ISACA WEBINARS

Securing Hybrid Environments

David Broggy,

Senior Solutions Architect, Trustwave

CPE CREDIT PROCESS

LIVE EVENT & ON DEMAND RECORDING

- You must view the live or recorded webinar for the required amount of time (50-minutes). Check the **CPE Credit** window to view the timer.

- Your CPE Certificate will automatically appear in the **ISACA CPE RECORDS** tab on the **MyISACA** page after completing the required viewing time.

- Please be patient. This process could take up to **48 hours** for your CPE Certificate and the CPE credit to be applied to your account.

- As a reminder, ALL ISACA webinars, the CPE credits and CPE certificates expire **365 DAYS POST LIVE EVENT.** Please make sure you save the appropriate documents to your personal records.

TODAY'S SPEAKER

David Broggy

Senior Solutions Architect,Trustwave

I've worked in cybersecurity since Y2K

WHO AM I

I work with the following Cyber Security categories/technologies:

- SIEM – Splunk, QRadar, Azure Sentinel
- SOAR – XSOAR, Microsoft Logic Apps, Phantom
- EDR – Defender, Carbon Black, XDR, Cybereason, Crowdstrike
- Cloud – Azure/AWS/GCP (in that order)
- Red/Blue/Purple team events – attack simulations.
- CASB
- DLP
- Information Protection
- IoT (layer 2 detections)
- Zero Trust
- MITRE ATT&CK/SHIELD/D3FEND

OUR FOCUS TODAY:

- Core components (“Building Blocks”) for network security architectures
- Popular security frameworks and standards (light overview)
- Important implementation topics for some core security tools
- Subjects/tips that have affected the security postures of my clients
- High-level view on tips/tools/technologies

WHAT IS A HYBRID COMPUTING ARCHITECTURE?

Simply put:

A computing environment that uses a mix of on-premises, private and third-party services with orchestration between these platforms.

"Where, and when, work gets done will be determined by what makes the most sense to drive the highest levels of productivity and engagement."   ~Gartner

HYBRID SECURITY CONCERNS

The rush to cloud-everything is causing security holes, challenges, misconfigurations and outages

Privacy will be a mess, with user revolts, new laws, confusion and self-regulation failing

Identity and multi-factor authentication (MFA) will take center stage

Tons of high-profile Internet of Thing (IoT) hacks

Ransomware will continue to worsen

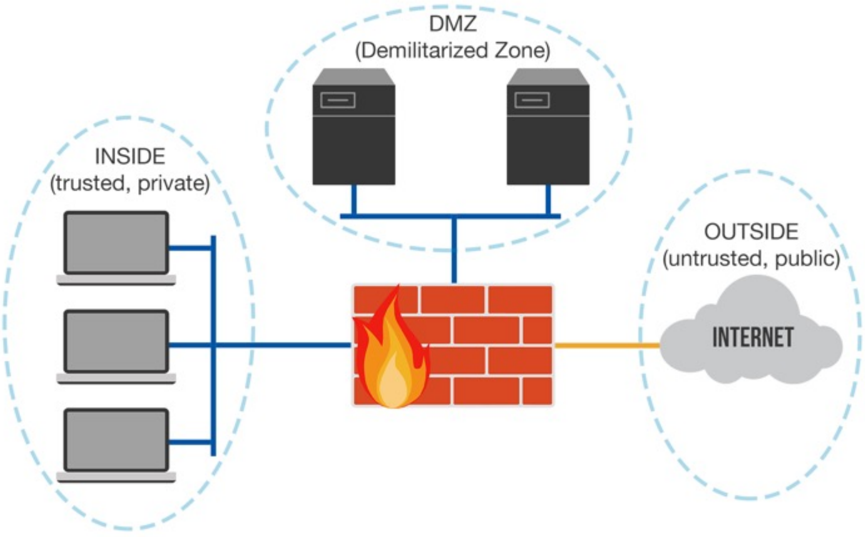
Teleworking setups will force organizations to confront hybrid environments and unsustainable security architectures

Attackers will quickly normalize newly disclosed vulnerabilities, leaving users with a narrow window for patching

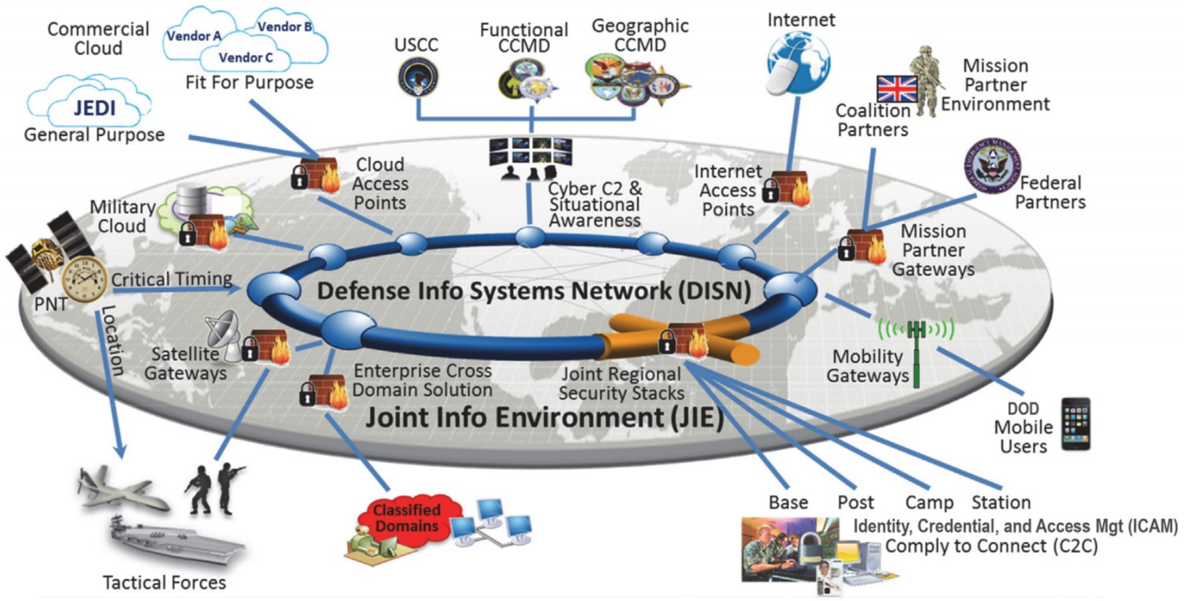
Exposed APIs will be the next favored attack vector for enterprise breaches

HYBRID SECURITY ARCHITECTURE – WHAT DOES IT LOOK LIKE?

Old – not much choice for hybrid

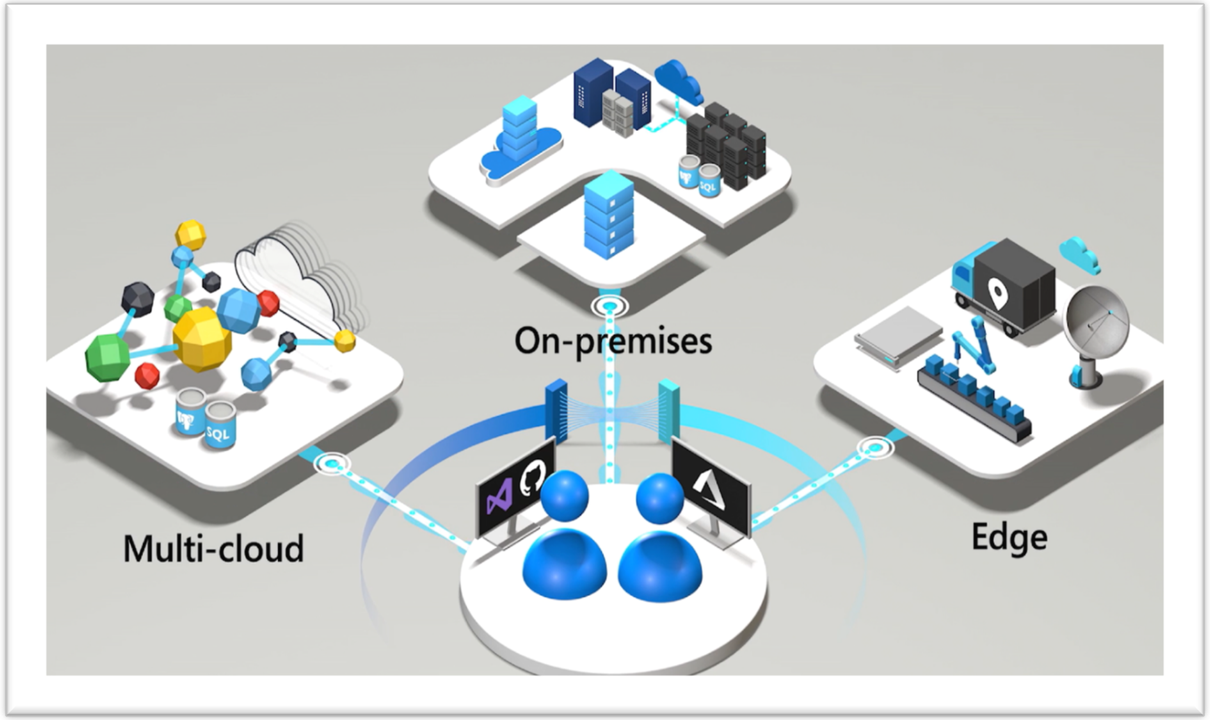


New – overwhelming choice for hybrid



HYBRID NETWORK ARCHITECTURE – SIMPLE MODEL

- Physical and Logical domains.
- Centralized Management



CREATING/TRANSFORMING A CYBERSECURITY ARCHITECTURE

- Design a high-level plan
- Retrain existing staff & add new hires with the needed experience
- Software and hardware changes
- Development new processes and tools
- Lots and lots of hours and change processes

Today, we'll be focusing on the planning, processes and technology

TOPICS SUMMARY

- Standards, Frameworks and Architectures
- Modern Cyber Security Defenses
- Cloud Security Topics
- Practical Cyber Security Solutions
- Closing Summary
- References

Strategy
Plan
Build
Operate
Learning & Adoption

STANDARDS, FRAMEWORKS & ARCHITECTURES

- Zero Trust Architecture
- MITRE Security Framework
- Data Logging/Alerting Framework
- Cyber Maturity Reference Model
- Cyber Maturity Templates

STANDARDS, FRAMEWORKS & ARCHITECTURES

- Standards are a great way to provide a well-structured checklist to ensure you're not missing obvious protections for your organization.
- Frameworks are often a high-level approach to a standard
- Architectures define the specific components of a concept or technology.
- Use all 3 depending on the requirement.
- One approach:
  - Start with a framework
  - Build out an architecture
  - Use a standard to settle compliance needs and fill in gaps.

