

CURS 1 - Curs introductiv

Atacatorii care vizează rețelele corporative pot avea diverse scopuri și obiective precum:

- Furt de date sensibile,
- Extorcarea (ransomware) - Atacatorii pot utiliza software de tip ransomware pentru a cripta datele de pe rețelele corporative și apoi solicita o răscumpărare în schimbul cheii de decriptare. Această metodă este utilizată pentru a obține bani de la organizații în schimbul recuperării datelor
- Spionaj industrial

Pentru a spori securitatea, vom folosi urmatoarele metode de preventie:

1. 2FA : (Two-Factor Authentication) sau autentificarea cu doi factori reprezintă o metodă suplimentară de securitate utilizată pentru a proteja conturile și accesul la sisteme. În contextul securității rețelelor corporative, implementarea 2FA poate aduce beneficii semnificative. Iată cum funcționează și de ce este importantă:

Funcționare: implică utilizarea a cel puțin doi dintre cei trei factori principali de autentificare:

- Ceva ce știi: Parola sau codul PIN.
- Ceva ce dești: Dispozitive precum token-uri hardware, carduri inteligente sau smartphone-uri.
- Ceva ce ești: Autentificarea biometrică, cum ar fi scanarea amprentelor digitale sau recunoașterea facială.

Importanța:

Creșterea securității: 2FA adaugă un strat suplimentar de securitate, deoarece un potențial atacator ar trebui să dețină nu doar parola, ci și accesul fizic la un dispozitiv sau informații biometrice.

Protecție împotriva atacurilor de tip phishing: Atacatorii care încearcă să obțină parole prin metode de pescuit (**phishing**) : este o formă de fraudă cibernetică în care atacatorii încearcă să obțină informații sensibile, cum ar fi parole, detalii ale cardurilor de credit sau alte informații personale, pretinzând a fi o entitate de încredere. Această tehnică implică adesea utilizarea mesajelor de e-mail, site-urilor web sau mesajelor text false pentru a manipula oamenii și a-i convinge să dezvăluie informații personale sau să facă

clic pe link-uri malefice) pot avea dificultăți în a accesa un cont protejat cu 2FA, deoarece au nevoie de mai mult decât o simplă parolă.

Reducerea riscului de acces neautorizat: Chiar dacă parola unui utilizator este compromisă, 2FA oferă o barieră suplimentară pentru a preveni accesul neautorizat.

Flexibilitate în implementare: 2FA poate fi implementată în diferite moduri, inclusiv prin mesaje text, aplicații mobile de autentificare, token-uri hardware sau alte tehnologii, oferind organizațiilor opțiuni în funcție de nevoile și resursele lor.

2. SSO (Single Sign-On) reprezintă o altă tehnologie de securitate utilizată în gestionarea accesului la sistemele informatiche.

Autentificare într-un singur pas (Single Sign-On): SSO permite utilizatorilor să acceseze mai multe aplicații și sisteme cu o singură autentificare. Cu alte cuvinte, utilizatorul trebuie să introducă credențialele (de exemplu, nume de utilizator și parolă) o singură dată pentru a obține acces la multiple resurse.

Conveniență și productivitate: Unul dintre principalele avantaje ale SSO este creșterea convenienței și eficienței. Utilizatorii nu mai trebuie să-și amintească și să introducă diverse seturi de credențiale pentru fiecare aplicație sau sistem. Acest aspect poate îmbunătăți productivitatea și poate reduce frustrarea asociată cu gestionarea mai multor parole.

Securitatea în spatele scenei: Chiar dacă SSO face ca procesul de autentificare să fie mai ușor pentru utilizatori, acesta adesea integrează protocoale de securitate puternice în spatele scenei. Protocoale precum SAML (Security Assertion Markup Language) sau OAuth sunt adesea folosite pentru a asigura o autentificare sigură între diferite aplicații.

3. Biometric Authentication:

Autentificarea biometrică este un proces de securitate care utilizează caracteristici unice biologice sau comportamentale pentru a verifica identitatea unei persoane. Această formă de autentificare se bazează pe faptul că anumite trăsături sunt distinctive pentru fiecare individ și dificil de replicat, oferind o modalitate mai sigură de control al accesului în comparație cu metodele tradiționale precum parolele sau codurile PIN.

Exemple de autentificare biometrică:

- Recunoașterea amprentelor
- Recunoașterea facială
- Scanarea irisului sau retinei
- Recunoașterea vocală
- Geometria mâinii
- Recunoașterea modelului venelor
- Biometrice comportamentale

4. Segmentarea rețelei (network segmentation) este o strategie de securitate în care o rețea mare este împărțită în segmente mai mici sau "zone" pentru a limita comunicarea între acestea. Aceasta contribuie la îmbunătățirea securității prin reducerea suprafeței de atac și izolarea potențialelor amenințări.

5 . User provisioning reprezintă procesul de creare, modificare și gestionare a conturilor de utilizator într-un sistem informatic. Acest proces este esențial pentru a asigura că utilizatorii au acces la resursele de care au nevoie în cadrul organizației și pentru a gestiona drepturile și privilegiile lor într-un mod eficient.

6. Monitorizarea posturii dispozitivului (Device Posture Monitoring) se referă la procesul de evaluare și urmărire a stării și a configurației unui dispozitiv (cum ar fi un computer, smartphone sau tabletă) într-o rețea. Scopul principal al acestei monitorizări este să asigure securitatea și conformitatea dispozitivului cu politici specifice sau standarde de securitate. Prin monitorizarea posturii dispozitivului, organizațiile pot evalua dacă un dispozitiv respectă anumite criterii de securitate, cum ar fi:

- Software și Pachete de Securitate: cum ar fi antivirus, firewall și actualizări de securitate.
- Sisteme de Operare Actualizate
- Politici de Parole și Autentificare
- Configurări de Securitate
- Detectarea Dispozitivelor Nedorite sau Neautorizate

7. Custom DNS : DNS (Domain Name System) reprezintă un sistem fundamental în arhitectura internetului care traduce numele de domeniu în adrese IP și facilitează accesul la site-uri web și servicii online.

Atunci când se menționează "custom DNS," se face referire la configurarea unor servere DNS personalizate sau alternative față de cele furnizate implicit de furnizorul de servicii de internet (ISP).

Securitatea cibernetica = starea de normalitate; asigurata prin apararea cibernetica
Apararea cibernetica = totalitatea activităților, mijloacelor și măsurilor utilizate pentru a contracara amenințările cibernetice și a atenua efectele acestora asupra sistemelor de comunicații și tehnologia informației, sistemelor de armament, rețelelor și sistemelor informatice, care susțin capabilitățile militare de apărare.

Securitate cibernetica - obiective:

Obiectivele securității cibernetice includ asigurarea rezilienței și protecției rețelelor și sistemelor informative critice, desemnarea autorităților competente și stabilirea unui cadru legal pentru dezvoltarea capabilităților în securitatea cibernetică, menținerea sau restabilirea climatului de securitate cibernetică națională prin cooperare și coordonare eficientă, stabilirea și separarea responsabilităților între actorii implicați și dezvoltarea unei culturi de securitate cibernetică la nivel național.

Securitate cibernetica - implementare:

- Arhitectura: poate exista sau nu; contine efectiv structura sistemului informational (datele + sistemul => sistem informational)
- Passive defense (aparare pasiva): un firewall, proxy, antivirus; acestea toate adăugate arhitecturii
- Active defense (aparare activa): toate cele de la apărare pasiva; se verifică configurarea lor sau chiar facem configurarea lor dacă nu există
- Intelligence - în securitatea cibernetică are scopul de a furniza informații relevante, o înțelegere mai profundă a amenințărilor și capacitați îmbunătățite de răspuns la incidente pentru a proteja sistemele și datele împotriva atacurilor cibernetice.
- Offense - masuri de auto apărare împotriva adversarilor

RISURI, AMENINȚARI ȘI VULNERABILITĂȚI

Facem management de vulnerabilitati, le prioritizam, asociem riscurile corespunzatoare si dam responsabilitatea.

Amenințare: pericol potențial de compromitere accidentală sau deliberată a securității unui SIC (Sistemul Informatic Centralizat) prin pierderea confidențialității, a integrității sau disponibilității informațiilor și serviciilor.

Vulnerabilitate: o slăbiciune sau lipsă de control de natură tehnică, procedurală sau operațională, care ar putea fi speculată în scopuri ilicite.

Risc: posibilitatea pierderii sau dezvăluirii informațiilor unor persoane neautorizate, modificării neautorizate și/sau distrugerii într-un mod neautorizat al acestora

Caracteristici ale unei amenintari cibernetice: capabilitatea, oportunitatea si intentia.

Riscul poate fi calculat în mai multe feluri în funcție de : impact, probabilitatea de aparitie (analiza de risc calitativa), nr de aparitii si analiza de risc cantitativa.

ATENUAREA RISCURILOR – CONTROALE DE SECURITATE

Un control atenueaza riscul!!

- Controale Tehnice (controlăază acțiunile utilizatorului final și ale sistemului; de exemplu: constrângeri de parole, liste de control al accesului, firewall-uri, criptare a datelor, software antivirus, software de prevenire a intruziunilor etc.)
- Administrative (dictează modul în care trebuie efectuate activitățile; de exemplu: politici, proceduri, linii directoare, standarde; Cartela de acces din atm)
- Operationale (dictează modul de lucru; de exemplu: managementul configurației, răspunsul la incident, conștientizarea; exemplu caz concret: cand cineva nu mai lucreaza la ATM si preda laptop ul primit, acesta trebuie curatat inainte sa fie dat altui angajat)
- Preventive (încercarea de a preveni apariția comportamentului și acțiunilor adverse; de exemplu: firewall, IPS - (Intrusion Prevention System) este un sistem de securitate cibernetică proactiv conceput pentru a detecta, bloca și raporta tentativele de intruziune într-o rețea sau sistem informatic., etc.)
- Descurajatoare (avertizarea unui posibil atacator că nu ar trebui să atace; de exemplu: gard, semn pentru câini etc.)

