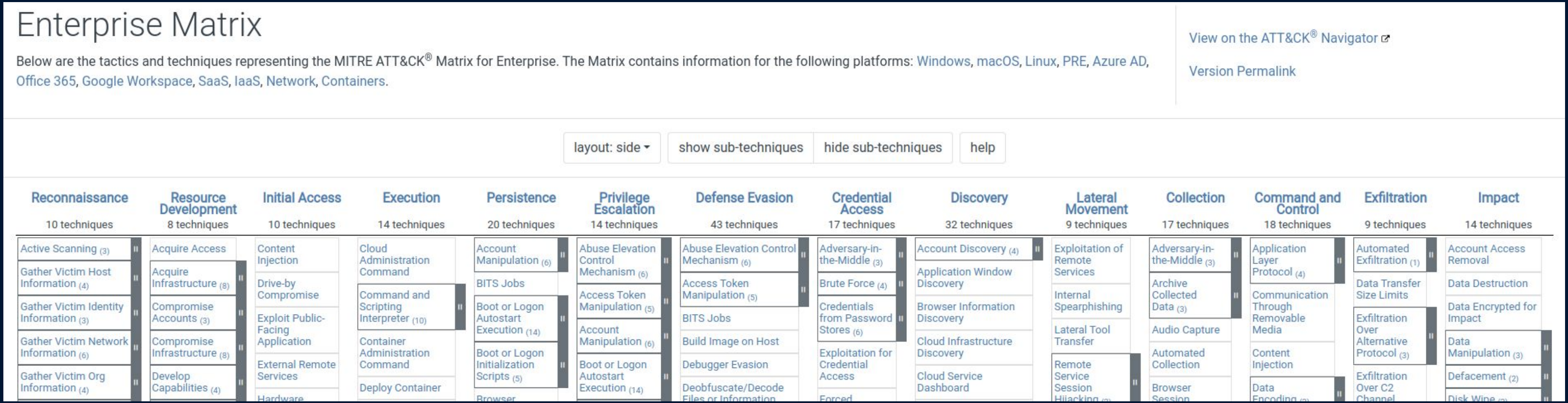
A07:2021-Identification and Authentication Failures

A08:2021-Software and Data Integrity Failures

A09:2021-Security Logging and Monitoring Failures

A10:2021-Server-Side Request Forgery

MITRE ATT&CK



Enterprise Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, PRE, Azure AD, Office 365, Google Workspace, SaaS, IaaS, Network, Containers.

View on the ATT&CK® Navigator

Version Permalink

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques	17 techniques	18 techniques	9 techniques	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		Browser		Debugger Evasion	Forced	Cloud Service Dashboard		Browser Session			Defacement (2)
						Deobfuscate/Decode Files or Information							Disk Wipe (2)

https://attack.mitre.org

Cyberattacks

- **Yahoo** - 2013/2014
  - **Notes:** Misconfigured database and unauthorized access
  - **Impact:** 3 billion user accounts exposed. PII & security questions & passwords
- **Equifax** - July 2017
  - **Notes:** Misconfigured database and unauthorized access
  - **Impact:** 143 million user’s PII exposed. 200,000 user’s credit cards exposed
- **SolarWinds** - September 2019
  - **Notes:** Supply chain attack
  - **Impact:** Massive financial loss in some industries. 18,000 customers received a compromised software update

Bob’s Coffee - Cyberattack

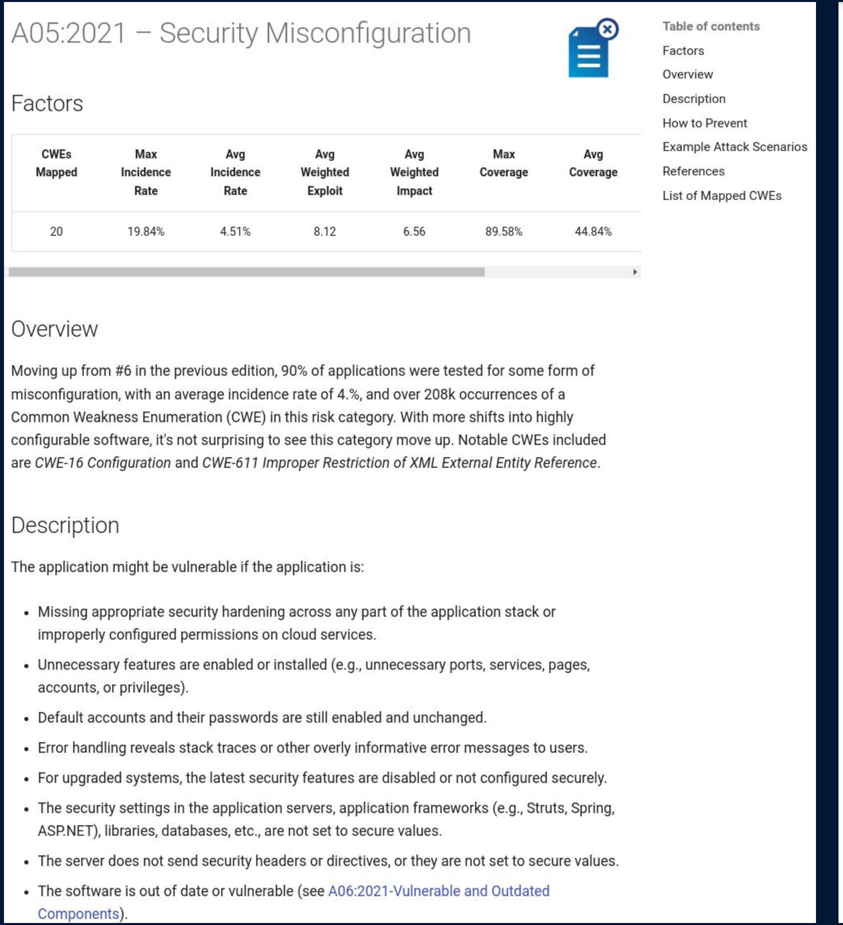
Incident: **A breach occurred by a group of hackers against coffee. (***Thousands of people were forced to drink tea.***)**

