PAUL SHERER

SightGain
Engineering Director

Mandiant/Google
CyberSecurity Instructor

OBJECTIVE

INTRODUCE THE FIELD OF CYBERSECURITY

QUESTION

Who is interested in cybersecurity?

What is cybersecurity?

What is cybersecurity?

Not This.

TYPES OF CYBER THREATS

TYPES OF CYBER THREATS

Malware

TYPES OF CYBER THREATS

Malware
Phishing

TYPES OF CYBER THREATS

Malware
Phishing
Social Engineering

TYPES OF CYBER THREATS

Malware
Phishing
Social Engineering
OWASP Top 10

MALWARE

MALWARE

- **Ransomware:** Disables victim's access to data until ransom is paid

MALWARE

- **Ransomware:** Disables victim's access to data until ransom is paid
- **Spyware:** collects user activity data without their knowledge

MALWARE

- **Ransomware:** Disables victim's access to data until ransom is paid
- **Spyware:** collects user activity data without their knowledge
- **Adware:** Serves unwanted advertisements

MALWARE

- **Ransomware:** Disables victim's access to data until ransom is paid
- **Spyware:** collects user activity data without their knowledge
- **Adware:** Serves unwanted advertisements
- **Trojan:** Disguises itself as desirable code

MALWARE

- **Ransomware:** Disables victim's access to data until ransom is paid
- **Spyware:** collects user activity data without their knowledge
- **Adware:** Serves unwanted advertisements
- **Trojan:** Disguises itself as desirable code
- **Rootkit:** Grants hackers remote control of victim's device

MALWARE

- **Ransomware:** Disables victim's access to data until ransom is paid
- **Spyware:** collects user activity data without their knowledge
- **Adware:** Serves unwanted advertisements
- **Trojan:** Disguises itself as desirable code
- **Rootkit:** Grants hackers remote control of victim's device
- **Keylogger:** Monitors user's keystrokes

PHISHING

PHISHING

- **Emails:** Emails are designed to appear to come from a legitimate source

PHISHING

- **Emails:** Emails are designed to appear to come from a legitimate source
- **Spear Phishing:** Targeted phishing email attack relies on data that a cyber criminal has previously collected about the victim or the victim's employer

PHISHING

- **Emails:** Emails are designed to appear to come from a legitimate source
- **Spear Phishing:** Targeted phishing email attack relies on data that a cyber criminal has previously collected about the victim or the victim's employer
- **Fake/Look-alike Websites:** Malicious website leverages subtle changes to a known URL to trick users

PHISHING

- **Emails:** Emails are designed to appear to come from a legitimate source
- **Spear Phishing:** Targeted phishing email attack relies on data that a cyber criminal has previously collected about the victim or the victim's employer
- **Fake/Look-alike Websites:** Malicious website leverages subtle changes to a known URL to trick users
- **"Evil Twin" Wi-Fi (MITM):** Spoofing free/open Wi-Fi access points. Victims unknowingly log into the wrong hotspot

SOCIAL ENGINEERING

SOCIAL ENGINEERING

- **Pretexting:** Process of lying to gain access to personal data or other privileged information

SOCIAL ENGINEERING

- **Pretexting:** Process of lying to gain access to personal data or other privileged information
- **Tailgating:** Attacker follows a person into a secure area. This type of attack relies on the person being followed assuming the intruder is authorized to access the targeted area.

SOCIAL ENGINEERING

- **Pretexting:** Process of lying to gain access to personal data or other privileged information
- **Tailgating:** Attacker follows a person into a secure area. This type of attack relies on the person being followed assuming the intruder is authorized to access the targeted area.
- **Quid Pro Quo:** Exploits the human tendency to reciprocate good gestures.

SOCIAL ENGINEERING

- **Pretexting:** Process of lying to gain access to personal data or other privileged information
- **Tailgating:** Attacker follows a person into a secure area. This type of attack relies on the person being followed assuming the intruder is authorized to access the targeted area.
- **Quid Pro Quo:** Exploits the human tendency to reciprocate good gestures.
- **Baiting:** Attacker leaves a physical device (like a USB) infected with a type of malware where it's most likely to be found. When a victim inserts the USB into their computer, a malware installation process is initiated.

