PENTERA

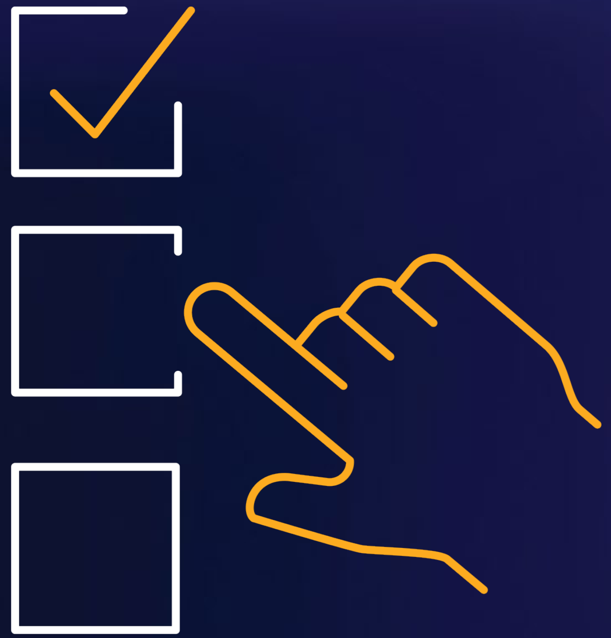
Reduce Your Cyber Exposure with **Pentera Cloud**

SysteCom

The Questions **We Answer:**

AM I **PROTECTED** AGAINST CLOUD-BASED ATTACKS?

