# Hyrje

Koncepti i përgjigjes ndaj një incidenti është i njohur për shumicën e njerëzve në kontekstin e situatave emergjente të tilla si ato të shkaktuara nga një fatkeqësi natyrore. Parimet themelore janë të njëjta edhe në përgjigjen e incidenteve në internet, duke përfshirë parandalimin, përgatitjen, planifikimin, menaxhimin e incidentit, recovery, zbutjen, rehabilitimin, analizën pas incidentit, dhe mësimet e nxjerra.

Ky material është i ndarë në katër pjesë kryesore. Pjesa e parë përqendrohet në planifikimin për një incident dhe përfshin krijimin e një ekipi të reagimit ndaj incidenteve kibernetike dhe ngritjen e një plani përgjigjeje me personelin e duhur, politikat dhe procedurat. Pjesa e dytë është ajo e menaxhimit të incidentit, i cila diskuton katër fusha: (1) zbulimin e çështjeve të mundshme ose faktike; (2) kontrollin e ngjarjes, sidomos kur kanë të bëjnë me malware të instaluara në serverat; (3) rehabilitimin duke përfshirë çrrënjosjen e malware; dhe në fund (4) rimëkëmbjen nga një ngjarje dhe rivendosjen e sistemit me funksionalitetet e tij të plota. Pjesa e tretë ka të bëjë me analizën pas incidentit, i cili përfshin përcaktimin e shkakut, rrugën e qasjes, dobësitë, dhe informacione të tjera të nevojshme për të kuptuar më mirë incidentin e ndodhur, si dhe mënyrat për ta parandaluar atë në të ardhmen. Pjesa e katërt dhe e fundit lidhet me përdorimin e tools-eve të ndryshme gjatë menaxhimit të incidenteve, rëndësia e përdorimit të tyre dhe llojet kryesore. Gjithashtu paraqitet dhe një tool konkret duke treguar dhe si mund të konfigurohet ai.

Një numër i madh dokumentesh ekziston dhe është në dispozicion rreth kësaj teme. Sidoqoftë, ky punim ofron një informacion background, praktikat më të mira dhe thekson konsideratat që duhen marrë parasysh në programet e përgjigjes ndaj incidenteve sidomos përsa i përket tools-eve që mund të përdoren.

Në kontekstin e sigurisë kibernetike, një incident në mënyrë tipike përfshin qasje të paautorizuar në rrjetet kompjuterike dhe pajisjet me veprime që rezultojnë me pasoja negative për pronarët e pasurive. Dëmtimi mund të përfshijë të dhëna të vjedhura, ekspozim të informacionit privat apo të dhënave të ndjeshme, ndërprerje të shërbimeve kryesore, mbyllje të operacioneve të prodhimit, dëmtim të pajisjeve fizike dhe mjedisit, dhe dëmtim të website-ve.

Reagimi ndaj një incidenti kibernetik është mënyra në të cilën një organizatë i përgjigjet një incidenti kibernetik të perceptuar që mund të ndikojë në asetet e organizatës ose në aftësinë e saj për të funksionuar. Një përgjigje e gabuar mund të rezultojë në veprime kaotike dhe reaksionare që janë të paefektshme ose shkaktojnë më shumë dëme. Çdo organizatë duhet të përpiqet për një përgjigje të planifikuar që ka ndikim minimal në operacionet e saj. Përmbushja e kësaj kërkon plane dhe procedura që janë krijuar dhe testuar para se të ndodhë një incident kibernetik.

Mundësitë e një ndërhyrje të suksesshme në rrjetet kompjuterike të çdo organizatë, janë të larta për të gjitha sistemet direkte ose indirekte të lidhura me sistemet e biznesit të një organizate dhe / ose me internet. Shumë kompani të profilit të lartë dhe organizata qeveritare raportojnë mijëra përpjekje për akses të palejuar çdo ditë. Sulmuesit përdorin një shumëllojshmëri të teknikave, të tilla si reconnaissance, botnets, backdoors, social engineering, dhe malware të fshehur, për të provuar dobësitë kibernetike.

# Planifikimi i përgjigjes ndaj incidenteve kibernetike

Pika fillestare në përgjigjen ndaj incidenteve është faza e planifikimit dhe përgatitjes. Të gjithë elementet janë sjellë së bashku për të parandaluar një incident nëse është e mundur, ose të jenë të gatshëm për t'iu përgjigjur një incidenti, nëse ai ndodh.

## Organizimi i ekipit

Hapi i pare për të qënë i aftë në përgjigjen ndaj incidenteve është organizimi i ekipit. Shumica e grupeve janë të organizuar në atë që zakonisht quhet një CSIRT. Përgjegjësitë e një CSIRT ndryshojnë në varësi të madhësisë së organizatës dhe strukturës së saj. Ato mund të përfshijnë:

* Veprimin si një burim ekspertësh kundrejt kërcënimeve të sigurisë kibernetike dhe dobësive
* Shërbimin si një qendër parandaluese e incidenteve, informacioni, dhe analize
* Zhvillimin e politikave dhe procedurave organizative në lidhje me reagimin ndaj incidenteve
* Identifikimin e ndikimeve operacionale të organizatës në rast të ndodhjes së një incidenti
* Krijimin dhe testimin e planit të përgjigjes ndaj incidenteve
* Veprimin si një pikë e vetme kontakti për raportimin e të gjithë incidenteve
* Përgjigjen ndaj incidentit kur ai ndodh
* Implementimin e masave për të parandaluar një përsëritje të incidentit

