Cybersecurity (elemente de securitate informatica)

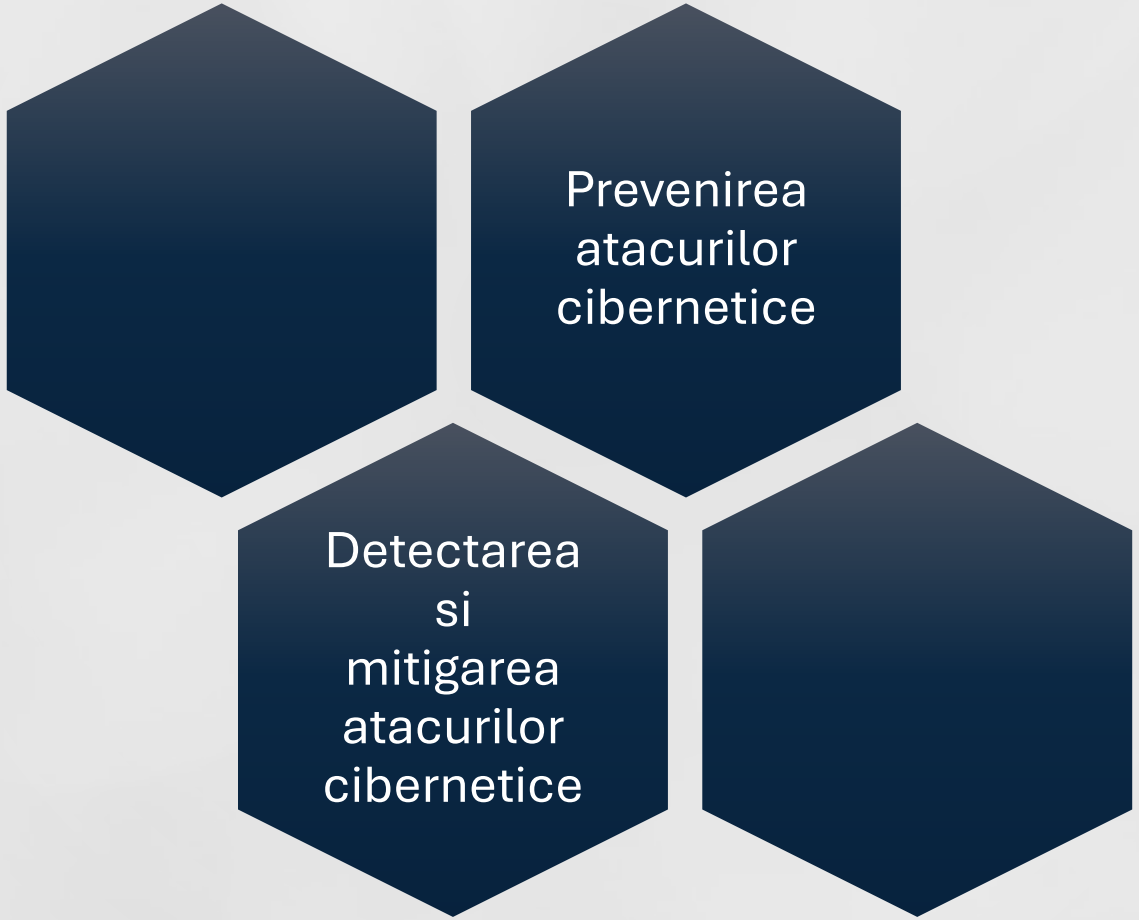
Nutescu Ciprian-Ionut

Software Arhitect Ph.D

Securitate informatica

- Wiki: **Securitatea informatică** este o ramură a informaticii care se ocupă cu identificarea riscurilor implicate de folosirea dispozitivelor informatice, cum sunt calculatoare, smartphone-uri, dar și rețele de calculatoare atât publice cât și private, și cu oferirea de soluții pentru înlăturarea lor.