HOW CAN I MOST EFFECTIVELY **REDUCE CLOUD EXPOSURE?**

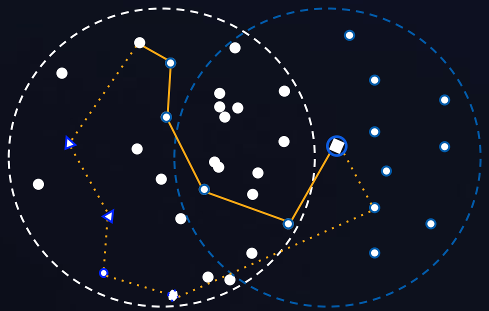


PENTERA

Cloud Security **Challenges**

1 Limited Exposure Visibility

Identifying exploitable cloud-native attack paths

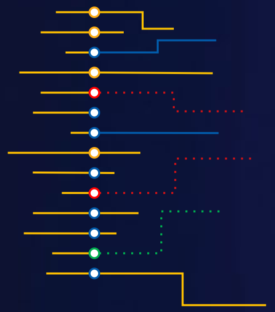


2 IT Environment Complexity

For attackers, complexity = opportunity

3 Ineffective Remediation

Lacking real impact context



SysteCom

Reduce Your **Cloud Security Exposure** with Pentera

1

Test

Resilience to cloud-native attacks

2

Find

Cloud ↔ on-prem exploitable attack paths

3

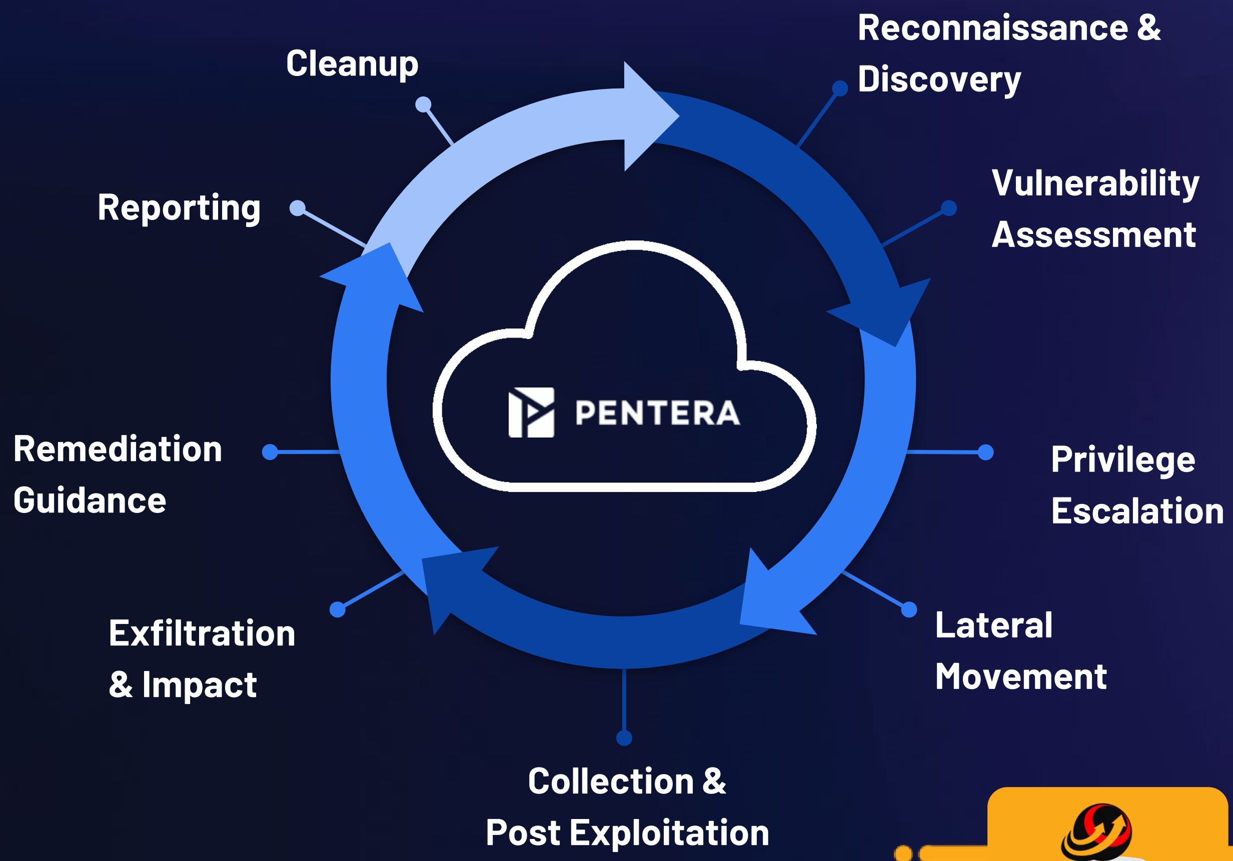
Remediate

Real cloud attack surface exposures

PENTERA