Root Cause: **Misconfigured network devices and unauthorized access.**

OWASP: **A05:2021 - Security Misconfiguration**

MITRE ATT&CK: **Initial Access: “Exploit Public-Facing Application” (T1190)**

Bob’s Coffee - OWASP



A05:2021 – Security Misconfiguration

Factors

CWEs Mapped	Max Incidence Rate	Avg Incidence Rate	Avg Weighted Exploit	Avg Weighted Impact	Max Coverage	Avg Coverage
20	19.84%	4.51%	8.12	6.56	89.58%	44.84%

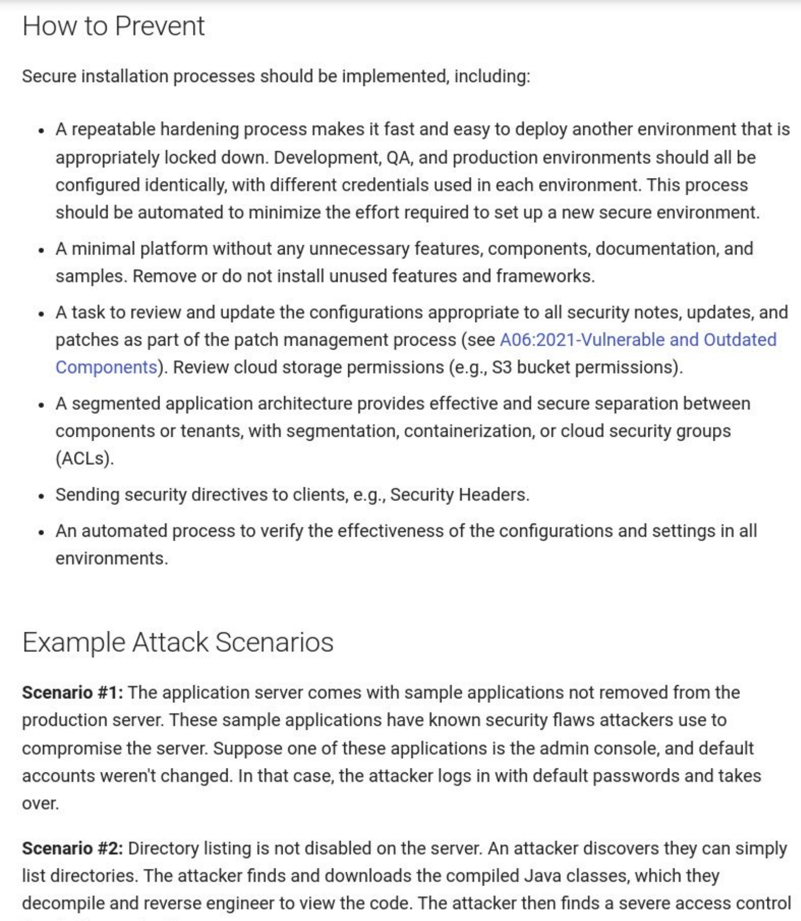
Overview

Moving up from #6 in the previous edition, 90% of applications were tested for some form of misconfiguration, with an average incidence rate of 4.%, and over 208k occurrences of a Common Weakness Enumeration (CWE) in this risk category. With more shifts into highly configurable software, it's not surprising to see this category move up. Notable CWEs included are *CWE-16 Configuration* and *CWE-611 Improper Restriction of XML External Entity Reference*.

Description

The application might be vulnerable if the application is:

- Missing appropriate security hardening across any part of the application stack or improperly configured permissions on cloud services.
- Unnecessary features are enabled or installed (e.g., unnecessary ports, services, pages, accounts, or privileges).
- Default accounts and their passwords are still enabled and unchanged.
- Error handling reveals stack traces or other overly informative error messages to users.
- For upgraded systems, the latest security features are disabled or not configured securely.
- The security settings in the application servers, application frameworks (e.g., Struts, Spring, ASP.NET), libraries, databases, etc., are not set to secure values.
- The server does not send security headers or directives, or they are not set to secure values.
- The software is out of date or vulnerable (see A06:2021-Vulnerable and Outdated Components).



How to Prevent

Secure installation processes should be implemented, including:

