
DIGINTO
Nätverkssäkerhet

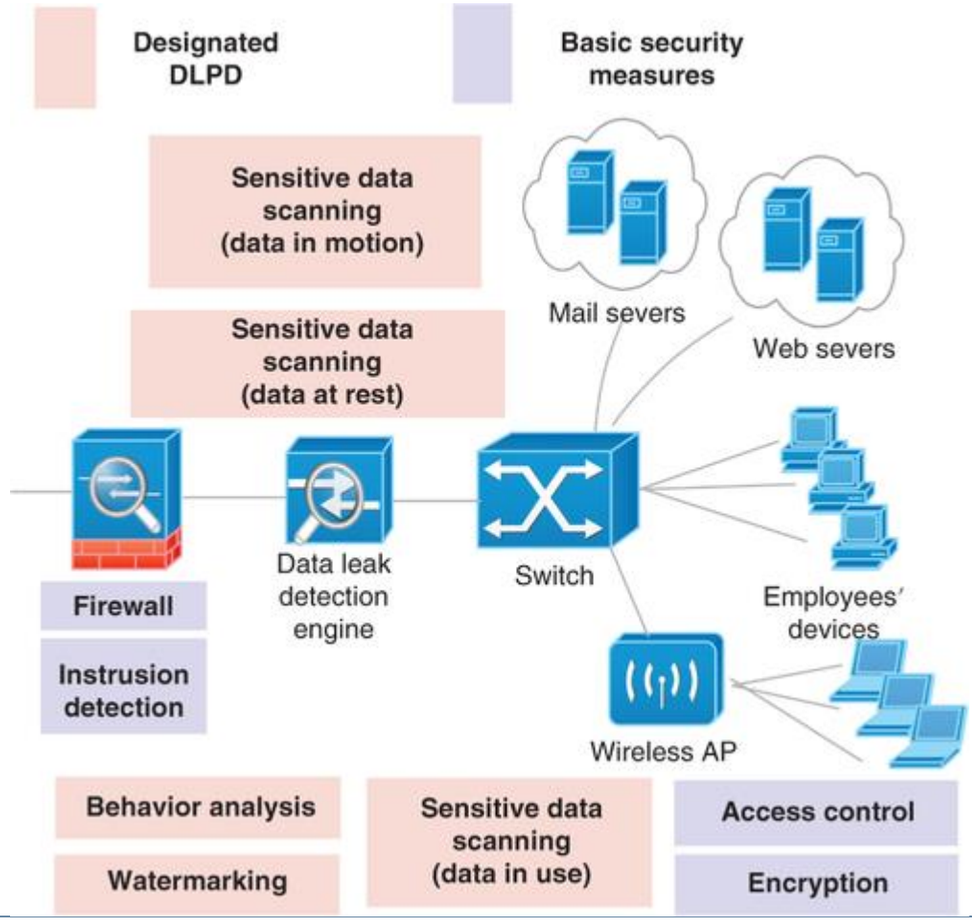
Informationssäkerhet - CIA

Informationssäkerhet

- Informationssäkerhet handlar om att hindra information från att läcka ut, förvrängas, förstöras samt säkerställa att informationen finns tillgänglig för en legitim användare.
- Beroende på organisation kan både risker och hot variera i typ och storlek.
- Till stor del handlar om att minimera och att hantera risker på ett adekvat sätt.
- CIA-modell - En enkel men viktig säkerhetsmodell består av tre principer:
  - **C**onfidentiality
  - **I**ntegrity
  - **A**vailability.
- Tre viktiga principer som bör implementeras i alla slags säkra system, från åtkomst till Internet för en användare till krypterad data över internet.

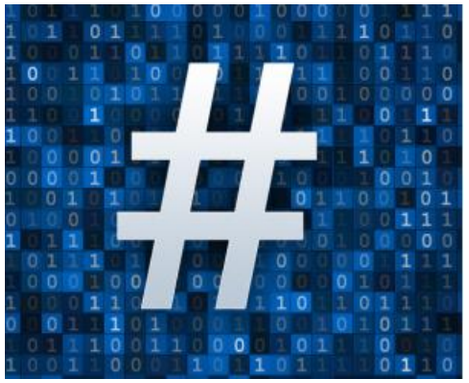
Informationssäkerhet - Confidentiality

- Datasekretess innebär att *endast auktoriserade personer/system kan komma åt känslig eller sekretessbelagd information*.
- Hot kan uppstå när:
  - *data är i gång*, när det rör sig över nätverket
  - *data är i vila*, när data finns på lagringsmedia (server, lokal arbetsstation, i molnet och så vidare)
  - *Data är i process*, när data används
- Det finns flera möjligheter för ett företag att skydda känslig data mot oavsiktliga eller skadliga läckage (information breaches, data leakage).
- Det finns tre typer av känslig information:
  - Enskild personlig information
  - Affärsinformation
  - Sekretessbelagd information
- Metoder: *datakryptering*, *autentisering* och *åtkomstkontroll*.