## Vendosja e Politikave dhe Procedurave

Ndërkohë që politikat dhe procedurat janë të rëndësishme në shumicën e funksioneve të biznesit, në procesin e reagimit ndaj incidenteve janë akoma më të rëndësishme, sepse vendimet janë duke u bërë nën presionin e ndalimit të aktivitetit, kostos së lartë financiare, shpesh në kohën më të papërshtatshme, dhe në situatat kur personat me autoritet nuk mund të jenë në dispozicion. Zhvillimi i procedurave dhe politikave mbështetëse, ndërkohë që anëtarët e ekipit nuk janë nën presion është vendimtar. Në atë kohë, anëtarët e ekipit mund të diskutojnë dhe të peshojnë mundësitë, testojnë qasjet, analizojnë ndikimet dhe alternativat, të marrin të dhëna nga menaxhimi si dhe miratimin e tij.

Procedura operative të shkruara qartë dhe të hollësishme duhet të zhvillohen për të zbatuar politikën e përgjigjes ndaj incidenteve. Procedurat e gjetura në një plan të përgjigjes ndaj incidenteve janë të ngjashme me ato që gjenden në raste urgjente jo kibernetike dhe duhet të testohen para se të ndodhë ngjarja. Problemet mekanike dhe afatet kohore të procedurave duhet të zbulohen gjatë fazës së zhvillimit, kur mund të bëhen rregullime, në vend të zbulimit gjatë një përgjigjeje reale.

## Ndërtimi i planit të përgjigjes ndaj incidenteve

Plani i përgjigjes ndaj incidenteve përcakton dhe dokumenton procedurat dhe veprimet që zbatojnë politikën e përgjigjes ndaj incidenteve. Ai përkufizon incidentet e sigurisë dhe përshkruan hapat që duhet të merren për të reaguar ndaj incidentit dhe për të zbutur dëmtimin e organizatës. Një shumëllojshmëri modelesh si plane për përgjigjen ndaj incidenteve dhe shembuj janë në dispozicion, disa prej të cilave i janë bashkëngjitur këtij dokumenti në fund. Ato mund të shërbejnë si një pikënisje e mirë për ndërtimin e planit. Seksionet kryesore në vijim duhet të merren parasysh gjatë krijimit të planit:

1. *Përmbledhja, Qëllimet dhe Objektivat.* Këto pjesë të planit përcaktojnë se çfarë do të realizohet.
2. *Përshkrimi i incidentit.* Shumë incidente klasifikohen mjaft lehtë. Këto përfshijnë sulmet denial-of-service, akses i paautorizuar në rrjet, aksesimi informacioneve të mbrojtur dhe private, dëmtimi i faqeve të internetit, keqpërdorimi i shërbimeve, etj
3. *Zbulimi i incidentit.* Kjo pjesë përfshin mënyrat sipas të cilave një incident është identifikuar dhe raportuar. Ndërkohë që disa raste incidentesh janë shumë të dukshme (një sulmues është gjetur i loguar në rrjet ose një faqe interneti është dëmtuar), zbulimi i incidenteve të tjerë kërkon tools-e analize të automatizuar, sisteme të modeleve të sjelljes dhe një vetëdije të operatorëve, mbikëqyrësve, dhe stafit tjetër rreth asaj se çfarë duhet kërkuar.
4. *Njoftimi i incidentit.* Pasi një ngjarje jonormale identifikohet, asaj duhet t’i jepet prioritet për të përcaktuar shkakun dhe nëse kjo është një ngjarje e vogël ose në qoftë se ajo kërkon përshkallëzim të menjëhershëm. Kjo pjesë e planit duhet të identifikojë pikën e kontaktit për raportimin e incidenteve.
5. *Analiza e incidentit.* Procedurat në plan duhet të adresojnë se si të vlerësohet dhe analizohet një incident i raportuar. Incidenti mund të raportohet nga burimet e brendshme apo të jashtme dhe mund të ndodhë në çdo kohë. Në këtë fazë të menaxhimit të incidentit, anëtarët e ekipit që marrin raportin duhet të përcaktojnë:

* Cilat janë rreziqe apo efektet në sigurinë e objektit që mund të shkaktohen nga ngjarja e ndodhur
* Nëse incidenti i raportuar është i vërtetë apo është një false positive
* Në cfarë faze është incidenti, është në fillim, në proces, apo ka ndodhur tashmë
* Çfarë ndikimi mund të ketë për organizatën
* Lloji i veçantë i incidentit
* Çfarë sistemesh dhe pajisjesh janë ndikuar ose mund të ndikohen nga incidenti
* Nëse incidenti ka potencial për t’u përhapur në të gjithë rrjetet e tjera apo edhe jashtë për partnerët apo konsumatorët

1. *Veprimet e përgjigjes.* Kjo pjesë është thelbësore për planin, sepse përcakton procedurat që duhen ndjekur për secilin lloj incidenti të zbuluar. Një incident në mënyrë tipike ndodh në kohën më të papërshtatshme, kështu rritet stresi dhe presioni ndaj stafit, ka pak kohë për mundësitë e testimit dhe nuk mund të realizohet një bashkëpunim efektiv me menaxhimin e lartë. Kështu bëhet i domosdoshëm fakti që veprimet të mendohen mirë, të përcaktohen dhe të testohen para se të ndodhë incidenti.

