Cloud Security

Core concepts for protecting your cloud infrastructure

Overview

- Identity Management
- OSI Model and various security layers
  - Protecting Web Applications
  - Encryption
- The importance of MITRE
  - CVE / CVSS
  - ATP / XDR / Campaigns
  - Attack Surface
- Tools to get started
- Demo

What is Identity Management

Traditional hosting typically meant having physical equipment in either a rack at a datacenter, or an office somewhere.

Accessing a rack in a datacenter means you are authorized to be there, and trusted as a member of that organization to manage the equipment. Think of Identity Management as a programmatic way to authorize someone accessing a specific resource or performing a specific action.

Zero Trust Security Model

The Zero Trust approach addresses the security concerns that emerge due to the evolving digital landscape. Today, nearly every organization has a mobile, remote or hybrid workforce, cloud applications, data stored in different environments, and devices enrolled from various locations. In the absence of a robust security model, all these factors can inadvertently lead to a major security breach.

Zero Trust Framework

Principle	Description
Verify explicitly	Always authenticate and authorize based on all available data points.
Use least privilege access	Limit user access with Just-In-Time and Just-Enough-Access (JIT/JEA), risk-based adaptive policies, and data protection.
Assume breach	Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

Zero Trust Framework

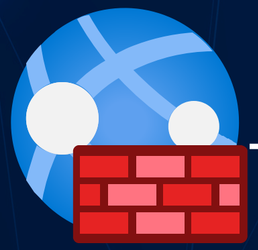
Principle	Description
Verify explicitly	Bearer Tokens / ID Tokens... ***eyj....***
Use least privilege access	Scopes and CAE
Assume breach	Remove access via CAE and Conditional Access

Security Layers

There are many layers to Security. One of the most basic ways to think of the layers of security is to visualize the OSI model.

The OSI (Open Systems Interconnection) model is a conceptual framework that standardizes the functions of a telecommunication or computing system without regard to its underlying internal structure and technology.

OSI model



Layer 7 - WAF

Layer 6 - SSL

Layer 5 - VPN

Layer 4 - TLS

OSI model

Layer 7 - WAF

Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities. Web applications are increasingly targeted by malicious attacks that exploit commonly known vulnerabilities. SQL injection and cross-site scripting are among the most common attacks.

Transport Layer Security (TLS), previously known as Secure Sockets Layer (SSL), is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and encrypted. Application gateway supports both TLS termination at the gateway as well as end to end TLS encryption.

Layer 6 - SSL

Layer 5 - VPN

Azure VPN Gateway is a service that can be used to send encrypted traffic between an Azure virtual network and on-premises locations over the public Internet. You can also use VPN Gateway to send encrypted traffic between Azure virtual networks over the Microsoft network. VPN Gateway uses a specific type of Azure virtual network gateway called a VPN gateway. Multiple connections can be created to the same VPN gateway. When you create multiple connections, all VPN tunnels share the available gateway bandwidth.

OSI model

Layer 7 - WAF

FuseGuard
Azure Web Application Firewall
CloudFlare
Antisamy Policy

Key Vault
Service Accounts
Service Principals (client_secrets)