- Detective (detectează încălcări reale sau tentative ale securității sistemului; de exemplu: senzori IDS etc.)
- Compensatorii (controale de rezervă care intră în joc numai atunci când toate celelalte au eşuat sau nu sunt aplicabile; de exemplu: generator de rezervă)

Reducerea riscului

Riscul il putem mosteni, manageria și poate fi rezidual (= ceea ce ramane)

- **Risc Innascut (Inherent Risk)**: Este nivelul de risc asociat unei activități, proces sau organizații în absența oricărora măsuri de gestionare a riscului. Este riscul natural sau inherent asociat cu o anumită activitate sau mediu, fără a lua în considerare acțiunile intenționate de gestionare a riscului.
- **Risc Gestionat (Managed Risk)**: Este nivelul de risc care rămâne după ce au fost implementate măsuri și strategii de gestionare a riscului. În această etapă, organizațiile identifică, evaluatează și implementează măsuri pentru a controla și a reduce riscul. Riscul gestionat reprezintă, prin urmare, nivelul de risc care persistă după ce au fost aplicate aceste măsuri de gestionare. Dacă nu există controale, riscul gestionat este riscul inherent
- **Risc Residual (Residual Risk)**: Este riscul care rămâne după implementarea măsurilor de gestionare a riscului și reflectă nivelul de risc pe care organizația îl acceptă conștient. Riscul rezidual este ceea ce rămâne, în ciuda tuturor eforturilor de gestionare a riscului, și poate fi o evaluare a riscului net pe care organizația este dispusă să-l suporte sau să-l accepte. Dacă nu există acțiuni suplimentare de atenuare planificate, riscul rezidual este riscul gestionat

Cei 3 piloni ai securitatii cibernetice sunt:

- Oamenii
- Procesul
- Tehnologia

În zona de **NIST**(e un framework) avem 5 elemente:

- **Identificare** : în cadrul elementului de identificare din cadrul NIST, obiectivul este să se înțeleagă și să se evaluateze risurile la adresa securității informațiilor și a sistemelor.
- **Protectie** : Elementul de protecție se concentrează pe implementarea măsurilor și controalelor necesare pentru a preveni, limita și gestiona impactul potențialelor amenințări
- **Detectie** : Detectarea reprezintă capacitatea de a identifica rapid și eficient orice incident de securitate care ar putea afecta integritatea, confidențialitatea sau disponibilitatea informațiilor

- Raspuns : Elementul de răspuns se referă la dezvoltarea și implementarea unui plan de răspuns la incidente care să permită organizației să gestioneze și să reducă impactul unui incident de securitate
- Recuperare : Recuperarea se referă la procesul de restaurare a serviciilor și a activităților normale după un incident de securitate

NIST e o varianta, ISO27001 este o alta varianta, dar ambele fac cam același lucru; ambele sunt pe partea de compliance - respectarea regulilor, normelor și ghidurilor stabilite pentru securitatea informației

CIS este o organizație responsabilă cu dezvoltarea celor mai bune practici pentru îmbunătățirea securității cibernetice și protejarea împotriva incidentelor de securitate.

VPN (Virtual private network) adaugă securitate și anonimitate userilor când vor să se conecteze la site-uri web. VPN-ul ascunde adresele IP publice ale utilizatorilor și face tunneling între dispozitivul userului și serverul remote.

Metode de a implementa **vectorii de atac/infectie** care sunt nedetectabili și dificil de neutralizat (**vectorii de atac/infectie** se referă la modalitățile sau căile prin care un atac cibernetic este inițiat sau un sistem informatic este infectat cu malware sau alte amenințări):

Phishing:

- Descriere: Atacatorii trimit e-mailuri sau mesaje care par să fie de la surse de încredere pentru a încuraja utilizatorii să dezvăluie informații sensibile sau să acceseze link-uri malicioase.
- Exemplu: Un e-mail care pretinde să fie de la o bancă și să solicite utilizatorului să introducă parolele sau să acceseze un link pentru a verifica contul.

Watering Hole Attacks:

- Descriere: Atacatorii compromisă site-uri web pe care țintele obișnuiesc să le viziteze, injectând malware pentru a infecta dispozitivele vizitatorilor.
- Exemplu: Atacatorii pot targeta site-uri frecventate de membrii unei organizații și pot injecta malware în codul sursă al site-ului.

Drive-By-Download:

- Descriere: Atacatorii exploatează vulnerabilități în browsere sau în alte aplicații pentru a descărca și instala automat malware pe dispozitivele utilizatorilor.

- Exemplu: Vizitarea unui site web compromis care exploatează o vulnerabilitate în browser pentru a descărca malware fără ca utilizatorul să ştie.

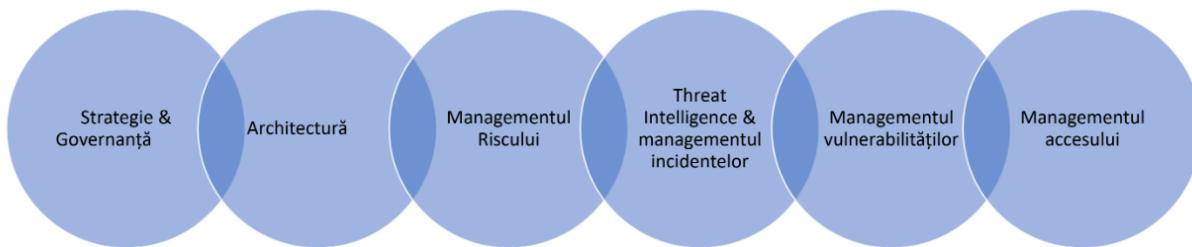
Ingineria Socială:

- Descriere: Atacatorii manipulează oamenii pentru a obține informații sensibile sau pentru a-i convinge să efectueze anumite acțiuni.
- Exemplu: O persoană care se prezintă ca un tehnician IT și îi convinge pe angajați să dezvăluie parole sau să ofere acces la sisteme.

FAMILII DE MALWARE - CATEGORII

- Backdoor - un program al cărui scop principal este de a permite unui actor să trimită în mod interactiv comenzi către sistemul pe care este instalat
- Credential Stealer - un utilitar al cărui scop principal este de a accesa, copia sau fura credențialele de autentificare.
- Downloader - un program al cărui singur scop este de a descărca (și poate lansa) un fișier de la o adresă specificată și care nu oferă nicio funcționalitate suplimentară și nu acceptă alte comenzi interactive.
- Dropper - un program al cărui scop principal este de a extrage, instalare și eventual lansa în execuție unuia sau mai multor fișiere.
- Launcher - un program al cărui scop principal este de a lansa în execuție unul sau mai multe fișiere. Diferă de un dropper sau un program de instalare prin faptul că nu conține sau configurează fișierul, ci doar îl execută sau îl încarcă
- Ransomware - un program al cărui scop principal este de a efectua o acțiune rău intenționată (cum ar fi criptarea datelor), cu scopul de a obține beneficii financiare de la victimă pentru a anula acțiunea.
- Tunneler - un program care oferă proxy sau tuneleză traficul de rețea.

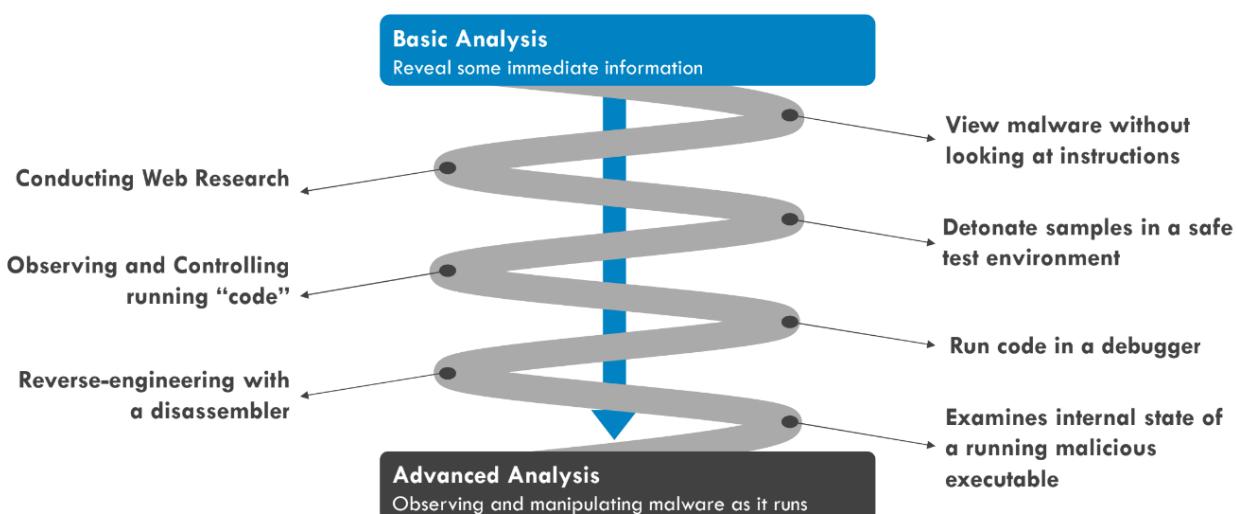
Componentele unui program de securitate cibernetică



IoC (Indicator of Compromise - Indicator al Compromiterii) este o notiță sau un semn care indică că un sistem sau o rețea poate fi compromisă sau a fost deja afectată de o amenințare cibernetică. IoC-urile sunt folosite în domeniul securității cibernetice pentru a detecta, investiga și răspunde la incidentele de securitate. Acestea pot fi indicii specifice sau modele de activitate asociate cu atacuri cibernetice.

IoC-urile sunt utilizate în tehnologiile de securitate cibernetică, cum ar fi sistemele de detectie a intruziunilor (IDS), sistemele de preventie a pierderii de date (DLP), platformele de securitate a endpoint-urilor și altele. Atunci când IoC-urile sunt detectate, acestea pot declansa alerte sau pot initia măsuri automate pentru a preveni sau limita impactul unei amenințări cibernetice. Utilizarea și schimbul eficient de IoC-uri sunt elemente esențiale ale gestionării incidentelor și a răspunsului la incidente în securitatea cibernetică.

MALWARE ANALYSIS



CURS 2 - Principii de securitate cibernetică. Zero trust.

OBIECTIVELE SECURITĂȚII

Confidențialitatea

- Asigură prevenirea dezvăluirii informațiilor clasificate persoanelor neautorizate

Disponibilitatea

- Asigură prezența datelor la locul, în timpul și forma potrivită

Integritatea

- Asigură prevenirea adăugărilor, modificărilor, alterării sau ștergerii neautorizate a informațiilor

Autenticitatea și non-repudierea

- Asigură veridicitatea mesajelor și a surselor

PRINCIPII DE SECURITATE CIBERNETICĂ

- Coordonarea – activitățile se realizează într-o concepție unitară, pe baza unor planuri de acțiune convergente destinate asigurării securității cibernetice, în conformitate cu atribuțiile și responsabilitățile fiecărei entități;
- Cooperarea – toate entitățile implicate (din mediul public sau privat) colaborează, la nivel național și internațional, pentru asigurarea unui răspuns adecvat la amenințările din spațiul cibernetic;
- Eficiența – demersurile întreprinse vizează managementul optim al resurselor disponibile;
- Priorizarea – eforturile se vor concentra asupra securizării infrastructurilor cibernetice ce susțin infrastructurile critice naționale.
- Diseminarea – asigurarea transferului de informații, expertiză și bune practici în scopul protejării infrastructurilor cibernetice.

PRINCIPII DE SECURITATE CIBERNETICĂ

- asigurarea protecției fizice a infrastructurii cibernetice;
- realizarea planurilor de securitate;
- asigurarea securității personalului;
- analizarea și evaluarea riscurilor de securitate cibernetică;
- procedurarea activităților de achiziție a sistemelor și serviciilor;
- asigurarea protecției produselor și serviciilor aferente infrastructurii cibernetice;
- managementul vulnerabilităților și alertelor de securitate cibernetică.

Rotirea Posturilor (Job Rotation):

Prin rotirea posturilor, angajații sunt asignați temporar sau periodic la diferite poziții sau roluri în organizație. Acest concept are ca scop diversificarea experienței angajaților, dezvoltarea abilităților lor și reducerea riscului de fraudă sau abuz, prin faptul că un singur individ nu deține constant aceleasi responsabilități cheie.

Separarea Atribuțiilor (Separation of Duties):

Prin separarea atribuțiilor, responsabilitățile și privilegiile sunt distribuite între mai mulți angajați sau sisteme. Scopul este să se reducă riscul de fraudă sau greșeli, deoarece nicio persoană sau entitate nu are control total asupra unui proces sau sistem.

Grijă Riguroasă (Due Care):

Due care reprezintă implementarea măsurilor preventive și de securitate adecvate pentru a minimiza riscurile și a asigura conformitatea cu standardele și politicile de securitate. Acest concept se referă la abordarea proactivă a securității, în care organizațiile se pregătesc și iau măsuri pentru a preveni incidente de securitate.