Gjatë përcaktimit të veprimeve të përgjigjes, duhen marrë në konsideratë cështjet e mëposhtme:

* Përgjigja duhet të jetë e lidhur direkt me llojin e incidentit, nuk mund të përshtatet me të gjitha situatat e njëjta qasje, dhe llojet e rinj te sulmeve duhet të konsiderohen në mënyrë të rregullt.
* Plani duhet të marrë parasysh dhe situata të jashtëzakonshme, duke përfshirë netët, fundjavat, festat, stafin e padisponueshëm, dhe mosfunksionimin e pajisjeve të komunikimit. Faktorët e jashtëm që ndikojnë në plan, të tilla si humbja e qëllimshme apo aksidentale e energjisë, gjithashtu duhet të merren parasysh.
* Veprimet e identifikuara në plan duhet të përfshijnë një përgjigje të plotë që mbulon kontrollin e problemit, rivendosjen e operacioneve në gjendje funksionale si dhe parandalimin e rindodhjes së incidentit. Siç u përmend më lart, veprimet do të varen nga lloji i incidentit dhe ndikimi i tij.
* Procedurat e përgjigjes duhet të testohen në një situatë sa më reale që të jetë praktik përcaktimi i elementëve që mungojnë, që janë keqkuptuar, ose që janë të paplotë ose të pasaktë. Mund të bëhen korrigjime dhe pastaj të ritestohen derisa të gjithë shqetësimet të jenë identifikuar.
* Veprimet e përgjigjes duhet të peshohen kundrejt ndikimit në organizatë. Disa aktivitete riparuese mund të shkaktojnë më shumë dëm për organizatën se sa vetë incidenti.

1. Seksione të tjera. Zonat e përmendura më sipër janë elemente thelbësore të planit të përgjigjes ndaj incidenteve. Megjithatë plani mund të ndahet dhe në mënyrë më të hollësishme, në qoftë se dëshirohet, dhe mund të përfshijë seksione të tjera, të tilla si gjurmimi i incidentit (e këshillueshme) dhe raportimi.

## Realizimi i planit

Edhe planet më të mirë të përgjigjes nuk mund të parashikojnë të gjitha pengesat me të cilat do të përballen, kur ndodh një incident i vërtetë, as nuk mund të parashikojnë, në të gjitha rastet, se si njerëzit do të reagojnë në situata të paparashikuara. Njerëzit të cilët duhet të përmbushin role të caktuara shpesh janë të padisponueshëm, njerëz të rinj mund të kenë zëvendësuar punëtorë të trajnuar më pare etj. Ngjarjet e paparashikuara mund të ndodhin kur vendimet kanë pak ose aspak kohë për analizë.

Shumë probleme që ndodhin në një incident të vërtetë mund të jenë të pranishme dhe gjatë fazës së testimit. Kjo do të thotë se ka një mundësi në dispozicion për të shqyrtuar, analizuar, dhe për të ndryshuar procedurat pa vuajtur efektet e vendimeve katastrofike.

Një shumëllojshmëri sistemesh janë në dispozicion për të mbledhur informacion të dobishëm. Disa lloje kryesore të tyre janë:

*Networks Intrusion Detection Systems (NIDS)*; *Protocol-based Intrusion Detection System (PIDS)*; *Host-based Intrusion Detection System (HIDS)*; *Intrusion Prevention System (IPS)*; *Netëork and Device Logging*; *Configuration of Data Generators*.

# Menaxhimi i incidenteve

## Zbulimi i Incidentit

Zbulimi i një incidenti që në fillim do të ndihmojë për të kufizuar apo edhe të parandaluar dëmtime të mëdha në organizatë dhe rivendosjen në funksionim sa më shpejt të sistemeve të dëmtuar. Ky seksion fokusohet në metodat e zbulimit të incidenteve duke diskutuar shenjat paralajmëruese që tregojnë kur një incident kibernetik është në pritje, gjithashtu kategorizimin dhe prioritizimin e incidenteve kibernetike, përgjigjet, si dhe hapat e rekomanduara të zbulimit.

### Raportimi dhe Koordinimi

Një shans i mirë ekziston kur situata me të cilën përballet organizata ka ndodhur më parë dhe informacioni për zbulimin, parandalimin dhe rikuperimin është menjëherë në dispozicion. Stafi mbështetës i CSIRT-it mund të ndihmojnë në të gjitha aspektet e menaxhimit të incidentit nëse është e nevojshme.

### Zbulimi nga vëzhgimi

Ka dy metoda kryesore për të zbuluar një incident. E para është nëpërmjet vëzhgimit nga përdoruesi të një sjelljeje jonormale të sistemit ose komponentëve të tij. Vëzhgimi mund të vijë nga cdo anëtar i organizatës, duke përfshirë këtu operatorët, inxhinierët e proceseve, ose administratorët e sistemit. Metoda e dytë është zbulimi automatik nëpërmjet aplikacioneve, të tilla si monitoruesit e rrjetit, aplikacionet e analizimit të trafikut të rrjetit, IDS-të dhe programet antivirus që mund të zbulojnë malëare të ndryshëm, përpjekjet për ndërhyrje, shkeljen e politikave, shfrytëzimet si dhe dështimet e komponentëve. Megjithatë edhe pse automatike kjo mënyrë e zbulimit kërkon dhe bashkëveprimin e njerëzve përsa i përket konfigurimit, rishikimit, analizës dhe veprimeve që do ndërmerren.