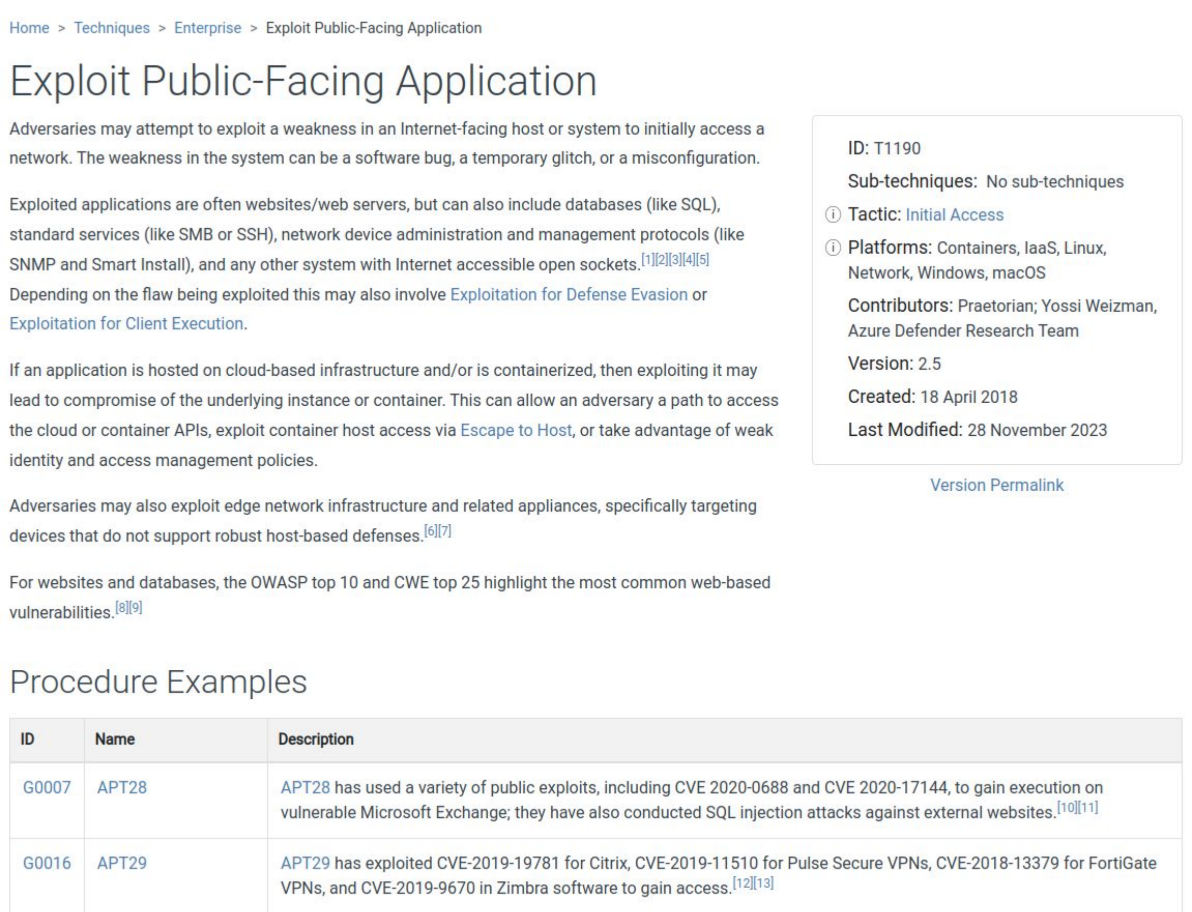
- A repeatable hardening process makes it fast and easy to deploy another environment that is appropriately locked down. Development, QA, and production environments should all be configured identically, with different credentials used in each environment. This process should be automated to minimize the effort required to set up a new secure environment.
- A minimal platform without any unnecessary features, components, documentation, and samples. Remove or do not install unused features and frameworks.
- A task to review and update the configurations appropriate to all security notes, updates, and patches as part of the patch management process (see A06:2021-Vulnerable and Outdated Components). Review cloud storage permissions (e.g., S3 bucket permissions).
- A segmented application architecture provides effective and secure separation between components or tenants, with segmentation, containerization, or cloud security groups (ACLs).
- Sending security directives to clients, e.g., Security Headers.
- An automated process to verify the effectiveness of the configurations and settings in all environments.

Example Attack Scenarios

Scenario #1: The application server comes with sample applications not removed from the production server. These sample applications have known security flaws attackers use to compromise the server. Suppose one of these applications is the admin console, and default accounts weren't changed. In that case, the attacker logs in with default passwords and takes over.

Scenario #2: Directory listing is not disabled on the server. An attacker discovers they can simply list directories. The attacker finds and downloads the compiled Java classes, which they decompile and reverse engineer to view the code. The attacker then finds a severe access control

Bob’s Coffee - MITRE ATT&CK



Home > Techniques > Enterprise > Exploit Public-Facing Application

Exploit Public-Facing Application

Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration.

Exploited applications are often websites/web servers, but can also include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other system with Internet accessible open sockets.[1][2][3][4][5] Depending on the flaw being exploited this may also involve Exploitation for Defense Evasion or Exploitation for Client Execution.

If an application is hosted on cloud-based infrastructure and/or is containerized, then exploiting it may lead to compromise of the underlying instance or container. This can allow an adversary a path to access the cloud or container APIs, exploit container host access via Escape to Host, or take advantage of weak identity and access management policies.

Adversaries may also exploit edge network infrastructure and related appliances, specifically targeting devices that do not support robust host-based defenses.[6][7]

For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities.[8][9]

ID: T1190

Sub-techniques: No sub-techniques

ⓘ Tactic: Initial Access

ⓘ Platforms: Containers, IaaS, Linux, Network, Windows, macOS

Contributors: Praetorian; Yossi Weizman, Azure Defender Research Team

Version: 2.5

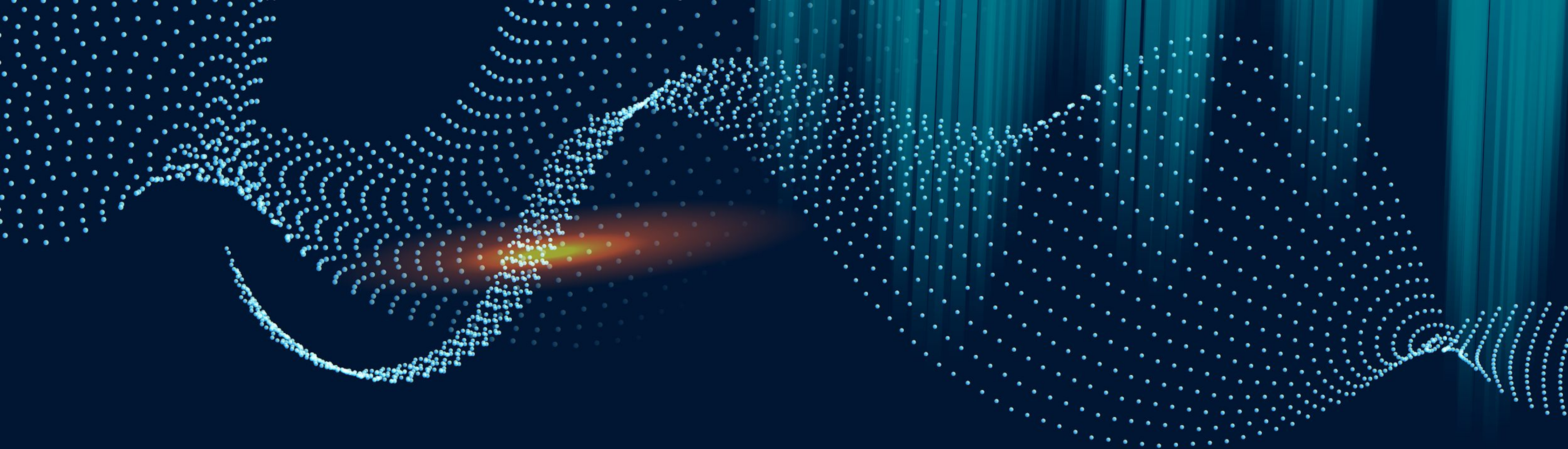
Created: 18 April 2018

Last Modified: 28 November 2023

Version Permalink

Procedure Examples

ID	Name	Description
G0007	APT28	APT28 has used a variety of public exploits, including CVE 2020-0688 and CVE 2020-17144, to gain execution on vulnerable Microsoft Exchange; they have also conducted SQL injection attacks against external websites.[10][11]
G0016	APT29	APT29 has exploited CVE-2019-19781 for Citrix, CVE-2019-11510 for Pulse Secure VPNs, CVE-2018-13379 for FortiGate VPNs, and CVE-2019-9670 in Zimbra software to gain access.[12][13]