Elemente ale securitatii ciberneticii



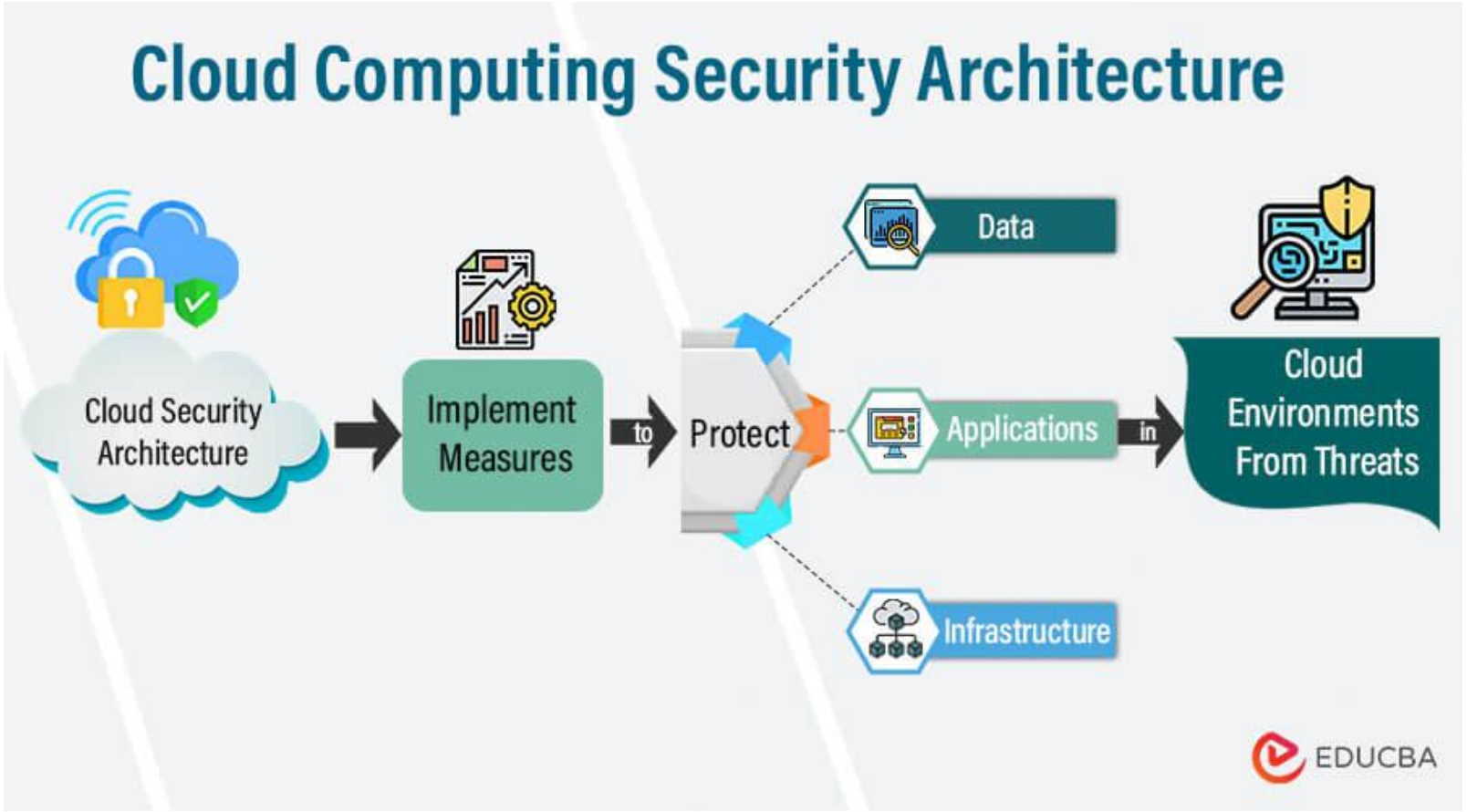
Prevenirea atacurilor cibernetice

- Trebuie sa raspundem la urmatoarele intrebari:
  - Ce vectori de atac putem preveni ?
  - La ce tipuri de atac suntem vulnerabili ?
  - Care este strategia de prevenire ?
    - La ce nivele o putem implementa ? Infrastructura ? Retealistica ? Aplicatie ?
    - Ce vulnerabilitati avem si cum le putem remedia ?
    - Cat de succeptibili suntem in fata unui atac ?
  - Cum ne putem testa propria strategie de prevenire ? Pen-testing?

Detectarea si mitigarea atacurilor cibernetice

- Trebuie sa raspundem la urmatoarele intrebari:
  - Cum putem detecta accesul unui intrus ?
  - La ce nivele acesta poate sa patrunda ? Ne gandim la veriga-cea-mai-slaba. Cel mai usor vector de atac intr-o arhitectura software este veriga cea mai slaba (de obicei cel mai de baza utilizator).
  - Ce putem face odata ce am detectat intrusul ?
  - Care sunt pagubele pe care acesta le poate face ?
  - Cum putem sa prevenim pe viitor acest lucru ?

- Hint: Cel mai bun hacker este cel de care nimeni nu stie ca exista!