Controlul Accesului (Access Control):

Controlul accesului implică gestionarea drepturilor de acces la resursele informaticе. Aceasta include autentificarea utilizatorilor, autorizarea pentru accesul la anumite informații sau funcționalități și monitorizarea activităților pentru a detecta și preveni accesul neautorizat.

Principiul Celor Mai Mici Privilegii (Least Privilege):

Principiul celor mai mici privilegii se referă la acordarea utilizatorilor sau entităților doar a celor privilegii sau permișuni necesare pentru îndeplinirea atribuțiilor lor. Scopul este de a minimiza riscul de acces neautorizat sau de utilizare greșită a privilegiilor.

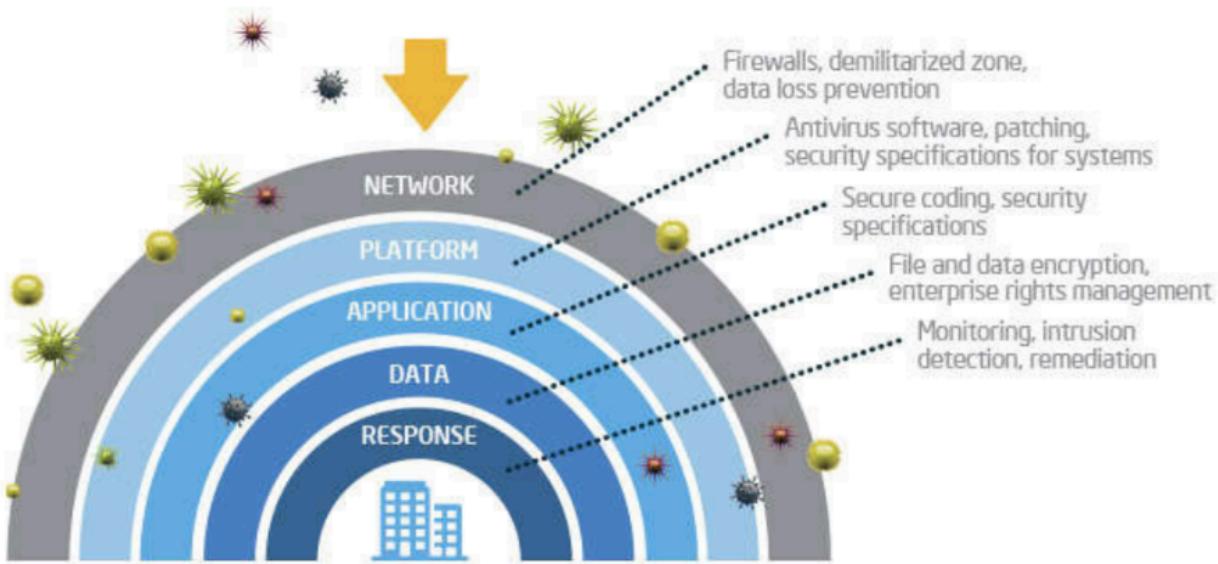
Principiul Necesității de Cunoaștere (Need to Know Basis):

Acest principiu se aplică în controlul accesului și se referă la limitarea accesului la informații doar la persoanele care au nevoie efectivă de acele informații pentru a-și îndeplini responsabilitățile de serviciu. Aceasta ajută la protejarea confidențialității datelor și reduce riscul de expunere inutilă.

CARACTERISTICILE CONFRUNTĂRII DIN SPAȚIUL VIRTUAL

- dificultatea precizării adversarilor;
- absența unor frontiere de natură geografică și/sau temporale;
- multitudinea de ținte;
- caracterul continuu;
- lipsa unor indicatori clari de avertizare;
- lipsa unor metode rapide de remediere a consecințelor;
- utilizarea unei tehnologii relativ simple, ieftine și larg răspândite;
- dificultatea stabilirii unor responsabilități clare și precise;

- costurile relativ scăzute ale derulării operațiilor informaționale în raport cu rezultatele ce se pot obține;
- posibilități sporite de manipulare.



Greseli comune facute de companii:

Lipsa Politicilor Formale Documentate:

Companiile nu au politici formale și documentate, inclusiv politici de securitate a serverelor, utilizare acceptabilă, auditare, complexitate a parolelor, și implementare a patch-urilor.

Servere Necorespunzător Securizate:

Politici inexistente sau neadecvate pentru securizarea serverelor, inclusiv construcția securizată a sistemului de operare și implementarea patch-urilor.

Lipsa Proceselor Formale de Management al Schimbărilor:

Companiile nu au procese formale pentru gestionarea modificărilor, ceea ce poate duce la o lipsă de control asupra modificărilor aduse sistemelor.

Gestionări Gresit Drepturile de Acces:

Multe sisteme sunt împărțite între grupuri cu multe conturi de utilizator în grupul de administratori, ceea ce crește riscul de utilizare necorespunzătoare a privilegiilor.

Lipsa Documentării Despre Instalare:

Lipsa documentării cu privire la ce ar trebui instalat pe un sistem în comparație cu ceea ce este instalat efectiv, creând o potențială vulnerabilitate.

Lipsa Datelor de Referință:

Fără date de referință, este dificil să se identifice comportamentele anormale. Actualizări periodice ale inventarului de software și scanări ale rețelei pot ajuta la identificarea și remedierea problemelor.

Incapacitatea de a Mări Investigația:

Dificultăți în extinderea investigației după confirmarea unui atac asupra unui grup de servere.

Lipsa unei Echipe Formale de Răspuns la Incidente:

Absența unei echipe formale de răspuns la incidente, adesea din cauza lipsei de buget și planificare. O echipă de răspuns la incidente actualizată și bine instruită este esențială.

Lipsa unui Plan de Continuitate a Afacerilor:

Companiile nu au un plan de continuitate a afacerilor pentru a gestiona incidente care pot necesita analiză offline.

Lipsa unui Set de Instrumente de Investigare de Încredere:

Absența unui set de instrumente automatizate pentru a facilita procesul de obținere a informațiilor de pe sistemele live și pentru a asigura o ieșire cunoscută și bine înțeleasă.

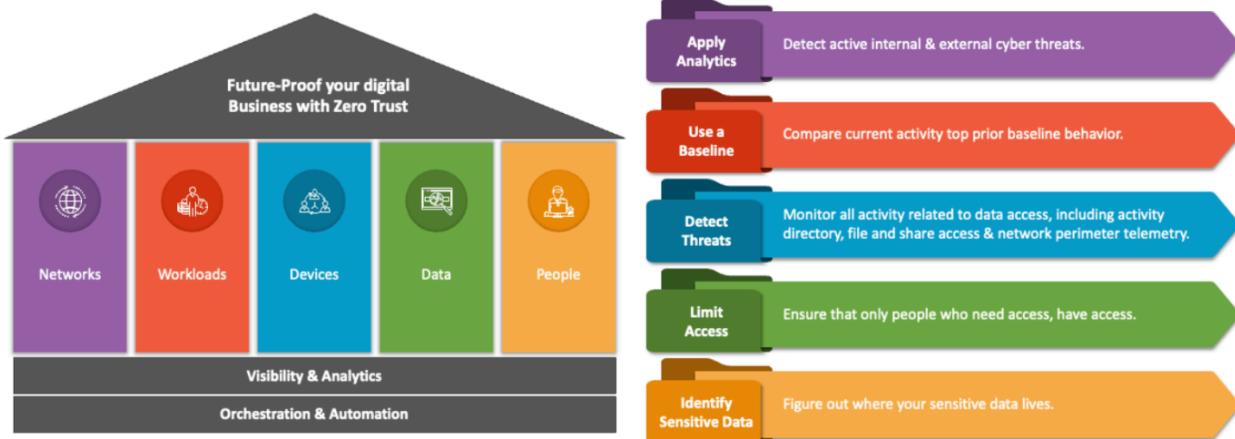
Security Information and Event Management (SIEM) este o tehnologie care colectează, analizează și gestionează evenimentele de securitate din diverse resurse într-un mediu IT; SIEM e un loc agregator, o zona centrală unde se face aggregarea informațiilor stranse despre alerte/atacuri. **Anomalia** înseamnă devierea de la comportamentul normal sau obișnuit. Anomaly Detection with SIEM implică identificarea și semnalarea activităților sau evenimentelor neobișnuite care ar putea indica o potențială amenințare sau incident de securitate.

UEBA (User and Entity Behavior Analytics) se concentrează în mod specific pe detectarea anomaliei în comportamentul utilizatorilor și al altor entități din sistem. Această abordare este utilă pentru identificarea amenințărilor interne și a atacurilor care implică compromiterea identității.

"Spear phishing" reprezintă o formă avansată de atac de phishing care vizează specific o țintă individuală sau o organizație în loc să trimită mesaje false în masă către un public larg. Acest tip de atac implică cercetarea și personalizarea atacului pentru a face ca mesajele să pară mai credibile și mai puțin susceptibile de a fi identificate ca frauduloase.

Ideea principală a modelului de securitate "Zero Trust" este că nu se acordă în mod implicit încredere niciunui activ sau cont de utilizator, indiferent de locația lor fizică sau de rețea. Acest model se bazează pe convingerea că amenințările pot proveni atât din interiorul, cât și din afara limitelor tradiționale ale rețelelor.

ZERO TRUST SECURITY MODEL



Principii zero trust:

- Verificare explicită
- Privilegii cat mai putine
- Presupunerea compromiterii (assume breach): poate veni atat din interior, cat si din exterior

CURS 3 - Tehnologii de securitate

Shellcode:

Un mic fragment de cod executabil folosit ca sarcină, construit pentru a exploata vulnerabilități într-un sistem sau pentru a efectua comenzi malefice. Poate fi creat pentru a profita de vulnerabilități specifice ale software-ului, permitând atacatorilor să ocolească măsurile de securitate și să obțină controlul asupra unui sistem compromis.

Exemple de Shellcode-uri:

Reverse Shell Shellcode:

Stabilește o conexiune între sistemul compromis și un sistem controlat de atacator, permitând atacatorului să acceseze mașina compromisă de la distanță.

Bind Shell Shellcode:

Creează o rețea pe sistemul compromis pentru a stabili conexiunea cu atacatorul, astfel încât să poată obține controlul asupra sistemului vizat.

File Download Shellcode:

Exploatează o vulnerabilitate pentru a descărca și executa un fișier malefic de pe un server remote pe sistemul compromis.

Meterpreter Shellcode:

Este un cadru popular de shellcode folosit în testarea penetrării, oferind testatorilor manipularea sistemului de fișiere, manipularea proceselor, explorarea rețelei și escaladarea privilegiilor.

Shellcode pentru Escaladarea Locală a Privilegiilor:

Acest tip de shellcode exploatează vulnerabilități într-un sistem de operare pentru a ridica privilegiile atacatorului, permitându-le să obțină acces administrativ sau de root.

Security zones:

- LAN: utilizatori, nimic permis din exterior în interior(pentru că e local)
- DMZ(demilitarized zone): servicii expuse, servere, mai permite și niste conexiuni din exterior
- Internet: zona în care noi suntem expuși

Proxy:

Acel layer intermediar care ne ajuta să interceptăm o comunicație, un fel de man in the middle; inspectează

Exemplu: proxy de mail(pot fi blocați, filtrat mailuri)

UTM (Unified Threat Management):

Unified Threat Management (UTM) reprezintă un dispozitiv de rețea sau un program software care ajută la reducerea complexității securizării unei rețele. Realizează acest lucru prin includerea unui set variat de funcționalități de securitate într-un singur pachet integrat.

