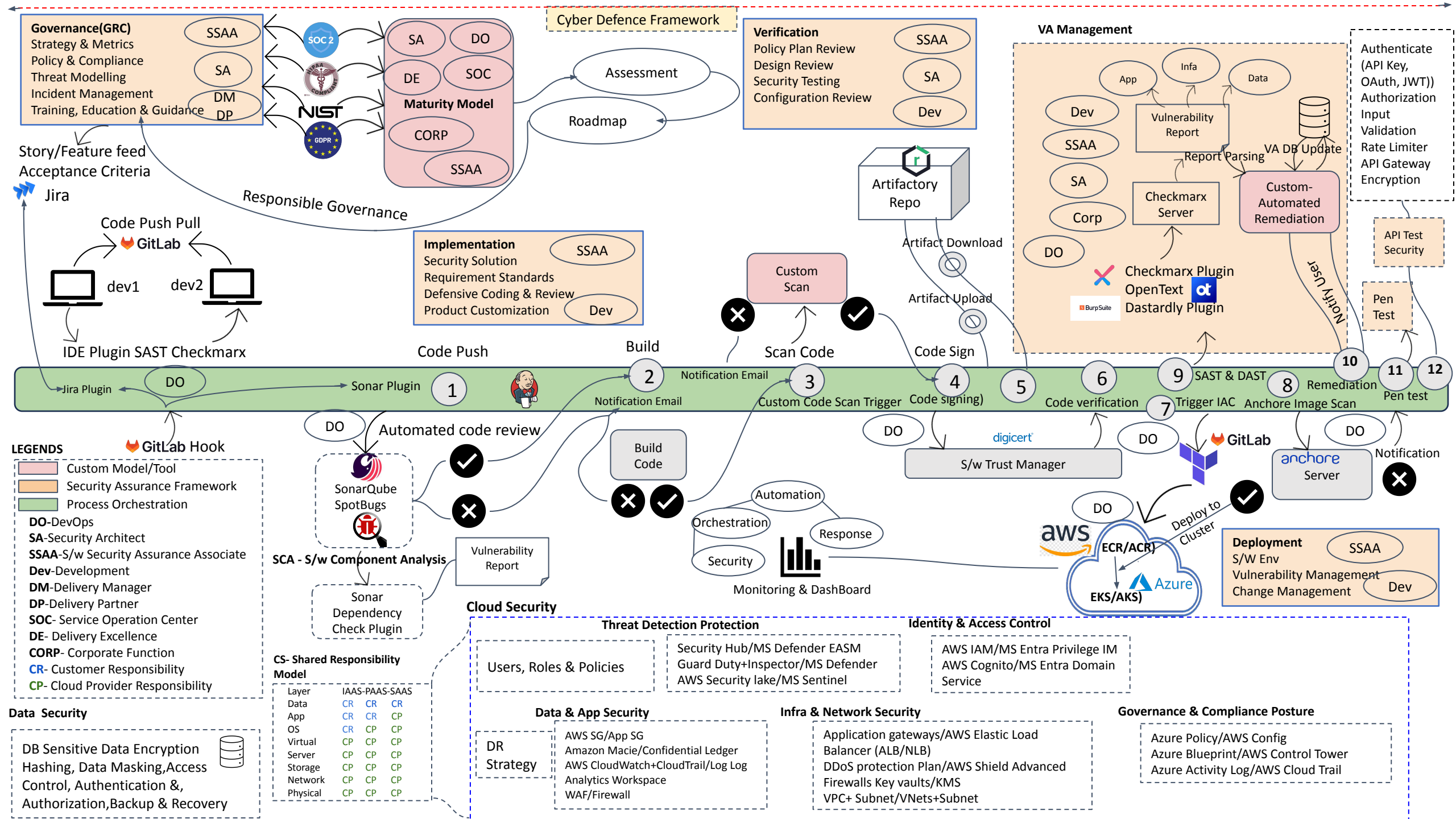
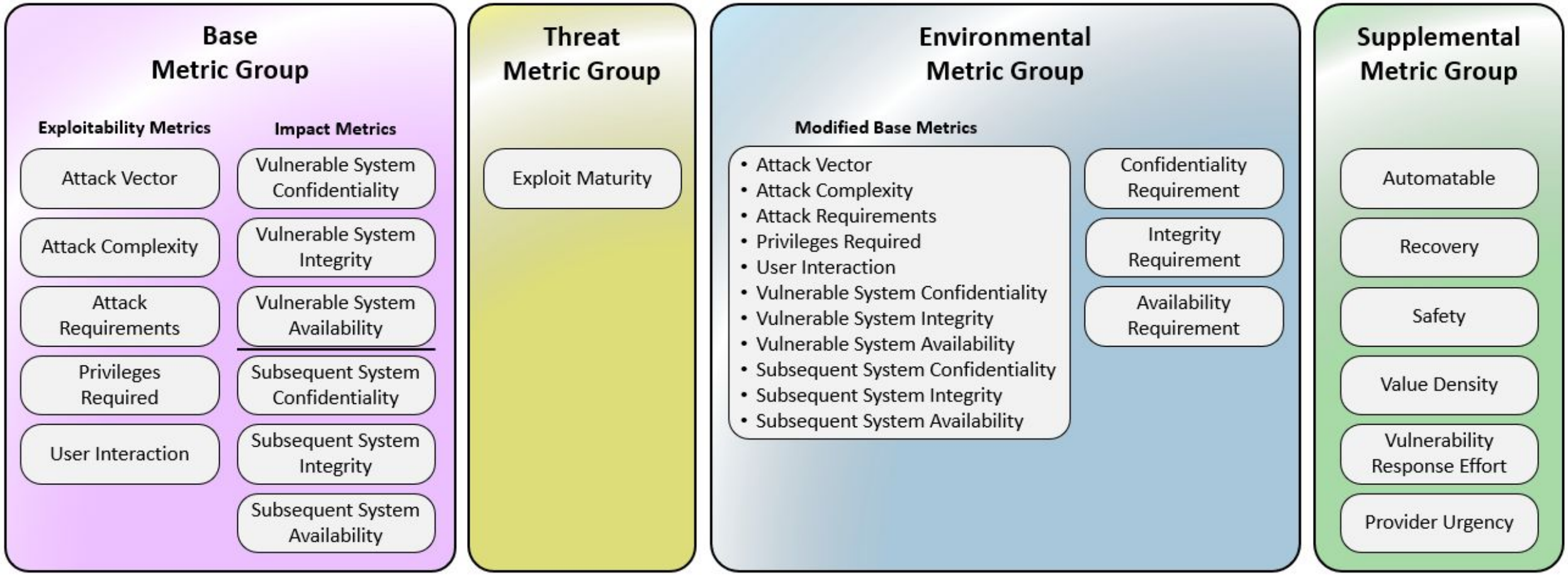
Enterprise Dev-Security-Operation(DSO) Architecture