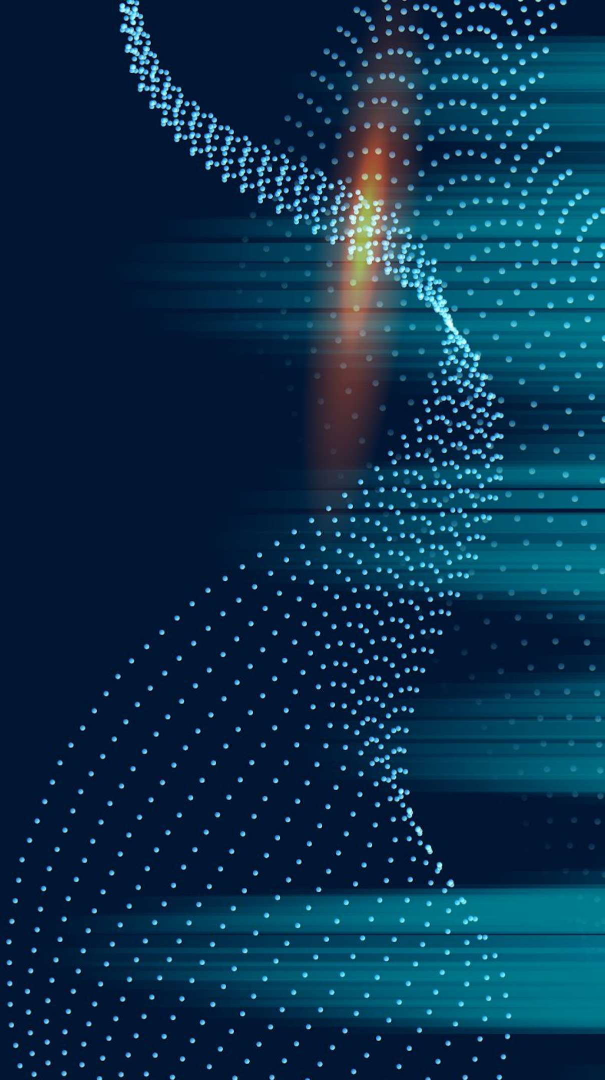
05

Compliance

I know....Just hear me out.

Compliance

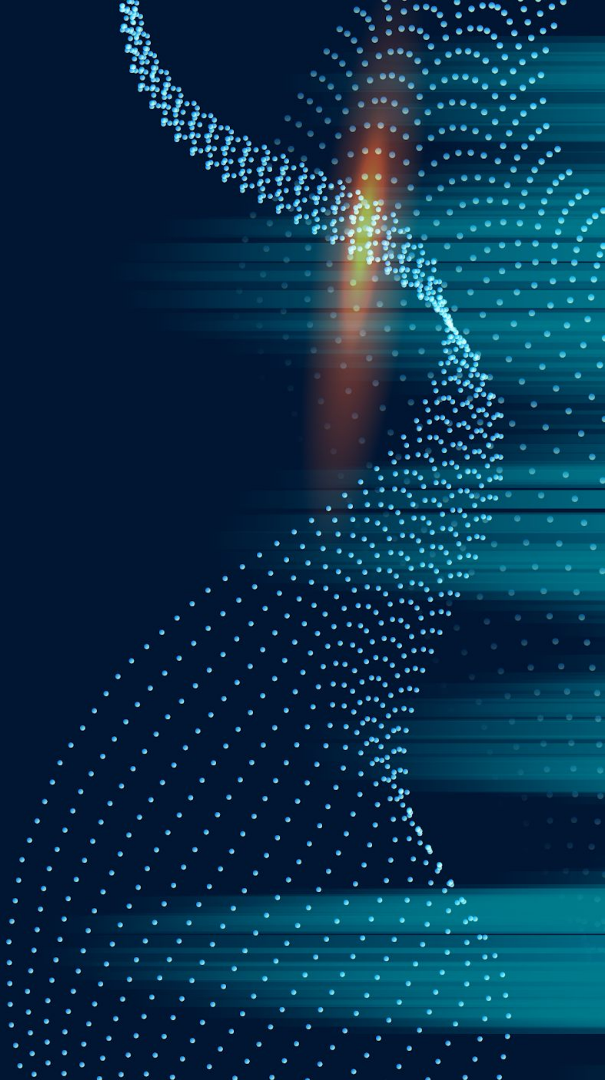
- NIST SP 800.53
- HIPAA (Health Insurance Portability and Accountability Act)
- PCI-DSS (Payment Card Industry Data Security Standard)
- FedRAMP (Federal Risk and Authorization Management Program)
- GDPR (General Data Protection Regulation)
  - European Union
- DISA STIG - Typically associated with the Department of Defense