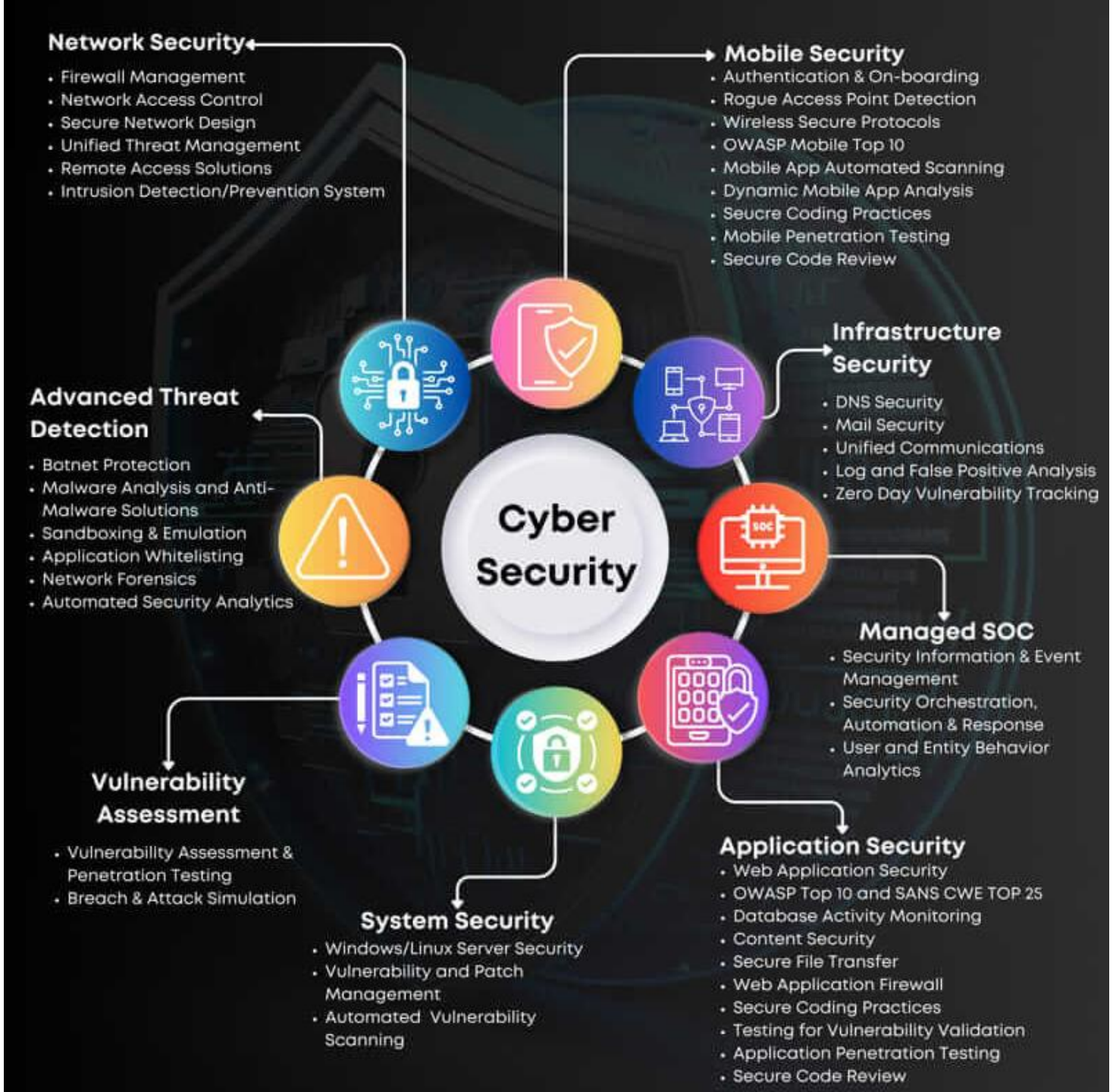
Cloud security

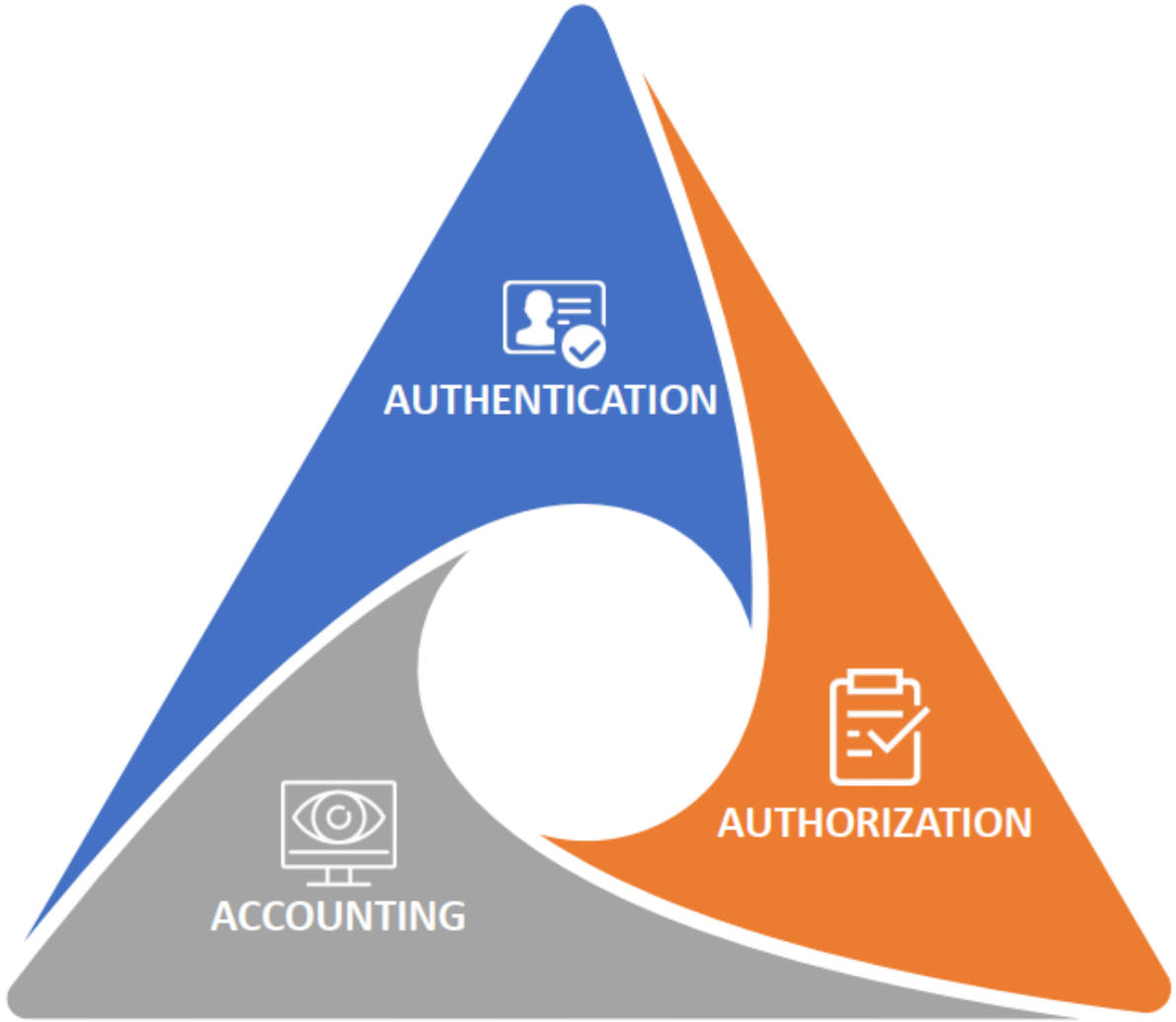
Nivele de securizare ale aplicatiilor (nu doar cloud)

- Nivelul de date:
  - encriptia datelor pe disc
  - encriptia comunicarii intre baza de date si client
  - multiplicarea datelor pentru redundanta
  - limitarea accesului la date (politici de access la date)
  - plasarea bazelor de date si al nivelului de persistenta in cadrul unor retele ascunse (bazele de date nu trebuie sa fie vizibile din Internet!)
  - folosirea strategiilor de CDCR pentru mitigarea riscului in cazul unei infrastructure penetrare/cazute

- Nivelul de infrastructura
  - trebuie vazuta ca niste palisate/fortificatii cu care ne inconjuram aplicatiile software
  - partea de infrastructura reprezinta baza (daca aceasta nu este securizata cum trebuie, partea de date si aplicatie devin foarte usor de accesat/”hack-uit”)
  - se face la nivelul retealisticii/serverelor:
    - configurarea unei retelor/subretelelor, routelor, DNS-uri, firewall-urilor, proxy-urilor, load-balancer-elor, etc… -> principii de baza: minimum-priviledge (spre exemplu se blocheaza toate porturile firewall-ului si se lasa traffic doar de la un numar nimic de porturi cu setul lor de IP-uri destinatie si sursa).
    - configurarea serverelor si masinilor virtuale, alegerea OS-ului cu numarul nimic de vulnerabilitati, politica de actualizare de sistem periodic, cat si al pachetelor instalate, restrictionarea utilizatorilor si crearea de politici stricte (de exemplu nu toata lumea trebuie sa aiba sudo/admin), se poate face penetration-testing doar la nivelul infrastructurii fara aplicatia instalat