Cyber Defence Framework
Governance(GRC)
Strategy & Metrics
Policy & Compliance
Threat Modelling
Incident Management
Training, Education & Guidance
SSAA
SA
DM
DP
SOC 2
NIST
GDPR
SA
DO
DE
SOC
Maturity Model
CORP
SSAA
Assessment
Roadmap
Responsible Governance
Story/Feature feed
Acceptance Criteria
Jira
Code Push Pull
GitLab
dev1
dev2
IDE Plugin SAST Checkmarx
Verification
Policy Plan Review
Design Review
Security Testing
Configuration Review
SSAA
SA
Dev
Implementation
Security Solution
Requirement Standards
Defensive Coding & Review
Product Customization
SSAA
Dev
VA Management
App
Infa
Data
Dev
SSAA
SA
Corp
DO
Vulnerability Report
Report Parsing
VA DB Update
Checkmarx Server
Custom-Automated Remediation
Checkmarx Plugin
OpenText
Dastardly Plugin
BurpSuite
Notify User
Authenticate (API Key, OAuth, JWT))
Authorization
Input Validation
Rate Limiter
API Gateway
Encryption
API Test Security
Pen Test
Artifactory Repo
Artifact Download
Artifact Upload
Custom Scan
Scan Code
Code Push
Build
Code Sign
Jira Plugin
DO
Sonar Plugin
1
2
Notification Email
Notification Email
3
Custom Code Scan Trigger
4
Code signing)
5
6
Code verification
9
SAST & DAST
7
Trigger IAC
8
Anchore Image Scan
10
Remediation
11
Pen test
12
GitLab Hook
DO
Automated code review
SonarQube
SpotBugs
Build Code
DO
S/w Trust Manager
digicert
DO
GitLab
DO
anchore
Server
Notification
LEGENDS
Custom Model/Tool
Security Assurance Framework
Process Orchestration
DO-DevOps
SA-Security Architect
SSAA-S/w Security Assurance Associate
Dev-Development
DM-Delivery Manager
DP-Delivery Partner
SOC- Service Operation Center
DE- Delivery Excellence
CORP- Corporate Function
CR- Customer Responsibility
CP- Cloud Provider Responsibility
SCA - S/w Component Analysis
Vulnerability Report
Sonar Dependency Check Plugin
Automation
Orchestration
Response
Security
Monitoring & DashBoard
DO
aws
ECR/ACR)
Azure
EKS/AKS)
Deploy to Cluster
Deployment
S/W Env
Vulnerability Management
Change Management
SSAA
Dev
Cloud Security
Threat Detection Protection
Users, Roles & Policies
Security Hub/MS Defender EASM
Guard Duty+Inspector/MS Defender
AWS Security lake/MS Sentinel
Identity & Access Control
AWS IAM/MS Entra Privilege IM
AWS Cognito/MS Entra Domain Service
CS- Shared Responsibility Model
Layer IAAS-PAAS-SAAS
Data CR CR CR
App CR CR CP
OS CR CP CP
Virtual CP CP CP
Server CP CP CP
Storage CP CP CP
Network CP CP CP
Physical CP CP CP
Data Security
DB Sensitive Data Encryption
Hashing, Data Masking,Access Control, Authentication &, Authorization,Backup & Recovery
Data & App Security
DR Strategy
AWS SG/App SG
Amazon Macie/Confidential Ledger
AWS CloudWatch+CloudTrail/Log Log Analytics Workspace
WAF/Firewall
Infra & Network Security
Application gateways/AWS Elastic Load Balancer (ALB/NLB)
DDoS protection Plan/AWS Shield Advanced
Firewalls Key vaults/KMS
VPC+ Subnet/VNets+Subnet
Governance & Compliance Posture
Azure Policy/AWS Config
Azure Blueprint/AWS Control Tower
Azure Activity Log/AWS Cloud Trail