Informationssäkerhet - Integrety

- Dataintegritet innebär att *endast auktoriserade individer/system får göra ändringar i specifika data*.
- Integritet är noggrannhet, konsekvens och trovärdighet för data under hela dess livscykel.
- Data genomgår ett antal operationer såsom användning, lagring, hämtning, uppdatering och överföring.
- Metoder som används för att säkerställa dataintegritet inkluderar *hashing*, *datavalideringskontroller*, *datakonsistenskontroller* och *åtkomstkontroller*.
- En integritetskontroll är ett sätt att mäta konsistensen i en datainsamling (fil, bild eller post).
- Integritetskontrollen utför en process som kallas hashing –funktion.
- Vanliga hashing-funktioner inkluderar MD5, SHA-1, SHA-256 och SHA-512.
- Dessa hash-funktioner använder komplexa matematiska algoritmer.
- En kontrollsumma (checksum) verifierar integriteten för filer eller teckensträngar före och efter att de överförs från en enhet till en annan över ett lokalt nätverk eller Internet.
- Checksummor konverterar helt enkelt varje del av informationen till ett värde och summerar värden.



Informationssäkerhet - Availability

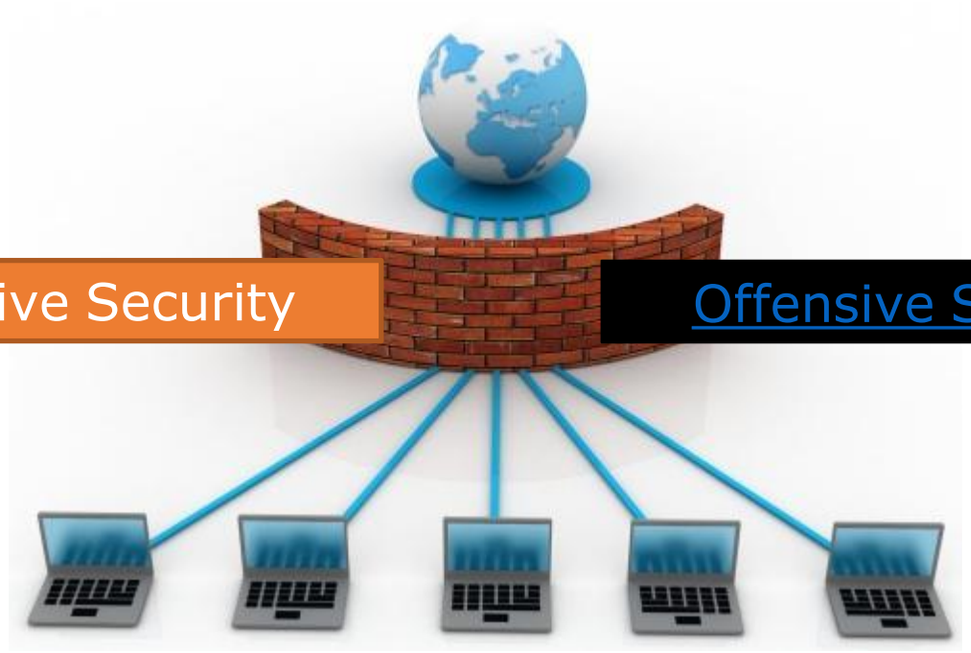
- Datatillgänglighet är principen som används för att beskriva behovet av att alltid ha tillgång till informationssystem och tjänster.
- Metoder som används för att säkerställa datatillgänglighet inkluderar *redundantsystem*, *backupsystem*, robust *resiliens-system*, underhåll av utrustning, uppdaterade operativsystem och programvara och strategier för att snabbt återhämta sig från oförutsedda katastrofer.
- Ordet "*resiliens*" är kapaciteten hos ett system att hantera förändringar och fortsätta utvecklas.
- Det handlar alltså om både motståndskraft och anpassningsförmåga samt fortsätta fungera.
- En av de mest populära metoderna för hög tillgänglighet är de så kallade *fem nior*.
- De fem niorna avser 99,999%.
- Det betyder att felmarginalstiden är mindre än 5,26 minuter per år.