Importanța UTM:

UTM simplifică administrarea și implementarea măsurilor de securitate într-o rețea, oferind o soluție comprehensivă și integrată pentru protejarea împotriva multiplelor amenințări cibernetice. Prin consolidarea acestor funcționalități într-un singur dispozitiv sau program, UTM reduce complexitatea și costurile asociate implementării separate a fiecărei componente de securitate.

Network Access Control (NAC) reprezintă o abordare în securitatea computerelor care încearcă să unifice tehnologiile de securitate la nivelul dispozitivelor finale (cum ar fi antivirus, prevenirea intruziunilor la nivel de gazdă și evaluarea vulnerabilităților), autentificarea utilizatorului sau sistemului și aplicarea securității în rețea.

Sandbox:

O sandbox este un mecanism de securitate utilizat pentru a separa programele care rulează, de obicei, pentru a atenua eșecurile de sistem sau vulnerabilitățile software pentru a preveni răspândirea acestora.

Este adesea folosit pentru a executa programe sau coduri netestate sau neverificate, în special din partea unor treți părți, furnizori, utilizatori sau site-uri web, fără a pune în pericol mașina gazdă sau sistemul de operare.

Poate fi plasat în orice zonă de securitate în funcție de necesitatea implementării.

Web Application Firewall (WAF):

- Un WAF sau Web Application Firewall ajută la protejarea aplicațiilor web prin filtrarea și monitorizarea traficului HTTP între o aplicație web și Internet.
- În mod tipic, protejează aplicațiile web de atacuri precum falsificarea cross-site (cross-site forgery), scripturile cross-site (cross-site scripting - XSS), includerea de fișiere și injectarea de SQL, printre altele.
- Un WAF reprezintă o apărare la nivelul protocolului de strat 7 (în modelul OSI) și nu este proiectat pentru a se apăra împotriva tuturor tipurilor de atacuri. Această metodă de atenuare a atacurilor face de obicei parte dintr-un set de instrumente care, împreună, creează o apărare holistică împotriva unei game de vectori de atac.
- Poate fi găsit în DMZ (Zona Deservită Demilitarizată).

Honeypot & Honeynets:

Honeypot:

Un honeypot este un sistem conectat la rețea configurat ca un decoy pentru a atrage atacuri cibernetice și pentru a detecta, devia sau studia încercările de hacking în vederea obținerii unui acces neautorizat la sistemele informatiche.

Honeypot-ul este construit pentru a îngăduia atacatorii să aibă locuri neinteresante.

Adesea, mașini virtuale sunt utilizate pentru a găzdui honeypot-uri, astfel încât, dacă este compromis de malware, de exemplu, honeypot-ul poate fi rapid restaurat.

Honeynet:

Două sau mai multe honeypot-uri pe o rețea formează o honeynet.

Honey Farm:

Un honey farm reprezintă o colecție centralizată de honeypot-uri și instrumente de analiză.

Honeypot-urile și honeynets sunt utilizate în principal în scopuri de învățare și cercetare pentru a înțelege modurile în care atacatorii încearcă să compromită sistemele informatiche și pentru a dezvolta strategii de apărare împotriva acestor amenințări.

VPN Service:

Remote-access VPN:

O conexiune VPN de tip remote-access permite unui utilizator individual să se conecteze la o rețea privată dintr-o locație remote folosind un laptop sau computer desktop conectat la internet.

Site-to-site VPN:

O conexiune VPN de tip site-to-site permite filialelor să utilizeze internetul ca un canal pentru a accesa intranetul sediului principal.

- Bazat pe Intranet:**

Dacă o companie are una sau mai multe locații remote pe care dorește să le conecteze într-o singură rețea privată, poate crea un VPN de tip intranet pentru a conecta fiecare LAN separat la un WAN comun.

- Bazat pe Extranet:**

Atunci când o companie are o relație strânsă cu o altă companie (cum ar fi un partener, furnizor sau client), poate construi un VPN de tip extranet care conectează LAN-urile acestor companii. Acest VPN de tip extranet le permite companiilor să lucreze împreună într-un mediu de rețea securizat și partajat, în timp ce previne accesul la intranetul lor separat.

Host-Based IDS (HIDS):

Un Host-Based IDS este responsabil pentru monitorizarea activității pe un sistem și alertarea asupra activității suspecte. Un punct cheie de reținut despre un HIDS este că monitorizează activitatea doar pe sistemul pe care software-ul a fost instalat.

Endpoint Detection and Response (EDR):

Endpoint Detection and Response extinde funcționalitățile HIDS pentru a include și capacitatea de a răspunde la incidente la nivelul dispozitivelor finale.

EDR furnizează capacitatea de a investiga, detecta și răspunde la amenințări, adesea cu funcții avansate precum analiza comportamentală și capacitatea de a bloca sau izola dispozitivele compromise. Este o abordare mai cuprinzătoare pentru securitatea la nivel de endpoint.

Antivirus software blocheaza aplicatii malicioase pe baza de hash(blocheaza toate hash urile) IDR/EDR e aproape ca si antivirus, doar ca nu blocheaza pe baza de hash, dar pot sa ii definesc eu politici

Data Loss Prevention (DLP):

Software-ul de prevenire a pierderii de date (DLP) detectează potențialele surgeri de date și transmisii neautorizate și le previne prin monitorizarea, detectarea și blocarea datelor sensibile în timpul utilizării (acțiuni la nivelul dispozitivului), în mișcare (traficul de rețea) și în repaus (stocarea datelor).

Scopurile Principale ale NAT:

- Ascunderea topologiei interne a rețelei.
- Economisirea adresei IP publice și utilizarea mai eficientă a spațiului de adresare IP.
- Sprijinirea conectivității multiplelor dispozitive interne printr-o singură adresă IP externă.

Dynamic Host Configuration Protocol (DHCP):

- DHCP este un serviciu care rulează pe un server.
- În arhitectura enterprise, pot exista mai mulți servere DHCP.
- Este situat într-o Zonă Demilitarizată (DMZ) sau în zona locală (local zone).

Domain Name System (DNS):

- DNS este un serviciu care rulează pe un server.
- În arhitectura enterprise, pot exista mai mulți servere DNS.
- Este situat într-o Zonă Demilitarizată (DMZ) sau în zona locală (local zone).

Web Service:

- Un server web este un program care utilizează HTTP (Hypertext Transfer Protocol) pentru a servi fișierelor care formează paginile web către utilizatori, în răspuns la solicitările acestora, care sunt trimise de clienții lor HTTP pe computer.
- Computerele dedicate și dispozitivele pot fi denumite și servere web.
- Procesul este un exemplu al modelului client/server. Toate computerele care găzduiesc site-uri web trebuie să aibă programe server web. Serverele web de top includ Apache, Internet Information Server (IIS) de la Microsoft și nginx (pronunțat engine X) de la NGNIX. Alte servere web includ serverul NetWare de la Novell, Google Web Server (GWS) și familia de servere Domino de la IBM.
- Situat în Zonă Demilitarizată (DMZ) sau în zona locală (local zone).

Email Service

Un serviciu de e-mail este un sistem informatic conectat la o rețea, care furnizează un loc pentru accesul comun la stocarea fișierelor de calculator (text, imagine, sunet, video). Această stocare este accesată de stațiile de lucru care pot atinge acest computer prin intermediul unei rețele de calculatoare.

Punctele cheie includ:

- Stocare Comună: Serviciul oferă un loc centralizat pentru a stoca și accesa fișierele, facilitând partajarea acestora între stațiile de lucru conectate la rețea.
- Acces prin Rețea: Stațiile de lucru pot accesa acest serviciu de la distanță prin intermediul rețelei de calculatoare.
- Locație în DMZ sau Zonă Locală: Serviciul poate fi plasat fie într-o zonă demilitarizată (DMZ), care este o zonă intermediară între o rețea de încredere și una nesigură (de obicei, internetul), fie într-o zonă locală (LAN), în funcție de necesitățile de securitate și arhitectura rețelei.

File Share / File Transfer Service:

- Scopul Principal: File share și transferul de fișiere sunt axate pe partajarea de fișiere, în timp ce serviciile de e-mail sunt orientate către schimbul de mesaje electronice.
- Tipurile de Conținut: File share se concentreză pe fișiere de diferite tipuri, în timp ce serviciile de e-mail transmit mesaje scrise și atașamente.
- Modul de Acces: File share poate implica acces direct la fișierele stocate, în timp ce e-mailurile sunt livrate în cutiile de e-mail ale utilizatorilor.
- Funcționalități Adiționale: Serviciile de e-mail pot oferi funcționalități adiționale, cum ar fi gestionarea calendarului și a contactelor, care nu sunt caracteristici principale ale serviciilor de partajare a fișierelor.

Scopul Principal al Rețelei BYOD(Bring Your Own Device):

Permite utilizatorilor să aducă și să utilizeze propriile dispozitive în rețeaua organizației, asigurând în același timp securitatea și controlul asupra acestora. Aceasta facilitează mobilitatea și flexibilitatea în mediul de lucru, dar necesită o gestionare atentă a accesului și a securității.

CURS 4 - Suprafața de atac. Modelarea amenințărilor cibernetice. Management acces și identitate (IAM, IdP, SSO)

Tipuri de amenintari:

- Asupra retelei(spoofed packets)
- Asupra host-ului(buffer overflow, illicit paths)
- Asupra unei aplicatii(sql injection, XSS, input tampering)

Suprafața de Atac a unei aplicații este:

- Suma tuturor căilor pentru date/comenzi care intră și ies din aplicație.
- Codul care protejează aceste căi (inclusiv conectarea la resurse și autentificarea, autorizarea, înregistrarea activității, validarea și codificarea datelor).
- Toate datele valoroase utilizate în aplicație, inclusiv secrete și chei, proprietate intelectuală, date de afaceri critice, date personale și informații cu caracter personal (PII).
- Codul care protejează aceste date (inclusiv criptarea și sumele de control, auditarea accesului și controalele de securitate operațională pentru integritatea și securitatea datelor).

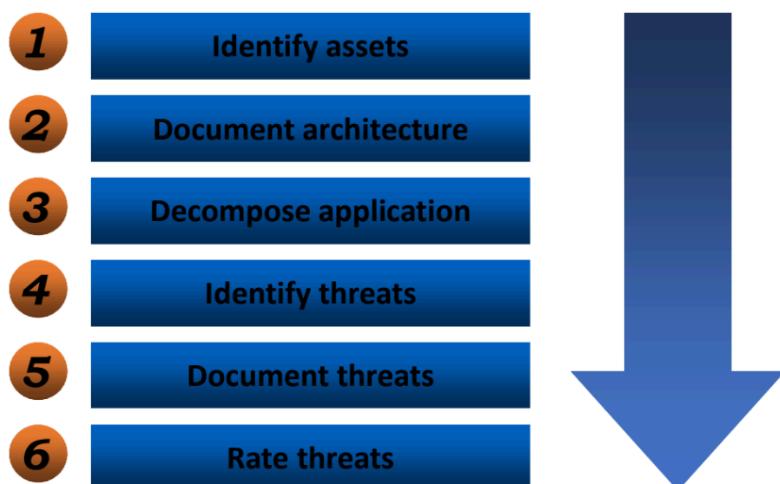
Identificare si maparea suprafetei de atac:

- Citim prin codul sursa și identificam diferite puncte de intrare/iesire
- Spargem modelul în diferite funcții, designuri și tehnologii

Masurarea si evaluarea suprafetei de atac

- Identificarea suprafetelor de risc ridicat
- Resurse pentru protejarea aplicației
- Controlul asupra codului și schimbările care apar asupra configurațiilor
- Backup pentru cod și date

The Threat Modeling Process



STRIDE este un model de categorizare a amenințărilor

Threat categorization - STRIDE

- S** **Spoofing**
Can an attacker gain access using a false identity?
- T** **Tampering**
Can an attacker modify data as it flows through the application?
- R** **Repudiation**
If an attacker denies doing something, can we prove he did it?
- I** **Information disclosure**
Can an attacker gain access to private or potentially injurious data?
- D** **Denial of service**
Can an attacker crash or reduce the availability of the system?
- E** **Elevation of privilege**
Can an attacker assume the identity of a privileged user?