Layer 6 - SSL

Layer 5 - VPN

Azure VPN (Entra Authentication)
OpenVPN

MIRTE

The Mitre Corporation (stylized as The MITRE Corporation and MITRE) is an American not-for-profit organization with dual headquarters in Bedford, Massachusetts, and McLean, Virginia. It manages federally funded research and development centers (FFRDCs) supporting various U.S. government agencies in the aviation, defense, healthcare, homeland security, and cybersecurity fields, among others.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	C	Exfiltration	Impact
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques		9 techniques	14 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (5)	Abuse Elevation Control Mechanism (5)		tomated filtration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (9)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)		Transfer Size its	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		xfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host			Data Manipulation
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion		Exfiltration Over C2 Channel	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Client Software Binary	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information		Exfiltration Over Other Network Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Create Account (3)	Domain Policy Modification (2)	Deploy Container		Exfiltration Over Physical Medium (1)	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 (4)	Escape to Host	Direct Volume Access		Exfiltration Over Web Service (4)	Financial Theft
Search Open Websites/Domains (3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (16)	Event Triggered Execution (16)	Domain Policy Modification (2)		Scheduled Transfer	Firmware Corruption
Search Victim-Owned Websites		Valid Accounts (4)	Shared Modules	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails (1)		Transfer Data to Cloud Account	Inhibit System Recovery
			Software Deployment Tools	Hijack Execution Flow (12)	Hijack Execution Flow (12)	Exploitation for Defense Evasion			Network Denial of Service (2)
			System Services (2)	Implant Internal Image	Process Injection (12)	File and Directory Permissions Modification (2)			Resource Hijacking
			User Execution (3)	Modify Authentication Process (8)	Scheduled Task/Job (5)	Hide Artifacts (11)			Service Stop
			Windows Management Instrumentation	Office Application Startup (6)	Valid Accounts (4)	Hijack Execution Flow (12)			System Shutdown/Reboot
				Power Settings		Impair Defenses (11)			
				Pre-OS Boot (5)		Impersonation			
				Scheduled		Indirect Command Execution			
						Masquerading (9)			
						Modify Authentication Process (8)			
						Modify Authentication Process (8)			
						Multi-Factor Authentication Interception			
						Multi-Factor Authentication Request Generation			
						Network Sniffing			
						OS Credential Dumping (8)			
						Steal Application Access Token			
						Steal or Forge Authentication Certificates			
						Steal or Forge Kerberos Tickets (4)			
							File and		
							Group Policy Dis		
							Log Enumeration		
							Network Service Discovery		
							Network Share Discovery		
							Network Sniffing		
							Password Policy Discovery		
							Peripheral Device Discovery		
							Permission Groups Discovery (3)		
							Process Discovery		
							Query Registry		
							Input Capture		
							Forge We Credentia		
							Forced A		
							Explo Creden		
							C Pa		
							B		
								nel (2)	
								nels	
								ol Transfer	
								ti-Stage Channels	
								Non-Application Layer Protocol	
								Non-Standard Port	
								Protocol Tunneling	
								Proxy (4)	
								Remote Access Software	
								Traffic Signaling (2)	
								Web Service (3)	
								network ed Drive	
								Data from Removable Media	
								Data Staged (2)	
								Email Collection (3)	
								Input Capture (4)	
								Screen Capture	
								Video Capture	

MIRTE Continuned

- Common Vulnerabilities and Exposures (CVE)
- Common Vulnerability Scoring System (CVSS)
- Understanding MITRE Tactics
- Defending against MITRE tactics