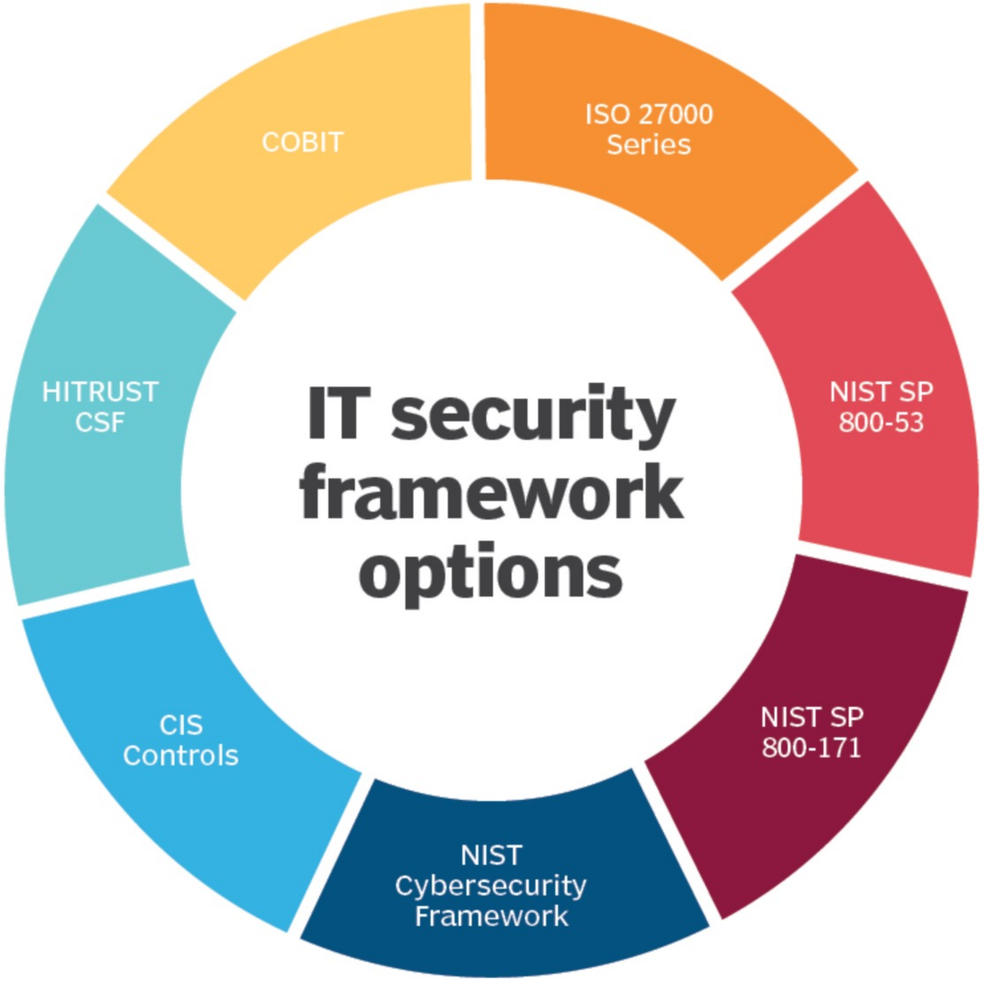
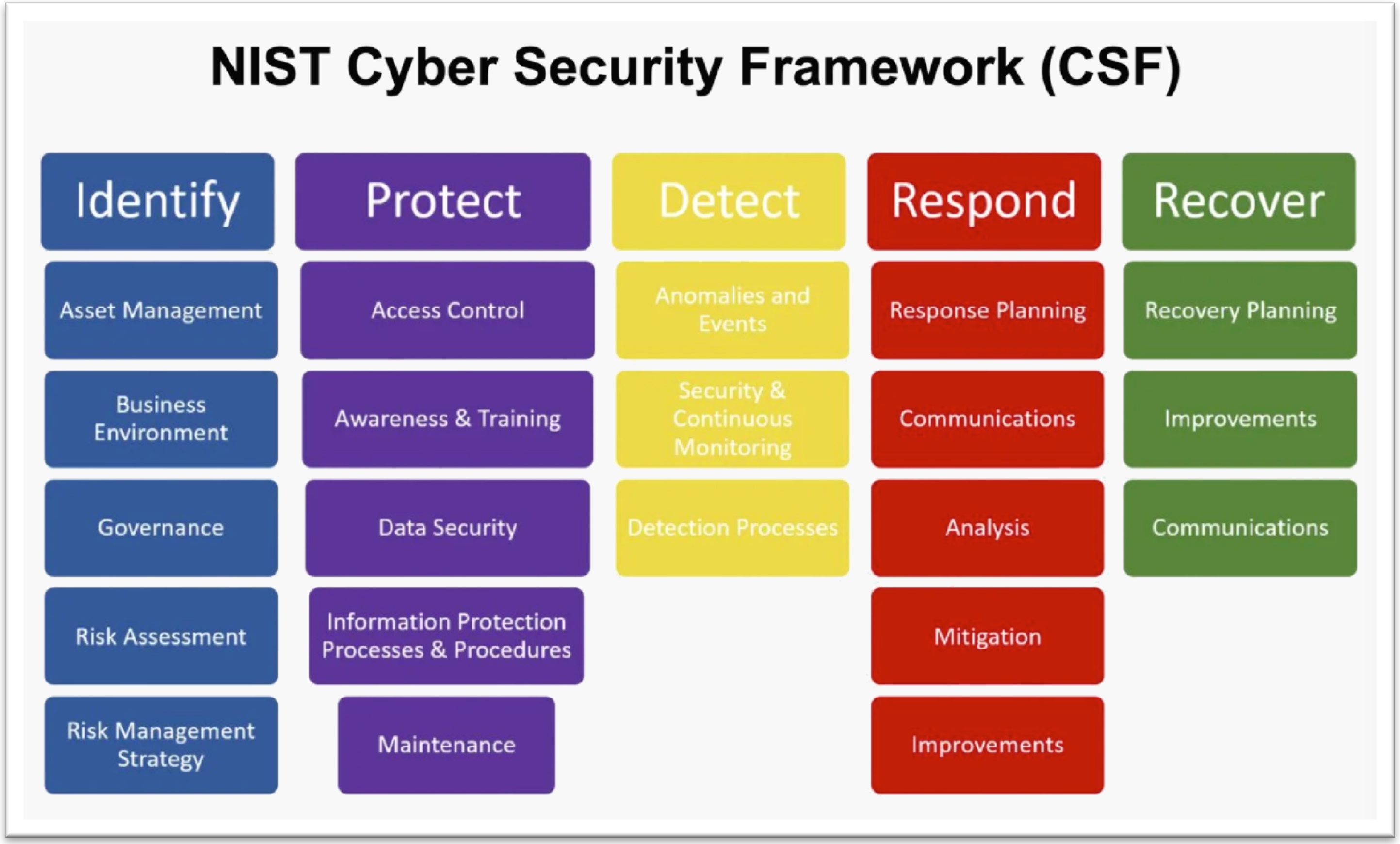


Image reference: https://searchsecurity.techtarget.com/tip/IT-security-frameworks-and-standards-Choosing-the-right-one

STANDARDS, FRAMEWORKS & ARCHITECTURES



NIST Cyber Security Framework (CSF)

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness & Training	Security & Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Information Protection Processes & Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	

- Standards are a great way to provide a well-structured checklist to ensure you're not missing obvious protections for your organization.
- Frameworks are often a high-level approach to a standard
- Architectures define the specific components of a concept or technology.
- Use all 3 depending on the requirement.
- One approach:
  - Start with a framework
  - Build out an architecture
  - Use a standard to settle compliance needs and fill in gaps.

Image reference:
https://searchsecurity.techtarget.com/tip/IT-security-frameworks-and-standards-Choosing-the-right-one

STANDARDIZATIONS AND BEST PRACTICES

Standards are terrific but can be overwhelming.

Problem: There are several Cyber Security standards, which one should I choose?

Solution:

If you MUST comply to a standard because of your industry, start there. eg.

- PCI – Payment Card Industry
- FedRAMP – US Gov.

Otherwise, consider NIST 800-53, ISO 27001, SOC2, CIS

Find a good reference and start reading:

https://securityscorecard.com/blog/top-cybersecurity-frameworks-to-consider

FRAMEWORKS

I’m a fan...

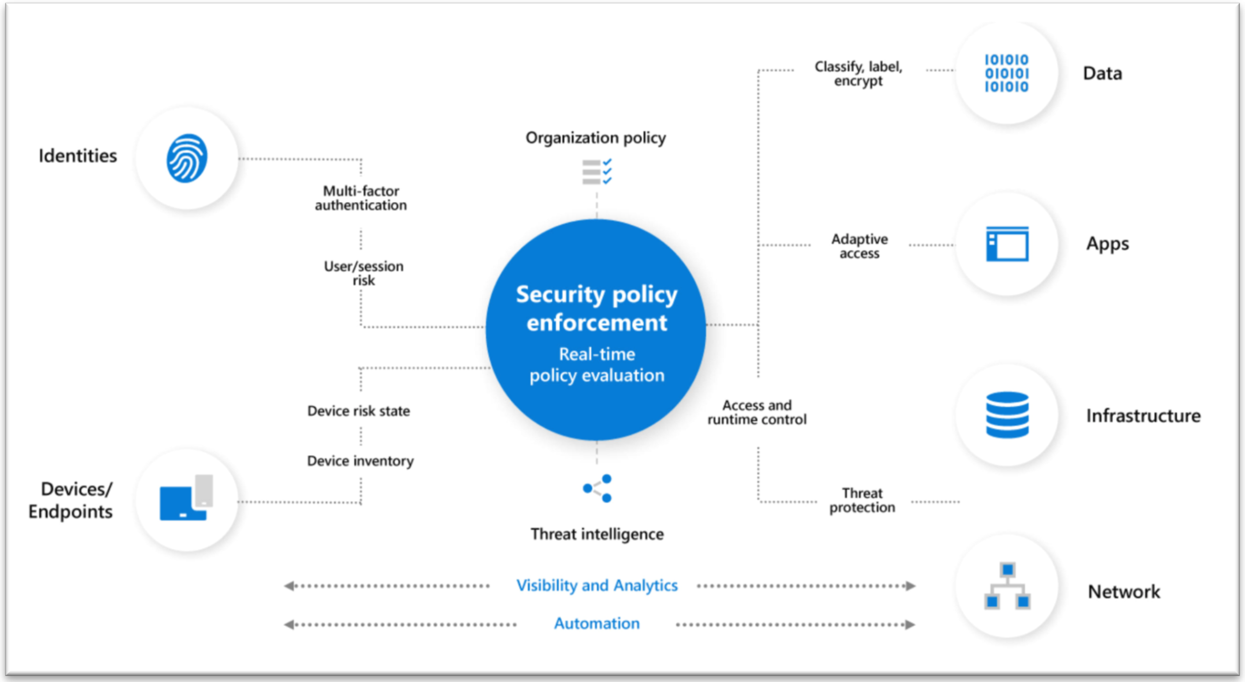
Examples:

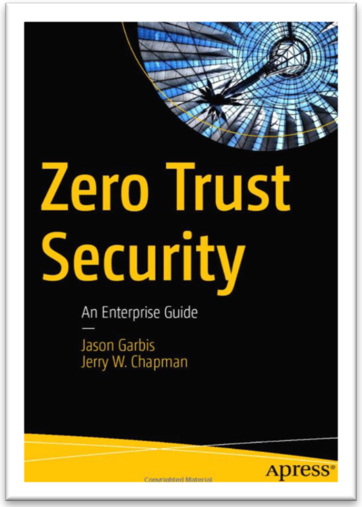
- Zero Trust
- MITRE ATT&CK
- Data Logging and Alerting (my own framework)
- Cyber Resilience

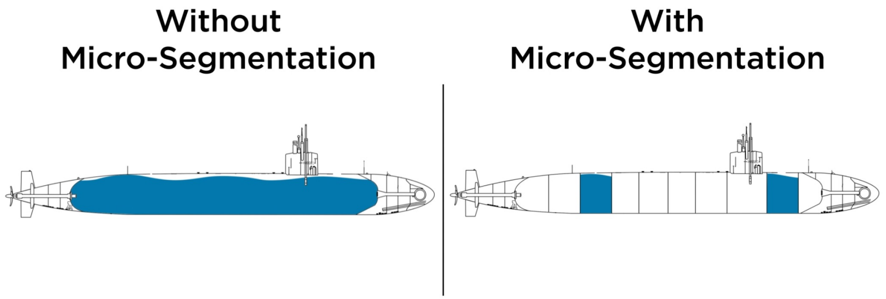
ZERO TRUST FRAMEWORK

- Begin mapping user access and roles to resources/objects
- Question what controls/tools are used to manage that access
- Identify easy places to start, like segmentation, VPN

“Never trust, always verify.”





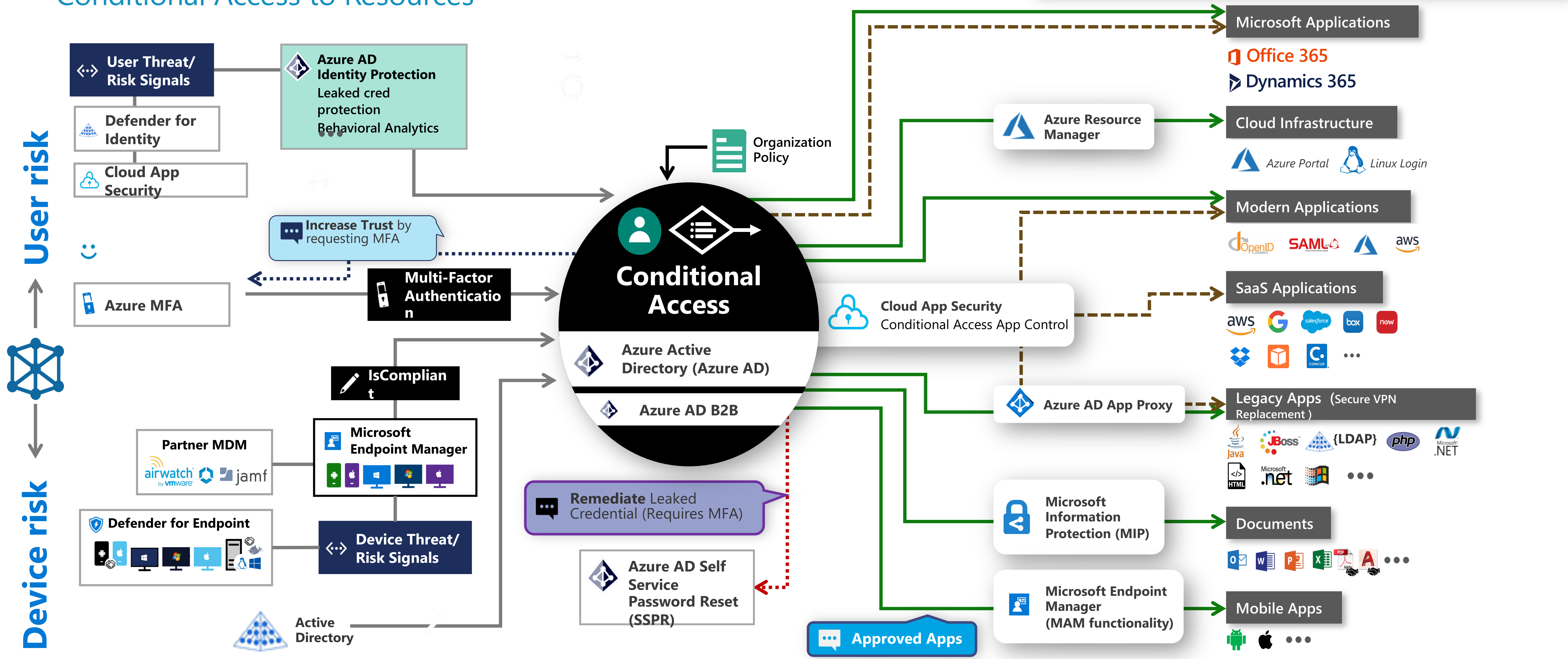


Zero Trust Access Control

Conditional Access to Resources

Legend

▬	Full access	╌ ╌	Limited access
▪▪▪	Risk Mitigation	💬	Remediation Path



User risk

Device risk

User Threat/ Risk Signals

Defender for Identity

Cloud App Security

Azure AD Identity Protection
Leaked cred protection
Behavioral Analytics

Increase Trust by requesting MFA

Azure MFA

Multi-Factor Authenticatio n

Organization Policy

Conditional Access

Azure Active Directory (Azure AD)