Metoda e cila kërkon vëzhgimin e përdoruesit është në thelb një qasje pas faktit dhe shoqërohet me një numër rreziqesh negative. Pas faktit do të thotë se një sulm apo ndërhyrje është duke u zhvilluar aktualisht apo ka ndodhur tashmë. Kështu, kjo metodë nuk ofron mbrojtje fillestare ose aftësinë e parandalimit të një incidenti kibernetik. Disa nga efektet negative që lidhen me këtë metodë janë të listuara më poshtë:

* Dëmtimi i sistemit fizik ose i pajisjeve
* Nxjerrje e të dhënave kritike të sistemeve të kontrollit
* Ndryshime në algoritmet e konfigurimit të softëare-ve për të prodhuar veprime të ardhshme të padëshiruara të sistemit
* Injektimin e programeve malware, të tillë si viruset apo worms, të cilët komprometojnë konfidencialitetin, integritetin dhe disponueshmërinë e sistemit.

Eksperienca e operatorit mund të jetë burimi më i mirë për zbulimin e devijimeve nga normalja, për shkak se ka dallime delikate në sjelljen e një pajisjeje të cilat janë të vështira për tu identifikuar. Shumë operatorë me përvojë e dinë se kur gjërat nuk janë duke punuar në mënyrën e duhur dhe mund të zbulojnë probleme të mundshme kibernetike.

Menaxhimi duhet t’iu sigurojë kontakte specifike dhe udhëzime për raportimin operatorëve dhe çdo personeli të tjera që mund të jetë në një pozicion për të zbuluar një sjellje të pazakontë të sistemit apo pajisjeve. Kjo duhet të përfshijë nr telefoni, e-mail dhe informacione të tjera që i mundësojnë operatorit të kontaktojë CSIRT. Këto udhëzime duhet të përfshijnë edhe një listë të informacionit të mbledhur dhe një raport për të ndihmuar CSIRT në analizimin e një sjellje të pazakontë. Informacionet e kontaktit dhe listë e plotë e udhëzimeve duhet të afishohen në vende të përshtatshme dhe lehtësisht të aksesueshme.

### Metodat e automatizuara të zbulimit

Metodat e automatizuara të zbulimit të incidenteve mund të jenë jashtëzakonisht të vlefshme për parandalimin e dëmtimeve në një organizatë. Natyra e sulmeve, numri i tentativave, dhe koha e harxhuar e përpjekjeve krijojnë një mjedis ku vëzhgimi manual është shumë i vështirë, nëse jo i pamundur. Shumica e organizatave kanë kapacitetet e duhura për një zbulim të automatizuar të incidenteve, duke përfshirë IDS komerciale të sofistikuara bashkangjitur rrjetit ose dhe një firewall logging të thjeshtë. Është thelbësore që një balancë e duhur automatizimi të arrihet, të konfigurohet si duhet, të punojë sipas qëllimit, dhe të përfshijë rishikimin e duhur njerëzor dhe bashkëveprimin.

Të gjithë sistemet e automatizuar të zbulimit të incidenteve kanë të paktën tre komponentë që janë të nevojshëm për të punuar në mënyrën e duhur:

1) *Një metodë e programuar për të zbuluar një ngjarje të jashtme ose në shënjestër.* Kjo mund të përfshijë zbulimin e një vargu string që përputhet me një nënshkrim virusi të njohur apo sjellje të caktuara të rrjetit të tilla si një sulm denial-of-service. Ajo gjithashtu mund të zbulojë përpjekjet për të hyrë në porta të caktuara të kufizuara, ose mund të njohë një adresë burim IP e identifikuar si e paligjshme.

2) *Aftësia për të kapur dhe për të raportuar ngjarjen ose ndryshimin.* Zbulimi i një ngjarje është fillimi; por më pas aplikacioni duhet të organizojë dhe të paraqesë të dhënat në një format të dobishëm. Sistemet e avancuara përfshijnë filtrimin dhe raportimin; të tjerët mund të shkruajnë vetëm informacion identifikues në një skedar teksti. Për të qënë të dobishëm, komponentët e specializuar duhet të jenë në gjendje për të shkruar ose paraqitur ndryshimet e gjendjes në një formë auditi ose log file. Disa procese nuk mund të shkruajnë në mënyrë të vazhdueshme një rrjedhë konstante të dhënash pa ndikuar operacionet e pajisjeve. Në këto raste, situata ideale do të ishte vendosja e rangjeve dhe raportimi vetëm jashtë tyre.

3) *Komunikimi i flagged events në një operator.* Disa sisteme të sofistikuara si një IPS mund të jenë në gjendje të ndërmarrin disa veprime parandaluese pa ndërhyrjen e njeriut. Megjithatë në një situatë më tipike, një njeri duhet të jetë i përfshirë për të dalluar false positive dhe për të ndarë problemet e mirëmbajtjes nga sulmet e mundshme kibernetike. Personeli gjithashtu duhet të jetë në gjendje për t'iu përgjigjur të dhënave dhe të fillojë veprimet e përshtatshme, duke përfshirë aktivizimin e CSIRT kur është e nevojshme.

Secili nga tre komponentët e një sistemi të automatizuar zbulimi incidentesh duhet të funksionojë në mënyrë të përshtatshme ose sistemi do dështojë. Ndërkohë që dy komponentët e parë kanë kufizime të caktuara, sfida më e madhe ka të bëjë me aspektet praktike të komponentit të tretë lidhur me vëzhgimin dhe përgjigjen e personelit. Vështirësitë më të mëdha hasen në disponueshmërinë, trajnimin në identifikimin e ngjarjeve dhe fillimin e një përgjigjeje të duhur kur një ngjarje e padëshiruar është zbuluar.