Modeling the Full **Cloud-Native Attack Lifecycle**

AUTOMATED CLOUD PENETRATION TESTING



SysteCom

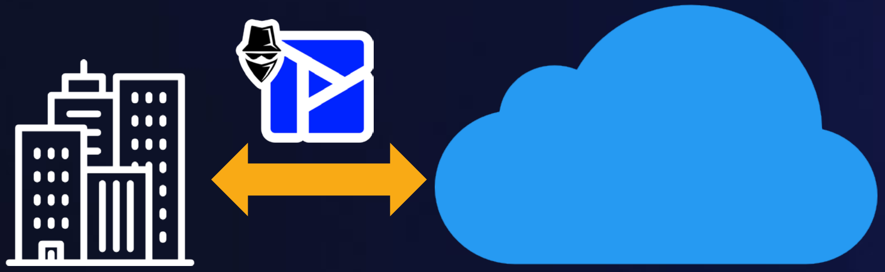
Cloud Penetration Testing **Use Cases**

Cloud Black Box

Cloud Gray Box

Cloud Configuration Review

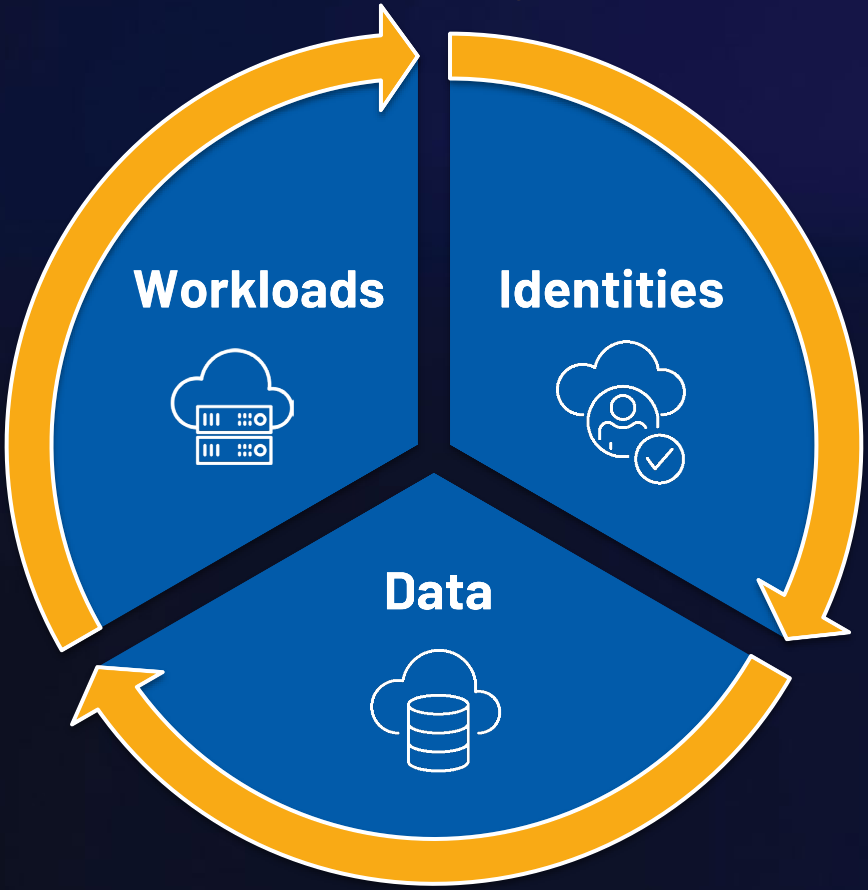
Hybrid Environment Testing



PENTERA

Test Key Cloud-Native Security Gaps

Misconfigurations
Vulnerabilities
Network hygiene
Unpatched resources
Unmanaged assets

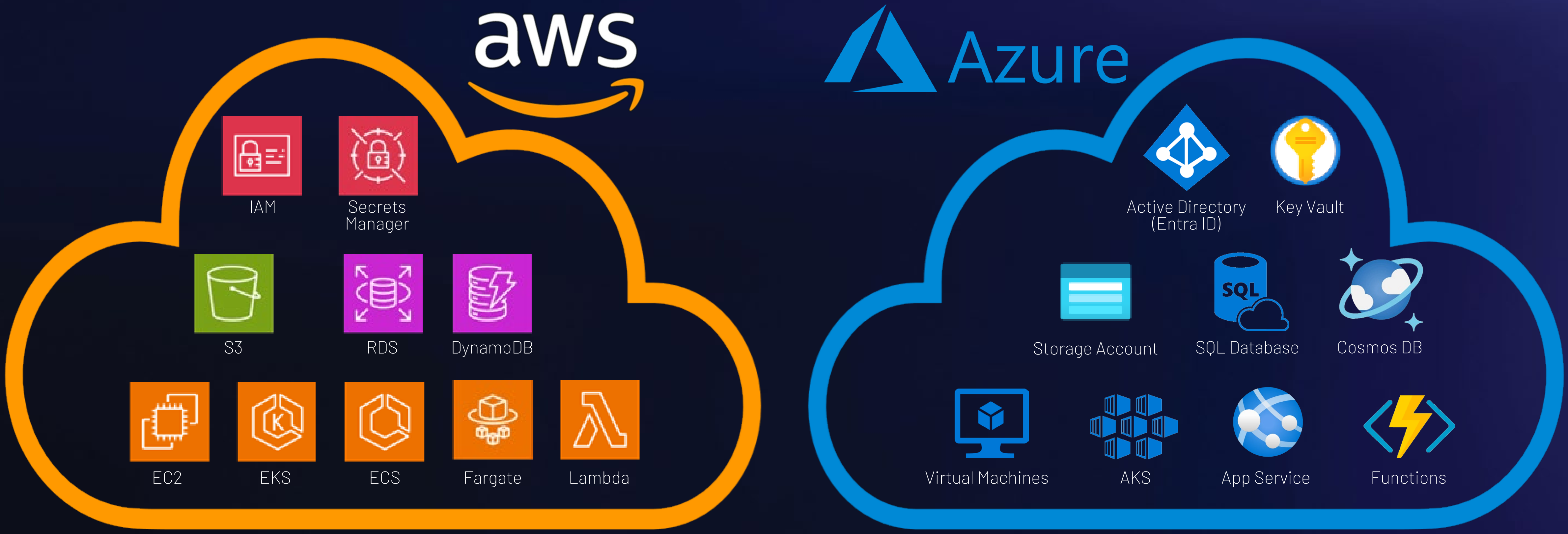


Excessive permissions
Unauthorized access
Neglected accounts
Lack of authentication

Publicly available resources
Exposed sensitive data
Stored credentials
Shadow and abandoned data