Azure AD B2B

IsComplian t

Partner MDM

Microsoft Endpoint Manager

Defender for Endpoint

Device Threat/ Risk Signals

Remediate Leaked Credential (Requires MFA)

Azure AD Self Service Password Reset (SSPR)

Active Directory

Azure Resource Manager

Cloud App Security
Conditional Access App Control

Azure AD App Proxy

Microsoft Information Protection (MIP)

Microsoft Endpoint Manager (MAM functionality)

Approved Apps

Microsoft Applications
Office 365
Dynamics 365

Cloud Infrastructure
Azure Portal
Linux Login

Modern Applications

SaaS Applications

Legacy Apps (Secure VPN Replacement)

Documents

Mobile Apps

ISACA

MITRE SECURITY FRAMEWORK

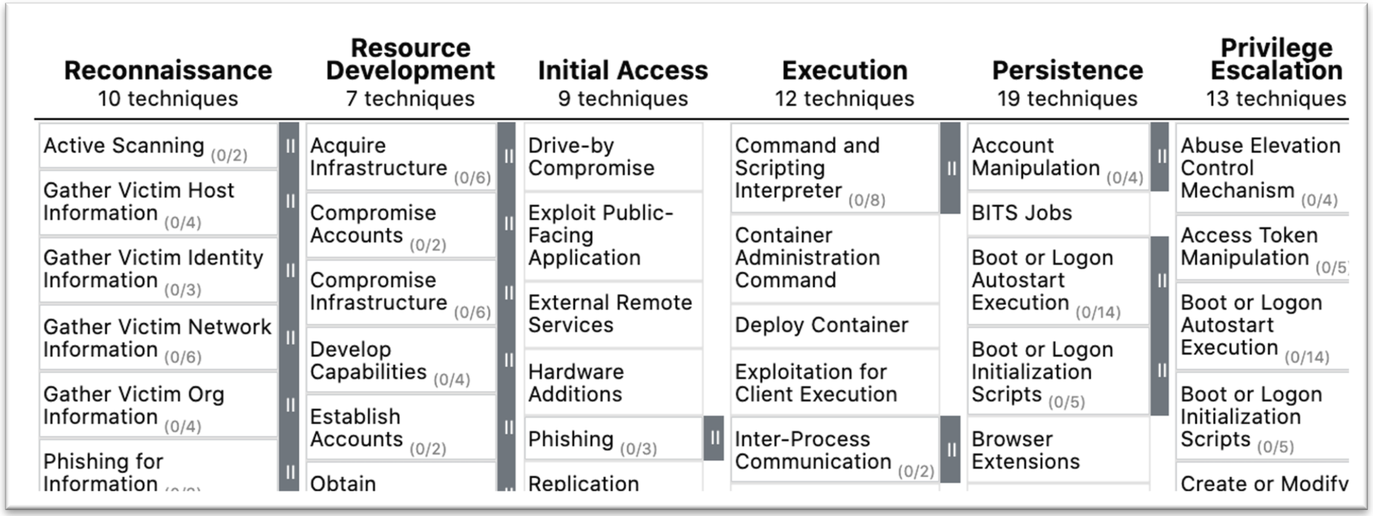
What is the MITRE Security Framework?

A matrix of tactics and techniques used by threat hunters, red teamers, and defenders to better classify attacks and assess an organization's risk.

The MITRE ATT&CK master list:

Enterprise techniques

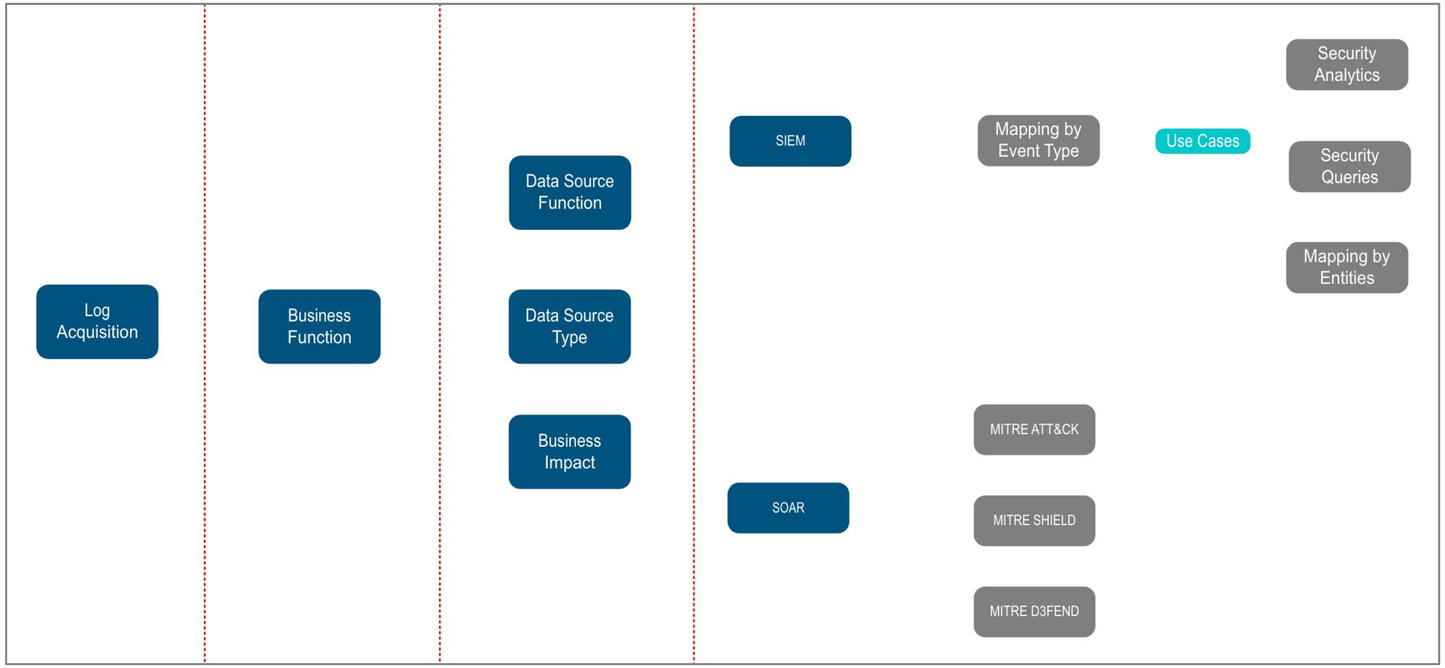
Attack navigator



Reconnaissance 10 techniques	**Resource Development** 7 techniques	**Initial Access** 9 techniques	**Execution** 12 techniques	**Persistence** 19 techniques	**Privilege Escalation** 13 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Inter-Process Communication (0/2)	Browser Extensions	Create or Modifv
Phishing for Information	Obtain	Replication			

DATA LOGGING/ALERTING FRAMEWORK

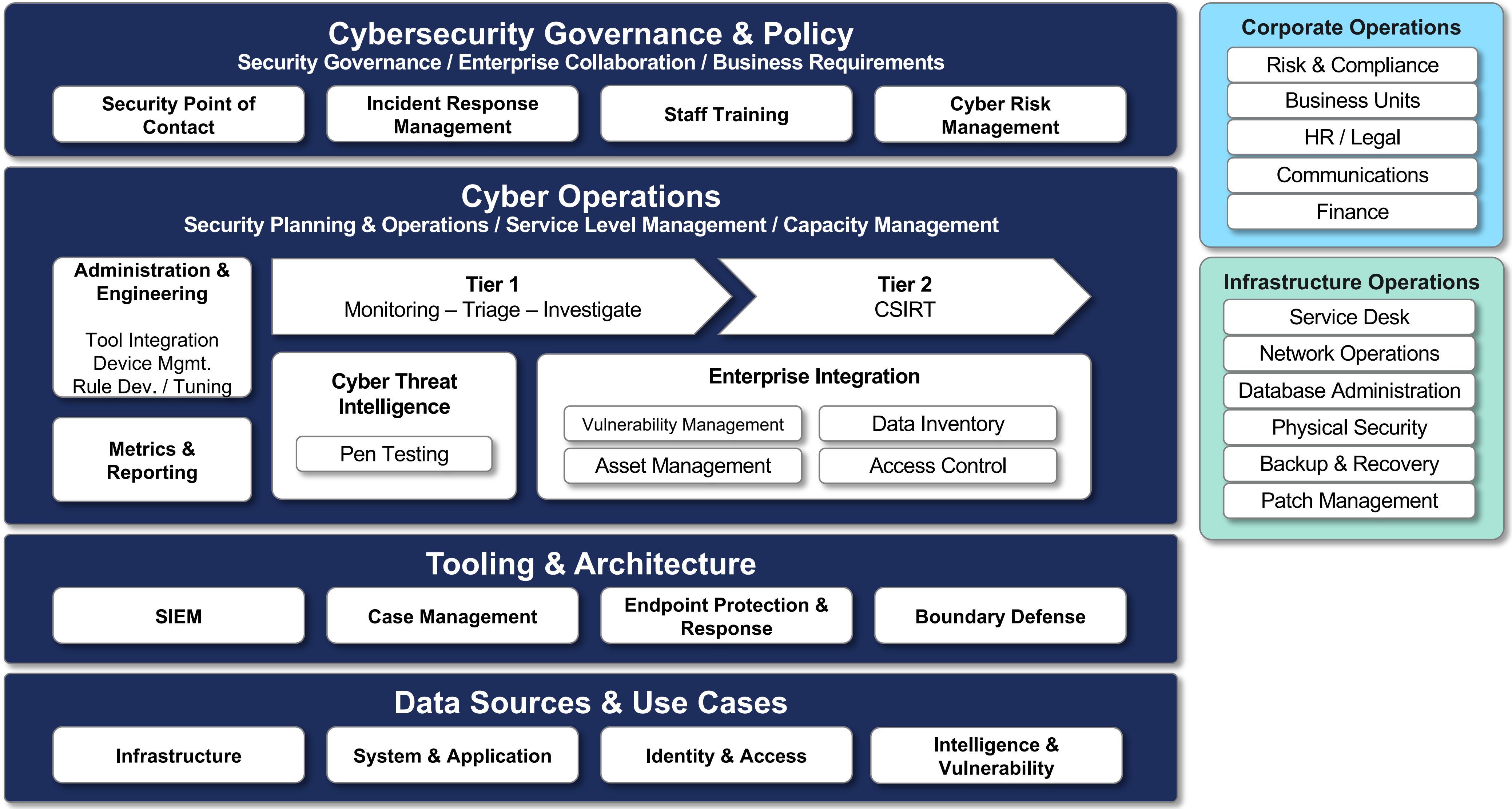
Proper implementation of SIEM/SOAR uses a well-structured logging/alerting framework



Framework topics

- Architecture
- Data Type Acquisition Summary
- Data Custodians
- Onboarding Tracking Sheet
- Data Source Acquisition (and gap analysis)
- Acquisition Form
- Syslog Facility
- Critical Assets
- Critical Apps
- Configuration
- Collection Tools
- Log Source Types
- Defender Asset Export
- Assets
- TI Feeds

CYBER MATURITY REFERENCE MODEL



Cybersecurity Governance & Policy

Security Governance / Enterprise Collaboration / Business Requirements

- Security Point of Contact
- Incident Response Management
- Staff Training
- Cyber Risk Management