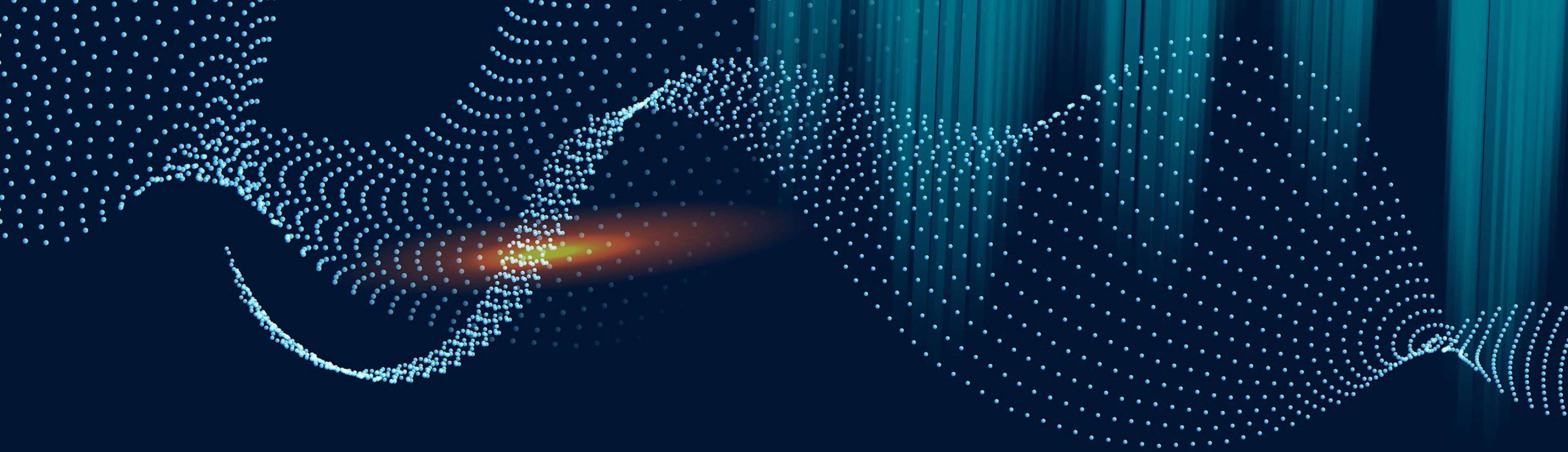


Compliance - NIST 800.53 rev 4

A total of 20 control families. Some of the notable families include:

- AC: Access Control
- AU: Audit and Accountability
- IA: Identification and Authentication
- IR: Incident Response
- SC: System and Communications Protection
- SI: System and Information Integrity





06

AI/Machine Learning

The robot elephant in the room

Artificial Intelligence/Machine Learning

Note: Output from LLMs (Large Language Models) should always be verified for authenticity

Educational/professional uses

- Research
- Summarization
- Code examples and reference information (grain of salt)

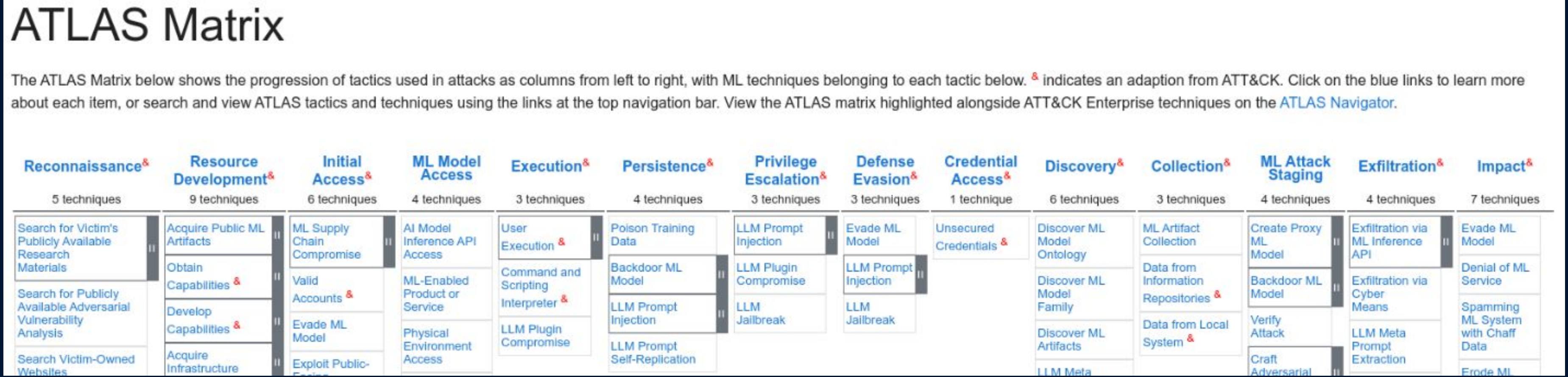
Red team

- Malware generation
- Phishing campaigns
- Deepfakes, fraud, hoaxes

Blue team

- Signals intelligence
- Detections engineering for anomalies in large datasets
- Documentation

MITRE ATLAS



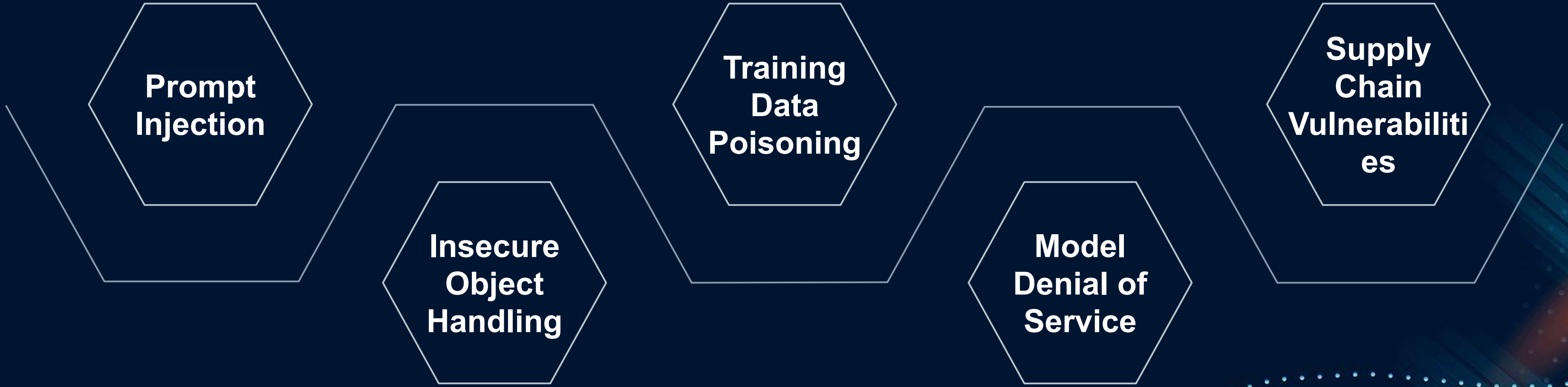
ATLAS Matrix

The ATLAS Matrix below shows the progression of tactics used in attacks as columns from left to right, with ML techniques belonging to each tactic below. & indicates an adaption from ATT&CK. Click on the blue links to learn more about each item, or search and view ATLAS tactics and techniques using the links at the top navigation bar. View the ATLAS matrix highlighted alongside ATT&CK Enterprise techniques on the ATLAS Navigator.