### Incident Response Tools

Në paragrafët më lart përmendëm tools-e të ndryshëm të automatizuar për të zbuluar një incident të mundshëm gjatë operacioneve rutinë. Tools-e të tjerë janë të dobishëm në kapjen dhe analizimin e të dhënave më specifike dhe të detajuara. Ka tools-e që mund të përdoren si për monitorimin e vazhdueshëm dhe zbulimin e incidentit dhe për zgjidhjen. Shembuj të tools-eve për përgjigjen ndaj incidenteve përfshijnë:

*Netflow Capture and Analysis.* Këto mjete ofrojnë metoda për të kapur dhe shfaqur llojin e trafikut që kalon në rrjet, duke përfshirë trafikun e drejtuar për brenda dhe atë për jashtë. Këto mjete mund të izolojnë të dhëna nga aplikacionet, biseda, domain-e, endpoints, dhe protokollet. Shumë nga këto tools-e ruajnë të dhënat për analizim dhe cështje ligjore.

*Network Performance Monitors.* Këto tools-e ofrojnë disa elemente shtesë përsa i përket performancës së rrjetit dhe mund të ndihmojnë në identifikimin e performancave jonormale që mund të ndodhin. Ata mund të përfshijnë gjithashtu dhe monitorimin e bandwidth dhe analiza, si psh dhe analizën e network routing.

*Availability Monitors.* Këto tools-e mund të ndihmojnë në përcaktimin nëse pajisjet e rrjetit janë në dispozicion duke përdorur komanda të avancuara ‘ping’ të cilat tregojnë përgjigje në kohë reale.

*Application Monitors.* Një aplikacion i veçantë mund të monitorohet nëse ekziston dyshimi për akses të paautorizuar ose manipulim. Këto tools-e lejojnë një analizë më të hollësishme të një aplikacioni të dyshuar në krahasim me monitorimin e përgjithshëm të rrjetit.

*Packet and Traffic Reconstructors.* Këto tools-ezakonisht shoqërohen ose janë pjesë e një network traffic monitor, dhe rivendosin filet së bashku në formatin e tyre origjinal në rrjet, duke kapur një pamje statike të rrjetit dhe trafikun përkatës.

*Protocol Analyzer.* I ngjashëm me tools-et e tjera të përmendura më lart, ky tool kap dhe ruan paketa të dhënash për analiza të mundshme ligjore, duke përfshirë informacion statistikor të konsoliduar.

*Trace Route dhe Whois tools.* Këto tools-e mund të jenë të dobishëm në gjetjen e ndërhyrësit nëpërmjet vendndodhjes së kompjuterit burim. Funksionet e lidhura lejojnë bllokimin e adresave IP dhe raportimin.

### Kategorizimi i incidenteve

Pasi është identifikuar, një sulm kibernetik duhet të kategorizohet, dhe përgjigjes i jepet përparësi bazuar në atë kategorizim. Kategorizimi duhet të bazohet në llojin e incidentit dhe dëmin potencial që ka ai për organizatën. Lloji i incidentit do të na cojë në nivelin e duhur të reagimit. Plani i përgjigjes ndaj incidenteve duhet të përshkruajë në detaje se çfarë niveli reagimi (dhe niveli përpjekjesh) duhet të jetë për secilin lloj të incidenteve.

Prioritizimi i përgjigjes duhet të bazohet në efektin aktual dhe të mundshëm të incidentit, si dhe rëndësinë e pajisjeve të prekura dhe të sistemit të operacioneve të organizatës. Pyetjet e mëposhtme ndihmojnë në përcaktimin e kritereve për kategorizimin/prioritizimin:

* Si ndodhi shfrytëzimi dhe mund të ndodhë përsëri? Në çfarë afati kohor?
* A ishte ky shfrytëzim i brendshëm apo i jashtëm për organizatën?
* Çfarë lloji mjetesh sulmuese janë vendosur në sistem, nëse ka?
* Cfarë rrjetesh dhe sistemesh janë prekur nga sulmi, dhe mund të përhapet problemi në hapësira të tjera?
* Ka probleme ligjore ose të sigurisë të shkaktuara nga sulmi?
* Sa rritet ndikimi nëse mungon një përgjigje ndaj incidentit brenda orëve apo ditëve?
* Sistemi do të dështojë me siguri apo do të vazhdojë të funksionojë?
* Sa të rëndësishme janë komponentët e prekur në organizatë dhe për operacionet në përgjithësi?

Në vijim jepen hapat e rekomanduar që duhen realizuar për kategorizimin / prioritizimin:

1. Caktimi i një investiguesi kryesor përgjegjës për identifikimin e çdo incidenti.
2. Vleresimi nëse incidenti ka ndodhur me qëllim të keq apo është i paqellimshëm. Në qoftë se ngjarja është jo me qëllim të keq nuk do të jetë e nevojshme përfshirja e plotë e CSIRT, edhe pse disa burime mund të përdoren për të zgjidhur problemin.
3. Identifikimi dhe vlerësimi i provave në mënyrë të detajuar dhe mbajtja e dokumentacionit të saktë me akses të kontrolluar në prova.
4. Koordinimi me personelin e veçantë që ofron shërbimet e rrjetit në sistemin e prekur.
5. Gjithashtu duhet të përfshihen hapa specifikë unikë të organizatës. Ato duhet të përcaktohen qartë në planin e përgjigjes ndaj incidenteve dhe duhet të drejtojnë veprimet e CSIRT gjatë kategorizimit dhe prioritizimit të një incidenti.