Cyber Operations

Security Planning & Operations / Service Level Management / Capacity Management

Administration & Engineering

Tool Integration
Device Mgmt.
Rule Dev. / Tuning

Metrics & Reporting

Tier 1
Monitoring – Triage – Investigate

Tier 2
CSIRT

Cyber Threat Intelligence

- Pen Testing

Enterprise Integration

- Vulnerability Management
- Data Inventory
- Asset Management
- Access Control

Tooling & Architecture

- SIEM
- Case Management
- Endpoint Protection & Response
- Boundary Defense

Data Sources & Use Cases

- Infrastructure
- System & Application
- Identity & Access
- Intelligence & Vulnerability

Corporate Operations

- Risk & Compliance
- Business Units
- HR / Legal
- Communications
- Finance

Infrastructure Operations

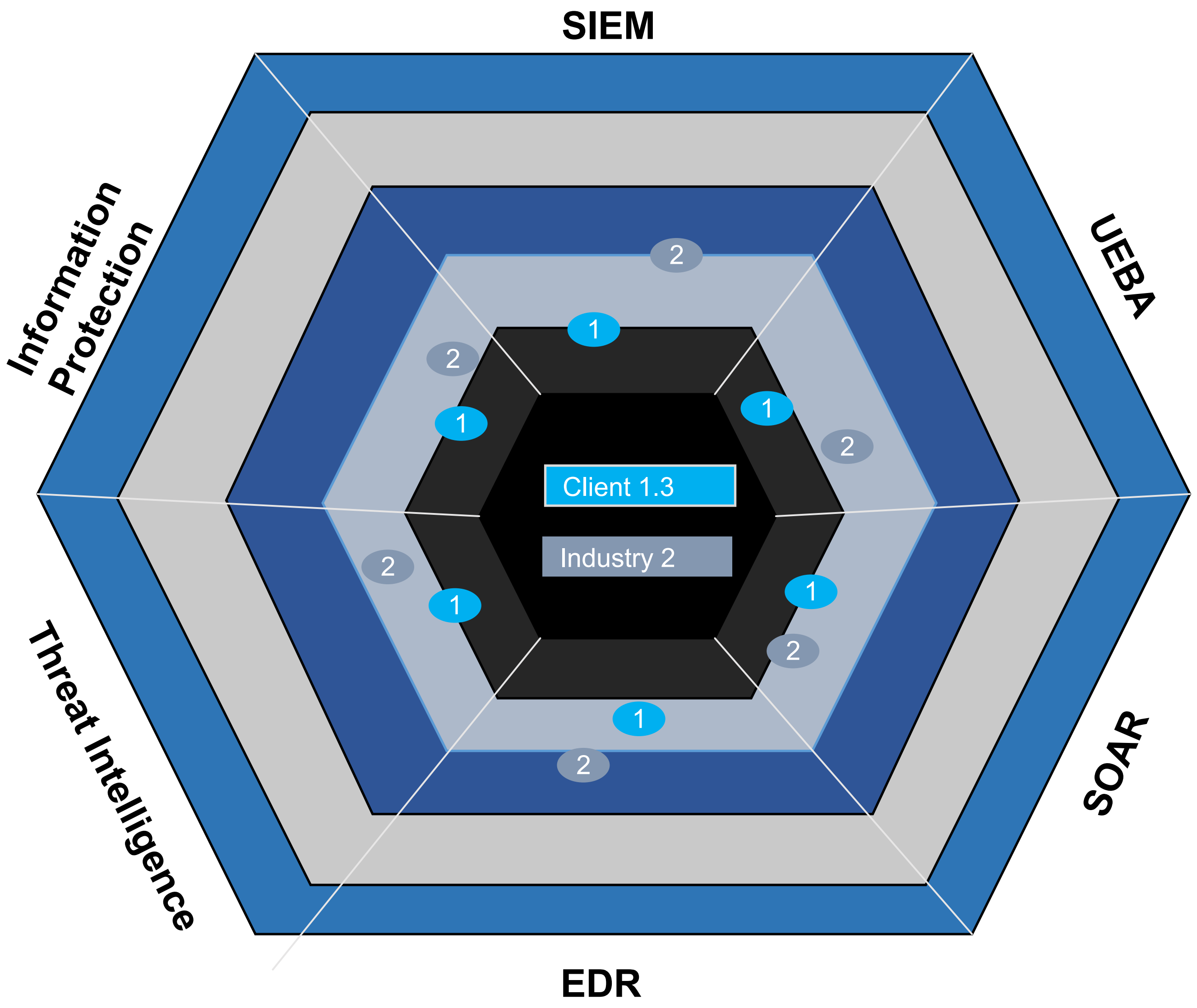
- Service Desk
- Network Operations
- Database Administration
- Physical Security
- Backup & Recovery
- Patch Management

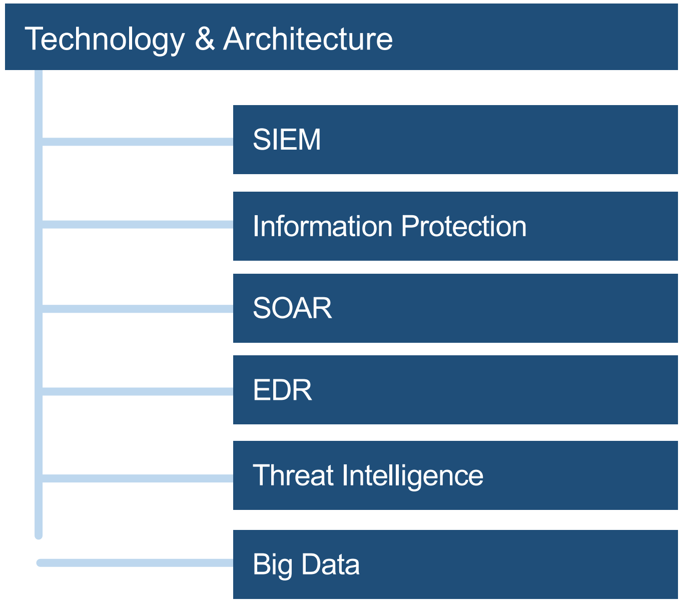
CYBER MATURITY TEMPLATES

Create a Target State Operating Model and Score yourself against it

- Tooling and Architecture
- Data Sources & Use Cases
- SOC IR Process & Playbooks
- Cyber Operations
- Metrics and Reporting
- Governance
  - Use Case Framework
  - Cost Models
  - Sponsorship

Example Maturity Template: Technology & Architecture





CORE DOMAIN RISK

No centralized logging system to capture and alert on logs.

QUESTION

What Security Standards, Frameworks and Architectures do you use? (choose 1 or more)

- NIST Cybersecurity Framework
- ISO 27001 and ISO 27002
- SOC2
- NERC-CIP
- HIPAA
- GDPR
- FISMA

MODERN SECURITY DEFENSES (TOOLING & ARCHITECTURE)

- SIEM
- SOAR
- EDR/XDR
- Threat Intelligence
- CSPM
- Cloud Defense Tools - Example

MODERN SECURITY DEFENSES

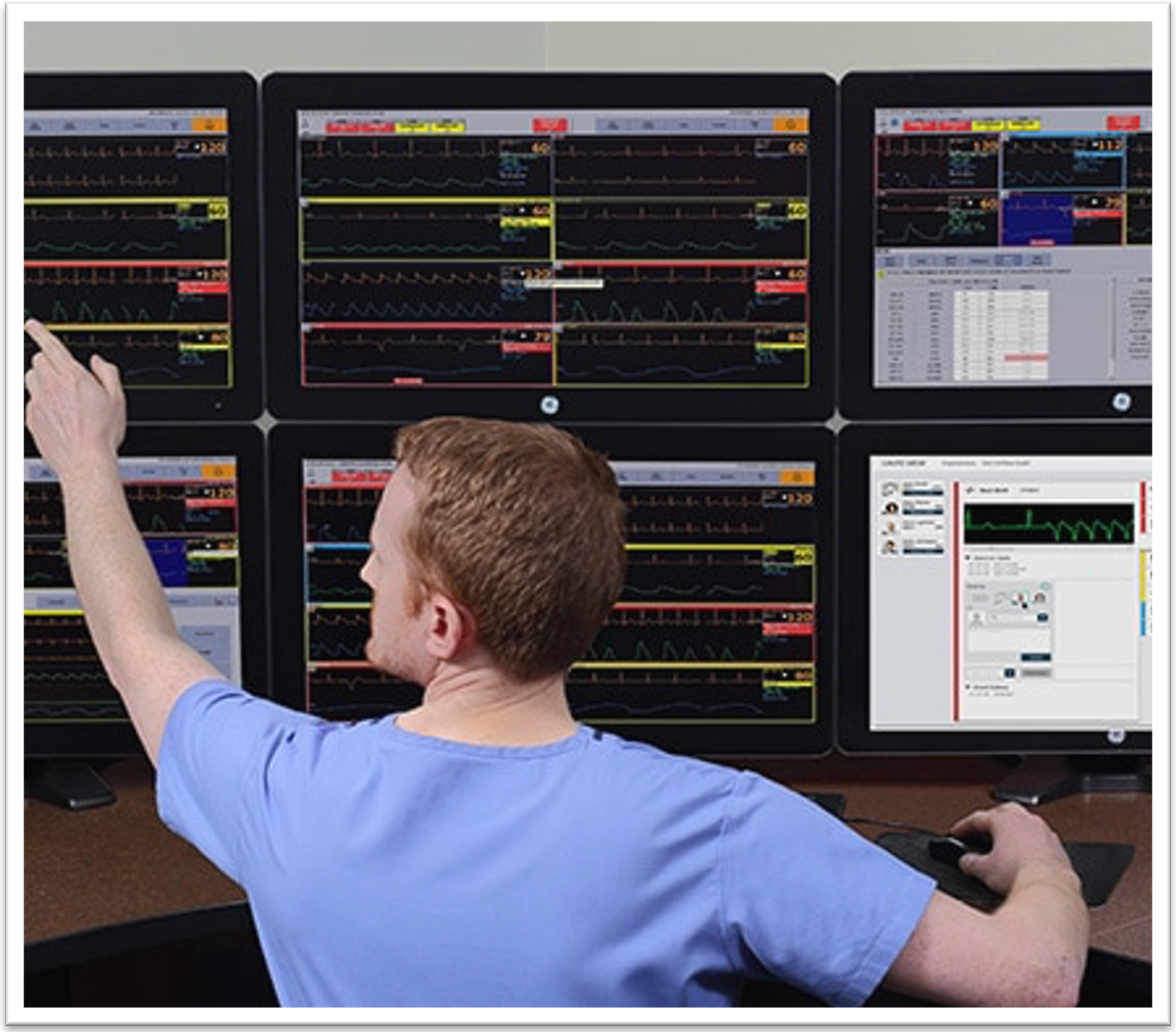
- This section will focus on the tooling section of the Cybersecurity Framework.
- You should have a basic understanding of the different security defenses.
- Use a list of defenses like this to identify gaps in your security posture.
- Some of these defenses will be discussed next.

AV/HIPS	Network FW	NIDS/NIPS	Database
Email Server/Mail gateway	WAF/Web Proxy/Content Filtering	EDR	System/File Integrity Checker
SIEM	CASB	DLP	Containers
NetFlow	System (OS)	SOAR	Physical access control
Remote Access & VPN	Wireless Access	Identity & SSO	CSPM
Vulnerability scanner	Honeypot	External/Internal TI Feed	User behavior monitoring
NAC	IoT/OT	Application Security	API Security

SIEM

- Heart of most Security Centers
- High Level Getting Started:
  - Connect log sources
  - Configure correlations/analytics (use cases)
  - TEST, TEST, TEST!