Reconnaissance&	Resource Development&	Initial Access&	ML Model Access	Execution&	Persistence&	Privilege Escalation&	Defense Evasion&	Credential Access&	Discovery&	Collection&	ML Attack Staging	Exfiltration&	Impact&
5 techniques	9 techniques	6 techniques	4 techniques	3 techniques	4 techniques	3 techniques	3 techniques	1 technique	6 techniques	3 techniques	4 techniques	4 techniques	7 techniques
Search for Victim's Publicly Available Research Materials	Acquire Public ML Artifacts	ML Supply Chain Compromise	AI Model Inference API Access	User Execution &	Poison Training Data	LLM Prompt Injection	Evade ML Model	Unsecured Credentials &	Discover ML Model Ontology	ML Artifact Collection	Create Proxy ML Model	Exfiltration via ML Inference API	Evade ML Model
Search for Publicly Available Adversarial Vulnerability Analysis	Obtain Capabilities &	Valid Accounts &	ML-Enabled Product or Service	Command and Scripting Interpreter &	Backdoor ML Model	LLM Plugin Compromise	LLM Prompt Injection		Discover ML Model Family	Data from Information Repositories &	Backdoor ML Model	Exfiltration via Cyber Means	Denial of ML Service
Search Victim-Owned Websites	Develop Capabilities &	Evade ML Model	Physical Environment Access	LLM Plugin Compromise	LLM Prompt Injection	LLM Jailbreak	LLM Jailbreak		Discover ML Artifacts	Data from Local System &	Verify Attack	LLM Meta Prompt Extraction	Spamming ML System with Chaff Data
	Acquire Infrastructure	Exploit Public-			LLM Prompt Self-Replication				LLM Meta		Craft Adversarial		Erode ML

https://atlas.mitre.org

OWASP Top Ten for LLM Applications (1-5)



Prompt Injection

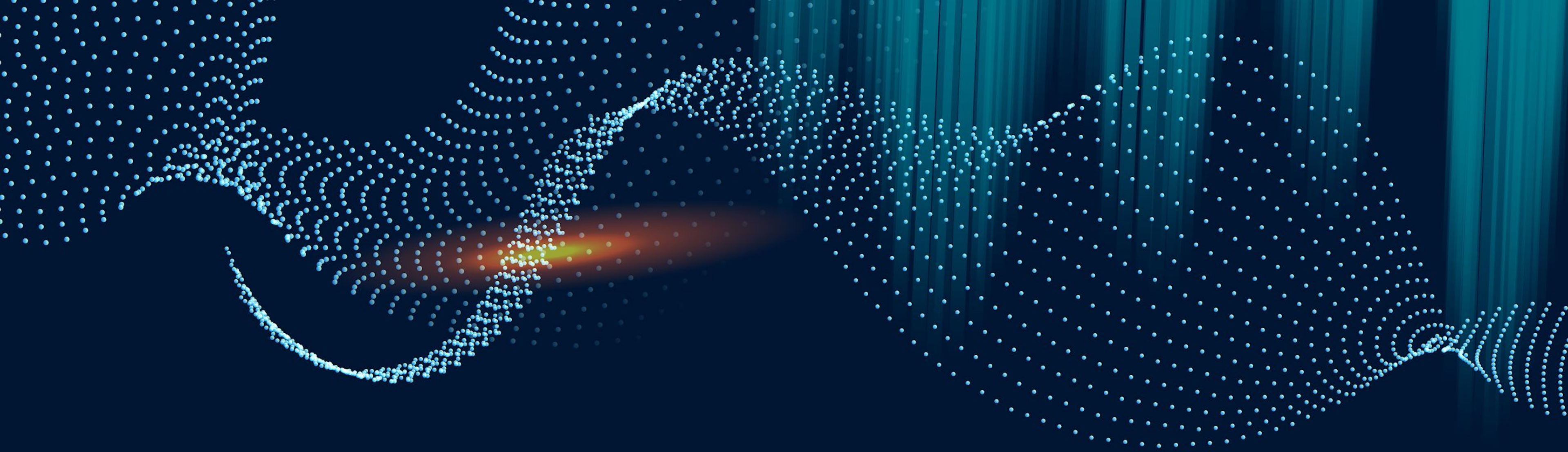
Insecure Object Handling

Training Data Poisoning

Model Denial of Service

Supply Chain Vulnerabiliti es

https://genai.owasp.org/resource/llm-top-10-for-llms-v1-1/



07

Continuous Learning

“Continuous improvement is better than delayed perfection”

It never stops...

“Upgrade your grey matter, cause one day it may matter.”