- Nivelul de aplicatia:
  - Se aplica pe toate durata software lifecycle policy:
    - la partea de design, se proiecteaza aplicatia astfel incat sa fie cat se poate de sigura
    - la partea de dezvoltare:
      - se verifica dependintele folosite astfel incat sa aiba nimin de vulnerabilitati (de examplu problema dependintelor log4j...)
      - se verifica codul scris (cross-team review) de catre diferiti membri al echipei
      - se verifica codul folosit analizatori static (code-static analyzers: Nesus/SonarQube)
      - se verifica codul prin teste functionale automate in cadrul CICD-ului
      - + alte multe teste
    - la partea de instalarea/deployment:
      - aplicatia comunica doar encriptat cu exteriorul
      - aplicatia se instaleaza doar de anumiti utilizatori experimentati
      - configurarea ei este permisa doar de anumiti utilizatori experimentati (spre exemplu, eroarea umane poate cauza mai multe probleme decat atacurile cibernetice)
      - se poate face penetration-testing si la nivel de aplicatie (nu doar infrastructura)
    - la partea de documentatie:
      - se prezinta eventualele probleme care pot aparea (known-issues)
      - se prezinta anumite API-uri pe care clientii pot integra
      - se prezinta scenario de configurare si de folosire ale aplicatiei


Network Security
Firewall Management
Network Access Control
Secure Network Design
Unified Threat Management
Remote Access Solutions
Intrusion Detection/Prevention System
Mobile Security
Authentication & On-boarding
Rogue Access Point Detection
Wireless Secure Protocols
OWASP Mobile Top 10
Mobile App Automated Scanning
Dynamic Mobile App Analysis
Seucre Coding Practices
Mobile Penetration Testing
Secure Code Review
Infrastructure Security
DNS Security
Mail Security
Unified Communications
Log and False Positive Analysis
Zero Day Vulnerability Tracking
Advanced Threat Detection
Botnet Protection
Malware Analysis and Anti-Malware Solutions
Sandboxing & Emulation
Application Whitelisting
Network Forensics
Automated Security Analytics
Cyber Security
SOC
Managed SOC
Security Information & Event Management
Security Orchestration, Automation & Response
User and Entity Behavior Analytics
Vulnerability Assessment
Vulnerability Assessment & Penetration Testing
Breach & Attack Simulation
System Security
Windows/Linux Server Security
Vulnerability and Patch Management
Automated Vulnerability Scanning
Application Security
Web Application Security
OWASP Top 10 and SANS CWE TOP 25
Database Activity Monitoring
Content Security
Secure File Transfer
Web Application Firewall
Secure Coding Practices
Testing for Vulnerability Validation
Application Penetration Testing
Secure Code Review



AUTHENTICATION

Is the first step in the AAA security process and describes the network or applications way of identifying a user and ensuring the user is whom they claim to be

AUTHORIZATION

Refers to the process of enforcing policies, such as determining the qualities of activities, resources, or services a user is permitted to use

ACCOUNTING

Is the process of keeping track of a user's activity while accessing the network / application

Autentificarea

- Demonstrarea identitatii (cine sunt eu de fapt)
- In sistemele modern : MFA (multi-factor authentication) -> o combinatie intre anumite elemente:
  - something you have: phone_number, app_on_phone, keycard, email_address, etc..
  - something you know: code, password, answer to secret question, otp_code
  - something you are: biometrics (fingerprint, face, eyes, voice, etc..)
- Cu cat avem mai multi factori, cu atat mai greu de spart, dar mai inconvenient pentru utilizator (imaginati-va cat de ciudat ar trebui sa bagati cate 3 parole mereu cand va logati pe email...)
- pentru MFA se foloseste contextul autentificarii/comportament

Autorizarea

- Vine dupa autentificare si raspunde la urmatoarele intrebari: ce poate sa faca utilizator autentificat ? la ce resurse are voie si la ce resurse din sistem nu are voie ?
- De obicei se poate face prin:
  - RBAC (pe baza de roluri) -> cea mai folosita
  - PBAC (pe baza de politici)
  - ACL (pe baza de liste de access)
  - ABAC (pe baza de attribute)
- Ca principii aici, aplicam minimum-priviledge (cel mai mic privilegiu): daca in cadrul functiei utilizatorul nu are dreptul la resursa, nu i se va oferi (se catalogheaza ce resurse are voie si ce nu pe baza Roles&Responsibilities sau fisa postului in RO)

Audit/Accounting

- Vine dupa autorizare
- Tot ce face utlizatorul in sistem este audit si poate fi interogat de catre administrator
- Stergerea auditului unui sistem reprezinta infractiune si puteti fi trasi la raspundere (este asemanator cum ati sterse camera video la un magazine)
- Foarte util pentru sistemele de detectare a intrusilor (spre exemplu, contul vostru este auditat in sistem de SOC ca doriti sa accesati baza de date de productie din Brazilia, in timp ce voi ati lucrat numai din Romania, fara a avea nevoie sa accesati o astfel de resursa -> Alerta de Securitate)
- Puteti fi trasi la raspundere pentru orice actiune faceti in cadrul sistemului informatic ! Majoritatea sistemelor deja implementeaza acest lucru...