  (simulate attacks and verify detections)
- Adding SOAR can be very powerful

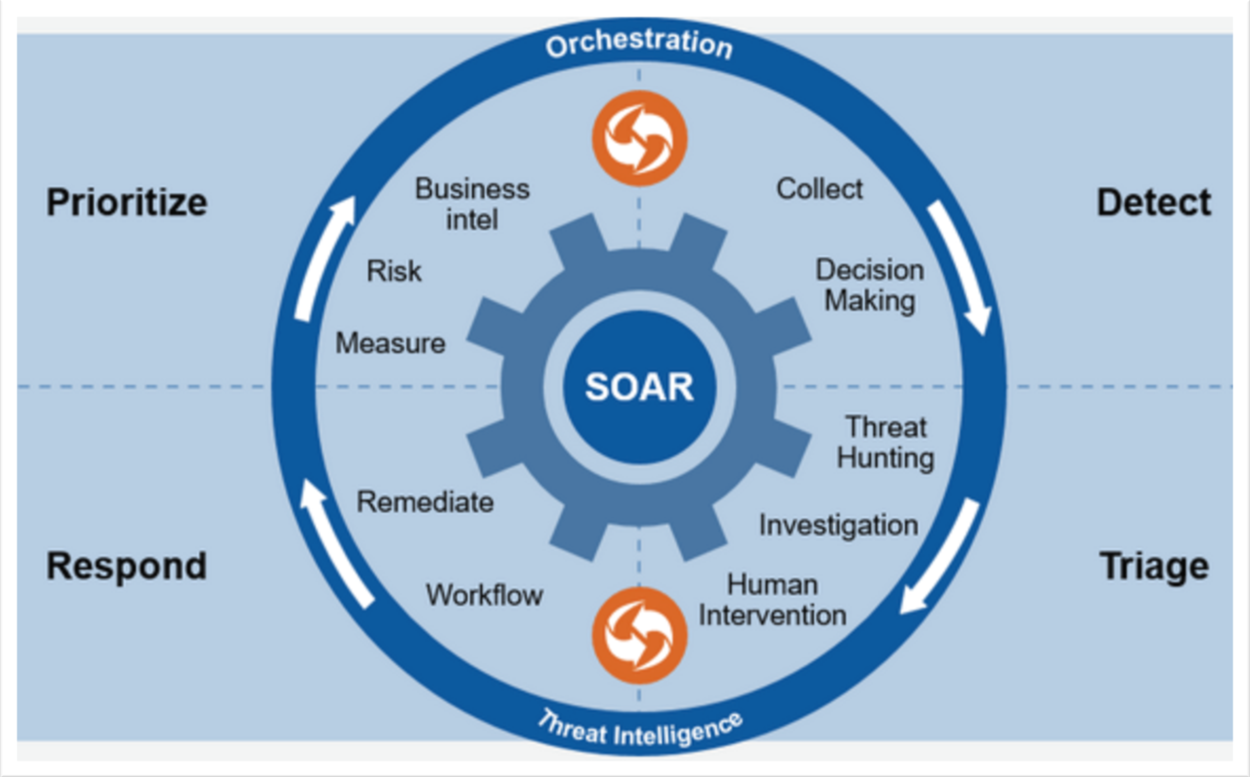


ref: gehealcare.com

SOAR

- SOAR is all about good “playbooks” – the logic you build for an automation.
- Think top-down:
  - Identify good SOC workflows
    - Learn from your SOC team how they investigate incidents
    - Create playbooks that match that workflow

  e.g., if an alert contains a username, investigate the user’s past activity
  - Create logic flow that performs ‘auto investigations’, based on ‘entities’ in the incident like username, source IP



EDR/XDR

Endpoint Detection and Response

Evolved significantly over the past few years.

Be sure SIEM can detect when EDR is down, or you’ll be blind

Can work great with additional security tools like NIDS and CASB

- Hey, that’s XDR! – Cross Platform Detection and Response

Microsoft Defender suite is a good example

- EDR shares logs with CASB, so CASB can recognize ‘shadow IT’ (unsanctioned web apps).

THREAT INTELLIGENCE

Used by SIEM, EDR, CASB, WAF, Proxy, Email, etc.

- Can help identify KBAs – Known Bad Actors
- Example values include:

  email addresses

  IP addresses

  Domain URLs

OSINT – Open-Source Intelligence

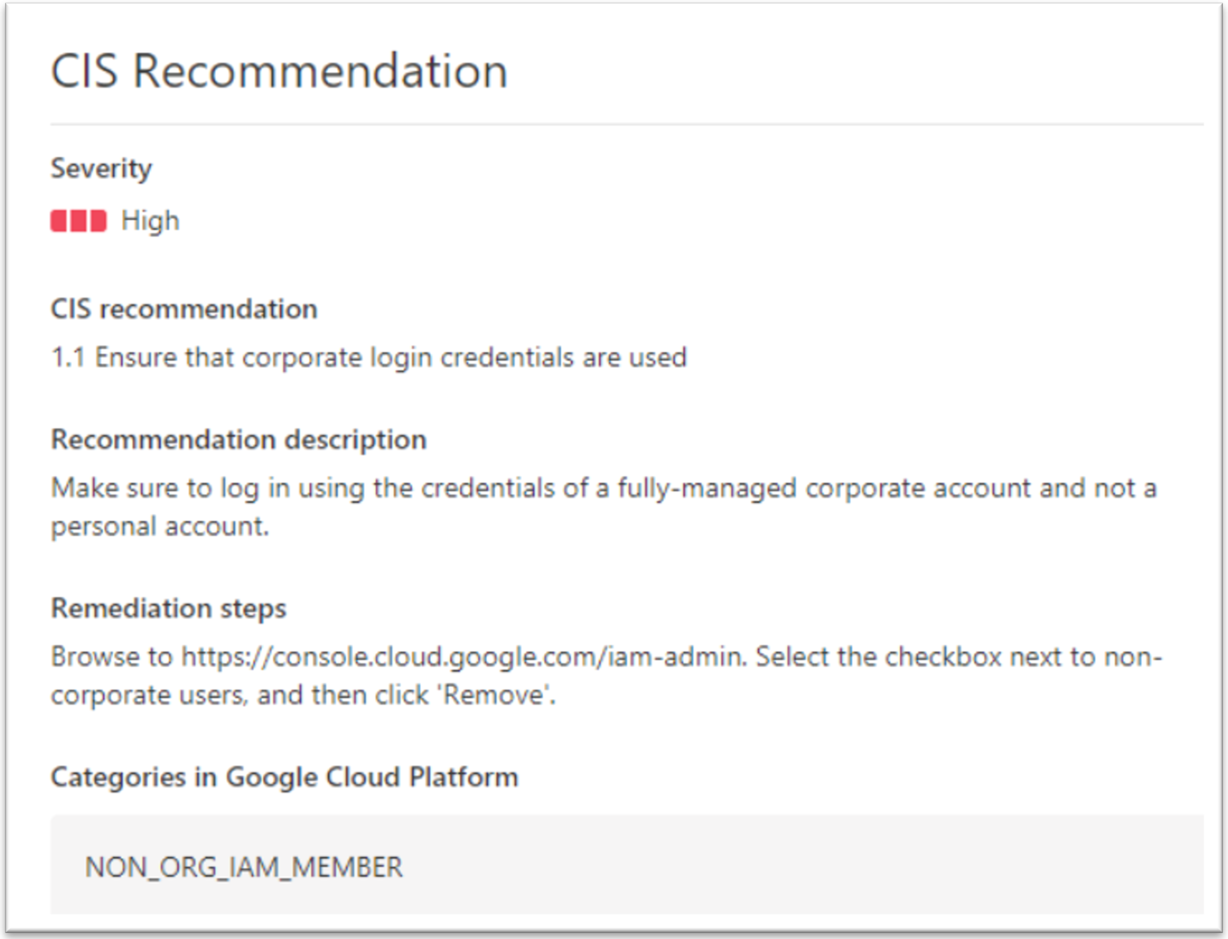
- Formerly thought of as free threat feeds but includes any open-source tools used to collect threat intelligence.

Commercial Threat Intelligence tools: Recorded Future, VirusTotal

CSPM

Cloud Security Posture Management

- Continuously audits the cloud for security risks and misconfigurations
- Uses an API and scripts/checks.
- May also ‘score’ 3rd party web sites as well as your own private cloud.
- Many good CSPM vendors to choose from.



CIS Recommendation

Severity

🟥🟥🟥 High

CIS recommendation

1.1 Ensure that corporate login credentials are used

Recommendation description

Make sure to log in using the credentials of a fully-managed corporate account and not a personal account.

Remediation steps

Browse to https://console.cloud.google.com/iam-admin. Select the checkbox next to non-corporate users, and then click 'Remove'.

Categories in Google Cloud Platform

NON_ORG_IAM_MEMBER

CLOUD DEFENSIVE TOOLS - EXAMPLE

Know these tools:

Azure Sentinel (SIEM/SOAR)

Defender Suite:

- Defender for Endpoint (ASR – Attack Surface Reduction)
- Defender for Identity
- Defender for O365 (phishing)
- Defender for OT/IOT

Cloud App Security (MCAS)

Microsoft Information Protection – especially useful with OneDrive.

QUESTION

What would you consider your top defensive security tools? (choose 1 or more)

- SIEM
- SOAR
- EDR
- IDS, IPS
- CASB, CSPM
- Identity Protection

CLOUD SECURITY TOPICS

- Example Kill Chain Evaluation using Cloud tools
- Migrating to the Cloud - Benefits and Challenges
- Security Tools Built for the Cloud
- Hybrid Architectures – Considering the best of both
- Cloud Adoption Frameworks
- A Cloud Security Example: Microsoft’s Azure Security Architecture

GET TO THE CLOUD!

Many opportunities to show cost effectiveness

So many features provided by cloud vendors to help secure your environment, including:

Conditional Access

Conditional Resource Creation

eg. ARM templates

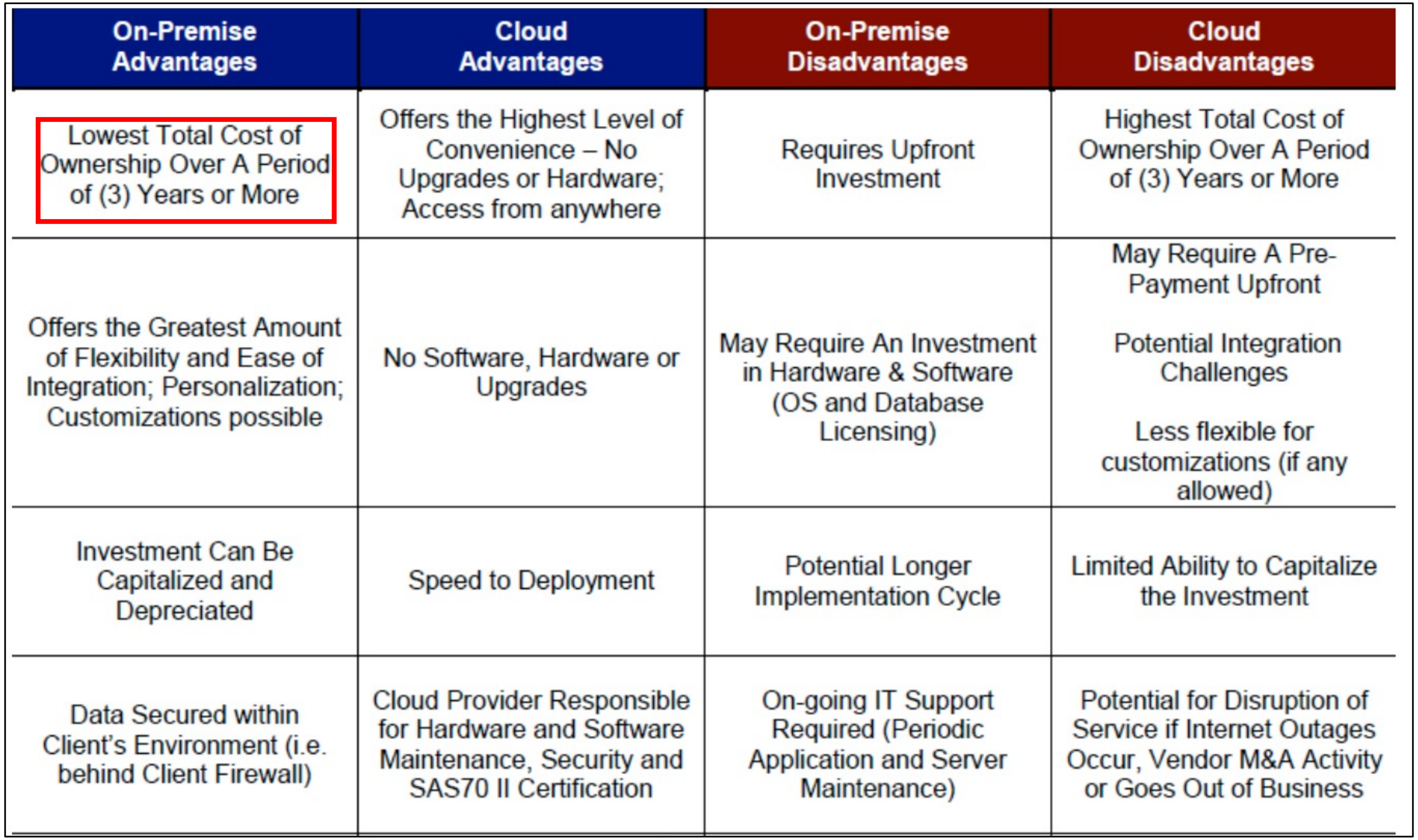
SIEM - much easier to manage, often much faster

SOAR – adds automation to a variety of tasks

CSPM – Cloud Security Posture Management

Automate configuration checks using CSPM

CLOUD MIGRATIONS – BENEFITS VS DISADVANTAGES



On-Premise Advantages	Cloud Advantages	On-Premise Disadvantages	Cloud Disadvantages
Lowest Total Cost of Ownership Over A Period of (3) Years or More	Offers the Highest Level of Convenience – No Upgrades or Hardware; Access from anywhere	Requires Upfront Investment	Highest Total Cost of Ownership Over A Period of (3) Years or More
Offers the Greatest Amount of Flexibility and Ease of Integration; Personalization; Customizations possible	No Software, Hardware or Upgrades	May Require An Investment in Hardware & Software (OS and Database Licensing)	May Require A Pre-Payment Upfront Potential Integration Challenges Less flexible for customizations (if any allowed)
Investment Can Be Capitalized and Depreciated	Speed to Deployment	Potential Longer Implementation Cycle	Limited Ability to Capitalize the Investment
Data Secured within Client's Environment (i.e. behind Client Firewall)	Cloud Provider Responsible for Hardware and Software Maintenance, Security and SAS70 II Certification	On-going IT Support Required (Periodic Application and Server Maintenance)	Potential for Disruption of Service if Internet Outages Occur, Vendor M&A Activity or Goes Out of Business

SECURITY TOOLS BUILT FOR CLOUD

XDR is arguably possible because of cloud

Moving to cloud brings new defense opportunities like information protection

CASB is XDR dependent

The more information it has access to, the better it works

Feeding CASB with data like access logs and EDR is recommended

This is easier to do when all security products all cloud-central or vendor-central

Information Protection –

If all data is in the cloud, IP tools can detect suspicious activity related to that sensitive data.