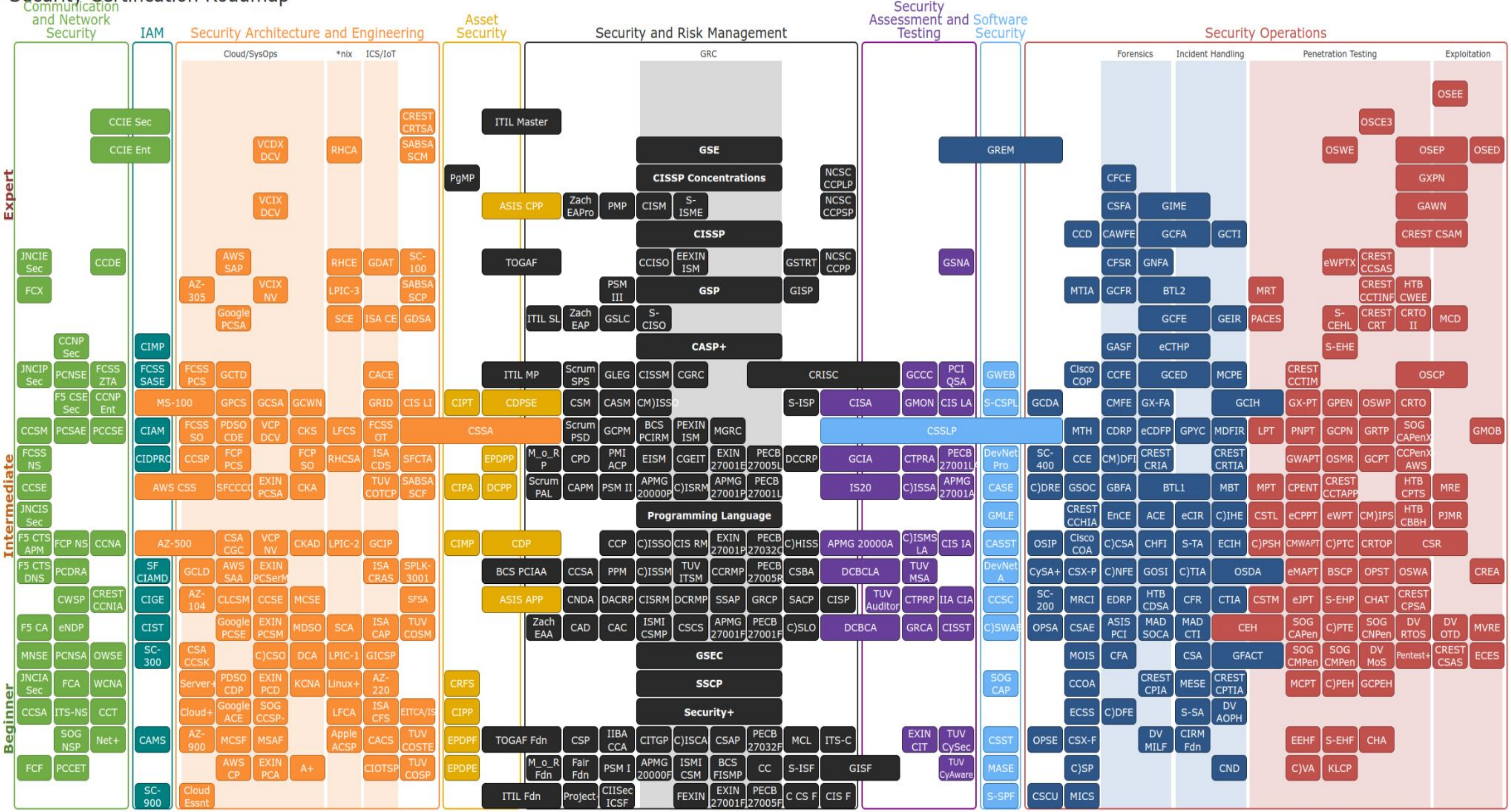
Deltron 3030

Homelabs and other resources

- **Repurpose old hardware**
  - Put that old laptop to use!
- **Install VirtualBox, VMWare, or KVM**
  - Doesn’t require any additional costs
  - Can be used to learn about virtualization, networking, and the cloud
- **Raspberry Pis**
  - Low powered, inexpensive, & can run Linux
- **Use cloud-based resources**
  - A bridge to understanding enterprise (large scale) environments
  - Can be very affordable if managed properly

I WAS TOLD THERE WOULD
BE CERTIFICATES

Security Certification Roadmap



Expert
Intermediate
Beginner

Communication and Network Security

CCIE Sec
CCIE Ent
JNCIE Sec, CCDE
FCX
CCNP Sec
JNCIP Sec, PCNSE, FCSS ZTA
F5 CSE Sec, CCNP Ent
CCSM, PCSAE, PCCSE
FCSS NS
CCSE
JNCIS Sec
F5 CTS APM, FCP NS, CCNA
F5 CTS DNS, PCDRA
CWSP, CREST CCNIA
F5 CA, eNDP
MNSE, PCNSA, OWSE
JNCIA Sec, FCA, WCNA
CCSA, ITS-NS, CCT
SOG NSP, Net+
FCF, PCCET

IAM

CIMP
FCSS SASE
CIAM
CIDPRO
SF CIAMD
CIGE
CIST
SC-300
CAMS
SC-900

Security Architecture and Engineering

Cloud/SysOps
*nix
ICS/IoT

CREST CRTSA
VCDX DCV, RHCA, SABSA SCM
VCIX DCV
AWS SAP, RHCE, GDAT, SC-100
AZ-305, VCIX NV, LPIC-3, SABSA SCP
Google PCSA, SCE, ISA CE, GDSA
FCSS PCS, GCTD, CACE
MS-100, GPCS, GCSA, GCWN, GRID, CIS LI
FCSS SO, PDSO CDE, VCP DCV, CKS, LFCS, FCSS OT, CSSA
CCSP, FCP PCS, FCP SO, RHCSA, ISA CDS, SFCTA
AWS CSS, SFCCCC, EXIN PCSA, CKA, TUV COTCP, SABSA SCF
AZ-500, CSA CGC, VCP NV, CKAD, LPIC-2, GCIP
GCLD, AWS SAA, EXIN PCSerM, ISA CRAS, SPLK-3001
AZ-104, CLCSM, CCSE, MCSE, SFSA
Google PCSE, EXIN PCSM, MDSO, SCA, ISA CAP, TUV COSM
CSA CCSK, C)CSO, DCA, LPIC-1, GICSP
Server+, PDSO CDP, EXIN PCD, KCNA, Linux+, AZ-220
Cloud+, Google ACE, SOG CCSP-, LFCA, ISA CFS, EITCA/IS
AZ-900, MCSF, MSAF, Apple ACSP, CACS, TUV COSTE
AWS CP, EXIN PCA, A+, CIOTSP, TUV COSP
Cloud Essnt