OWASP TOP 10

OWASP TOP 10

- **Broken Access Control:** Access control enforces policy such that users cannot act outside of their intended permissions

OWASP TOP 10

- **Broken Access Control:** Access control enforces policy such that users cannot act outside of their intended permissions
- **Cryptographic Failures:** Data permisisons in transit and at rest. GDPR, PCI. Is any data transmitted in clear text? Old or weak cryptographic algorithms

OWASP TOP 10

- **Broken Access Control:** Access control enforces policy such that users cannot act outside of their intended permissions
- **Cryptographic Failures:** Data permisisons in transit and at rest. GDPR, PCI. Is any data transmitted in clear text? Old or weak cryptographic algorithms
- **Injection:** User-supplied data is not validated, filtered or sanitized by the application. SQL Injection

OWASP TOP 10

- **Broken Access Control:** Access control enforces policy such that users cannot act outside of their intended permissions
- **Cryptographic Failures:** Data permisisons in transit and at rest. GDPR, PCI. Is any data transmitted in clear text? Old or weak cryptographic algorithms
- **Injection:** User-supplied data is not validated, filtered or sanitized by the application. SQL Injection
- **Insecure Design:** Risks related to design and architectural flaws. Incorrect threat modeling or missing security controls

OWASP TOP 10

- **Broken Access Control:** Access control enforces policy such that users cannot act outside of their intended permissions
- **Cryptographic Failures:** Data permisisons in transit and at rest. GDPR, PCI. Is any data transmitted in clear text? Old or weak cryptographic algorithms
- **Injection:** User-supplied data is not validated, filtered or sanitized by the application. SQL Injection
- **Insecure Design:** Risks related to design and architectural flaws. Incorrect threat modeling or missing security controls
- **Security Misconfiguration:** Application missing security harding. Unneccesssary features are enabled or installed (ports, services, accounts, privileges). Default accounts and passwords still enabled and unchanged. Error handling reveals stack traces or other overly informative error messages to users

OWASP TOP 10

OWASP TOP 10

- **Vulnerable and Outdated Components:** Unknown versions of components. Unsupported or out of date software. Not upgrading applications or dependecies in a timely fashion.

OWASP TOP 10

- **Vulnerable and Outdated Components:** Unknown versions of components. Unsupported or out of date software. Not upgrading applications or dependecies in a timely fashion.
- **Identification and Authentication Failures:** Application permits brute force, weak or well-known passwords, weakly hashed passwords, missing multi-factor authentication

OWASP TOP 10

- **Vulnerable and Outdated Components:** Unknown versions of components. Unsupported or out of date software. Not upgrading applications or dependecies in a timely fashion.
- **Identification and Authentication Failures:** Application permits brute force, weak or well-known passwords, weakly hashed passwords, missing multi-factor authentication
- **Software and Data Integrity Failures:** Application relies on plugins, libraries, or modules from untrusted sources. Supply chain attacks