HYBRID ARCHITECTURES – CONSIDERING THE BEST OF BOTH

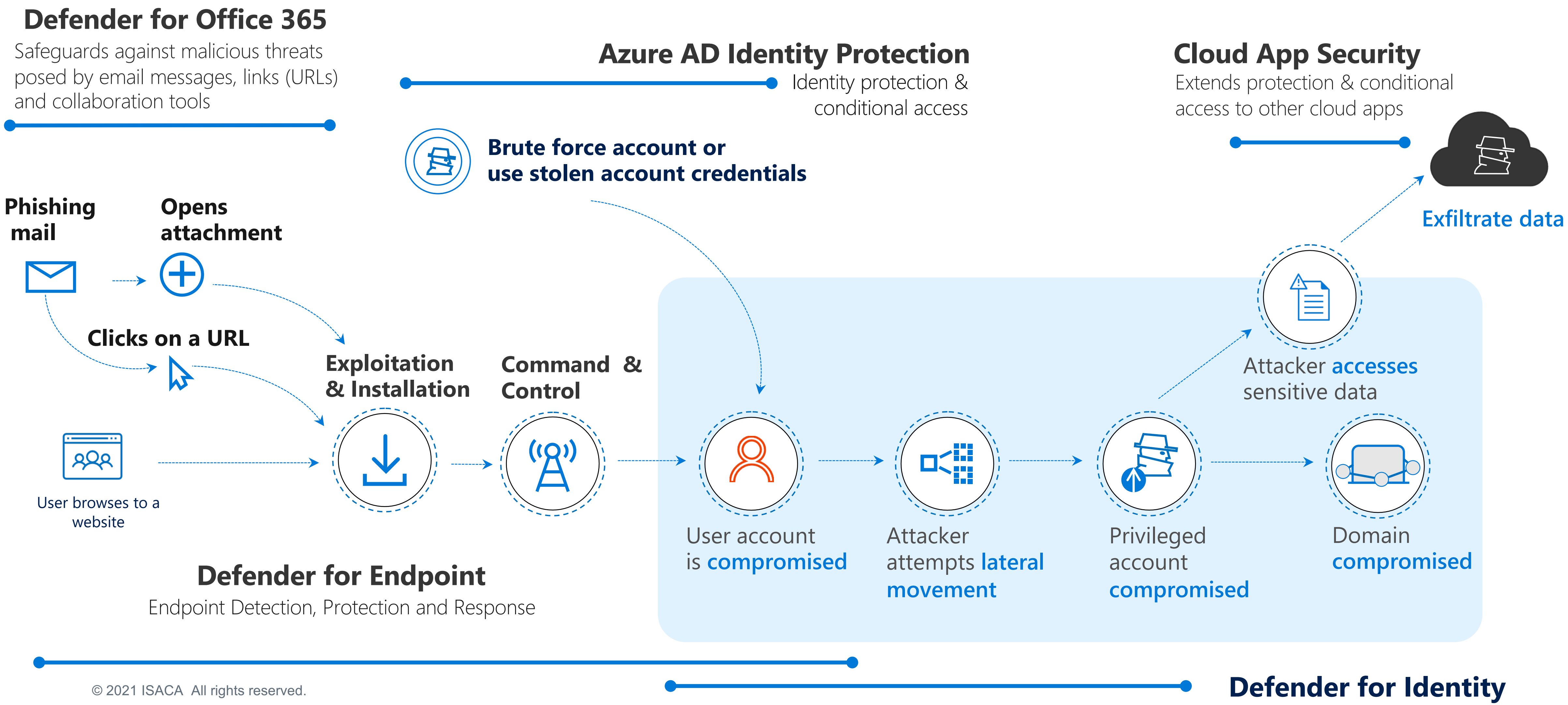
VMs on-prem may be more cost effective

- Plan for more resiliency to match cloud benefits

Cloud SaaS may be more attractive than IaaS

- Security tools from cloud vendors are very price competitive

EXAMPLE KILL CHAIN DETECTED USING CLOUD TOOLS



Defender for Office 365

Safeguards against malicious threats posed by email messages, links (URLs) and collaboration tools

Azure AD Identity Protection

Identity protection & conditional access

Cloud App Security

Extends protection & conditional access to other cloud apps

Brute force account or use stolen account credentials

Phishing mail

Opens attachment

Clicks on a URL

User browses to a website

Exploitation & Installation

Command & Control

User account is **compromised**

Attacker attempts **lateral movement**

Privileged account **compromised**

Domain **compromised**

Attacker **accesses** sensitive data

Exfiltrate data

Defender for Endpoint

Endpoint Detection, Protection and Response

Defender for Identity

CLOUD ADOPTION FRAMEWORKS

Cloud vendors can help with the transition to cloud:

Microsoft

AWS

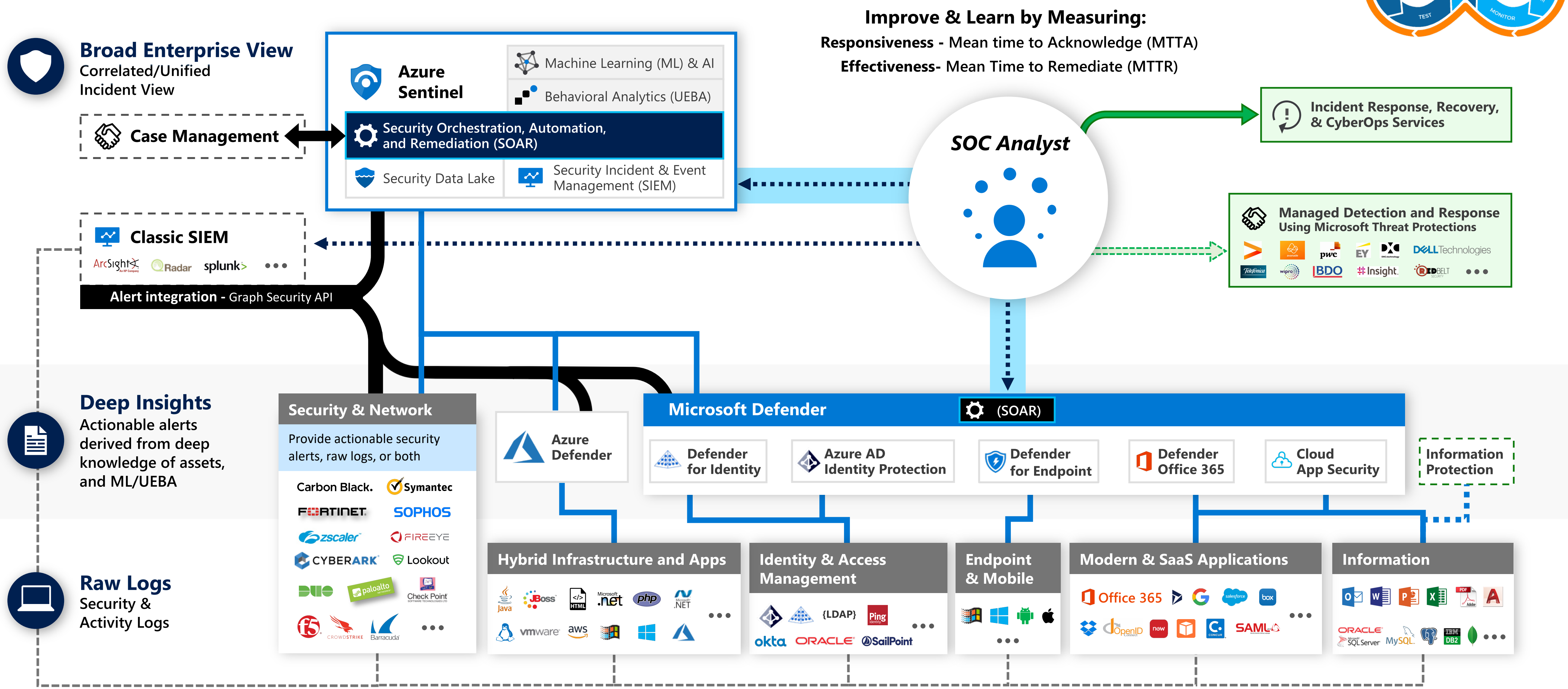
Google

A CLOUD SECURITY EXAMPLE

Microsoft's Azure Security Reference Architecture

Legend

‒ ‒ ‒ Event Log Based Monitoring	⇢ Outsourcing
▪▪▪▪ Investigation & Proactive Hunting	➜ Consulting and Escalation
	▬ Native Resource Monitoring



Broad Enterprise View
Correlated/Unified Incident View

Case Management

Azure Sentinel
- Machine Learning (ML) & AI
- Behavioral Analytics (UEBA)
- Security Orchestration, Automation, and Remediation (SOAR)
- Security Data Lake
- Security Incident & Event Management (SIEM)

Classic SIEM

Alert integration - Graph Security API

Improve & Learn by Measuring:
Responsiveness - Mean time to Acknowledge (MTTA)
Effectiveness- Mean Time to Remediate (MTTR)

SOC Analyst

Incident Response, Recovery, & CyberOps Services

Managed Detection and Response Using Microsoft Threat Protections

Deep Insights
Actionable alerts derived from deep knowledge of assets, and ML/UEBA

Raw Logs
Security & Activity Logs

Security & Network
Provide actionable security alerts, raw logs, or both

Azure Defender

Microsoft Defender (SOAR)
- Defender for Identity
- Azure AD Identity Protection
- Defender for Endpoint
- Defender Office 365
- Cloud App Security