Availability	Downtime / Year	Downtime / Month	Downtime / Week	Downtime / Day
99.999%	5.256 Minutes	0.438 Minutes	0.101 Minutes	0.014 Minutes
99.995%	26.28 Minutes	2.19 Minutes	0.505 Minutes	0.072 Minutes
99.990%	52.56 Minutes	4.38 Minutes	1.011 Minutes	0.144 Minutes
99.950%	4.38 Hours	21.9 Minutes	5.054 Minutes	0.72 Minutes
99.900%	8.76 Hours	43.8 Minutes	10.108 Minutes	1.44 Minutes
99.500%	43.8 Hours	3.65 Hours	50.538 Minutes	7.2 Minutes
99.250%	65.7 Hours	5.475 Hours	75.808 Minutes	10.8 Minutes
99.000%	87.6 Hours	7.3 Hours	101.077 Minutes	14.4 Minutes


DIGINTO
Säkerhetspolicy

Defensiv eller offensiv försvarsteknik?

- Defensiv säkerhet – Försvarsteknik t e antivirus, antimalware
- Offensiv säkerhet – simulering av hack-attacker så att man kan attackera tillbaka, men betraktas som cyber-brott.



Defensive Security

Offensive Security

IINS - Cisco

CCSP - Cisco

CCIE- Cisco

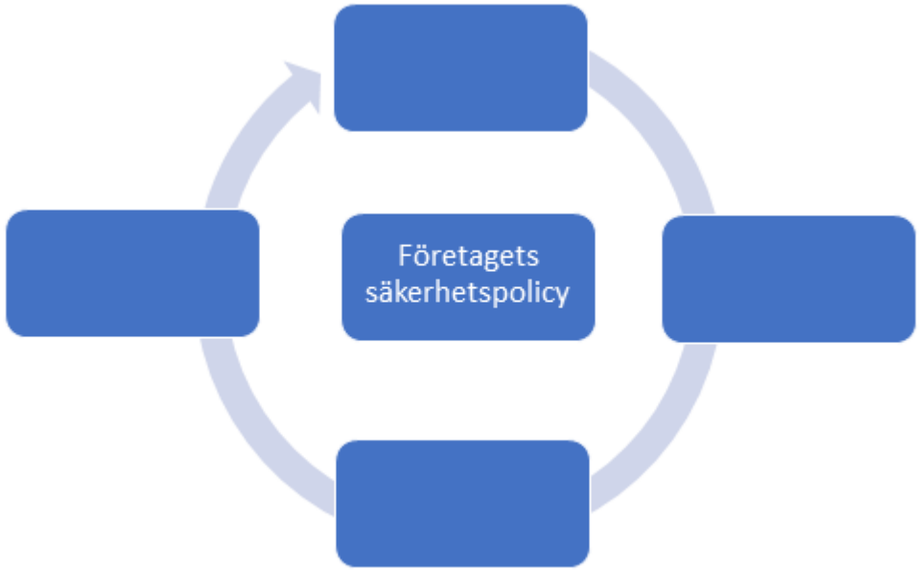
Ethical Hackning

WAPT

others

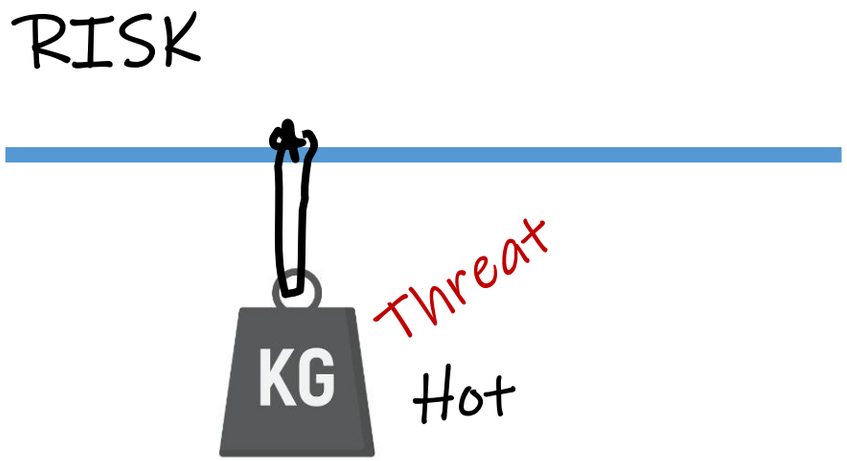
Säkerhetspolicy

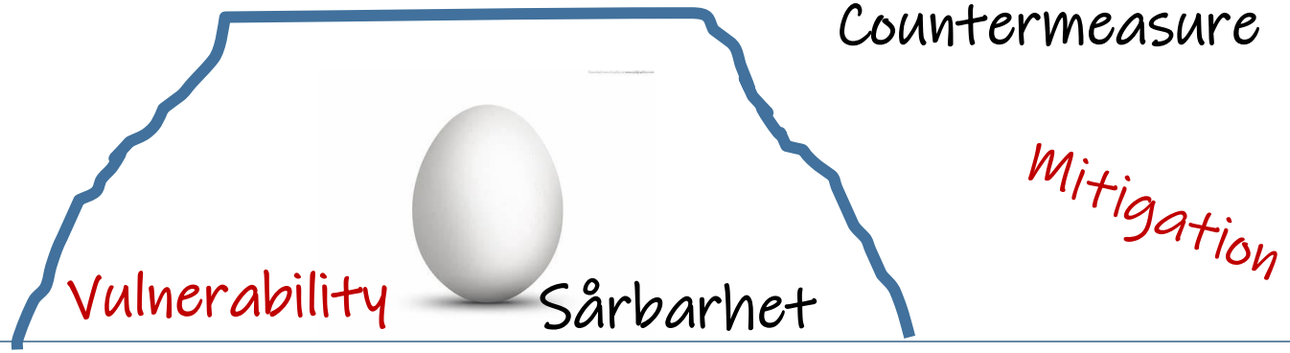
- Att upprätta en säkerhetsplan är ett viktigt steg för alla företag.
- Risker bör identifieras och definieras.