DREAD este un model de evaluare a riscului

Subjective Model: DREAD

- D** **Damage potential**
How big would the damage be if the attack succeeded? / What are the consequences of a successful exploit?
- R** **Reproducibility**
How easy is it to reproduce an attack? / Would an exploit work every time or only under certain circumstances?
- E** **Exploitability**
How much time, effort, and expertise is needed to exploit the threat? / How skilled must an attacker be to exploit the vulnerability?
- A** **Affected users**
If a threat were exploited, what percentage of users would be affected? / How many users would be affected by a successful exploit?
- D** **Discoverability**
How easy is it for an attacker to discover this threat? / How likely is it that an attacker will know the vulnerability exists?

Identity and Access Management (IAM):

IAM descrie categoria generală a soluțiilor de gestionare a identității utilizate pentru administrarea identităților utilizatorilor și a accesului la resursele IT.

Categoria IAM cuprinde mai multe subcategorii, printre care IdP (Identity Provider), Identity-as-a-Service (IDaaS), Privileged Identity/Access Management (PIM/PAM), Multi-factor/Two-factor Authentication (MFA/2FA) și altele.

Identity Provider (IdP) as a Security Token Service (STS):

Un IdP este un Serviciu de Token de Securitate (STS) care acționează ca furnizor de verificare a identității și date într-o federație prin generarea și trimiterea de token-uri de securitate.

IdP facilitează gestionarea eficientă a accesului pe baza protocolelor standard de acces federat, cum ar fi SAML (Security Assertion Markup Language) și OIDC (OpenID Connect).

CURS 5 - Alertă, evenimente și incidente cibernetice. Sisteme de management al incidentelor. SIEM. SOAR. XDR

Managementul incidentelor cibernetice:

1. Defineste rolurile și responsabilitatile
2. Identifica amenintările și bunurile (pe ce se bazează aplicația/afacerea ta, ce poate fi atacat)
3. Detinerea unui plan
4. Logging, alertare și automatizarea rezolvării incidentului
5. Păstrează consecvența (fii constient), raportează progresul și îmbunătățește-l tot timpul

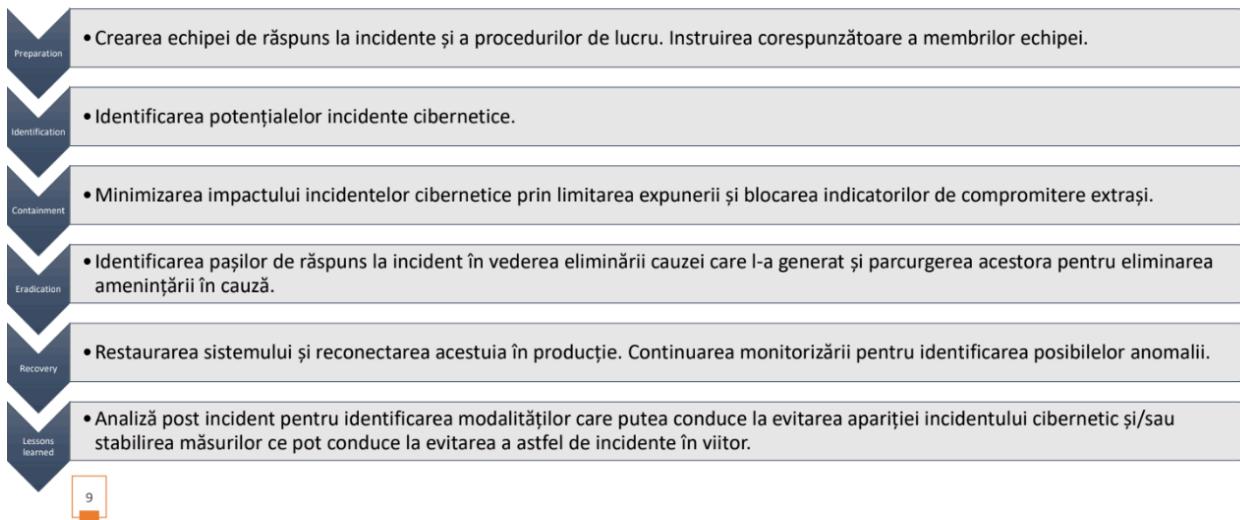
Evenimente, alertă, incidente

- **Eveniment:** are cel mai mic grad de complexitate, nu ne facem griji; este o schimbare observată la comportamentul normal
- **Alertă:** toate evenimentele se centralizează într-un singur punct, evenimente aggregate;
- **Incident:** Avem impact => avem incident



Managementul incidentelor cibernetice

Abordarea SANS.



9

- Preparation
- Investigation
- Containment(izolare)
- Eradication
- Recovery
- Lessons learned

SIEM = Security Information Event Management

= SEM (gestionare a evenimentelor de securitate) + SIM (gestionare a informațiilor de securitate)

- Colectare de loguri, agregarea informațiilor și corelarea lor
- Ne ajuta să facem detectii
- La baza este un log storage

SIEM FUNCTIONS

SIEM, when successfully implemented, helps organizations with its following functions:

- Reveals potential known and unknown threats
- Monitors the activities of authorized users and their privileged access to various resources
- Compiles a regular report
- Backs up incident response (IR)



Arhitectura generica SIEM:

SIEM preia logurile de la urmatoarele surse:

- Dispozitive de securitate: IDS, IPS, antivirus, Data loss prevention, VPN , Honeypots, Firewalls
- Dispozitive de retea: routere, switch uri, DNS servere
- Serveuri: Servere de aplicatii, baze de date, servere tinute in cloud
- Aplicatii: aplicatii intranet, aplicatii WEB

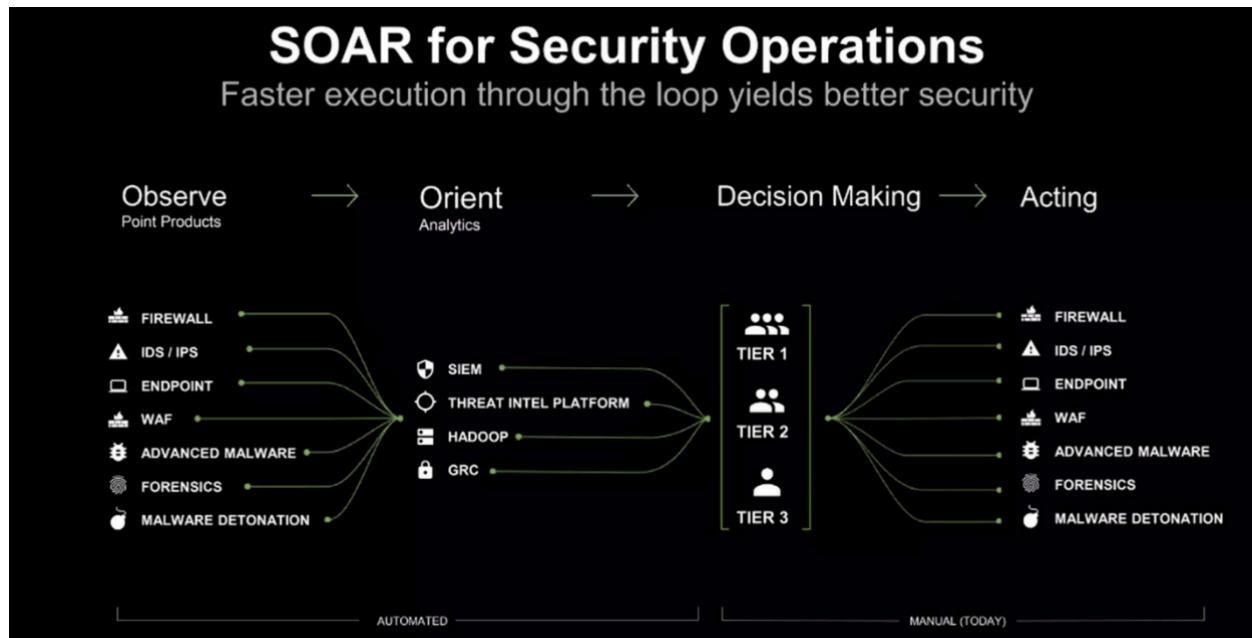
Componente si functionalitati ale SIEM-ului:

- **Agregarea datelor**: consta in adunarea datelor de la diferite surse(ex: loguri de la mai multe surse)
- **Informatii despre amenintari**: vom avea atat date din interior, cat si din exterior despre anumite amenintari
- **Corelari intre evenimente si monitorizare**: se analizeaza comportamentele neasteptate intr-o firma/aplicatie, apoi se face legatura cu evenimente malitioase
- **Analize**: se face o analiza a evenimentelor si se trag anumite concluzii/solutii
- **Alerte**: SIEM, dupa ce analizeaza automat evenimentele, are capacitatea de a trimite alerte catre echipa care se ocupa cu segmentul respectiv.
- **Dashboards**
- **Compliance**: SIEM genereaza rapoarte care respecta standarde date de HIPAA, GDPR
- **Pastrarea logurilor**: tine datele intre 1 si 7 ani, le va sterge pe cele de care nu se foloseste

SIEM: SPLUNK - Splunk este o platformă puternică de management și analiză a datelor;

no tables, no schema, no structure; Real-time architecture - as soon as an event is happening it is forwarded to Splunk; Data is stored into indexes;

Peste SIEM putem avea SOAR(security orchestration, automation and response)



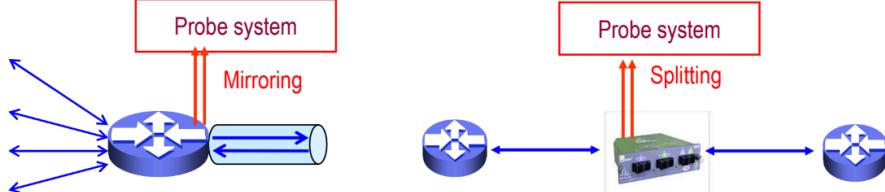
Diferente intre XDR si SIEM:

- SIEM: actionez manual, ofera o vizibilitate mai buna
- XDR: actionez automat, ca un fel de antivirus, ofera vizibilitate granulara doar acolo unde pot instala agentul

CURS 6 - Investigații cibernetice efectuate la nivelul unui SIC

- Packet Capturing

- Packets can be captured using Port Mirroring or Network Splitter (Tap)



	Port Mirroring	Network Splitter
How it works	- Copies all packets passing on a port to another port	- Splits the signal and sends a signal to original path and another to probe
Advantage	- No extra hardware required	- No processing overhead on router/switch
Disadvantage	- Processing overhead on router/switch	- Splitter hardware required

Flow:

Un flow este o colecție de pachete cu aceleasi {adresă IP SRC și DST, numărul porturilor SRC și DST, numărul de protocol}.

Datele de flow pot fi colectate direct de la rutere sau de la un generator de flow-uri independent cu capacitate de captare a pachetelor.