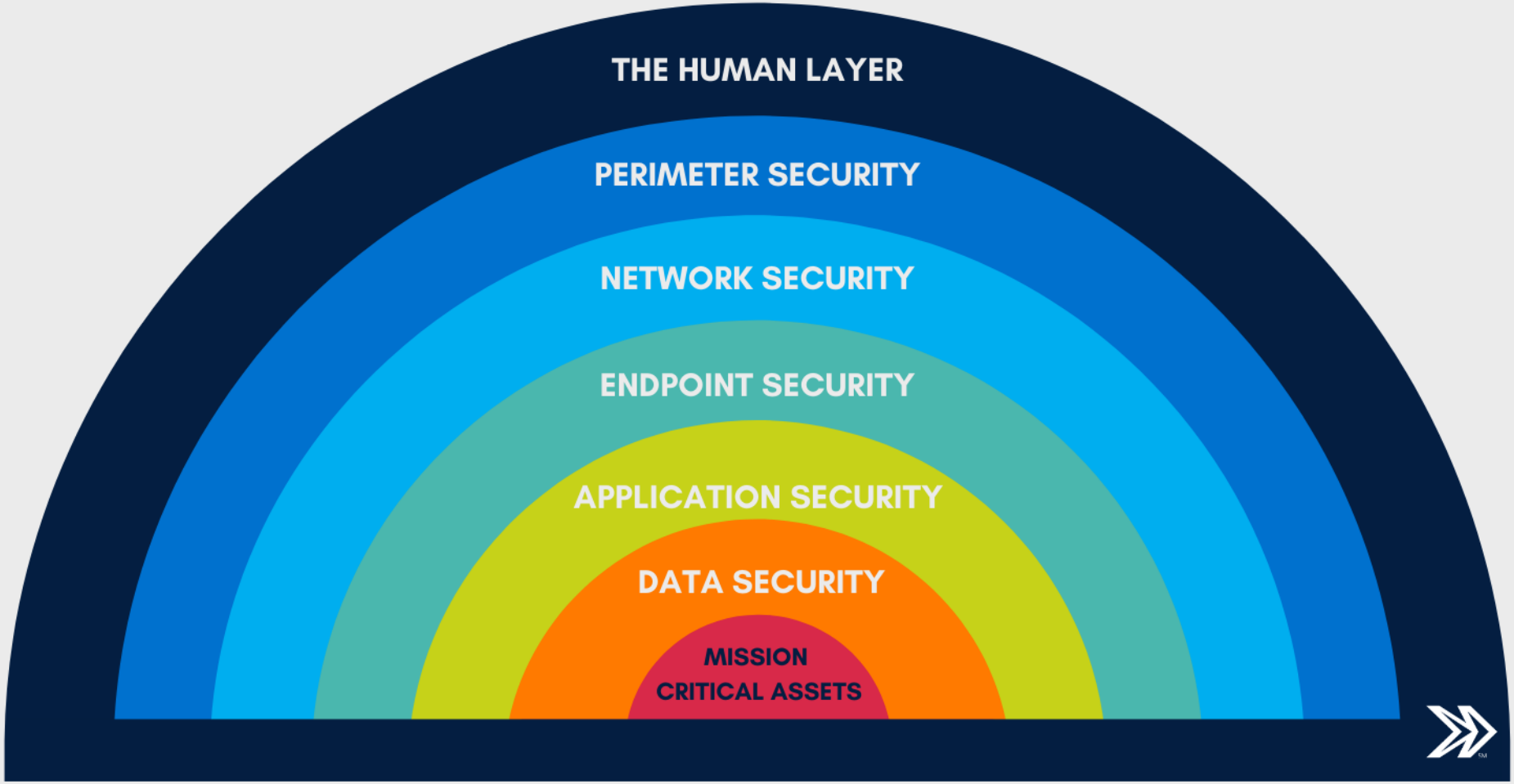
OWASP TOP 10

- **Vulnerable and Outdated Components:** Unknown versions of components. Unsupported or out of date software. Not upgrading applications or dependecies in a timely fashion.
- **Identification and Authentication Failures:** Application permits brute force, weak or well-known passwords, weakly hashed passwords, missing multi-factor authentication
- **Software and Data Integrity Failures:** Application relies on plugins, libraries, or modules from untrusted sources. Supply chain attacks
- **Security Logging and Monitoring Failures:** Without logging breaches cannot be detected. Auditable events should be logged and actively monitored for suspicous activity