- Hanteringsprocess för risker och incidenter.
- En effektiv metod att beskriva den löpande säkerhetsprocessen är det s.k. säkerhetshjulet.
- *Hur kan nätverket säkras?*
- Med säkerhetssystem och nätverksutrustning som stödjer säkerhetskontroller.
- Övervaka systemet kontinuerligt, identifierar eventuella avvikelser och åtgärder.
- Testa systemet regelbundet och då även genomför penetration test.
- Tester sker ofta med hjälp av externa konsulter, men även med automatiserade analysverktyg.
- Utveckla systemet kontinuerligt.
- *Vad är sårbarhet (vulnerability)?*



Säkerhetspolicy - Sårbarhet

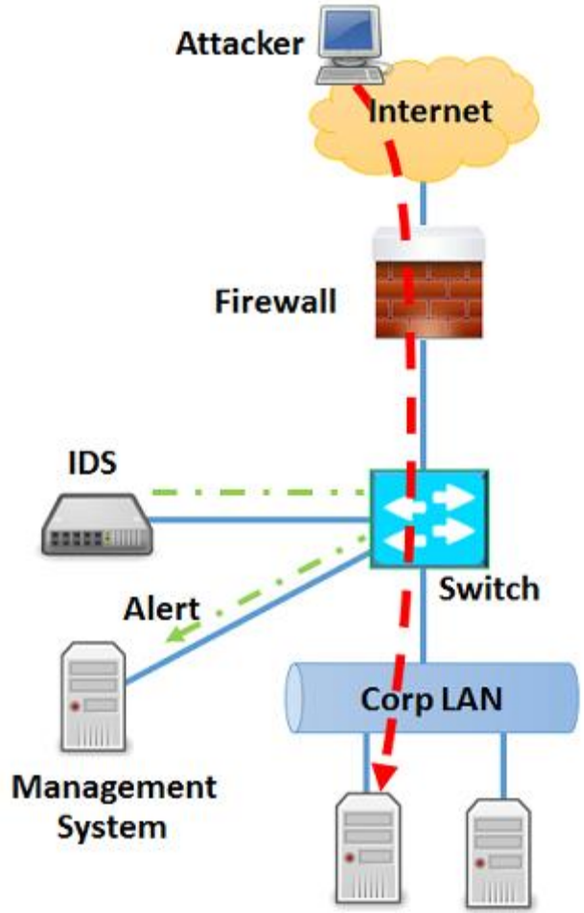
- Automatiserade sårbarhetsscanningar identifierar och klassificerar sårbarheter i datorer, nätverk och applikationer.
- Sårbarhetsscanningar:
  - autentiserad och icke-autentiserad
  - Testar säkerhetskontroller
  - Identifierar sårbarheter
  - Identifierar felaktiga konfigurationer
  - Behörig och obehörig åtkomst
- Penetration testning:
  - Verifiera om hot existerar (RISK)
  - Testar säkerhetskontroller
  - Utnyttjande av identifierade sårbarheter
- Penetrationstestrapport inkluderar konkreta slutsatser, tydliga och precisa rekommendationer.