Există diferențe semnificative între **NetFlow și sFlow**, două tehnologii folosite pentru monitorizarea traficului în rețele de calculatoare.

Protocol:

NetFlow: Este un protocol dezvoltat de Cisco, utilizat pentru colectarea și monitorizarea datelor de trafic în rețele.

sFlow: Este un standard deschis dezvoltat de către InMon Corporation și sprijinit de diverse companii și echipamente de rețea.

Arhitectura:

NetFlow: Funcționează într-un mod bazat pe fluxuri. Înregistrează informații despre fluxurile de trafic distincte, precum adresele IP sursă și destinație, porturile sursă și destinație, durată și volumul traficului.

sFlow: Colecțează pachete de eșantionare și transmite datele agregate, reducând astfel volumul de date trimise pentru analiză.

Frecvența Eșantionării:

NetFlow: Monitorizează toate pachetele într-un flux. Frecvența eșantionării poate varia, dar în general este bazată pe volumul de trafic sau pe timp.

sFlow: Folosește eșantionarea la nivel de pachet, adică selectează pachete pentru analiză la anumite intervale de timp, reducând astfel cantitatea de date colectate.

Aspecte ale Analizei Traficului:

Aspect Spațial:

- Modelele de flux de trafic în raport cu topologia rețelei.
- Important pentru proiectarea și planificarea corespunzătoare a rețelei.
- Identificarea bottleneck-urilor (blocajelor) și evitarea congestiilor.
- Exemplu: Agregarea de fluxuri după adresele IP SRC, DST sau numărul AS (Autonomous System).

Aspect Temporal:

- Comportamentul stocastic al unui flux de trafic, descris în termeni statistici.
- Important pentru gestionarea resurselor și controlul traficului.
- Important pentru politici de modelare și memorare temporară a traficului.
- Exemplu: Pachet sau byte pe oră, zi, săptămână, lună.

Compoziția Traficului:

- O descompunere a traficului în funcție de conținut, aplicație, lungimea pachetului, durata fluxului.
- Ajută la explicarea caracteristicilor temporale și spațiale ale traficului.
- Exemplu: Trafic de jocuri, media streaming pentru o săptămână de la un furnizor de servicii internet.

CURS 7 - Investigații cibernetice efectuate la nivelul unui SIC - analiza probelor digitale

Structurile fizice și logice ale discului reprezintă modul în care sistemul de fișiere NTFS (New Technology File System) organizează și urmărește informațiile despre fișierele și directoarele stocate pe un volum.

Master File Table (MFT):

- NTFS utilizează o componentă numită Master File Table (Tabelul Maestru de Fișiere) pentru a urmări fiecare fișier din cadrul volumului.
- MFT conține cel puțin o intrare pentru fiecare fișier, numită File Record, căruia î se atribuie un număr unic.

File Records în MFT:

- MFT este asemănător cu o tabelă de bază de date relatională și conține diverse atribute despre diferitele fișiere.
- Primele 16 intrări în MFT sunt fișiere de metadate, prima înregistrare listată fiind pentru \$MFT însuși, care descrie locația și dimensiunea sa pe volumul NTFS.

Procesarea \$MFT:

- \$MFT necesită procesare pentru a cunoaște propria dimensiune și locație pe disc.
- Acest proces implică accesarea și citirea informațiilor din \$MFT pentru a obține detaliile necesare.

Intrări în \$MFT pentru Toate Fișierele:

- Toate fișierele de pe un volum NTFS, inclusiv directorul rădăcină, au o intrare de înregistrare în \$MFT care descrie dimensiunea și locația lor în același mod.

Windows artifacts:

- Shell link files
- Jump lists
- Event logs
- Wireless network history
- Prefetch/SuperFetch : Prefetching speeds up computer performance by bringing the data and code pages of programs used during boot process and in subsequent program launches into memory from the disk before that data and code is actually demanded.

CURS 8 - Investigații cibernetice efectuate la nivelul unui SIC – analiză RAM

Analiza Forensică a Memoriei:

Analiza forenscă a memoriei este procesul de captare a memoriei în timpul funcționării unui dispozitiv și ulterior analizarea rezultatelor captate pentru a identifica eventualele dovezi ale existenței unor programe malware sau a altor activități suspecte. În contrast cu forensica pe hard-disk, unde sistemul de fișiere al dispozitivului este clonat, iar fiecare fișier de pe disc poate fi recuperat și analizat, analiza forenscă a memoriei se concentrează asupra programelor reale care rulează pe dispozitiv în momentul capturării memoriei.

"Process hollowing" (hollowing este tradus în română ca "golire" sau "spart") reprezintă o tehnică de injectare a codului într-un proces, utilizată în mod frecvent în cadrul atacurilor cibernetice. Această tehnică implică crearea unui proces suspicios în care se încarcă un program malitios, iar apoi se substituie spațiul de memorie al procesului cu conținutul unui alt proces legitim. Prin utilizarea tehnicii de process hollowing, atacatorii încearcă să ascundă prezența lor în sistem și să evadeze

detectarea, deoarece procesul gazdă poate apărea inițial inofensiv sau similar cu procese legitime.

Memory analysis with Redline

Este important să subliniem că analiza memoriei este doar o componentă a investigației de securitate cibernetică mai amplă. Utilizarea Redline sau altor instrumente similare poate oferi o perspectivă detaliată asupra memoriei sistemului, contribuind la descoperirea și remedierea incidentelor de securitate.

Redline este o unealtă de analiză a memoriei dezvoltată de Mandiant, o companie specializată în securitate cibernetică.

Memory analysis with volatility

- Volatility is one of the best framework analysing memory images
- It is a command line based and is written completely in Python
 - Has a lot of plugins: malfind, apihooks, orphanthreads, etc.

În contextul securității cibernetice, termenul "API Hooks" este adesea asociat cu tehniciile utilizate de malware pentru a obține control asupra sistemului și pentru a ascunde activitatea dăunătoare. Iată câteva exemple de moduri în care malware-ul utilizează API Hooks:

Interceptarea Apelurilor de Sistem:

- Malware-ul poate folosi hook-uri pentru a intercepta apelurile de sistem și pentru a modifica sau ascunde comportamentul acestora.

Ascunderea Prezenței:

- Prin interceptarea apelurilor de funcții care returnează informații despre procese sau fișiere, malware-ul poate ascunde prezența sa în sistem.

Keylogging:

- Hook-urile pot fi utilizate pentru a intercepta evenimentele de tastatură, permitând unui malware să captureze parole sau alte informații sensibile.

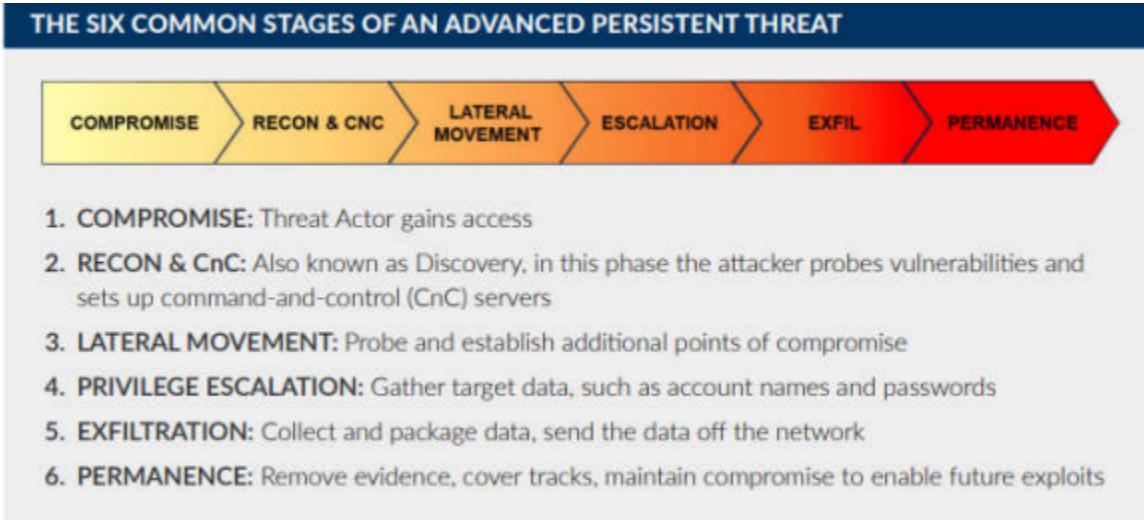
Detectarea sau Modificarea Traficului de Rețea:

- Malware-ul poate utiliza hook-uri pentru a intercepta și modifica pachetele de rețea, permitând manipularea comunicațiilor.

CURS 9 - Investigații cibernetice efectuate la nivelul unui SIC. Threat Hunting.

Abordare proactivă - hunting (actionezi înainte să apara evenimentul/alerta/incidentul)

Abordare reactivă - alerting (actionezi abia în momentul în care ești alertat că se întâmplă ceva neobișnuit)



CURS 10 - Investigații cibernetice efectuate la nivelul unui SIC. Threat intelligence

Threat Intelligence = "Informații despre Amenințări"

CTI (Cyber Threat Intelligence)

Protejam bunurile (assets)

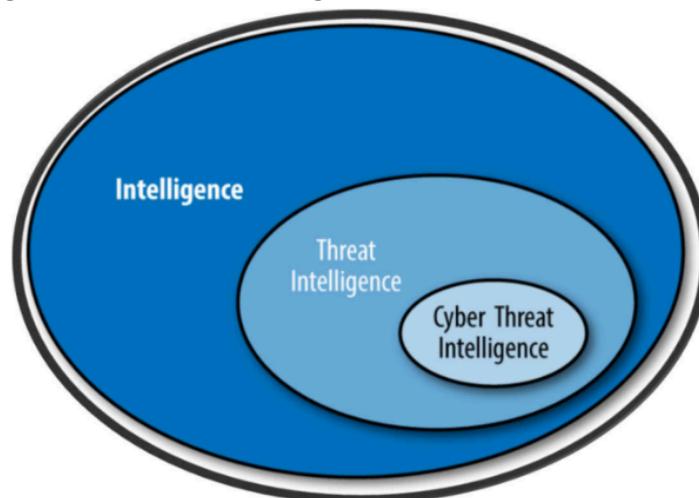
Popular CTI Analytics

Analytical Approach	Description	Examples	Value	Major Companies Using
Summary Statistics	High level summary of collected data	Number of blocked IP's, locations of attacks, counts over time	Good overview for executives	All
Event Correlation	Analyzes relationships between events	Identifying machine sending malicious traffic by checking firewall log	Integrates multiple sources of data together (usually internal network)	All
Reputation Services	Identifying the quality of an IP	IP "X" has a poor reputation	Identify which IP addresses to block	Akamai, NSFOCUS, FireEye, AlienVault
Malware Analysis	Analyzing malicious files on a network	Decompiling ransomware	Bolster technical cyber-defenses	FireEye, AlienVault
Anomaly Detection	Detecting abnormal behaviors	Unusual user logins	Detect malicious activity	Splunk
Forensics	Identifying and preserving digital evidence	Examining RAM from a malicious system	Identifying how an attack occurred	LIFARS, Blue Coat, FireEye
Machine Learning*	Algorithms that can learn from and make predictions on data	Classifying malware	Automated analysis	Splunk, FireEye, Cylance

Threat intelligence - definitii:

- Asset(bunuri)
- Threat(actiunile reale asupra bunurilor); capabilitati, oportunitati, intentii
- Threat agent/actor
- Atac
- Vector de atac: the path or the route used by a threat agent to gain access to the targeted asset
- TTP - tactici, tehnici si proceduri
- IOA - indicatori de atac(proactiv)
- IOC - indicator de compromitere(reactiv)

Cyber Threat intelligence vs Threat Intelligence



CURS 11 - Asigurarea securității cibernetice pentru dispozitive mobile, rețele wireless. Securitate informatică medii cloud.