OWASP TOP 10

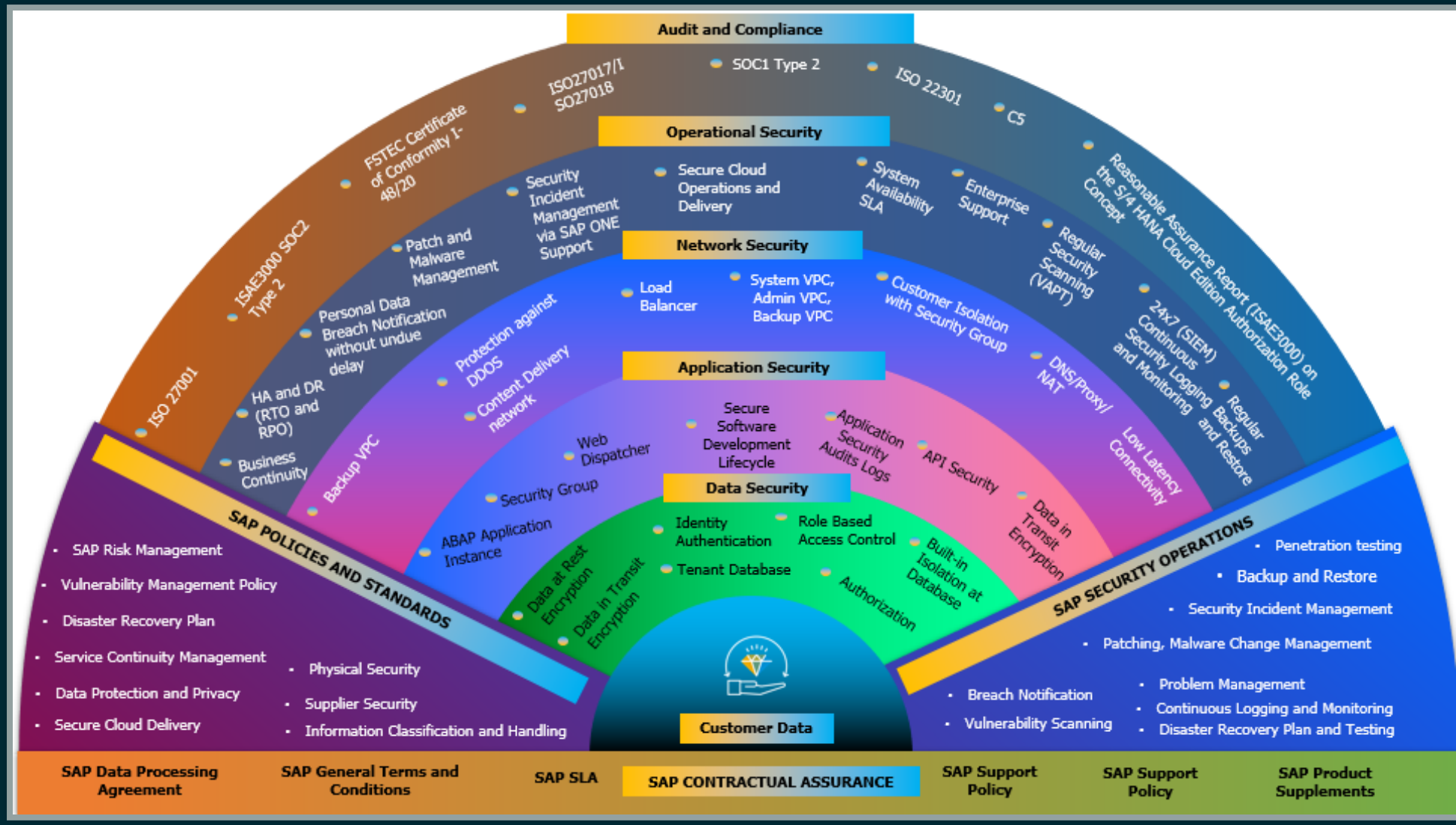
- **Vulnerable and Outdated Components:** Unknown versions of components. Unsupported or out of date software. Not upgrading applications or dependecies in a timely fashion.
- **Identification and Authentication Failures:** Application permits brute force, weak or well-known passwords, weakly hashed passwords, missing multi-factor authentication
- **Software and Data Integrity Failures:** Application relies on plugins, libraries, or modules from untrusted sources. Supply chain attacks
- **Security Logging and Monitoring Failures:** Without logging breaches cannot be detected. Auditable events should be logged and actively monitored for suspicous activity
- **Service-Side Request Forgery:** Application fetches remote resource without validating the user-supplied URL.