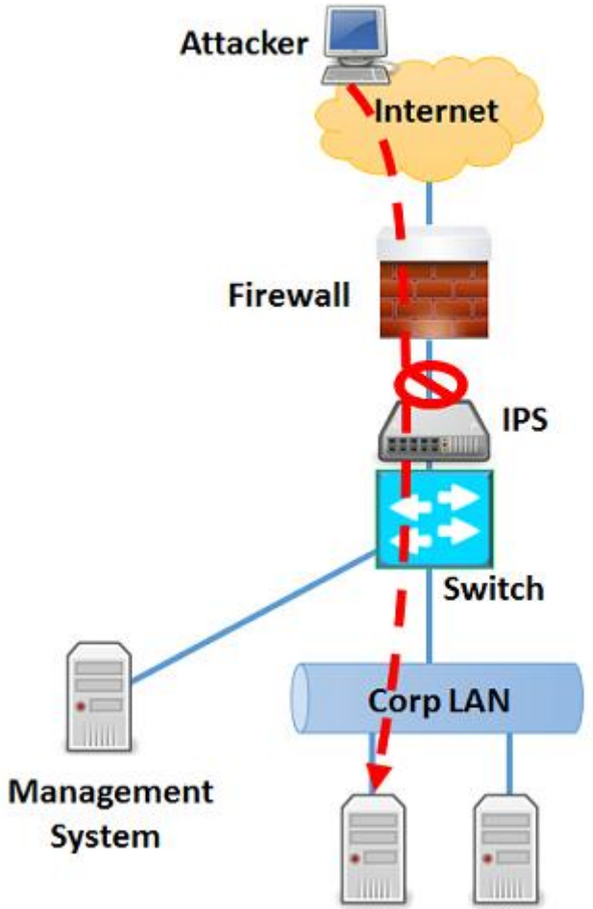
Säkerhetspolicy – Övervakning via IDS

- Intrusion Detection System – intrångsdetekteringssystem 1984
- Övervakar all inkommande och utgående nätverksaktivitet och identifierar eventuella misstänkta attackmönster.
- Nätverkssäkerhetsspecialister kan minska effekterna.
- Ett passivt övervakningssystem som detekterar och varnar vid misstänkta aktivitet.
- Från billiga shareware eller fritt distribuerade program till en mycket dyrare och säker leverantörsprogramvara.
- Från programvaror och hårdvaruapparater till sensorer på strategiska platser.



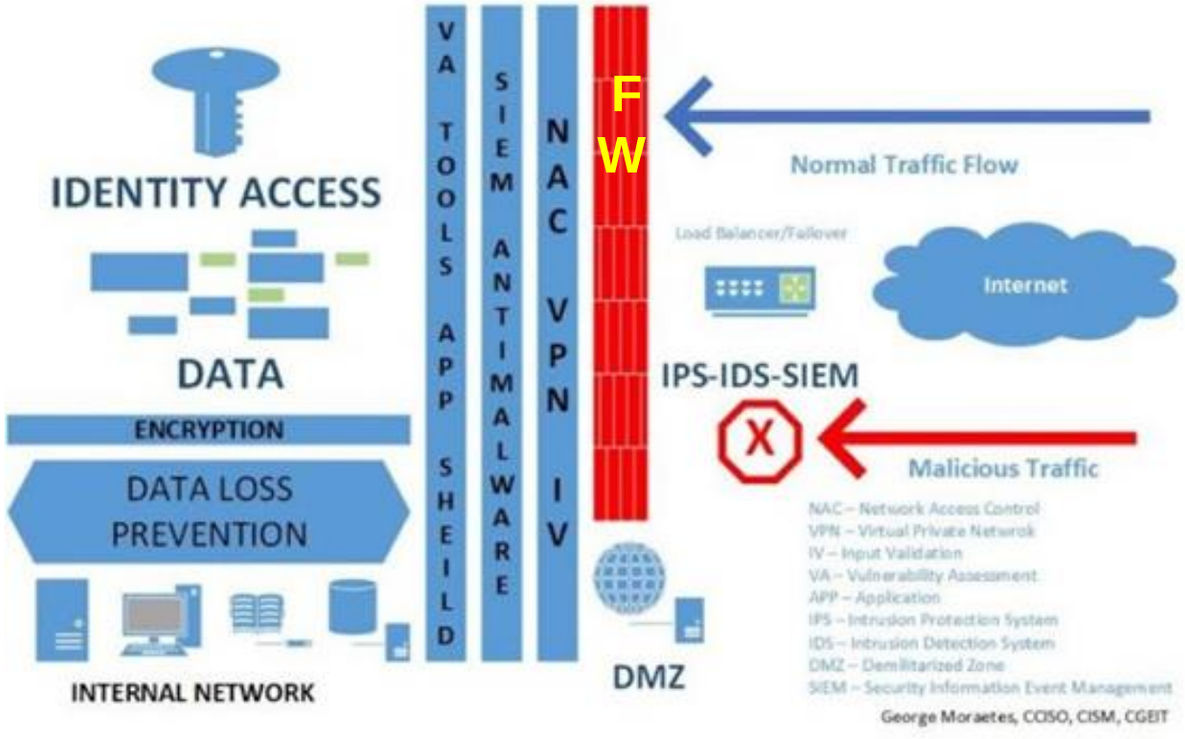
Säkerhetspolicy – Övervakning via IPS

- IPS upptäcker skadlig aktivitet och automatiskt blockerar det.
- IPS tillhandahåller säkerhet från OS till datapaket.
  - Signaturbaserad detektion
  - Anomalibaserad detektion
  - Reputation-baserad detektion
- För närvarande finns det två typer av IPS:
  - host-baserade HIPS
  - nätverksbaserade NIPS
- IDS och IPS kan implementeras i Cisco IOS
- Skillnader mellan IDS och IPS
  - IDS informerar om en eventuell attack
  - IPS kan stoppa den.