Asset Security

PgMP
ASIS CPP
CIPT, CDPSE
EPDPP
CIPA, DCPP
CIMP, CDP
ASIS APP
CRFS
CIPP
EPDPF
EPDPE

Security and Risk Management

GRC

ITIL Master
GSE
CISSP Concentrations, NCSC CCPLP
Zach EAPro, PMP, CISM, S-ISME, NCSC CCPSP
CISSP
TOGAF, CCISO, EEXIN ISM, GSTRT, NCSC CCPP
PSM III, GSP, GISP
ITIL SL, Zach EAP, GSLC, S-CISO
CASP+
ITIL MP, Scrum SPS, GLEG, CISSM, CGRC, CRISC
CSM, CASM, CM)ISSO, S-ISP
Scrum PSD, GCPM, BCS PCIRM, PEXIN ISM, MGRC
M_o_R P, CPD, PMI ACP, EISM, CGEIT, EXIN 27001E, PECB 27005L, DCCRP
Scrum PAL, CAPM, PSM II, APMG 20000P, C)ISRM, APMG 27001P, PECB 27001L
Programming Language
CCP, C)ISSO, CIS RM, EXIN 27001P, PECB 27032C, C)HISS
BCS PCIAA, CCSA, PPM, C)ISSM, TUV ITSM, CCRMP, PECB 27005R, CSBA
CNDA, DACRP, CISRM, DCRMP, SSAP, GRCP, SACP, CISP
Zach EAA, CAD, CAC, ISMI CSMP, CSCS, APMG 27001F, PECB 27001F, C)SLO
GSEC
SSCP
Security+
TOGAF Fdn, CSP, IIBA CCA, CITGP, C)ISCA, CSAP, PECB 27032F, MCL, ITS-C
M_o_R Fdn, Fair Fdn, PSM I, APMG 20000F, ISMI CSM, BCS FISMP, CC, S-ISF, GISF
ITIL Fdn, Project+, CIISec ICSF, FEXIN, EXIN 27001F, PECB 27005F, C CS F, CIS F

Security Assessment and Testing

GSNA
GCCC, PCI QSA
CISA, GMON, CIS LA
CSSLP
GCIA, CTPRA, PECB 27001LA
IS20, C)ISSA, APMG 27001A
APMG 20000A, C)ISMS LA, CIS IA
DCBCLA, TUV MSA
TUV Auditor, CTPRP, IIA CIA
DCBCA, GRCA, CISST
EXIN CIT, TUV CySec
TUV CyAware

Software Security

GREM
GWEB
S-CSPL
DevNet Pro
CASE
GMLE
CASST
DevNet A
CCSC
C)SWAE
SOG CAP
CSST
MASE
S-SPF

Security Operations

Forensics
Incident Handling
Penetration Testing
Exploitation

OSEE
OSCE3
OSWE, OSEP, OSED
CFCE, GXPN
CSFA, GIME, GAWN
CCD, CAWFE, GCFA, GCTI, CREST CSAM
CFSR, GNFA, eWPTX, CREST CCSAS
MTIA, GCFR, BTL2, MRT, CREST CCTINF, HTB CWEE
GCFE, GEIR, PACES, S-CEHL, CREST CRT, CRTO II, MCD
GASF, eCTHP, S-EHE
Cisco COP, CCFE, GCED, MCPE, CREST CCTIM, OSCP
GCDA, CMFE, GX-FA, GCIH, GX-PT, GPEN, OSWP, CRTO
MTH, CDRP, eCDFP, GPYC, MDFIR, LPT, PNPT, GCPN, GRTP, SOG CAPenX, GMOB
SC-400, CCE, CM)DFI, CREST CRIA, CREST CRTIA, GWAPT, OSMR, GCPT, CCPenX AWS
C)DRE, GSOC, GBFA, BTL1, MBT, MPT, CPENT, CREST CCTAPP, HTB CPTS, MRE
CREST CCHIA, EnCE, ACE, eCIR, C)IHE, CSTL, eCPPT, eWPT, CM)IPS, HTB CBBH, PJMR
OSIP, Cisco COA, C)CSA, CHFI, S-TA, ECIH, C)PSH, CMWAPT, C)PTC, CRTOP, CSR
CySA+, CSX-P, C)NFE, GOSI, C)TIA, OSDA, eMAPT, BSCP, OPST, OSWA, CREA
SC-200, MRCI, EDRP, HTB CDSA, CFR, CTIA, CSTM, eJPT, S-EHP, CHAT, CREST CPSA
OPSA, CSAE, ASIS PCI, MAD SOCA, MAD CTI, CEH, SOG CAPen, C)PTE, SOG CNPen, DV RTOS, DV OTD, MVRE
MOIS, CFA, CSA, GFACT, SOG CMPen, SOG CMPen, DV MoS, Pentest+, CREST CSAS, ECES
CCOA, CREST CPIA, MESE, CREST CPTIA, MCPT, C)PEH, GCPEH
ECSS, C)DFE, S-SA, DV AOPH
OPSE, CSX-F, DV MILF, CIRM Fdn, EEHF, S-EHF, CHA
C)SP, CND, C)VA, KLCP
CSCU, MICS

481 certifications listed | July 2024

THANKS!

Do you have any questions?

- alonzotech3030@gmail.com
- linkedin.com/in/alonzo-perry-782b915

(additional reference information and a copy of this presentation can be found on Github)

https://github.com/alonzoperry/CAM2024

CREDITS: This presentation template was created by Slidesgo, including icons by Flaticon, and infographics & images by Freepik.

Lab ideas

- Set up a virtual machine server (see homelabs slide)
- Set up a basic file server (as a bare metal host or VM)
- Set up a SIEM (Wazuh, Splunk) and analyze data from other machines on your network
    - Learn how to create detections and alerts
- Set up “Security Onion” (Linux based infosec distro with several great tools out of the box including a SIEM)
- Create a backup server

Red Team

- Install Kali Linux and learn about Red Team capabilities.
- Research password cracking with hashcat and “Jack the Ripper”
- Install “nmap” (network mapper/scanner)
- Set up a Malware analysis lab