Information Protection

Hybrid Infrastructure and Apps

Identity & Access Management

Endpoint & Mobile

Modern & SaaS Applications

Information

PRACTICAL CYBER SECURITY SOLUTIONS

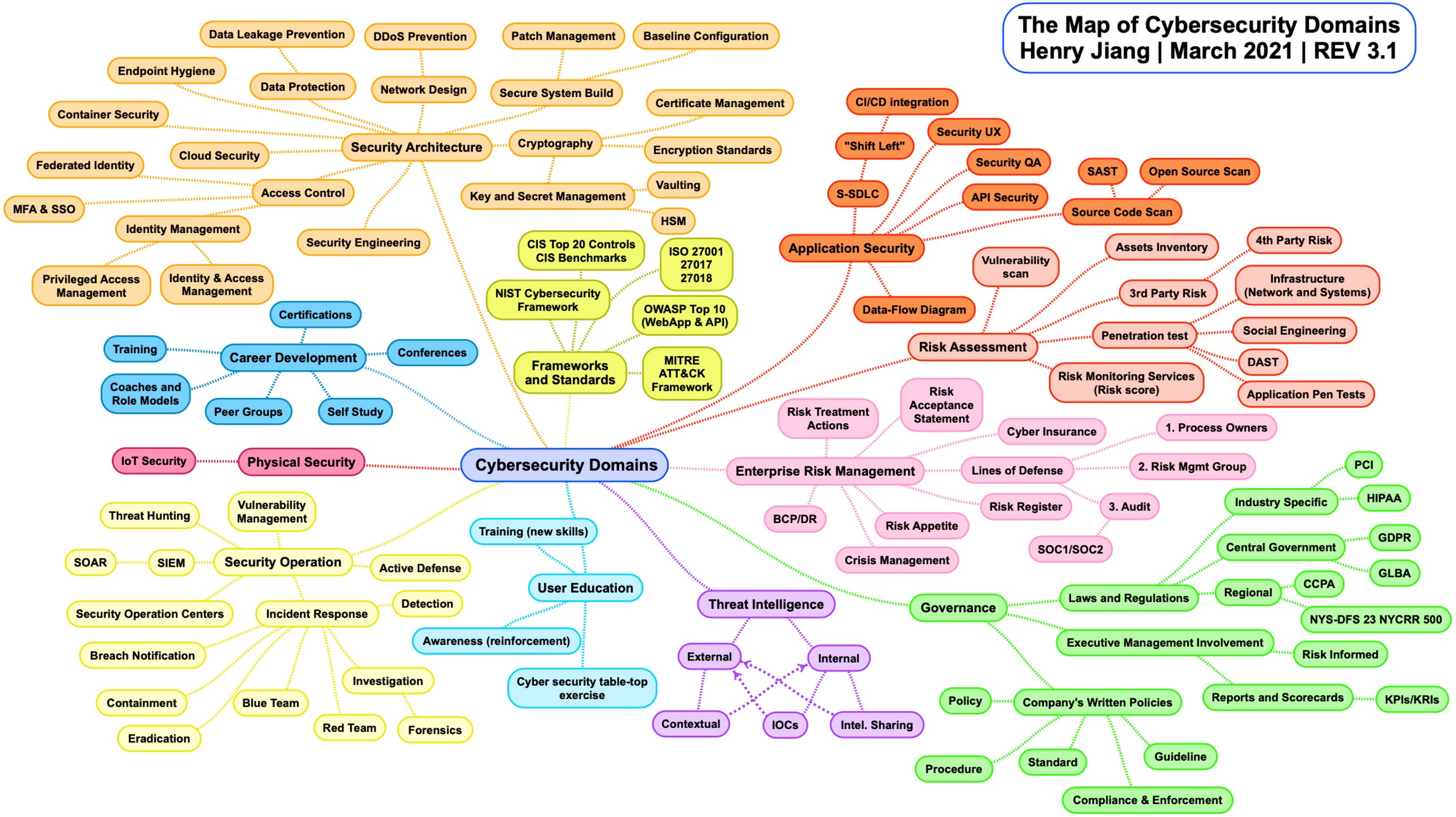
- Data Source Gap Analysis
- Use Case Catalog
- Asset and Identity Management
- Testing Lab/Attack Simulations
  - Building a Test Lab
  - Attack Simulation Tools

DATA SOURCE GAP ANALYSIS – BY TECHNOLOGY

Category	Data Source Type	Current State	Use Case Recommendations	Category Observations & Recommendations
Network & Security	AV/HIPS		Malware	
	Network FW		Early detection, connections to bad destinations	
	NIDS/NIPS		XSS injection, vulnerability detection	
	Database		Unauthorized use	
	Email Server/Mail gateway		Phishing, data exfiltration	
	WAF/Web Proxy/Content Filtering		Blacklisted web sites, malicious files	
	EDR		Advanced threats - full kill chain detection	
	System/File Integrity Checker		Unauthorized file changes	
	SIEM		Full kill chain detection	
	CASB		Unauthorized access, data loss, performance issues	
	DLP		Data exfiltration	
	EDR		Advanced threats - full kill chain detection	
System & Apps	NetFlow		Unauthorized traffic/ports, unusual traffic	
	System (OS)		Unauthorized privileged access/changes, errors	
	Virtual		Unauthorized privileged access/changes, errors	
Identity & Access	Physical access control		Unauthorized/abnormal access	
	Remote Access & VPN		Login from suspicious location	
	Wireless Access		Rogue access point	
	Identity & SSO		Unauthorized privileged access	
	NAC		Unauthorized connection	
Threat & Vulnerability	Vulnerability scanner		Identified exploits, attacks on known vulnerabilities	
	Honeypot		Preemptive attacks	
	External/Internal TI Feed		External/internal attacks from known bad sites	
	User behavior monitoring		Unusual user behavior	

ISACA®

DATA SOURCE GAP ANALYSIS – BY DOMAIN



The Map of Cybersecurity Domains
Henry Jiang | March 2021 | REV 3.1

Cybersecurity Domains

Security Architecture
- Data Protection
  - Data Leakage Prevention
- Network Design
  - DDoS Prevention
- Secure System Build
  - Patch Management
  - Baseline Configuration
- Endpoint Hygiene
- Container Security
- Cloud Security
- Cryptography
  - Certificate Management
  - Encryption Standards
  - Key and Secret Management
    - Vaulting
    - HSM
- Access Control
  - Federated Identity
  - MFA & SSO
  - Identity Management
    - Privileged Access Management
    - Identity & Access Management
- Security Engineering

Career Development
- Certifications
- Training
- Conferences
- Coaches and Role Models
- Peer Groups
- Self Study

Frameworks and Standards
- CIS Top 20 Controls CIS Benchmarks
- ISO 27001 27017 27018
- NIST Cybersecurity Framework
- OWASP Top 10 (WebApp & API)
- MITRE ATT&CK Framework

Application Security
- CI/CD integration
- "Shift Left"
- S-SDLC
- Security UX
- Security QA
- API Security
- Source Code Scan
  - SAST
  - Open Source Scan
- Data-Flow Diagram

Risk Assessment
- Vulnerability scan
- Assets Inventory
- 3rd Party Risk
  - 4th Party Risk
- Penetration test
  - Infrastructure (Network and Systems)
  - Social Engineering
  - DAST
  - Application Pen Tests
- Risk Monitoring Services (Risk score)

Physical Security
- IoT Security

Enterprise Risk Management
- Risk Treatment Actions
- Risk Acceptance Statement
- Cyber Insurance
- Lines of Defense
  - 1. Process Owners
  - 2. Risk Mgmt Group
  - 3. Audit
- Risk Register
- SOC1/SOC2
- BCP/DR
- Risk Appetite
- Crisis Management

Security Operation
- Threat Hunting
- Vulnerability Management
- SIEM
  - SOAR
- Active Defense
- Security Operation Centers
- Incident Response
  - Detection
  - Breach Notification
  - Containment
  - Eradication
  - Blue Team
  - Red Team
  - Investigation
  - Forensics

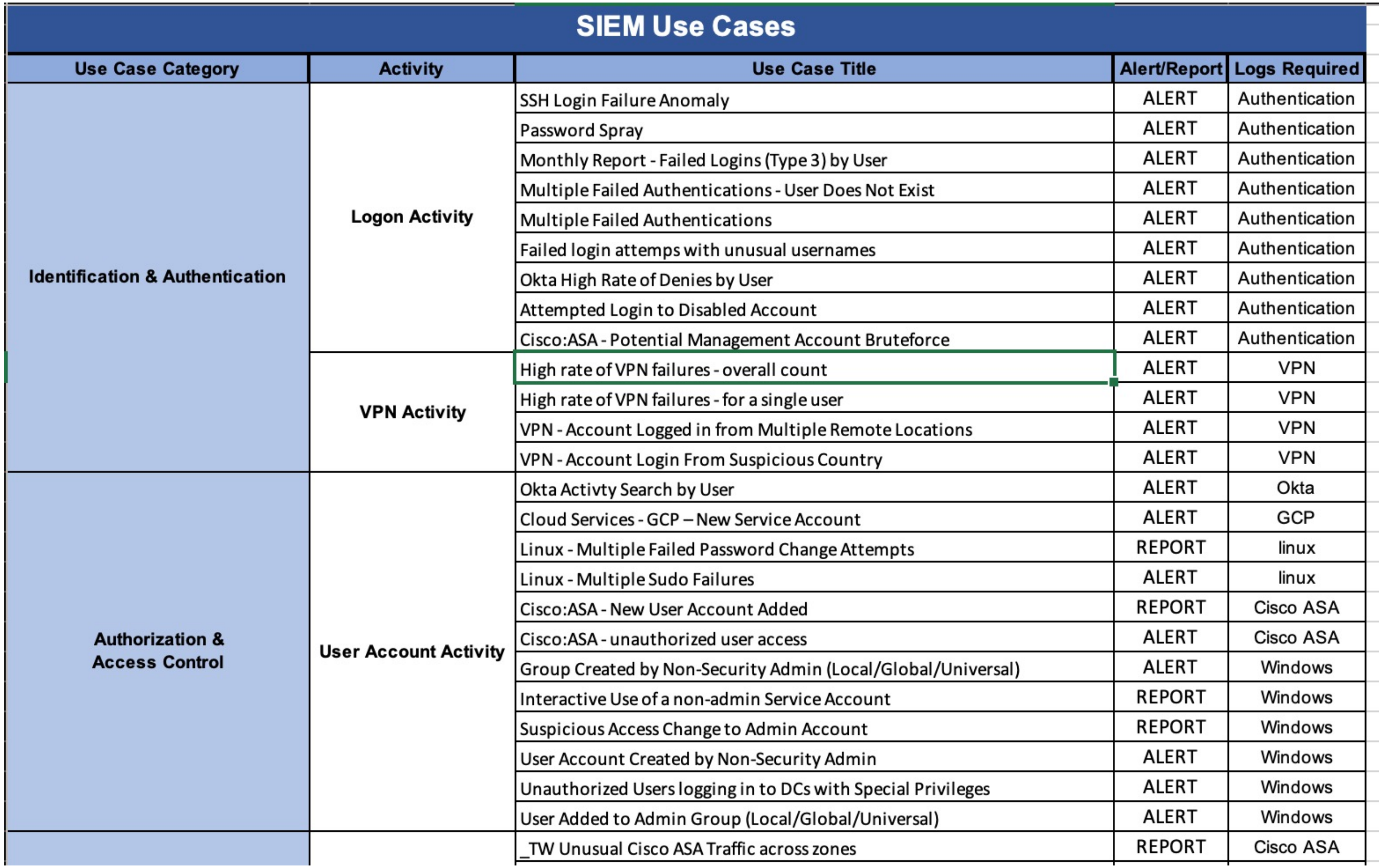
User Education
- Training (new skills)
- Awareness (reinforcement)
- Cyber security table-top exercise

Threat Intelligence
- External
- Internal
- Contextual
- IOCs
- Intel. Sharing

Governance
- Laws and Regulations
  - Industry Specific
    - PCI
    - HIPAA
  - Central Government
    - GDPR
    - GLBA
  - Regional
    - CCPA
    - NYS-DFS 23 NYCRR 500
- Executive Management Involvement
  - Risk Informed
  - Reports and Scorecards
    - KPIs/KRIs
- Company's Written Policies
  - Policy
  - Procedure
  - Standard
  - Guideline
  - Compliance & Enforcement

USE CASE CATALOG

- Use Cases can apply to any technology, but often discussed with SIEM.
- Critical planning tool for any security infrastructure
- Dependent on the available analytics.
- Should be considered a living document, requiring regular review/updates.



SIEM Use Cases

Use Case Category	Activity	Use Case Title	Alert/Report	Logs Required
Identification & Authentication	Logon Activity	SSH Login Failure Anomaly	ALERT	Authentication
		Password Spray	ALERT	Authentication
		Monthly Report - Failed Logins (Type 3) by User	ALERT	Authentication
		Multiple Failed Authentications - User Does Not Exist	ALERT	Authentication
		Multiple Failed Authentications	ALERT	Authentication
		Failed login attemps with unusual usernames	ALERT	Authentication
		Okta High Rate of Denies by User	ALERT	Authentication
		Attempted Login to Disabled Account	ALERT	Authentication
		Cisco:ASA - Potential Management Account Bruteforce	ALERT	Authentication
	VPN Activity	High rate of VPN failures - overall count	ALERT	VPN
		High rate of VPN failures - for a single user	ALERT	VPN
		VPN - Account Logged in from Multiple Remote Locations	ALERT	VPN
		VPN - Account Login From Suspicious Country	ALERT	VPN
Authorization & Access Control	User Account Activity	Okta Activty Search by User	ALERT	Okta
		Cloud Services - GCP – New Service Account	ALERT	GCP
		Linux - Multiple Failed Password Change Attempts	REPORT	linux
		Linux - Multiple Sudo Failures	ALERT	linux
		Cisco:ASA - New User Account Added	REPORT	Cisco ASA
		Cisco:ASA - unauthorized user access	ALERT	Cisco ASA
		Group Created by Non-Security Admin (Local/Global/Universal)	ALERT	Windows
		Interactive Use of a non-admin Service Account	REPORT	Windows
		Suspicious Access Change to Admin Account	REPORT	Windows
		User Account Created by Non-Security Admin	ALERT	Windows
		Unauthorized Users logging in to DCs with Special Privileges	ALERT	Windows
		User Added to Admin Group (Local/Global/Universal)	ALERT	Windows
		_TW Unusual Cisco ASA Traffic across zones	REPORT	Cisco ASA

ASSET AND IDENTITY MANAGEMENT

- Often ignored
- Very challenging to triage alerts without good asset and identity management
- Many great vendors to choose from

TESTING LAB/ATTACK SIMULATIONS

Attack Simulations

- Mix of cloud and on-prem Virtual machines
- Much cheaper to build a Hypervisor server than to pay for cloud hours, but you may need both in order to practice various attack scenarios
- Create basic attack scenarios (eg. using atomic red team), add defenses, and practice with both common detections and threat hunting procedures based on entities and MITRE APTs

Attack Simulation Tools

- Great way to test security posture
- Start with free tools like Atomic Red Team, Caldera
- Paid tools: Mandiant/fireeye, Red Canary, Azure Defender

BUILDING A TEST LAB

Include both on-prem and cloud-based resources

- eg. vsphere for on-prem – cheaper than cloud since reliability needs are low.