1. Base Metrics(intrinsic qualities of a vulnerability that are constant over time and across user environments,)
    - Exploitability Metrics
    - Vulnerable System Impact Metrics
    - Subsequent System Impact Metrics
2. Supplemental Metrics(do not modify final score)
3. Environmental(Modified Base Metrics)(Unique to an user environment)
    - Exploitability Metrics
    - Vulnerable System Impact Metrics
    - Subsequent System Impact Metrics
4. Environmental(Security Requirements)
5. Threat Metrics(change over time)


Base
Metric Group
Exploitability Metrics
Attack Vector
Attack Complexity
Attack Requirements
Privileges Required
User Interaction
Impact Metrics
Vulnerable System Confidentiality
Vulnerable System Integrity
Vulnerable System Availability
Subsequent System Confidentiality
Subsequent System Integrity
Subsequent System Availability
Threat
Metric Group
Exploit Maturity
Environmental
Metric Group
Modified Base Metrics
• Attack Vector
• Attack Complexity
• Attack Requirements
• Privileges Required
• User Interaction
• Vulnerable System Confidentiality
• Vulnerable System Integrity
• Vulnerable System Availability
• Subsequent System Confidentiality
• Subsequent System Integrity
• Subsequent System Availability
Confidentiality Requirement
Integrity Requirement
Availability Requirement
Supplemental
Metric Group
Automatable
Recovery
Safety
Value Density
Vulnerability Response Effort
Provider Urgency

Basic Metrics

Attack Vector (**AV**)- (path or method attacker takes)
Phishing, Malware ,Social Engineering,Unpatched Software,Brute Force Attacks,Drive-by Downloads,Insider Threats,Man-in-the-Middle

Attack Complexity (**AC)**- (Difficulty level to exploit vulnerability)
High Target specific bypassing mitigation technique (Race condition in file reading for small time window) address space randomization **(ASLR) or** data execution prevention **(DEP)**
Low Straightforward no special condition requirement (SQl injection)

Attack Requirements (**AR)**-prerequisite deployment and execution conditions or variables of the vulnerable system
None - Does not depend on deployment and execution conditions or variables
Present - Network injection

Privileges Required(**PR**) -level of privileges an attacker must possess *prior to* successfully exploiting the vulnerability.
None - No authentication required to carry on attack (settings files)
examples - SQL Injection on a public-facing web app (no login needed).
Heartbleed (OpenSSL bug) → attacker just connects to the service.
Remote buffer overflow in a service listening on a port.

Low -Non sensitive resource, resources owned by a single low-privileged user
Local Privilege Escalation in Linux (user → root).
Viewing sensitive data in a web app after login (IDOR vulnerability).
WordPress plugin vulnerability that requires attacker to be a logged-in subscriber.

High-privileges that provide significant (e.g., administrative) control (full access)
Vulnerability in Windows Active Directory that requires Domain Admin.
Misconfigured database settings exploitable only by a DBA account.
Cisco router bug requiring privileged EXEC mode access.

User Interaction (**UI**) -requirement for a human user, other than the attacker, to participate in the successful compromise of the vulnerable system.
None - No human interaction needed
example- a remote attacker is able to send packets to a target system a locally authenticated attacker executes code to elevate privileges

Passive-requires limited interaction by the targeted user with the vulnerable system and the attacker's payload
example-

- utilizing a website that has been modified to display malicious content when the page is rendered (most stored **XSS** or **CSRF**)
- running an application that calls a malicious binary that has been planted on the system
- using an application which generates traffic over an untrusted or compromised network (vulnerabilities requiring an on-path attacker)

Active-requires a targeted user to perform specific, conscious interactions with the vulnerable system and the attacker's payload
Examples -

- importing a file into a vulnerable system in a specific manner
- placing files into a specific directory prior to executing code
- submitting a specific string into a web application (e.g. reflected or self XSS) dismiss or accept prompts or security warnings prior to taking an action (e.g. opening/editing a file, connecting a device).

Impact Metrics