SysteCom

Covering the **Most Commonly Used** Services



aws

IAM

Secrets Manager

S3

RDS

DynamoDB

EC2

EKS

ECS

Fargate

Lambda

Azure

Active Directory (Entra ID)

Key Vault

Storage Account

SQL Database

Cosmos DB

Virtual Machines

AKS

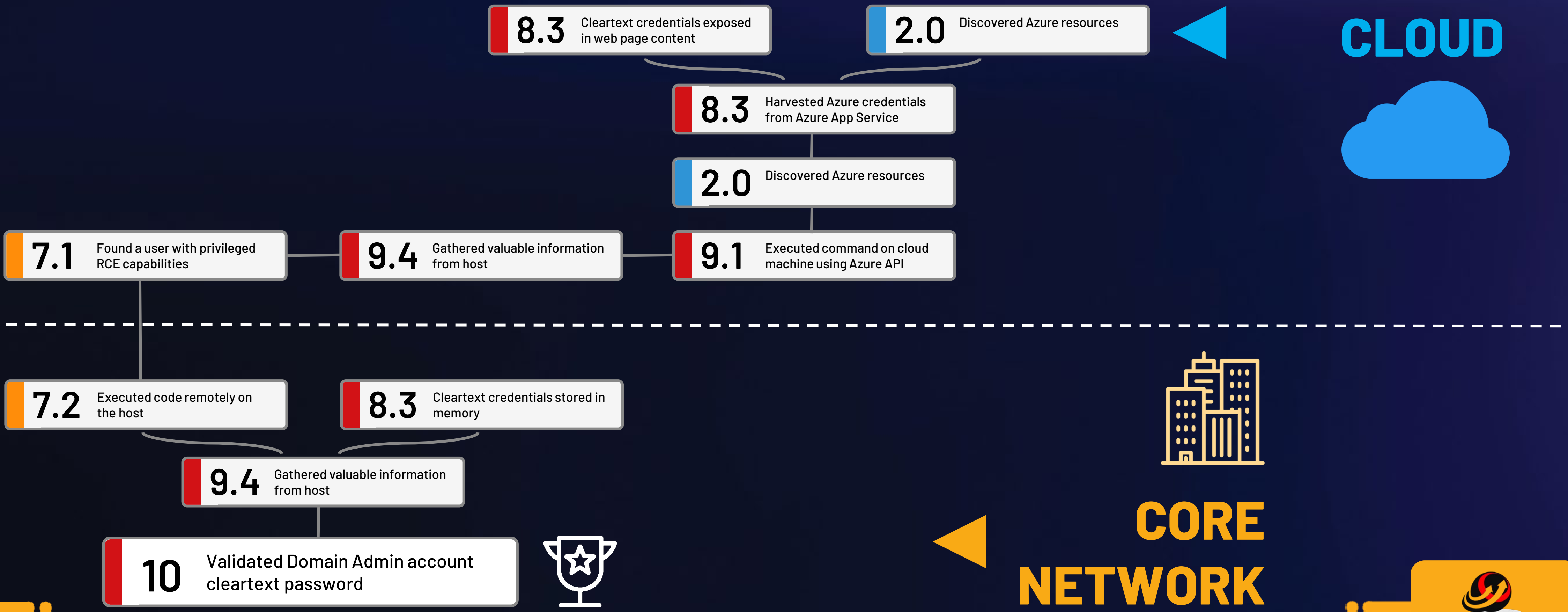
App Service

Functions

PENTERA

Find Exploitable Attack Paths Across Environments

Hybrid Cloud ↔ On-Premises Testing



CLOUD

8.3 Cleartext credentials exposed in web page content

2.0 Discovered Azure resources

8.3 Harvested Azure credentials from Azure App Service

2.0 Discovered Azure resources

9.1 Executed command on cloud machine using Azure API

9.4 Gathered valuable information from host

7.1 Found a user with privileged RCE capabilities

7.2 Executed code remotely on the host

8.3 Cleartext credentials stored in memory

9.4 Gathered valuable information from host

10 Validated Domain Admin account cleartext password

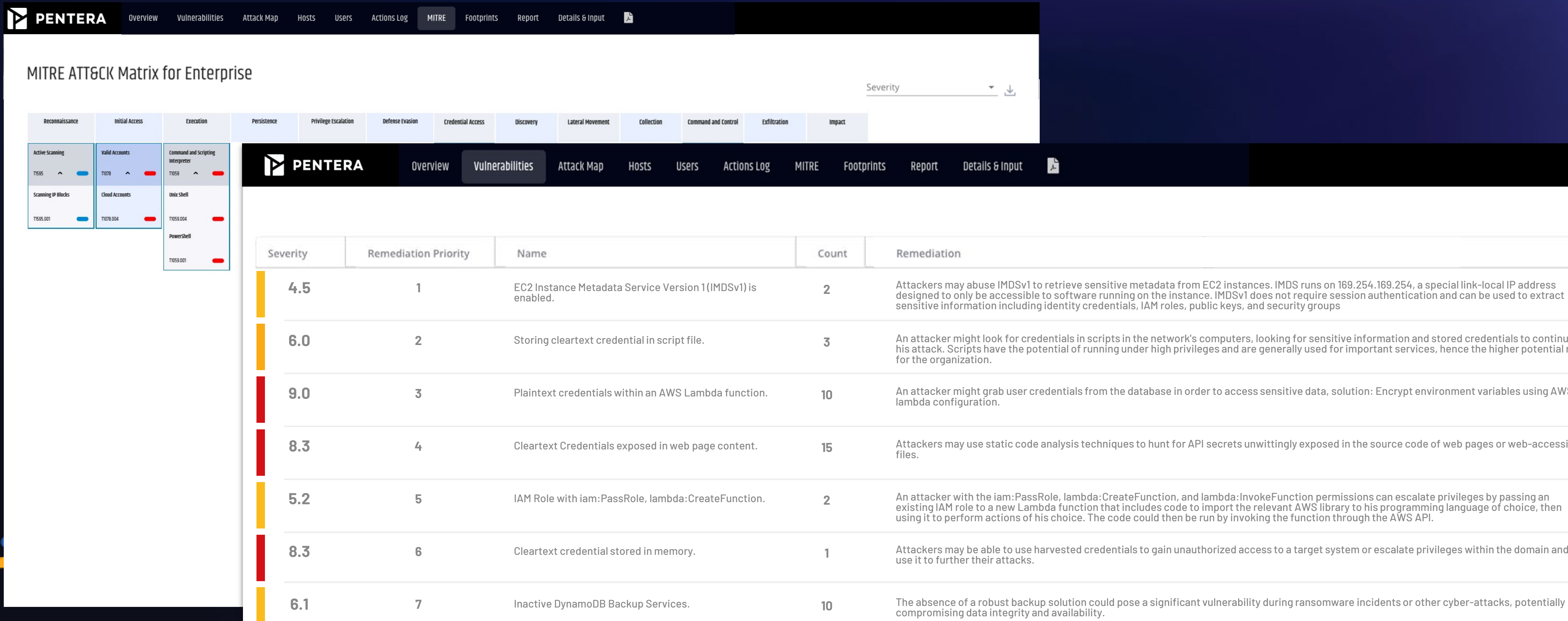
CORE NETWORK

SysteCom

PENTERA

SysteCom

Remediate Based on Evidence



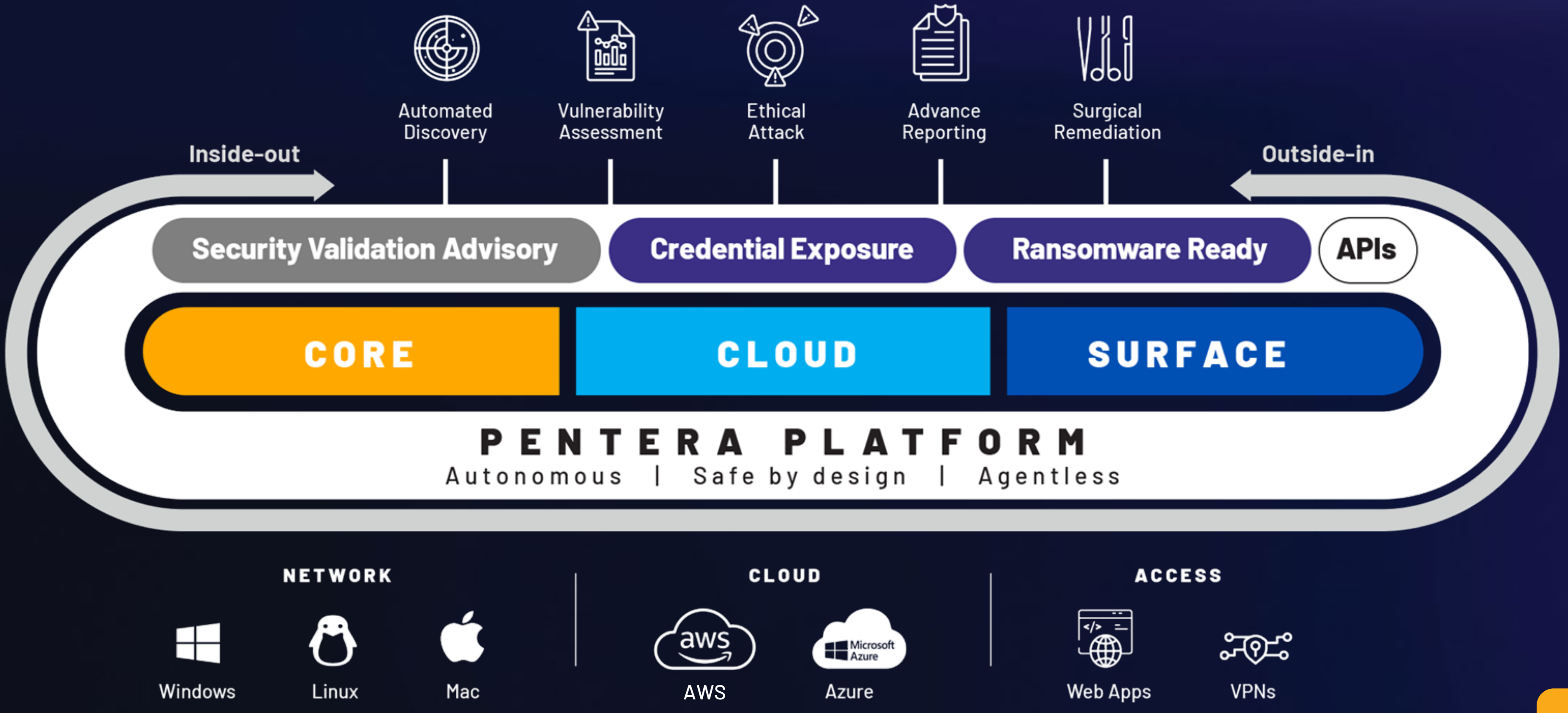
MITRE ATT&CK Matrix for Enterprise

Reconnaissance	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning T1595	Valid Accounts T1078	Command and Scripting Interpreter T1059										