SSO – Single Sign-On

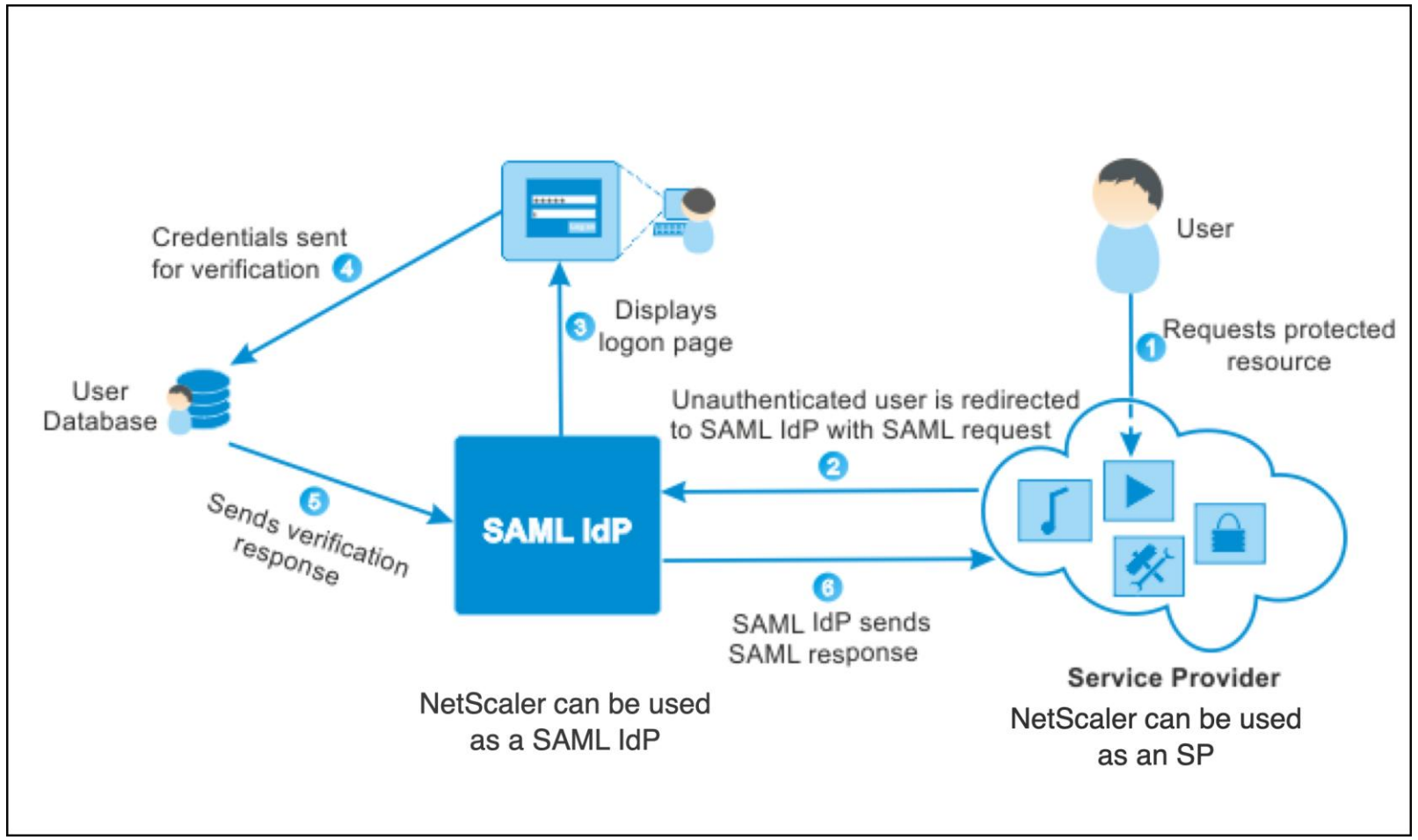
- Este un principiu aplicat pentru sistemele orientate pe servicii
- Ajuta la user-convenience : utilizator se logheaza o singura data, dar are access la mai multe servicii din spate (spre examplu autentificarea in Google : Youtube/Gmail/Hangouts/GoogleDrive/etc...)
- De obicei exista o perioda cat dureaza sesiunea (minute/zile), depinzand de politica de securitate aplicata si de tipul de aplicatie
- Se folosesc doua protocoale mari: SAML/OpenID connect
- Se pastreaza de obicei in cookies sau pe headere detaliile de autentificare/autorizare

SAML vs OpenID connect

PROTOCOL	OpenId	OAuth	SAML
What is it?	Open standard for authentication	Open standard for authorization	Open standard for authorization and authentication
History	Developed by the OpenId Foundation in 2014	Developed by Twitter and Google in 2006	Developed by OASIS in 2001
Current Version	OpenId Connect 1.0 released in 2014	2.0 released in 2012	2.0 released in 2005
Purpose	Provides an authentication layer over OAuth2.0	Enables delegated authorisation for internet resources	Allows 2 web entities to exchange authentication and authorization data
When to use	To authenticate users to your web or mobile app without requiring them to create an account	To provide temporary resource access to a 3rd party application on a legitimate user's behalf	To allow a use or corporate partner to use single sign-on to access a web service
Primary use case	SSO for consumer apps	API authorization	SSO for enterprise apps
Format	JSON	JSON	XML
Supported protocols	XRDS, HTTP	HTTP	HTTP, SOAP, and any protocols that can transport XML