Säkerhetspolicy – Interna och skalsäkerhet

- Brandvägg bra att ha, men skalsäkerhet är inte tillräcklig.
  - *Ökad mobilitet*. En bärbar – och oskyddad – dator, som ena dagen var uppkopplad mot Internet på en kafeteria utanför företaget, kan nästa dag kopplas upp på företagets interna nätverk.
  - *Sofistikerade attacker*. Många av dagens attacker från hackare och virus gömmer sig i applikationer – t.ex. webb och e-post – som brandväggen tillåter.
  - *Dynamiska relationer*. När ett företag utökar samarbete med andra företag och gör fusioner, partnerskap och nya affärsrelationer blir det interna nätet alltmer komplext.
- Säkerhetsmodeller inkluderar flera system.
- Inklusive befintliga utrustning som routrar, switchar och accesspunkter.
- AAA system tillsammans med AD.
- Att addera säkerhetsfunktioner till existerande utrustning minimerar både kapital- och driftskostnader.

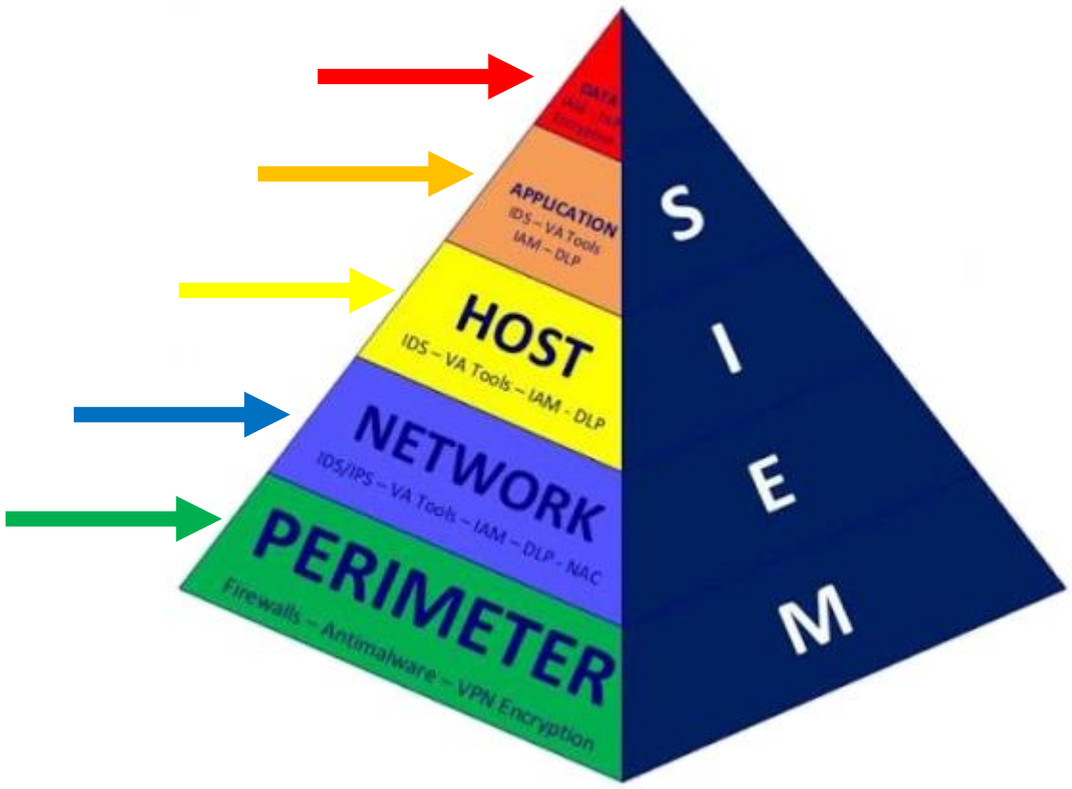


Säkerhetsarkitekturmodell

Säkerhetsarkitekturmodell

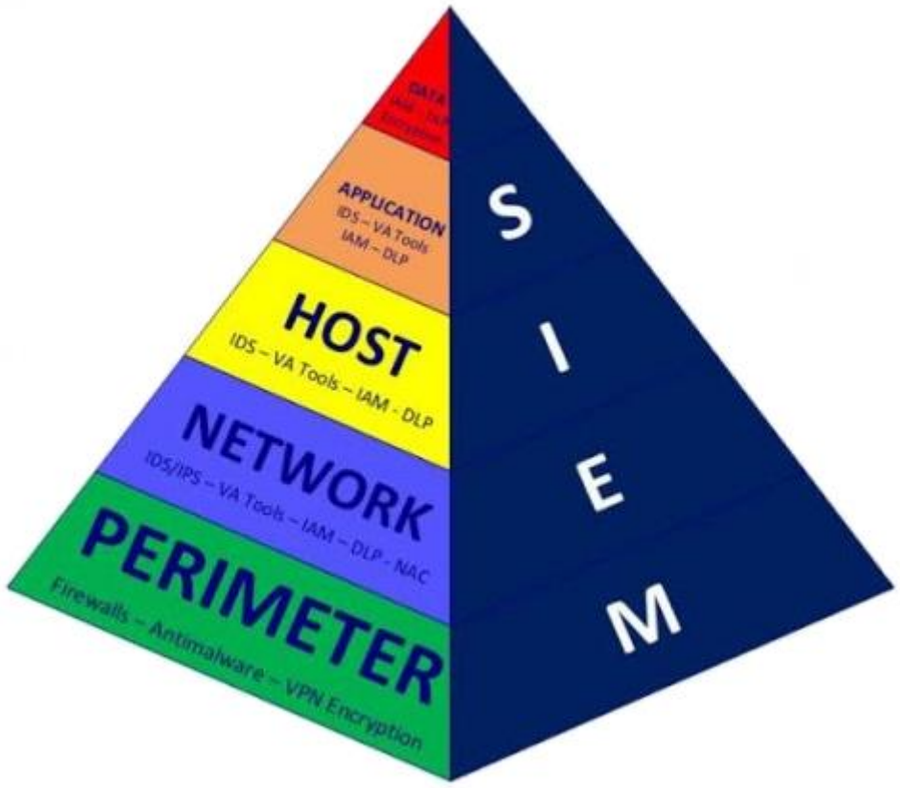
- Med OSI-referens modellen i bakgrunden byggs upp olika säkerhetsmodeller som är också nivåbaserade.
- Nätverkssäkerhetspolicy kan grundas i en säkerhetsarkitekturmodell som till exempel SIEM – Security Information and Event Management:

1. Perimeter – FW, antimalware, VPN, Kryptering
2. Network – IDS, IPS, VA, IAM, DLP, NAC
3. Host – IDS, VA, IAM, DPL
4. Application - IDS, VA, IAM, DPL
5. Data



