**Intelegjenca Kërcënuese**

Organizatat e intelegjencës kërcënuese si **CERT, MITER, SANS** ofronjë informata të hollësishme rreth kërcënimeve që janë jetike për sigurinë kibernetike.

**CERT** grup i hakerave të bardhë.

**Cisco** ofronë raportin e sigurisë kibernetik gjdo vit, siguron përditësim të gadishmërisë së sigurisë, analizës së dobësive.

**Blog dhe prodcast** të sigurisë ndihmojnë profesionistët e sigurisë kibernetike të kuptojnë dhe të zbusin kërcnimet.

Shërbimet e intelegjencës kërcënuese mundësojnë shkëmbimin e informacioneve të kërcnimeve të tilla si dobësitë, teknikat e kompromisit dhe teknikat për zbutje dhe zbulim.

**Cisco Talos** mbledh informata rreth këecënimeve aktive, ekzistuese dhe ato që janë duke ndodhur, pastaj i siguron mbrojtie të plotë abonentëve ndaj këtyre sulmeve dhe malware.

**Fire Eye** : Është kompani siguri që ofronë shërbime për ndërmarrjet të sigurojnë rrjetet e tyre.

**AIS** mundëson që sektori privat dhe aj qeveritarë të ndajnë treguesit e kërcnimit, krijon një ekozistem që sapo që njihet një kërcënim informohet i gjith komunitieti.

**CVE** është databaz ku ruhen të gjitha dobësitë të standarizuara dhe të emëruara.

Intelegjenca kërcënuese i ka dy standarde të cilat mundësonë shkëmbinin e informacionit të kërcënimit, **STIX** dhe **TAXII**.

STIX është specifikim për shkëmbimin e informatave të kërcënimeve kiberenetike mes organizatave.

TAXII është specifikim për një protokoll që lejon komunikimin e CTI mbi HTTPS.

Kriptografia ndihmon në realizimin e katër objektivave kryesore të siguris së informacionit : **Konfidencialiteti i të dhënave** : Të dhënat mund të qasen vetëm nga personat e autorizuar. **Integriteti i të dhënave** : Të dhënat nuk mund të ndryshohen nga personat e pa autorizuar. **Authenticiteti i origjinës** : Të dhënat kanë origjin nga burimi i pritshëm. **Mosdeklarimi** : Integrimi i mesazhit është i pa kundërshtueshëm nga dërguesi.

**Kriptologjia** është shkenca e krijimit dhe thyerjes së kodeve, ndahet në dy disiplina : **Kriptografia** : Merret me krijimin dhe përdorimin e kodeve për komunikime private. **Kriptoanaliza** : Merret me thyerjen e kodeve.

Një shifër është një algoritëm që përbëhet nga një seri hapasht të përcaktuar mirë të cilët mund të përdoren gjatë enkriptimit dhe dekriptimit të mesazheve.

Llojet e shifrave : **Zëvendësimi i shifrave** : e ruan frekuencën e mesazhit origjinal. **Shifra e transpozimit** : shkronjat nuk zëvendësohen thjesht ndryshohen. **Shifra polyaplfabetike** : Bëhen zëvendësime duke përdorur alfabeta të shumtë.

**Plain text** – mesazhi origjinal. **Cypher Text** – Mesazhi i shifruar.

Disa nga metodat e kriptonalizës janë : **Brute force**, **CypherText**, **PlainText**, **Zgjedhur-PlainText**, **Zgjedhur-CypherText**, **Meet-in-the-middle**.

Siguria e ekriptimin sot qëndron në sekretin e qelsave e jo në algoritëm.

Dy Terma që kanë të bëjn me qelsa : **Gjatësia kryesore** : ne e quajm gjatësia kyce matet me bit (copa). **Hapsira e Qelsit** : Numri i mundësive që krijohen nga një gjatësi specifike kyqe.

**Hierat** kriptografike përdoren për të verifikuar dhe siguruar integritetin e të dhënave.

**Hashing** bazohet në një funksion matematikor të një anshëm i cili pranon input binar të qfardo gjatësie me qfado përmbajtie dhe si rezultat jep një vlerë fikse që quhet **hash**. Dy grupe të ndryshme të dhënave është e pa mundur të ken hash të njëjtë.

Tri algoritmet më të njohur të hashing : **MD5 128-bit, SHA-1** dhe **SHA-2**. MD5 dhe SHA-1 janë algoritme të trashëguara dhe nuk preferohet të përdoren.

