**Hyrje ne sigurine e te dhenave**

Llojet e sulmeve : **Hijacked people** – Lidhen me hotspote të hapura mashtruese të cilat janë të ngritura nga një mashtrues, kështu pasi që viktima viziton webe të ndryshme si ai I bankës sulmuesi fiton qasje në resurset e viktimës. **Ransomware** – Ransomware gjindet I instaluar në kompjuterin e viktimës I cili është në gjendje të grumbulloj të dhënat e tij , të cilat mund të përdoren për kërcnime me qëllim të dëmshpërblimit. **Stuxnet Worm** – Instalohet në windows os dhe për qëllim ka kontrollimin PLC me qrast mund të dëmtoj centrifugat në objektet bërthamore, transmetohet me anë të USB. **Sulmuesit Amator** – Njihen si kiddies script, kan pak eksperienc ose nuk kanë fare , përdorin mjetet ekzistuese dhe udhëzimet e gjendura në internet. **Sulmuesit Hacktivist** – Protestojnë kundër organizatave ose qeverive, shkruajn video dhe publikojn video, marrin të dhëna konfidenciale që pastaj I vendosin në publik, zakonisht ndalojn shërbimet e web duke përdorur sulmet DDos. **Sulmet për përfitimet financiare** – Gjdo lloj aktiviteti I piratërisë bëhet për qëllime të fitimeve financiare, sulmet e bankave, vjedhia e informative personale dhe gjdo gjë që sjell përfitime financiare. **Sekretet e tregëtis dhe politikat globale** – Shtet gjithashtu përfshihen në hapsirën kibernetike për qëllime të ndryshme si sulmi I vendeve tjera, përgjimet indistruale, ndërhyrja në politikat e brendshme, për përfitim të përparsis në tregëtin globale.

**PII** – Informacioni personal identifikues është gjdo informacion që mund ta indetifikoj pozitiv një person, si ID personale, emri, data lindjes, llogarit bankare, adresat. Kto informata shiten në tregun e zi dhe në web e zi, që më vonë të përdoren për qëllime të falsifikimit të dokumentave.

**PHI** – Janë informata personale të mjekësis që gjitashtu mund të keqpërdoren.

Kërcnimet kibernetike mund të ndikojn në humbjen e përparsis në konkurrenc kjo si rrjedhoj e mos besimit nga ana e klientit bazuar në atë që nuk je në gjendje të mbrosh të dhënat personale të tyre(PII).

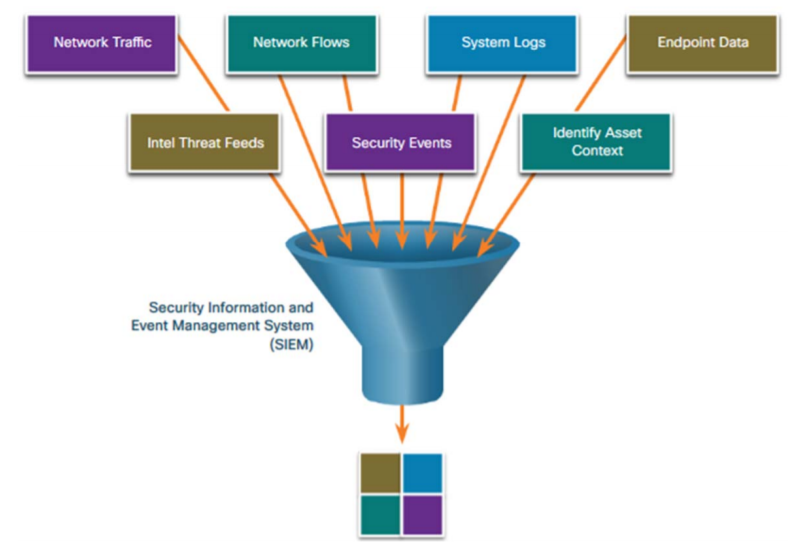
**Qendra e operacioneve të sigurisë** (SOC) – Ofrojnë shërbime si monitorim, udhëheqje dhe zgjedhje të kërcnimeve, mund të jet në shtëpi, në pronësi si dhe duke operuar nga një biznes.

Elementet kryesore të SOC janë : njerëzit, proceset dhe teknologjit.

Sipas institutit SANS njerëzit në SOC ndahen në 4 nivele : **1.Analistët e alertit**, **2.Reaguesit e incidetit**, **3.Eksperet e lëndës(SME)**, **4.Menaxheri I SOC**.

Analistët e alertit I motiorojnë rreshtat e alarmit të siguris, e verifikojn nëse alarmi I shkaktuar paraqet rrezik, nëse po e përciellin tek hetuesit nëse jo e deklarojn si alaram të rrem.

**SIEM** – Sistemi I informacioneve të sigurisë dhe menaxhimin e ngjarjeve : I mbledh dhe I filtron të dhënat, zbulon dhe klasifikon kërcnimet, analizon dhe heton kërcnimet, zbaton masat parandaluese dhe I adreson kërcnimet e ardhshme.



Një sistem konsidetohet të jet aktvin deri në 99.999% të kohës nëse gjat gjith vitit ka pasur ndërprerje max 5 minuta e 26 sekonda.