## Frenimi (Containment) kufizimi

Ndërsa frenimi shpesh fokusohet në parandalimin e përhapjes dhe efekteve të programeve malware, disa lloje të tjera incidentesh kërkojnë veprime të tjera që lidhen me frenimin. Një shembull i tillë është një punonjës i cili akseson informacion të paautorizuar duke përdorur account-in e një personi tjetër dhe fjalëkalimin e tij. Frenimi i situatës do të kërkonte ndalimin e aksesit të punonjësit në informacionet dhe më pas zbatimin e masave disiplinore sipas nevojës.

Rasti kryesor i frenimit është kur malware i një forme të caktuar është vendosur në sistem. Ky seksion do të fokusohet në çështjet e kufizimit lidhur me software që janë vendosur në servera ose komponentë të tjerë për të krijuar një rrugë aksesi për sulmuesin, ose në mënyrë të pavarur të shkaktojë dëme në sistem. Informacion shtesë mund të gjendet në NIST PS 800-83, "Guide to Malware Incident Prevention and Handling", lëshuar në nëntor të vitit 2005.

Ka dy qëllime kryesore në frenimin e malware-ve. Qëllimi i parë është ndalimi i përhapjes në pjesë të tjera të sistemit. Qëllimi i dytë është parandalimi i dëmtimit të mëtejshëm të organizatës. Edhe në qoftë se malware është i izoluar nga përhapja në komponentët apo rrjetet e tjera të organizatës, ose në të gjithë objektet, ai mund të vazhdojë të shkaktojë dëme në segmentin e izoluar.

Frenimi i malware nuk ndjek një rrugë standard në çdo organizatë. Ai ndryshon bazuar në llojin e malware, në rëndësinë e sistemit të prekur, si dhe bazuar në nivelin e pranueshëm të rrezikut. Kështu, çdo organizatë duhet të përcaktojë veprimet e duhura bazuar në kërkesat unike të sistemit të saj. Kriteret e frenimit duhet të dokumentohen mirë dhe të kuptohen nga anëtarët e organizatës dhe nga CSIRT.

Ka disa metoda për frenimin e malware-ve në dispozicion. Metoda e parë përdor teknologji të automatizuara të tilla si programet për heqjen e virusit që eleminojnë problemin dhe rivendosin funksionet e sistemit. Metoda e dytë ndalon shërbimet, ndërsa incidenti është duke u trajtuar, dhe metoda e tretë bllokon lidhje të caktuara të rrjetit duke përdorur një proces filtrimi.

Përdorimi i teknologjive të automatizuara siguron zbulimin e menjëhershëm dhe përgjigjen në qoftë se përdoruesi zgjedh në program aplikacionin në këtë mënyrë. Kjo metodë mund të veprojë vetëm kundër malware-ve të njohur dhe nuk mund të rregullojë Zero Day vulnerabilities. Zero Day shfrytëzon dobësitë e synuara për të cilat nuk ka asnjë mbrojtje në dispozicion. Këto tools-e mund të reduktojnë ndjeshëm kërcënimet kibernetike duke vepruar si një proces filtrimi mbrojtës, dhe kështu mund të shpëtojnë burimeve organizative dhe të zvogëlojnë dështimet e sistemit.

Ndalimi përkohësisht i shërbimeve është një masë më drastike dhe potencialisht shkatërruese zakonisht e ekzekutueshme në nivel aplikacioni psh bërja e një shërbimi joaktiv. Kjo mund të ndodhë në një server, ose në nivelin e rrjetit psh duke përdorur firewall për të bllokuar adresat IP ose portat e lidhura me një shërbim. Ndalimi i shërbime të veçanta ndalon veprimin keqdashës dhe parandalon përhapjen e shpejtë të tij, duke ruajtur funksionimin e komponentëve të paprekur për të shmangur humbjen e plotë të shërbimit. Qëllimi i dëshiruar është që të frenojë incidentin në mënyrë efektive me sa më pak humbje në funksionalitetin e sistemit. Për t'u përgatitur në mënyrë efektive për ndalimin e shërbimeve, një organizatë duhet të mbajë një listë të shërbimeve të rrjetit që përdoren, së bashku me portat e tyre shoqëruese Transmission Control Protocol dhe User Datagram Protocol.

Përdorimi i frenimit të incidenteve nëpërmjet bërjes se lidhjes disable (joaktive) është një mjet efektiv dhe i shpejtë i kufizimit përkohësisht të lidhjes së rrjetit në sistemet e infektuara në përpjekje për të krijuar lidhje me një sistem të jashtëm. Kjo mund të parandalojë shkarkimin e malware dhe parandalimin e përhapjes së tij në sistemet e tjera të brendshme në rrjet. Qëllimi është izolimi i sistemit nga rrjeti duke hequr pikën e komunikimit networking dhe më pas testimi dhe verifikimi i izolimit pa ndikuar shërbimet kritike.

## Rehabilitimi (Remediation)

Para se të bëhet recovery gjithë sistemi, përpjekjet e rehabilitimit duhet të kryhen fillimisht për të rregulluar burimin e problemit. Kjo mund të përfshijë zhdukjen e çdo programi malware të mbetur në sistem, heqjen ose zëvendësimin e pajisjeve të prekshme, rikonfigurimin dhe patching e pajisjeve ose programeve, dhe anulimin e mundshëm të aksesit për persona të caktuar.

Nëse incidenti përfshin akses të paautorizuar, atëherë duhet të bëhen përpjekje për të mbyllur rrugën e aksesit. Kjo mund të përfshijë ndryshimin e të gjithë fjalëkalimeve dhe emrave të përdoruesve të caktuar. Përpjekjet mund të përfshijnë edhe bllokimin e aksesit nga adresa IP të identifikuara dhe ndryshimin e portave të konfiguruara në firewall.