**HMAC** përdoret për të shtuar autentifikimin në integritetin e të dhënave, HMAC përdorë edhe një qelsët sekret i cili i ipet hash funksionit së bashku me mesazhin për të fituar hash. Vetëm dërguesi dhe pranuesi e din qelsin sekret, dhe pa kët qelës nuk mund ta thyesh HMAC. Nëse hash i dërguesit është i njëjt me atë të pranuesit atëher mesazhi nuk është i ndryshuar.

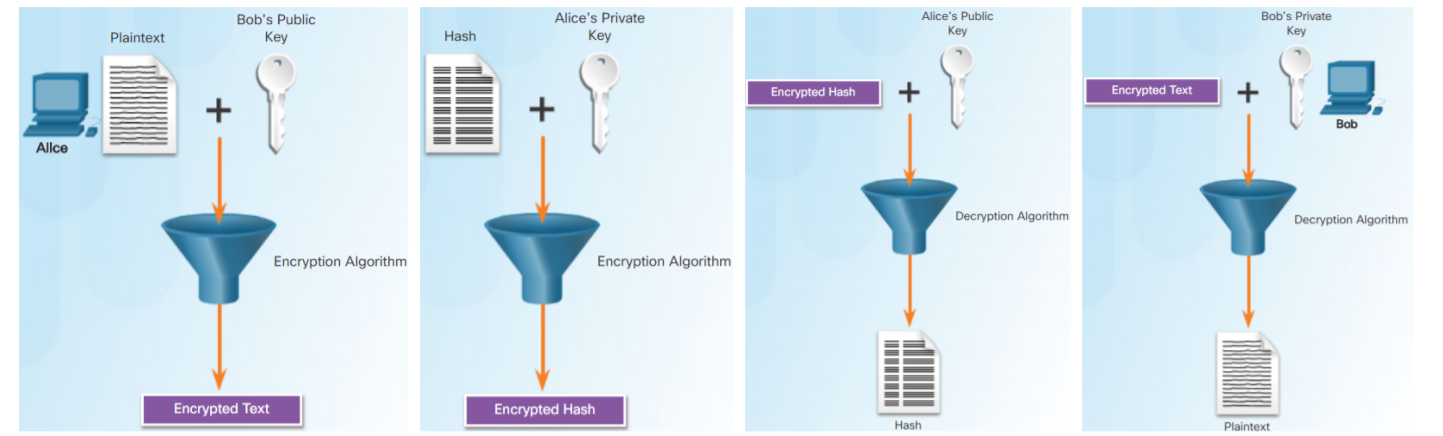
Algoritmet e enkriptimit ndahen në dy klasa : **Algoritmet simetrike** : Përdorin vetëm një qelës për kriptim dhe dekriptim, përdoren në VPN, përdorin pak cpu, gjatësia e qelësit zakonisht është mes 112 bit - 256bit. **Algoritmet asimetrike** : Përdorin dy qelsa një për kriptim dhe një për dekriptim, përdoret nga HTTPS.

Algoritmet e kriptimit simetrik klasifikohen në : **Shifra të bllokut** : Transmetojnë tekstin normal në blloqe 64-bit ose 128-bit të kriptuara. **Shifra e drejtpërdrejt** : Transpetojnë bit për bit testin e kriptuar.

**Algoritmet më të njohura simetrike** : DES, 3DES, RC, AES, SEAL.

Algoritmet asimetrike përdorin dy qelsa një privat dhe një publik, konfidencialiteti mund të ruhet duhet përdorur formulën qelës publik + qelës privat = konfidencialitet, Pra e dhëna kriptohet me qelsin publik dhe dekriptohet vetëm me qelsin privat.

Algoritmet asimetrike mund të përdoren për autentifikim : kjo arrihet kur përdoret qelsi privat për kriptim, qelsin privat e ka vetëm një burim, dhe nga pranuesi përdoret qelsi publik për dekriptim, nëse dekriptohet verifikohet se mesazhi ka ardhur nga burimi i dëshiruar.

Kombinimi i të dyave siguron konfidencialitet, integritet dhe autentifikim të mesazhit. 

Algoritëm asimetrik tjetër është edhe **Diffie-Hellman** është algoritëm matematikor ku dy kompjuter gjenerojnë një qelës të përbashkët identik, dhe dërgoj mesazhe duk i kriptuar me kët qelës mirpo nuk dërgohet qelësi përshkak se ai gjenerohet me anë të algoritmit. Bëhen shumë llogaritje të cilat mund ta ngadalsojnë sistemin.