Cum functioneaza SSO

- Doi actori: IDP si SP
- IDP: identity provider (cel care autentifica si autorizeaza)
- SP: service provider (cel care verifica autorizarea si ofera serviciul)
- Cei doi initiaza o relatie de trust apriori (isi fac schimb de metadate)
- Cei doi isi intershimba certificate, care vor fi folosite ca sa semneze diferite asertii de securitate (SAML assertion sau JWT tokens)
- Cei doi comunica musai encriptat

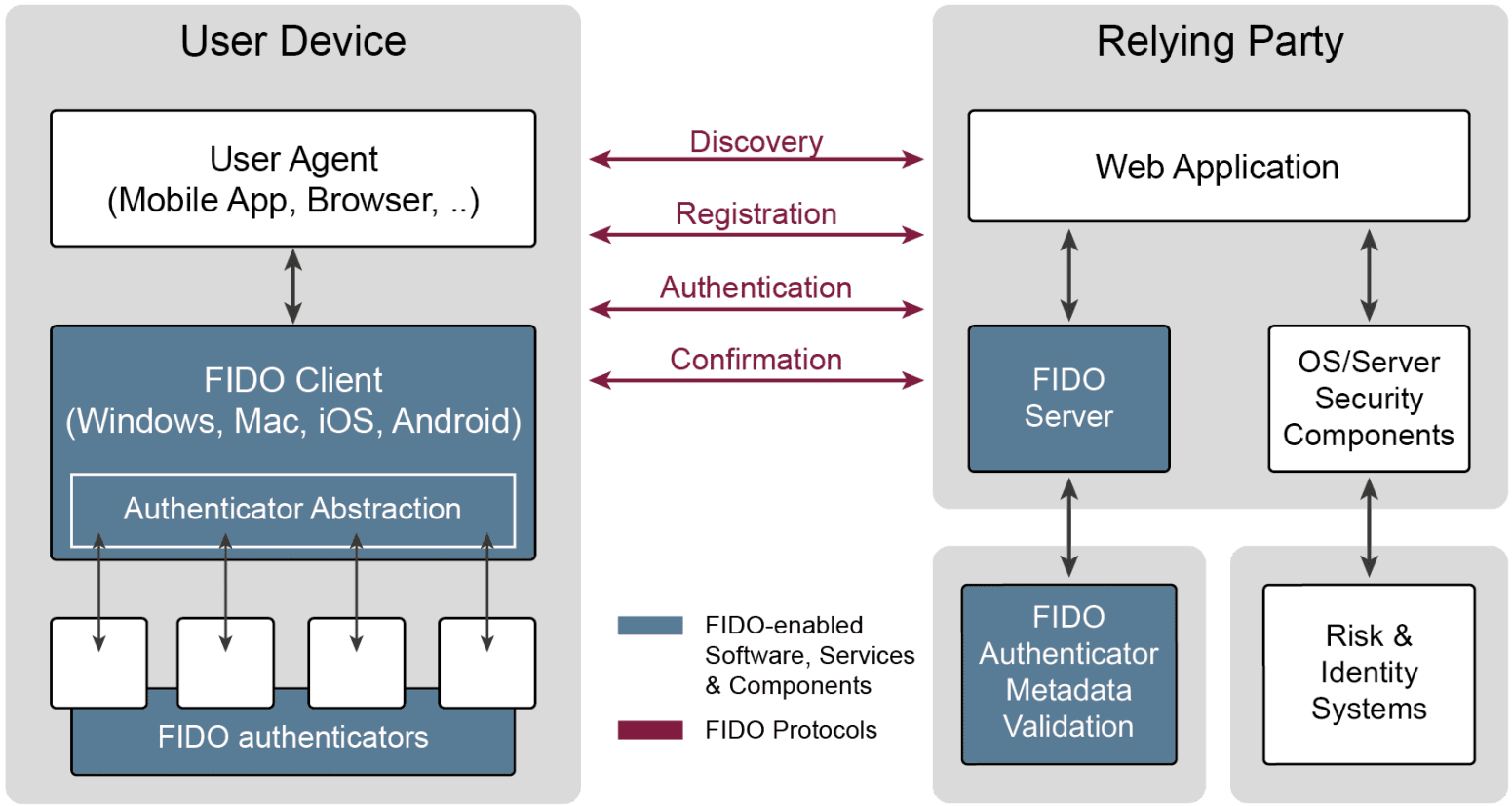


SAML/SSO integration

Pasi pentru autentificare/autorizare

- Utilizatorul acceseaza pagina de serviciu (acesta va avea in cookies sau in headere anumite informatii)
- Daca nu le are, nu este auntentificat -> este redirectat catre IDP pentru autentificare, daca le are poate accesa serviciul
- IDP-ul, pe baza politicii de autentificare poate aplica 1F-A, 2F-A sau MFA
- Daca utilizatorul este autentificat cu success, i se ofera o dovada pentru autorizare (in cadrul SAML se folosc cookies si SAML assertion, pentru OpenID se folosesc JWT tokens)
- Utilizator este redirectionat catre serviciu, care il autorizeaza pe baza dovezii

FIDO architecture



Fido (Fast Identity Online)

- Foloseste un protocol nou (WebAuthN) pe baza a unei relatii de trust intre 3 entitati:
  - Autentificator (cel care autentifica utlizatorul respective)
  - Relying party (cel care este providerul de servicii)
  - Fido server (cel care gestioneaza implementarea si verificariile in cadrul algoritmilor FIDO)
- Se bazeaza pe folosirea biometriei (in detrimentul parolei sau al metodelor mai clasice)
- Dispune de o verificare foarte ampla a tuturor participantilor in cadrul logicii FIDO

Tipuri de atacuri

- DoS and DDoS attacks
- MITM attacks
- Phishing attacks (Whale-phishing attacks)
- Spear-phishing attacks (Targeted)
- Ransomware
- Password attacks
- SQL injection attacks
- Malware attack
- URL interpretation
- DNS spoofing
- Session hijacking
- Brute force attacks
- Web attacks
- Insider threats
- Trojan horses

Malware/Phishing

- Atacatorii cibernetici folosesc software dăunător, cum ar fi spyware, viruși, ransomware și viermi cunoscuți sub numele de malware pentru a accesa datele sistemului. Când faceți clic pe un atașament sau un link rău intenționat, malware-ul se poate instala singur și devine activ pe dispozitivul dvs.
- Atacurile de tip phishing se bazează pe metode de comunicare precum e-mailul pentru a vă convinge să deschideți mesajul și să urmați instrucțiunile din interior. Dacă urmați instrucțiunile atacatorilor, aceștia obțin acces la date personale, cum ar fi cardurile de credit și pot instala programe malware pe dispozitivul dvs.