Risks to wireless networks:

- **Piggybacking:** reprezintă un fenomen în care o persoană utilizează conexiunea la internet a cuiva fără permisiune, profitând de faptul că rețeaua wireless nu este securizată. În cazul în care o rețea wireless nu este protejată corespunzător, oricine cu un computer echipat cu capacitate wireless în raza de acțiune a punctului de acces (access point) poate utiliza conexiunea respectivă.
- **Wardriving :** reprezintă o formă specifică de piggybacking. Raza de emisie a unui punct de acces wireless poate face conexiunile la internet disponibile în afara casei dvs., chiar și la distanțe considerabile, cum ar fi pe strada în care locuți. Utilizatorii experimentați de computere știu acest lucru și unei dintre ei au transformat această cunoștință într-un hobby, conducând prin orașe și cartiere cu un computer echipat cu capacitate wireless – uneori cu o antenă puternică – căutând rețele wireless nesecurizate. Această practică este cunoscută sub numele de "wardriving."
- **Evil Twin Attacks:** Atacurile "Evil Twin" reprezintă o formă de amenințare în domeniul securității cibernetice, în special în ceea ce privește rețelele wireless. Aceste atacuri implică crearea unui punct de acces fals (Hotspot) care pare a fi legitim, dar este controlat de un atacator. Atacul "Evil Twin" își dătorează numele faptului că rețeaua falsă creată pare a fi "geamănă" cu o rețea autentică.
- **Wireless Sniffing :** Captarea informațiilor wireless, cunoscută și sub denumirea de "wireless sniffing," este procesul de interceptare și monitorizare a transmisiei de date prin rețelele fără fir (Wi-Fi). Această activitate poate fi realizată cu diverse scopuri, inclusiv pentru analiza traficului de rețea, pentru diagnosticarea problemelor de rețea sau, în unele cazuri, în moduri mai malefice, cum ar fi interceptarea datelor sensibile.
- **Unauthorized Computer Access :** Unauthorized computer access se referă la intrarea sau utilizarea unui sistem informatic, dispozitiv sau rețea fără permisiunea sau autorizarea corespunzătoare. Această activitate poate implica diverse intenții, inclusiv spionaj cibernetic, furt de date, acces la informații confidențiale, manipularea sistemelor sau orice altă acțiune care încalcă drepturile de acces legitime.
- **Shoulder Surfing:** Shoulder surfing este o tehnică de spionaj vizual în care un atacator încearcă să obțină informații sensibile sau date confidențiale, observând direct sau înregistrând indirect activități sau informații pe care o persoană le introduce sau le afișează într-un mediu nesigur. Această metodă se bazează pe observarea atentă a tastelor tastaturii, a ecranului dispozitivului sau a altor activități sensibile pentru a obține acces la informații personale sau la sistem.

Minimizarea riscurilor asupra retelei tale wifi:

- Schimbarea parolelor default
- Restrictioneaza accesul
- Cripteaza datele din retea
- Protejeaza SSID-ul(service set identifier)
- Instaleaza Firewall
- Mentine antivirus
- Foloseste file sharing cu grija
- Updateaza mereu software-urile
- Verifica configurarile dispozitivelor din reteua proprie
- Conecteaza prin VPN

Cloud Types:

- Public
- Private
- Hybrid
- Community

CLOUD COMPUTING SERVICES

- **IaaS: Infrastructure-as-a-service.** Cloud provider rents its infrastructure to customer. This can be servers, virtual machines or other hardware.
- **PaaS: Platform-as-a-service.** Designed for customers who want to develop, run or manage their applications without worrying about the underlying necessary infrastructure, such as databases and storage.
- **SaaS: Software-as-a-service.** Software delivered over the Internet. Can be either on demand or subscription based.
- **FaaS: Functions-as-a-service.** Developers can upload blocks of code that only execute when certain criteria are met.
- **BaaS: Backup-as-a-service:** Customers can purchase backup and recovery services for their data.

Improve your security posture with AWS

On-premises	On AWS
<ul style="list-style-type: none">■ Big Perimeter■ End-to-End Ownership■ Build it all yourself■ Server-centric approach■ De-centralised Administration■ Focus on physical assets■ Multiple (manual) processes	<ul style="list-style-type: none">■ Micro-Perimeters■ Own just enough■ Focus on your core values■ Service-Centric approach■ Central control plane (API)■ Focus on protecting data■ Everything is automated

Security Assurance

On-premises	On AWS
<ul style="list-style-type: none">■ Start with bare concrete■ Periodic checks■ Workload-specific compliance checks■ Must keep pace and invest in security innovation■ Heterogeneous governance processes and tools■ Typically reactive	<ul style="list-style-type: none">■ Start on accredited services■ Continuous monitoring■ Compliance approach based on all workload scenarios■ Security innovation drives broad compliance■ Integrated governance processes and tools■ Focus on prevention

AWS SECURITY SERVICES:

- **AWS WAF (Web Application Firewall)**
- **AWS Shield** : este un tool pentru protectia de DDoS (Un atac DDoS (Distributed Denial of Service) constă în efortul coordonat al unui grup de dispozitive sau computere compromise pentru a suprasolicita resursele unui sistem, serviciu sau rețea, astfel încât să devină inaccesibile sau să funcționeze cu performanță redusă pentru utilizatorii legitimi. Acest tip de atac are ca obiectiv principal să nege accesul utilizatorilor legitimi la servicii sau resurse online.)

- **AWS Macie** : serviciu de securitate destinat să protejeze datele sensibile din s3. (Simple Storage Service) este un serviciu de stocare în cloud oferit de Amazon Web Services (AWS). S3 este conceput pentru a oferi scalabilitate, durabilitate și performanță ridicată pentru stocarea și recuperarea datelor.
- **Amazon CloudWatch** : este un serviciu de monitorizare și gestionare a resurselor în mediul AWS; loguri, metriki și evenimente.
- **Inspector** : este un serviciu care ajută la identificarea și remedierea automată a problemelor de securitate și conformitate în instanțele EC2.
- **GuardDuty**: este un serviciu de detectie a amenințărilor care monitorizează activitățile neregulate din conturile AWS.
- **Trusted Advisor**: oferă recomandări pentru optimizarea resurselor, îmbunătățirea securității și reducerea costurilor în mediul AWS.

LOGGING AND EVENTS:

- AWS CloudTrail
- AWS Cloud Watch Events
- AWS Config
- Amazon S3 Access Logs
- Amazon CloudWatch Logs
- Amazon VPC Flow Logs
- AWS WAF Logs
- Other AWS Log

VISIBILITY AND ALERTING:

- AWS Security Hub
- Amazon GuardDuty
- Amazon CloudWatch
- Amazon Detective

CURS 12 - Principii și metode de integrare a securității informaticice în SDLC. DevSecOps

SDLC, sau Ciclul de Viață al Dezvoltării Software, este un proces structurat care guvernează planificarea, implementarea și întreținerea unui sistem software.

CI/CD (Continuous Integration/Continuous Deployment) reprezintă o practică în dezvoltarea software care încurajează automatizarea procesului de integrare a codului sursă și deplasarea automată a aplicației în mediul de producție.

CI/CD fundamentals

1. A single source repository

Source code management (SCM) that houses all necessary files and scripts to create builds is critical. The repository should contain everything needed for the build. This includes source code, database structure, libraries, properties files, and version control. It should also contain test scripts and scripts to build applications.

2. Frequent check-ins to main branch

Integrate code in your trunk, mainline or master branch — i.e., trunk-based development — early and often. Avoid sub-branches and work with the main branch only. Use small segments of code and merge them into the branch as frequently as possible. Don't merge more than one change at a time.

3. Automated builds

Scripts should include everything you need to build from a single command. This includes web server files, database scripts, and application software. The CI processes should automatically package and compile the code into a usable application.

4. Self-testing builds

CI/CD requires continuous testing. Testing scripts should ensure that the failure of a test results in a failed build. Use static pre-build testing scripts to **check code for integrity, quality, and security compliance.** Only allow code that passes static tests into the build.

CI/CD fundamentals

5. Frequent iterations

Multiple commits to the repository results in fewer places for conflicts to hide. Make small, frequent iterations rather than major changes. By doing this, it's possible to roll changes back easily if there's a problem or conflict.

6. Stable testing environments

Code should be tested in a cloned version of the production environment. You can't test new code in the live production version. Create a cloned environment that's as close as possible to the real environment. Use rigorous testing scripts to detect and identify bugs that slipped through the initial pre-build testing process.

7. Maximum visibility

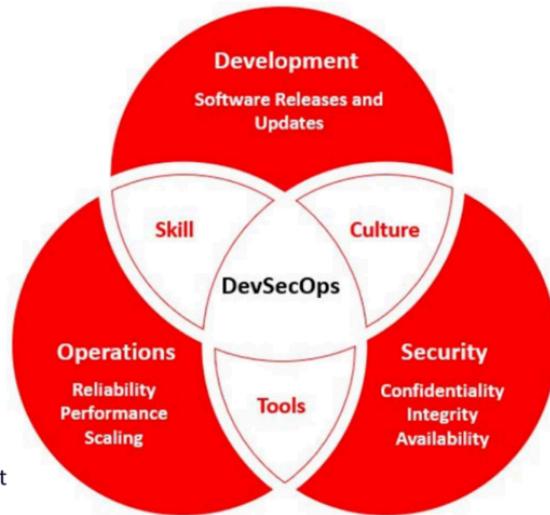
Every developer should be able to access the latest executables and see any changes made to the repository. Information in the repository should be visible to all. Use version control to manage handoffs so developers know which is the latest version. Maximum visibility means everyone can monitor progress and identify potential concerns.

8. Predictable deployments anytime

Deployments should be so routine and low-risk that the team is comfortable doing them anytime. CI/CD testing and verification processes should be rigorous and reliable, giving the team confidence to deploy updates at any time. Frequent deployments incorporating limited changes also pose lower risks and can be easily rolled back.

DevSecOps - benefits

- Finds vulnerability and bugs at an earlier stage of development
- Streamlined compliance
- Speedy recovery
- Secure supply chain
- Cost saving
- Can include AI-based monitoring for detecting anomalies
- Reduces the risk of surface attack and increases confidence
- Full visibility of potential threats and possible ways to remediate it



DevSecOps CI/CD pipeline

1. Plan/Design
2. Develop
3. Build and Code analysis
4. Test
5. Deploy
6. Monitor and Alert

TLS/SSL

SSL (Secure Socket Layer) si successorul acestuia TLS (Transport Layer Security) sunt protocoale ce asigura siguranta traficului in internet de la nivel transport la nivel aplicatie. Acestea asigura confidentialitate, integritate si autenticitate, prin utilizarea criptografiei cu chei publice si simetrice, algoritmi de hash, certificate digitale si un proces de "handshake" pentru a negocia setarile si pentru a stabili o conexiune securizata..