THE 7 LAYERS OF CYBERSECURITY



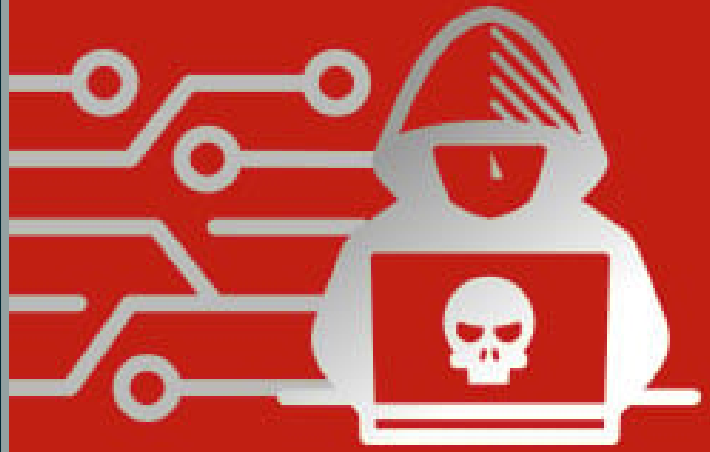
Mindsight
Technology. Transparency. Trust.

Learn more at **www.gomindsight.com**.


Audit and Compliance
ISO 27001
ISAE3000 SOC2 Type 2
FSTEC Certificate of Conformity 1-48/20
ISO27017/I SO27018
SOC1 Type 2
ISO 22301
C5
Reasonable Assurance Report (ISAE3000) on the S/4 HANA Cloud Edition Authorization Role Concept
Operational Security
HA and DR (RTO and RPO)
Business Continuity
Personal Data Breach Notification without undue delay
Patch and Malware Management
Security Incident Management via SAP ONE Support
Secure Cloud Operations and Delivery
System Availability SLA
Enterprise Support
Regular Security Scanning (VAPT)
24x7 (SIEM) Continuous Security Logging and Monitoring
Regular Backups and Restore
Network Security
Backup VPC
Protection against DDOS
Content Delivery network
Load Balancer
System VPC, Admin VPC, Backup VPC
Customer Isolation with Security Group
DNS/Proxy/ NAT
Low Latency Connectivity
Application Security
Security Group
ABAP Application Instance
Web Dispatcher
Secure Software Development Lifecycle
Application Security Audits Logs
API Security
Data in Transit Encryption
Data Security
Data at Rest Encryption
Data in Transit Encryption
Identity Authentication
Tenant Database
Role Based Access Control
Authorization
Built-in Isolation at Database
Customer Data
SAP POLICIES AND STANDARDS
SAP Risk Management
Vulnerability Management Policy
Disaster Recovery Plan
Service Continuity Management
Data Protection and Privacy
Secure Cloud Delivery
Physical Security
Supplier Security
Information Classification and Handling
SAP SECURITY OPERATIONS
Penetration testing
Backup and Restore
Security Incident Management
Patching, Malware Change Management
Breach Notification
Vulnerability Scanning
Problem Management
Continuous Logging and Monitoring
Disaster Recovery Plan and Testing
SAP Data Processing Agreement
SAP General Terms and Conditions
SAP SLA
SAP CONTRACTUAL ASSURANCE
SAP Support Policy
SAP Support Policy
SAP Product Supplements

RED TEAM

Simulated adversary, attempting to identify and exploit potential weaknesses within the organization's cyber defenses...

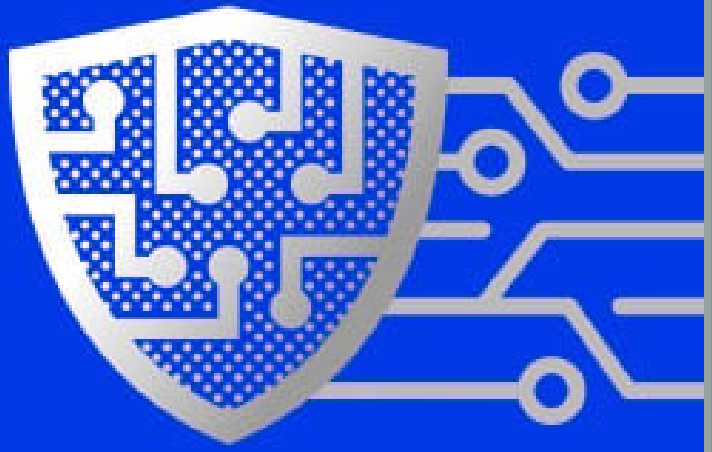


...identifying an attack path that breaches the organization's security defense through real-world attack techniques