MITM attacks

- Atacul unui om în mijloc (MITM) este un termen general pentru atunci când un făptuitor se poziționează într-o conversație între un utilizator și o aplicație - fie pentru a asculta cu urechea, fie pentru a uzurpa identitatea uneia dintre părți, făcând să pară un schimb normal de informații. este în derulare.

- Scopul unui atac este de a fura informații personale, cum ar fi datele de conectare, detaliile contului și numerele cardului de credit. Țintele sunt de obicei utilizatorii aplicațiilor financiare, companiilor SaaS, site-urilor de comerț electronic și alte site-uri web unde este necesară autentificarea.

Spoofing

- Atacatorii cibernetici vor imita uneori oameni sau companii pentru a vă păcăli să renunțați la informațiile personale. Acest lucru se poate întâmpla în moduri diferite. O strategie comună de falsificare implică utilizarea unui ID de apelant fals, în care persoana care primește apelul nu vede că numărul este falsificat. Alte metode de falsificare includ subminarea sistemelor de recunoaștere facială, utilizarea unui nume de domeniu fals sau crearea unui site web fals.

Backdoor Trojan

- Atacurile troiene Backdoor implică programe rău intenționate care pot instala în mod înșelător programe malware sau date și pot deschide ceea ce se numește „ușa din spate” pentru sistemul computerului dumneavoastră. Când atacatorii obțin acces la ușa din spate, pot deturna dispozitivul fără ca acesta să fie cunoscut de utilizator.

Ransomware

- Ransomware-ul este un software rău intenționat pe care atacatorii cibernetici îl pot instala pe dispozitivul dvs., permițându-le să vă blocheze accesul până când le plătiți atacatorilor o răscumpărare. Cu toate acestea, plata răscumpărării nu garantează eliminarea software-ului, așa că experții sfătuiesc adesea persoanele să nu plătească răscumpărarea dacă este posibil.

Password attacks

- Atacurile prin parole pot fi la fel de simple ca cineva să ghicească corect parola dvs. sau alte metode, cum ar fi keylogging, în care atacatorii pot monitoriza informațiile pe care le introduceți și apoi pot identifica parolele. Un atacator poate folosi, de asemenea, abordarea de phishing menționată mai sus pentru a se preface ca un site de încredere și pentru a încerca să vă păcălească să vă dezvăluie acreditările contului.

Thank you!

- Q&A...