Metodele pentru schimbul de chei:

- Bazat pe RSA: Serverul cripteaza cu cheia publica pre-shared key-ul si il trimit clientului.
- fixed Diffie-Hellman: intr-un asemenea schimb serverul are o suita de parametrii criptografici certificati de CA-ul ce i-a semnat certificatul. Clientul tine cont de acestia si genereaza o pereche de chei, si trimit valoarea publica serverului.
- ephemeral Diffie-Hellman: Ambele entitati genereaza perechi One-pad DH si le schimba valorile publice intre ele. Serverul semneaza propria valoarea publica si poate cere clientului sa

o autentifice. In cazul in care si clientul e autentificat si acesta poate semna propriile perechi publice.

– anonymous Diffie-Hellman: Ambele entitati isi trimit cele perechi DH si le schimba in mod neautentificat.

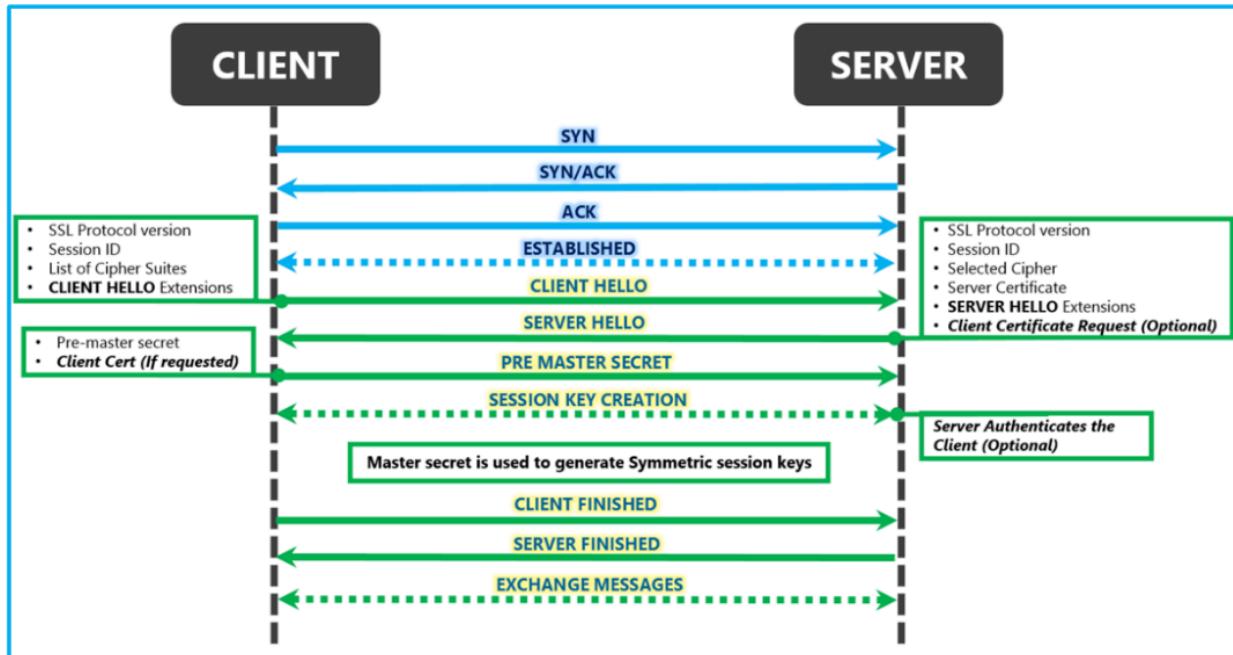


Figure 3: SSL Exchange

GRILE

1. Care dintre suitele de mai jos se pot regasi intr-o suita buna de algoritmi pentru a putea fi folosita in TLS 1.2?

- a. AES 256 GM, ChaCha20 , Salsa 20 , SHA512
- b. AES - 256 CBC, Salsa 20 , 3DES , SHA 1
- c. DES CTS , MD5 , 3DES CBC , SHA 256
- d. SHA 256, AES-128 CBC, AES 256 GCM, SHA 1

Se recomanda ca 3DES, SHA1 sa fie scosi din uz => alegem a prin eliminare

2. Ce varianta de schimb de chei impune parametrii matematici in care sa se faca operatiile necesare crearii secretului?

- a. fixed Diffie Hellman
- b. ephemeral Diffie Hellman
- c. anonymous Diffie Hellman
- d. RSA based

Este corect a

3. Despre autentificarea in TLS/SSL putem spune:

- a. Serverul se autentifică, iar clientul doar dacă își cere de către server
- b. Clientul este mereu autentificat iar serverul optional
- c. Clientul nu se autentifică iar serverul da
- d. Ambele entități au obțională aceasta posibilitate

Este corect a

4. In cazul intreruperii pentru scurta durata a conexiunii care dintre urmatoarele actiunii este cea mai probabila :

- a. Sesiunea nu mai poate fi reluată iar cele 2 entități vor trebui să aștepte o perioadă până vor putea relua conexiunea
- b. clientul va încerca să reia sesiunea întreruptă. Dacă serverul permite atunci aceasta se reia, dacă nu trebuie refăcut handshake-ul TLS/SSL.
- c. Clientul initializează un nou handshake TLS/SSL
- d. Serverul cere clientului să se autentifice și reface handshake-ul automat.

Raspuns corect b

Argument: session id: ID-ul ales de server. Da că clientul vrea să reia anumita sesiune, serverul verifică ca aceasta sesiune poate fi reluată și răspunde ori cu ID-ul sesiunii ce poate fi reluată ori cu un nou ID generat.

5. Modurile protocolului AH sunt :

- a. Tunel și Criptat
- b. Transport și Tunel
- c. Doar Transport
- d. Doar Tunel

2.2 AH protocol – modul transport pentru IPv4

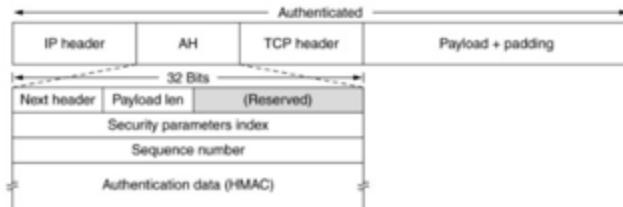
6. Pentru modul tunnel este adevarata afirmatie:

- a. Pachetul initial TCP este encapsulat în pachetul AH
- b. Pachetul initial IP este encapsulat în pachetul AH
- c. Pachetul initial IP este encapsulat în pachetul ESP
- d. Pachetul initial TCP este encapsulat în pachetul ESP

7. În privința AH, care afirmație este adevarată?

Protocolul AH oferă un mecanism numai pentru autentificare. AH oferă integritatea datelor, autentificarea originii datelor și un serviciu optional de protecție împotriva reluării unor pachete. Integritatea datelor este asigurată prin utilizarea unui rezumat al mesajelor care este generat de un algoritm precum HMAC-MD5 sau HMAC-SHA. Autentificarea originii datelor este asigurată prin utilizarea unei chei secrete (HMAC) (shared key) pentru a crea digestul mesajelor.

- a. Își inserează antetul după antetul de nivel transport
- b. Oferă integritate
- c. Își insează antetul înainte de antetul IP
- d. Oferă confidențialitate



8. Selectati functia asigurata de implementare a unei solutii SIEM :

Raspuns:

Colecteaza date din retea, dispositivo, servere, domenii, le stocheaza, le normalizeaza, le agrega si aplica analize asupra datelor sa descopere comportamente, sa detecteze amenintari sau sa arunce alerte.

9. Pentru a limita infectia unui sistem informatic si de comunicatii implicați intr-o comp. de phishing, care implica conexiuni catre adrese IP publice, este necesara instalarea si configurarea urmatoarelor mecanisme de protectie:

Raspuns:

Antivirus, Firewall, Filtrare a adreselor IP, Software anti-phishing, Actualizari de securitate regulare, Educatie privind siguranta

10. Selectati 2 motive pentru care analiza de memorie este necesara in cazul unui incident cybernetic

11. Enumerati in ordine corecta fazele Kill chain

Raspuns: Recon, Weaponization, Delivery, Exploitation, Instalation, Command and Control, Exfiltration

12. A/F: Analiza statica a proprietății presupune rularea specimenului într-un mediu izolat pentru a-i observa comportamentul prin intermediul instrumentului de monitorizare

Raspuns: F

13. Selectati faza de raspuns la incidente cibernetice in care engine-ul YARA poate fi utilizat pentru a scana reteaua in cauza in vederea localizarii sistemului infectat

Raspuns : Identification

14. Ce reprezinta semnatura unui fisier(magic number)?

Raspuns : Magic numbers are the first bits of a file which uniquely identify the type of file.

15. Selectati pasul care nu face parte din recomandarile NIST prin care organizatia ar trebui sa se asigure ca sunt luate masurile adevcate pentru a proteja continutul Web importanta accesului sau modificarea neautorizata

Raspuns:

Acestia sunt toti pasii:

In zona de **NIST**(e un framework) avem 5 elemente:

- Identificare
- Protectie
- Detectie
- Raspuns
- Recuperare

16. Tipul de inregistrare DNSKEY->pentru a semna alta inregistrare DNS

Raspuns: Key signing keys (KSK):

17. Atribute de pachet care nu sunt stocate in cadrul datelor unui flow

ASTEA SUNT CELE PE CARE LE CONTINE: Un flow este o colecție de pachete cu aceleași {adresă IP SRC și DST, numărul porturilor SRC și DST, numărul de protocol}.

18. PAS nu face parte din detectarea anomaliei folosirii modulului comportamental

Raspuns:

19. Clase de jurnale de log existente in SO WINDOWS

Raspuns:

Events are categorized into 2 main classes:

- Windows Logs
- Application and Services Logs

20. Limitarea extinderii informatiei->care faza de raspuns la incidente cibernetice

Raspuns:

Containment/izolarea dispozitivului de restul retelei

21. Un user primeste mesaje despre metode specifice => atac

Raspuns:

Phishing

22. Asigura persistenta

Raspuns: Probabil APT (Advanced Persistent Threats)

23. SNMP -> componente de baza

Raspuns: Network Management station, Network Management System (NMS), Agent, Management Information Base (MIB)

24. PE header -> informatii despre import/export (sectiunea)

Raspuns:.rdata – contain the imports and exports information. Contain read-only data used by the program: literals, constant strings, etc.

25. 1. A/F threat hunting reactive

Raspuns: F, threat hunting e proactive

26. Selectati protocolul care ofera autentificare, verificare de integritate si criptare(in IPSEC):

Raspuns: ESP ;Encapsulating Security Payload (ESP): Este un protocol de securitate utilizat în cadrul protocolelor IPSec (Internet Protocol Security) pentru a oferi confidențialitatea datelor transmise peste o rețea. ESP oferă servicii de criptare, autentificare și protecție împotriva jefuirii.

27. Selectati 2 elemente caracteristice ale unei ipoteze de Threat Hunting

Raspuns: de exemplu din curs ·Unusual PowerShell scripts are being used by attackers to collect details about the environment.; The attacker will use brute force “password spraying” to seek access to additional systems.; A keylogger is used by the attacker to collect credentials.

28. Detectii AV

Raspuns: Pe baza de anomalii, de semnaturi, euristice

29. Windows Registry

Raspuns: Windows registry is a central hierarchical database in which Microsoft Windows stores information that is necessary to configure the system for one or more users, applications, and hardware devices (profiles for each user, applications that are installed on the computer, types of documents that each can create, property sheet settings for folders and application icons, hardware that exists on the system, and the ports that are being used etc.) The highest element of the hierarchy is known as a hive , which maps to one or more file s in the file system that contains a binary database of registry keys and values. Hives are designed to store specific types of information.

30. Smallest unit de pe disc care poate fi alocat unui fisier

Raspuns: File Record