Get feedback from all levels – Management*, Architects, Devops, Operations

- Share ideas via mindmap, visio, etc.

Tell a story – Pick a ‘threat group’ and plan an attack around that scenario.

- eg. Red Team Ops with Cobalt Strike – MANY threat groups are using this.
- The pdf below maps threat groups by industry – eg. healthcare, financial, etc:
  - https://www.thaicert.or.th/downloads/files/A_Threat_Actor_Encyclopedia.pdf

Plan attack simulations and make it fun.

Purple Team and share the results.

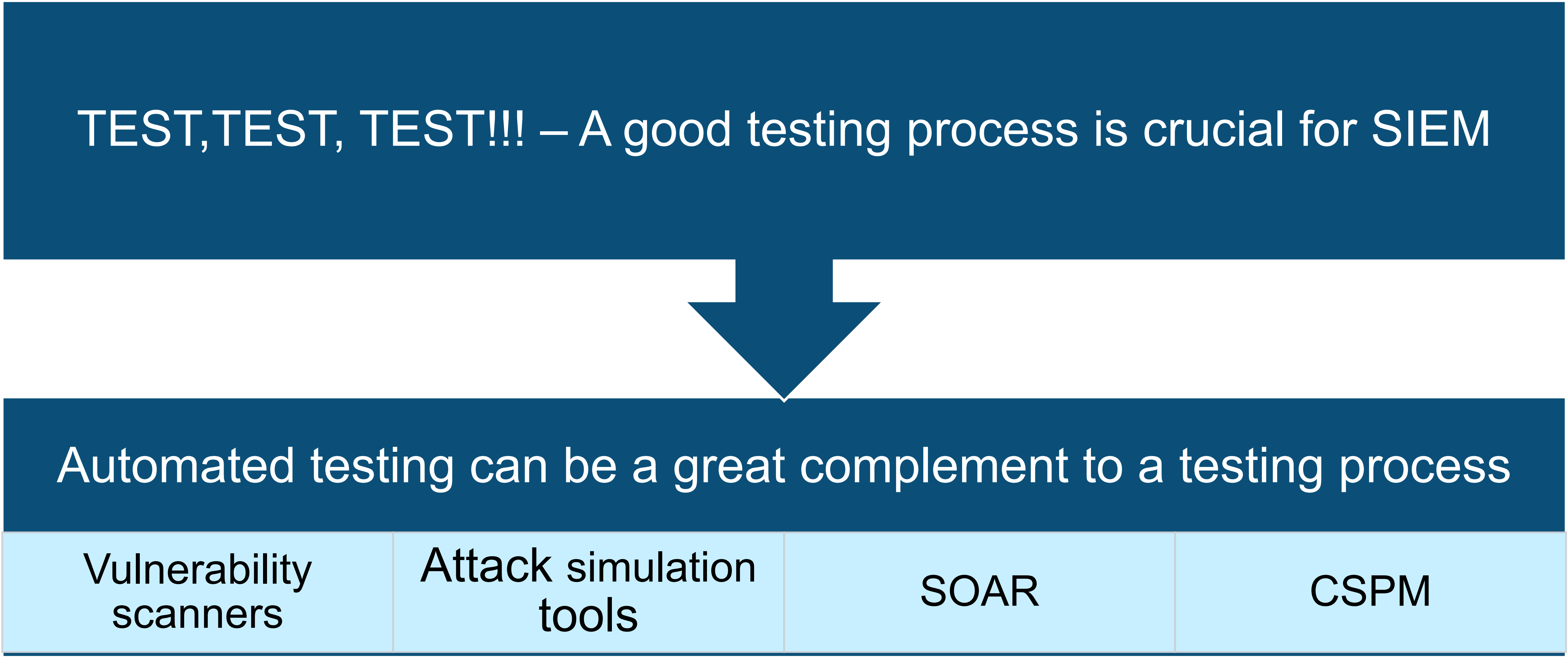
- Make Purple teaming part of your Incident Response procedures.

Get an Azure/AWS/GCP license! cheaper than you think.

Look for pre-built attack labs – eg. github

Rent a lab

CONTINUOUS TESTING



TEST,TEST, TEST!!! – A good testing process is crucial for SIEM

Automated testing can be a great complement to a testing process

Vulnerability scanners	Attack simulation tools	SOAR	CSPM

QUESTION

What additional topics would you consider important to your security solution? (choose 1 or more)

- Security 'diagnostics' – identifying scope requirements for each security domain.
- Building cyber security frameworks and architectures
- Red/blue/purple teaming
- Threat hunting
- Identity access controls
- Attack simulations for specific security domains
- Risk Assessments
- Vulnerability scans
- Security Governance
- Threat Intelligence
- Triage and Incident Response
- Finding/qualifying cyber security staff

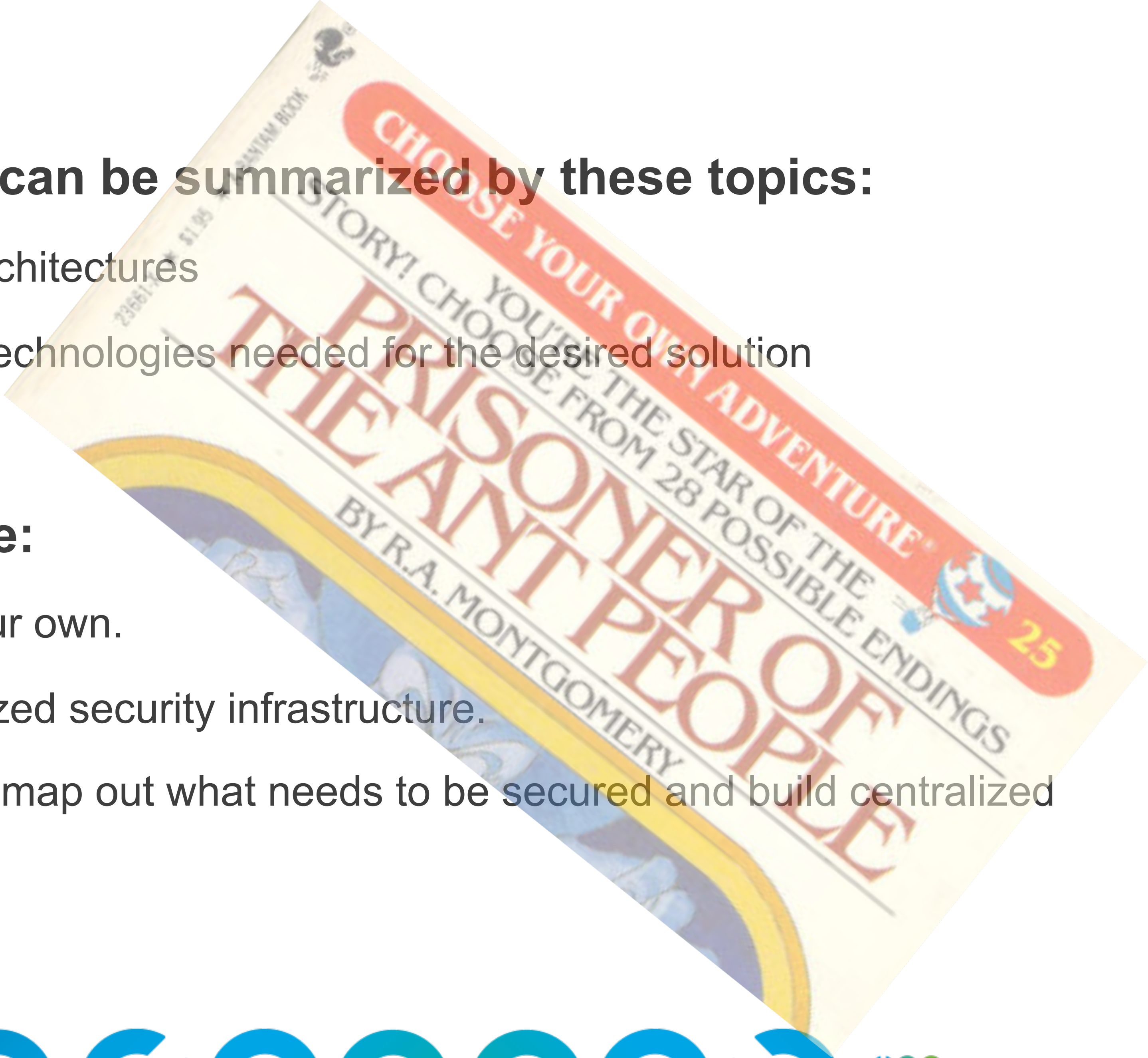
SUMMARY

Securing a hybrid environment can be summarized by these topics:

- Start with Standards, Frameworks, Architectures
- Build out the people, processes and technologies needed for the desired solution

Another more direct perspective:

- Choose your frameworks or make your own.
- Work towards a cloud-based, centralized security infrastructure.
- Consider Zero Trust concepts to both map out what needs to be secured and build centralized policy-based access controls.


CHOOSE YOUR OWN ADVENTURE®
25
YOU'RE THE STAR OF THE STORY! CHOOSE FROM 28 POSSIBLE ENDINGS
PRISONER OF THE ANT PEOPLE
BY R.A. MONTGOMERY
BANTAM BOOK
$1.95

QUESTIONS?

ISACA®

REFERENCES AND RECOMMENDED LINKS

Note: review the comments in the above slides for several more reference links

Short bios for the world's top 10 hackers

AWS: A Cloud Guru

Google Cloud

Azure Architecture with John Savill

Azure Architecture with Matt Soseman

SOC Maturity Framework with Matt Soseman

CSPM
https://www.paloaltonetworks.com/prisma/cloud/cloud-security-posture-management
https://www.netskope.com/products/public-cloud-security
https://docs.microsoft.com/en-us/azure/governance/policy/overview
https://azure.microsoft.com/en-us/resources/videos/azure-friday-cloud-security-posture-management-cspm-with-azure-security-center/
https://azure.microsoft.com/en-in/blog/new-azure-blueprint-simplifies-compliance-with-nist-sp-800-53/
https://docs.microsoft.com/en-us/cloud-app-security/tutorial-cloud-platform-security

RECOMMENDED READING

- Cyber Strategy: Risk-Driven Security and Resiliency
- Hacking Exposed 7: Network Security Secrets and Solutions
- Hacking: The Art of Exploitation, 2nd Edition
- Hands on Hacking: Become an Expert at Next Gen Penetration Testing and Purple Teaming
- How to Hack Like a GHOST: A detailed account of a breach to remember (Hacking the planet Book 8)
- How to Hack Like a GOD: Master the secrets of hacking through real life scenarios (Hacking the planet Book 2)
- How to Hack Like a LEGEND: A hacker’s tale breaking into a secretive offshore company (Hacking the planet Book 7)
- Hunting Cyber Criminals: A Hacker's Guide to Online Intelligence Gathering Tools and Techniques
- Learn Azure Sentinel: Integrate Azure security with artificial intelligence to build secure cloud systems
- Linux Basics for Hackers: Getting Started with Networking, Scripting, and Security in Kali
- Metasploit: The Penetration Tester's Guide
- Microsoft 365 Compliance: A Practical Guide to Managing Risk
- Microsoft Azure Security Infrastructure (IT Best Practices - Microsoft Press)
- Microsoft Azure Sentinel: Planning and implementing Microsoft’s cloud-native SIEM solution (IT Best Practices - Microsoft Press)
- PTFM: Purple Team Field Manual
- Pentesting Azure Applications: The Definitive Guide to Testing and Securing Deployments
- Red Team Development and Operations: A practical guide
- The Hacker Playbook 3: Practical Guide To Penetration Testing
- The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws
- Web Application Defender's Cookbook: Battling Hackers and Protecting Users
- Zero Trust Security: An Enterprise Guide

This training content (“content”) is provided to you without warranty, “as is” and “with all faults”. ISACA makes no representations or warranties express or implied, including those of merchantability, fitness for a particular purpose or performance, and non-infringement, all of which are hereby expressly disclaimed.

You assume the entire risk for the use of the content and acknowledge that: ISACA has designed the content primarily as an educational resource for IT professionals and therefore the content should not be deemed either to set forth all appropriate procedures, tests, or controls or to suggest that other procedures, tests, or controls that are not included may not be appropriate; ISACA does not claim that use of the content will assure a successful outcome and you are responsible for applying professional judgement to the specific circumstances presented to determining the appropriate procedures, tests, or controls.

ISACA
WEBINARS

THANK YOU FOR ATTENDING THIS ISACA WEBINAR

ISACA