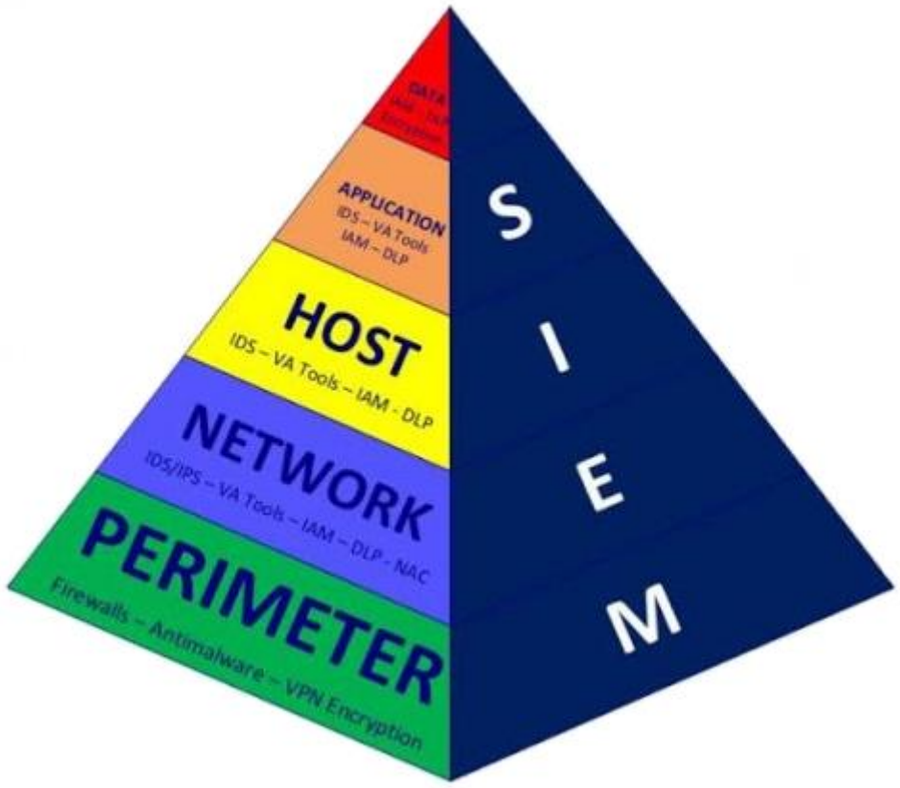
Säkerhetsarkitekturmodell - Applikation

- Säkerhet på applikationsnivå får för närvarande stor uppmärksamhet.
- Dåligt skyddade applikationer kan ge enkel åtkomst till konfidentiella data och register.
- De flesta programmerare inte kodar med säkerhet i åtanke.
- Du kan bli medveten om säkerhetsbrister i programvaran, men du kan vara maktlös för att rätta till dem.
- Försäljningssystem, kundrelationshantering eller finansiella system, kan vara mål för hackers.
- Därför är det särskilt viktigt att införa en övergripande säkerhetsstrategi för varje nätverksorienterat applikation.



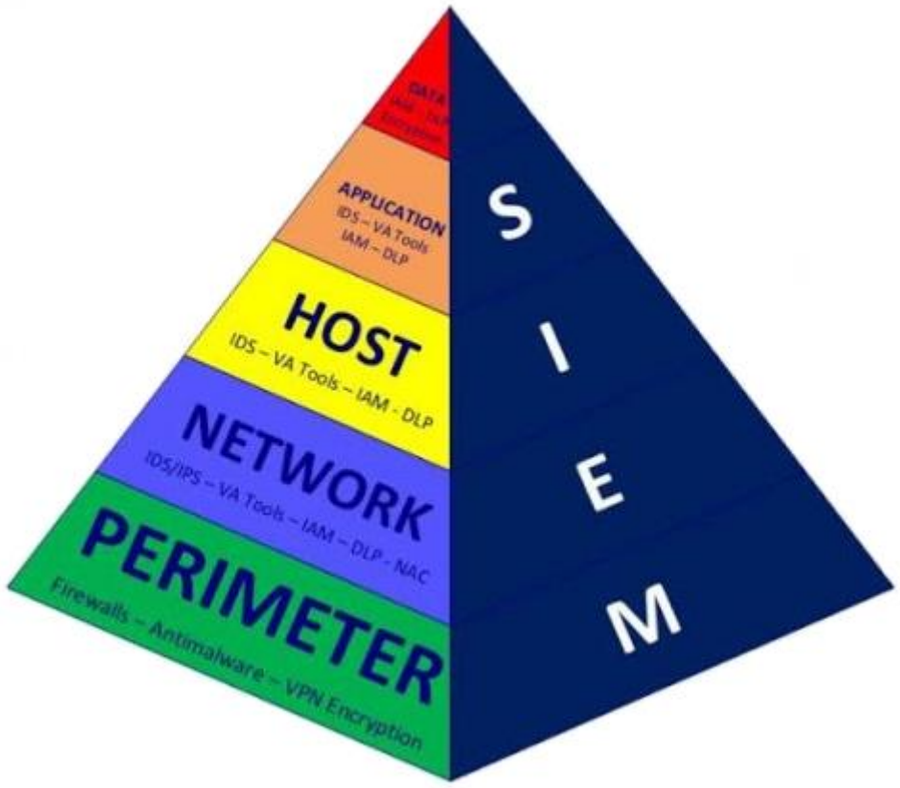
Säkerhetsarkitekturmodell - Host

- Nätverksenheter i den synliga delen av ett nätverk har var och en säkerhetsinställningar.
- Felaktiga konfigurationer kan generera oväntade risksituationer.
- Följande säkerhetsteknik kan tillämpas på host-nivå:
  - IDS som övervakar enskilda trafik i själva host
  - Hostbaserade VA verktyg, penetration test, personlig brandvägg, skanner.
  - Anti-malware applikationer
  - Data Loss Prevention, DLP, övervakar data i bruk, data i viloläge, och data i rörelse.
  - Autentisering, kontrollerar åtkomstroller till enheten.
  - SIEM tillhandahåller real-tids analyser av loggar.



Säkerhetsarkitekturmodell - Nätverk

- Nätverksskiktet i säkerhetsarkitekturmodellen refererar till det interna lokala nätverket (LAN) och Wide Area (WAN).
- Det interna systemet inkluderar datorklienter och servrar eller kan vara mer komplicerat med punkt-till-punkt-anslutningar för fjärranslutningar.
- Följande teknik används:
  - IDS och IPS, normalt inbyggda i brandväggar
  - VA tools, kända som penetration test scanner teknik
  - AAA via TACACS+, RADIUS, Kerberos, LDAP, Active Directory
  - DLP eller Data Loss Prevention övervakar intern nätverkstrafik
  - NAC, NAP, DNA, ISE
  - SIEM: Security Information Event Management tillhandahåller real-tids analyser av säkerhetsloggar.




DIGINTO
Nätverkssäkerhet