Duhet të kryhet një analizë e kujdesshme në organizatë për të verifikuar rrugën që ka ndjekur sulmuesi. Kjo jo vetëm që vë në dukje dobësitë aktuale, por ai gjithashtu mund të nxjerrë në pah hapësira të ngjashme që mund të kenë nevojë për vëmendje.

Nëse incidenti përfshin instalimin e programeve malëare në sistem, atëherë është e nevojshme largimi i tyre. Në mënyrë ideale, cinstalimi do të heqë malware-in me sa më pak ndërprerje të operacioneve të objektit. Ky proces i heqjes së malware mund të marrë kohë për ta kryer me sukses, në varësi të llojit të malware, shkallës së ndikimit dhe metodës së kontrollit të përdorur.

Shumë teknika mund të heqin programet malware nga një sistem i infektuar. Metoda më e zakonshme është përdorimi i mjeteve të automatizuara të heqjes të tilla si programet antivirus, zbulimi spyware dhe heqja e shërbimeve etj. Metoda të tjera përfshijnë rivendosjen e një sistemi në një pikë të caktuar para se infektimit. Këto mjete mund të gjejnë shpejt dhe të heqin malware-in në qoftë se ata kanë zbuluar shenja të tij. Për fat të keq, shumica e programeve të tipit antivirus përqëndrohen në sistemet tipike IT dhe nuk arrijnë të zbulojnë malware në sisteme më të specializuara kontrolli. Ekziston edhe rreziku që këto shërbime të heqin ose të ndryshojnë sistemin ose file-t e të dhënave. Në këto situata, mund të jetë e nevojshme heqja manuale me ndihmën e shitësit, ose shitësi vetë mund të jetë në gjendje të sigurojë software për heqjen që është testuar kundrejt sistemit të synuar.

Për raste më të rënda të infeksionit malware, mund të jetë i nevojshëm një rindërtim. Kjo teknikë do të përfshijë riinstalimin dhe sigurimin e sistemit operativ dhe aplikacioneve shoqëruese duke rimarrë të dhënat nga filet backup.

Duhet të konsiderohet një rindërtim i plotë nëse janë të pranishme karakteristikat e mëposhtme të sistemit:

* Ndërhyrësi ka fituar akses në sistem në nivelin rrënjë ose në nivelin e administratorit.
* Kemi të bëjmë më akses të tipit back door, i cili nuk identifikohet lehtë. Rreziku është se mund të zbulohet një back door, por shumë të tjerët mbeten të pazbuluar
* Filet e sistemit janë zëvendësuar nga programi malware ose direkt nga ndërhyrësi.
* Sistemi është i paqëndrueshëm ose nuk funksionon siç duhet, edhe pasi ka vepruar softëare antivirus, apo programe ose teknika të tjera të heqjes së malware. Kjo tregon se ose malware nuk është zhdukur plotësisht ose ka shkaktuar një dëmtim serioz të sistemit.

Kur përpjekjet për zhdukjen janë përfunduar, është shumë e rekomandueshme të kryhet një testim për të verifikuar se sistemi është duke punuar si duhet. Kjo përfshin jo vetëm vëzhgimin e sjelljes, por edhe rishikimin e informacionit të zbulimit të incidentit për të kërkuar shenja sinjifikante të mbetura të kodit mashtrues.

# Rëndësia e përdorimit të tools-eve gjatë një gjurmimi efektiv të incidenteve

Në këtë punim ndër të tjera paraqitet dhe fakti që shumë faktorë hyjnë në lojë gjatë vlerësimit të CSIRT apo pjesëtarëve të saj. Qëllimi i tij është që të përqëndrohet në mënyrë specifike në përdorimin e programeve kompjuterike dhe sistemeve për të ruajtur, analizuar dhe shpërndarë të dhënat e mbledhura gjatë gjurmimit të incidenteve. Kjo përfshin si të dhënat e mbledhura dhe të krijuara gjatë investigimit, ashtu dhe vetë punën investiguese.

## Avantazhet e një gjurmimi efektiv të incidenteve

Gjurmimi efektiv i incidenteve përfshin aplikimin kompetent të software-ve dhe sistemeve të përshtatshëm për menaxhimin e investigimeve. Duke ndjekur këtë praktitë avantazhet e përfituara janë të mëdha.

### Një investigim më i plotë

Investiguesit përdorin tools-et e gjurmimit të incidenteve për të menaxhuar përgjigjen ndaj incidenteve dhe për ta bërë procesin më të plotë. Këto tools-e mund të përshtaten për të përfshirë menu, për të siguruar që anëtarët e duhur të ekipit në çdo investigim të kryer ndjekin hapa të qëndrueshëm. Tools-et mund të kërkojnë gjithashtu që pjesë të veçanta informacioni të mblidhen para se një incident të konsiderohet i mbyllur ose të kalohet në hapin pasardhës. Pa këto kërkesa, investiguesit mund të harrojnë ose të zgjedhin të mos kryejnë veprime të caktuara investiguese, të mbledhin të dhëna të caktuara dhe kështu të humbasin prova kyçe ose të marrin vendime të varfra analitike. Me to, CSIRT mund të sigurohet që të gjitha incidentet janë investiguar duke përdorur të njëjtat procese përsëritëse që janë vendosur nga ekipi.