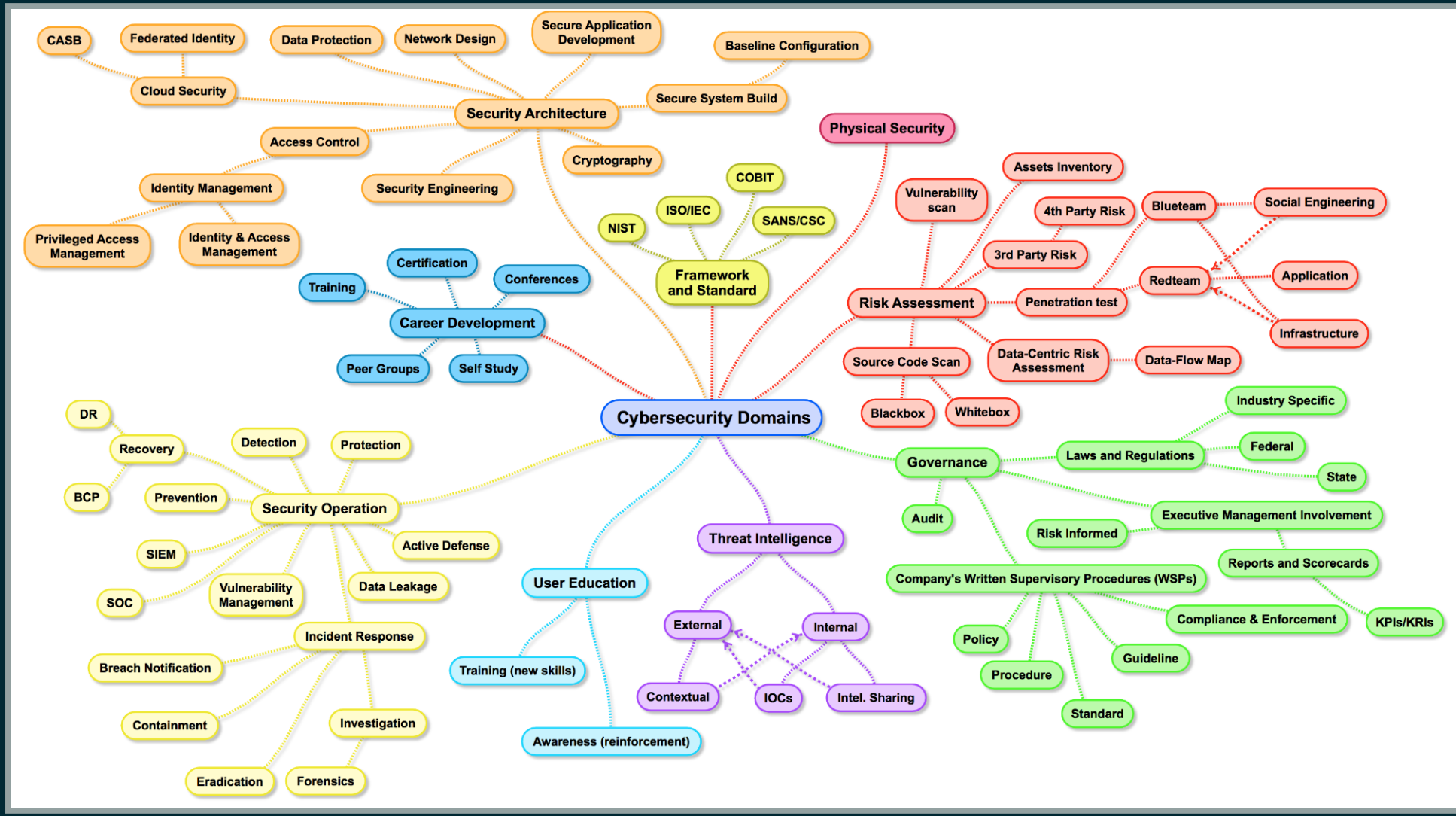
VS

BLUE TEAM

Incident response consultants guide the IT security team on where to make improvements to stop sophisticated types of cyberattacks and threats...