CVE

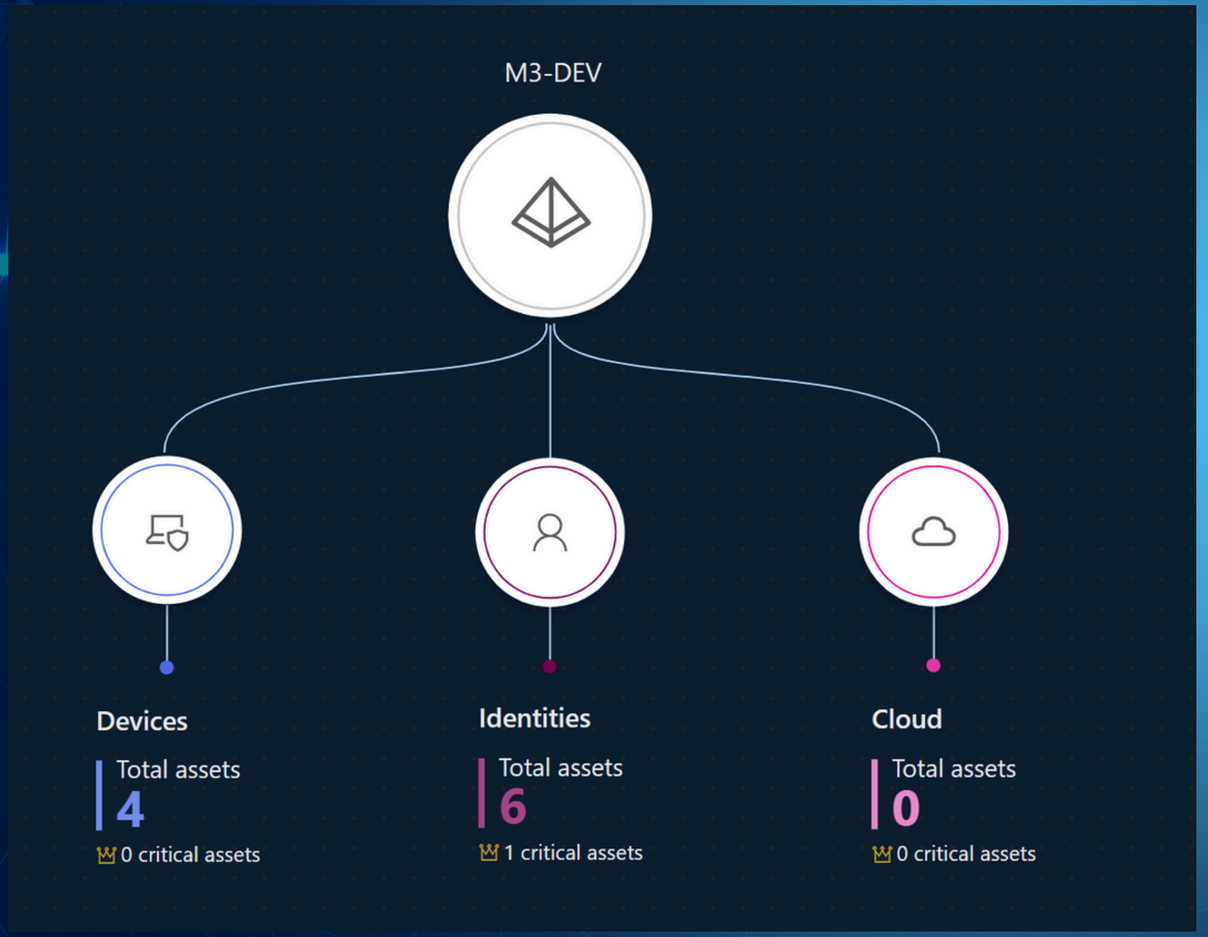
Origin: The CVE system was launched in 1999 by MITRE, a nonprofit that operates research and development centers sponsored by the federal government. It was created to standardize the identification of vulnerabilities.

Purpose: CVE is a list or database of information about security vulnerabilities and exposures. Each entry, known as a CVE Entry, is identified by a unique CVE ID (e.g., CVE-2021-44228, or log4j). This ID allows security professionals to share information about vulnerabilities in a standardized way, ensuring everyone is talking about the same issue without confusion.

CVSS

Common Vulnerability Scoring System (CVSS)
Origin: First released in 2005, CVSS was designed to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. The CVSS is currently maintained by the Forum of Incident Response and Security Teams (FIRST).
Purpose: The CVSS provides an open framework for communicating the characteristics and impacts of IT vulnerabilities.
Its scores range from 0 to 10, where 10 represents the most severe vulnerabilities.

Attack Surface



Tactics

Lateral Movement
Exfiltration
Reconnaissance

Credential Access
Privilege Escalation

Free Tools

- https://msrc.microsoft.com/update-guide/vulnerability
- https://attack.mitre.org/
- https://developer.microsoft.com/en-us/graph/graph-explorer
- https://www.kali.org/get-kali/
  - This is also free on WSL (windows subsystem for linux)

Paid / License

- Advanced Threat Detection
- Web Application Firewall
- Log Analytics

Demo!

Azure Infra

GCP Infra