Scanning IP Blocks T1595.001	Cloud Accounts T1078.004	Unix Shell T1059.004										
		PowerShell T1059.001										

Severity	Remediation Priority	Name	Count	Remediation
4.5	1	EC2 Instance Metadata Service Version 1 (IMDSv1) is enabled.	2	Attackers may abuse IMDSv1 to retrieve sensitive metadata from EC2 instances. IMDS runs on 169.254.169.254, a special link-local IP address designed to only be accessible to software running on the instance. IMDSv1 does not require session authentication and can be used to extract sensitive information including identity credentials, IAM roles, public keys, and security groups
6.0	2	Storing cleartext credential in script file.	3	An attacker might look for credentials in scripts in the network's computers, looking for sensitive information and stored credentials to continu his attack. Scripts have the potential of running under high privileges and are generally used for important services, hence the higher potential for the organization.
9.0	3	Plaintext credentials within an AWS Lambda function.	10	An attacker might grab user credentials from the database in order to access sensitive data, solution: Encrypt environment variables using AW lambda configuration.
8.3	4	Cleartext Credentials exposed in web page content.	15	Attackers may use static code analysis techniques to hunt for API secrets unwittingly exposed in the source code of web pages or web-accessi files.
5.2	5	IAM Role with iam:PassRole, lambda:CreateFunction.	2	An attacker with the iam:PassRole, lambda:CreateFunction, and lambda:InvokeFunction permissions can escalate privileges by passing an existing IAM role to a new Lambda function that includes code to import the relevant AWS library to his programming language of choice, then using it to perform actions of his choice. The code could then be run by invoking the function through the AWS API.
8.3	6	Cleartext credential stored in memory.	1	Attackers may be able to use harvested credentials to gain unauthorized access to a target system or escalate privileges within the domain and use it to further their attacks.
6.1	7	Inactive DynamoDB Backup Services.	10	The absence of a robust backup solution could pose a significant vulnerability during ransomware incidents or other cyber-attacks, potentially compromising data integrity and availability.

PENTERA

Pentera Platform: Total Security Validation



SysteCom

PENTERA

COME & SEE US!

Booth: **SysteCom**

Thank you!

SysteCom