...leaving the IT security team responsible for maintaining the internal network against various types of risk


Cybersecurity Domains
Security Architecture
CASB
Federated Identity
Cloud Security
Data Protection
Network Design
Secure Application Development
Baseline Configuration
Secure System Build
Access Control
Cryptography
Identity Management
Security Engineering
Privileged Access Management
Identity & Access Management
Physical Security
Framework and Standard
NIST
ISO/IEC
COBIT
SANS/CSC
Career Development
Certification
Training
Conferences
Peer Groups
Self Study
Risk Assessment
Vulnerability scan
Assets Inventory
4th Party Risk
3rd Party Risk
Penetration test
Blueteam
Redteam
Social Engineering
Application
Infrastructure
Source Code Scan
Data-Centric Risk Assessment
Data-Flow Map
Blackbox
Whitebox
Security Operation
DR
Recovery
BCP
Detection
Protection
Prevention
SIEM
SOC
Vulnerability Management
Active Defense
Data Leakage
Incident Response
Breach Notification
Containment
Investigation
Eradication
Forensics
User Education
Training (new skills)
Awareness (reinforcement)
Threat Intelligence
External
Internal
Contextual
IOCs
Intel. Sharing
Governance
Industry Specific
Laws and Regulations
Federal
State
Audit
Executive Management Involvement
Risk Informed
Reports and Scorecards
Company's Written Supervisory Procedures (WSPs)
Compliance & Enforcement
KPIs/KRIs
Policy
Procedure
Guideline
Standard

ROLES

- Cybersecurity Analyst (SOC Analyst)
- Application Security Engineer (AppSec)
- Network Security Engineer
- Security Researcher
- Pentester

GOOD CYBER HYGIENE

(what you can do now)

GOOD CYBER HYGIENE

(what you can do now)

UPDATE SOFTWARE REGULARLY

Update apps, web browers, ect regularly to ensure you are using the latest versions. Delete apps you no longer use and only download apps from reputable or offical sources.

GOOD CYBER HYGIENE

(what you can do now)

UPDATE SOFTWARE REGULARLY

Update apps, web browers, ect regularly to ensure you are using the latest versions. Delete apps you no longer use and only download apps from reputable or offical sources.

RESPONSIBLE PASSWORD MANAGEMENT

Use passwords with a minimum of 12 characters and containing uppercase, lowercase, numbers and symbols. Better yet, use a password manager and 24 character passwords!

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

HIVE SYSTEMS

› Learn how we made this table at hivesystems.io/password

USE MULTI-FACTOR AUTHENTICATION (MFA)

Factors include: (i) something you know (e.g., password/personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Authentication using two or more different factors to achieve authentication.

USE MULTI-FACTOR AUTHENTICATION (MFA)

Factors include: (i) something you know (e.g., password/personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Authentication using two or more different factors to achieve authentication.

BACK UP REGULARLY (3-2-1 RULE)

Ensure you have regular, automated backups. You should have **3** copies of your data on **2** different media with **1** copy off-site for disaster recovery.

USE MULTI-FACTOR AUTHENTICATION (MFA)

Factors include: (i) something you know (e.g., password/personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Authentication using two or more different factors to achieve authentication.

BACK UP REGULARLY (3-2-1 RULE)

Ensure you have regular, automated backups. You should have **3** copies of your data on **2** different media with **1** copy off-site for disaster recovery.

PRIVACY

Avoid quizzes, games, or surveys on social media that ask for sensitive information. Don't post private information publicly on social media. Be cautious about the permissions you accept for the apps you use. Use a VPN when connecting to public Wi-Fi. **Always** use https.

WATCH OUT FOR SOCIAL ENGINEERING ATTACKS

Avoid clicking on suspicious links. Avoid downloading suspicious attachments or files. Never disclose security codes over the phone. Hang up and call back if you receive a suspicious call.

RESOURCES

- @hak5
- @LiveOverflow
- @_JohnHammond
- @NetworkChuck
- hackthebox.com
- hackthissite.org
- tryhackme.com
- www.kali.org
- www.sans.org
- www.cybrary.it
- pwn.college

Who has questions?

DEMO

Physical Device Access

DEMO

Objective: Gain administrative access to:
https://ecosystem.ects-cmp.com/