Ekziston mundësia që informacionet ose shënimet të humbasin gjatë një investigimi nëse një investigues i ruan ato në nivel lokal në një workstation, ose në të dhënat personale dhe nuk i merr këto të dhëna në mënyrë të përgjegjshme, ose pa dashje i humbet ato për shkak të një dështimi hardware. Tools-et për gjurmimin e incidenteve tipikisht drejtohen nga një vendndodhje e centralizuar dhe ruajnë të gjithë të dhënat e ekipit në një bazë të dhënash, të cilat mund të rimerren mbështetur në politikat bazë të organizatës dhe në një mënyrë më të efektshme dhe të qëndrueshme se sa një mënyrë individuale.

### Bashkëpunim më i mirë

Shumica e CSIRT-eve janë të përbërë nga disa pjesëtarë ekipi, shpesh të përqëndruar në fusha të ndryshme të mjedisit të informatikës apo me specializime të ndryshme. Shpërndarja e të dhënave midis pjesëtarëve të shumtë të ekipit, duke përdorur document files, të tilla si spreadsheets ose përpunues teksti, dhe duke shfrytëzuar tools-et e mesazheve si psh email paraqet një sfidë. Rrallë të gjithë pjesëtarët e ekipit posedojnë dhe të punojnë me të dhënat e fundit, dhe është e vështirë që të mblidhen në mënyrë efektive të gjitha të dhënat në një skedar të veçantë që mund të aksesohet dhe të përditësohet nga të gjithë pjesëtarët e ekipit në të njëjtën kohë.

Sistemet e gjurmimit të incidenteve, të cilat janë zakonisht ticket ose case-based, mund të menaxhojnë përdorues të shumtë që përditësojnë një rast incidenti. Pjesëtarët e ekipit mund të aksesojnë master ticket pa u shqetësuar në lidhje me faktin nëse të dhënat janë të reja ose jo. Të dhënat e mbledhura nga çdo pjesëtar i grupit mund të paraqiten, aksesohen dhe të kontrollohen nga të gjithë nëpërmjet një ndërfaqe të vetme pa patur nevojë për të menaxhuar filet e shpërndara në rrjet apo të hyjnë nëpër arkivat e e-mail-it.

Përdorimi i menusë në tools-et e gjurmimit të incidenteve mund të përmirësojë paralelizmin e detyrave. Nga një vend, mbledhja e të dhënave, analiza, zhvillimi i inteligjencës së re, dhe detyrat në lidhje me riparimin mund të caktohen për përdoruesit e shumta në të njëjtën kohë dhe të gjithë mund të kryejnë detyrat e tyre dhe të raportojnë përsëri në master ticket.

Kjo është veçanërisht e dobishme kur CSIRT duhet të drejtojë operacionet IT të ekipeve, të tillë si administratorët e rrjetit ose të ndihmojë stafin helpdesk, për të kryer detyra të tilla si zbatimi i rregullave të firewall-it. Në vend të transferimit të të dhënave në mënyrë manuale nga CSIRT në tools-et e përdorura nga një ekip i operacioneve IT, mund të caktohet një detyrë në tools-et e gjurmimit të incidentit dhe kështu do të realizohet një ndërveprim më i thjeshtë me sistemin e operacioneve IT. Disa CSIRT sigurojnë qasje direkte në sistemin e gjurmimit të incidenteve për stafin përkatës të operacioneve IT. Në këtë mënyrë, stafi i operacioneve IT mund të shohë gjithmonë një informacion të përditësuar dhe gjendjen nga burimi.

### Historiku i gjurmimit dhe zbulimi i kërcënimeve

Një CSIRT i mirë do tju kushtojë rëndësi të dhënave nga investigimet e fundit, kur fillon një investigim të ri - përcaktimin nëse një tool, kredencial ose host ka qenë i përfshirë në një incident të mëparshëm. Kjo mund të kursejë kohën e çmuar të analizës dhe ndihmon për të krijuar një modul kërcënimi – karakteristikat e tij të zakonshme, strategjitë apo modelet. Ky lloj i kërkimit mund të jetë i vështirë kur përdoren file individualë të ruajtur në shumë vende dhe në formate të ndryshëm.

Përdorimi i të dhënave historike është zakonisht i parëndësishëm kur përdoren tools-e të gjurmimit të incidenteve. Një investigues mund të kërkojë shumë shpejt të gjitha të dhënat e paraqitura nga pjesëtarë të ndryshëm të grupit dhe të përfitojë nga kjo analizë. Kjo është shumë e thjeshtë, njësoj si të kërkosh për një emër specifik domain ose një adresë IP për të gjetur kërcënimet e tjera që janë përdorur. Gjithashtu kjo eliminon harxhimin e orëve për përcaktimin se cilat mjete mund të jenë përdorur, apo cili ka qënë qëllimi i sulmuesit gjatë incidentit më të fundit. Në disa raste, zbulimi i të dhënave të reja gjatë një investigimi mund të shkaktojë edhe që një CSIRT të shqyrtojë incidentet e mëparshme të lidhura dhe të rihapë rastet duke përdorur informacionin e ri.

Këto të dhëna shpesh janë të vlefshme për një ekip të zbulimit të kërcënimeve të devotshëm në zhvillimin dhe zbatimin e treguesvë që tregojnë që një kërcënim është aktiv në mjedis, që mund të përdoret nga tools-et e monitorimit të sigurisë. Këto tools-e, duke përfshirë sistemet e zbulimit të ndërhyrjeve (IDS) dhe tools-et e sigurisë së informacionit dhe menaxhimit të ngjarjeve (SIEM), kanë nevojë për përditësime të vazhdueshme të shenjave apo rregullave të bazuara në sjellje për të zbuluar në mënyrë efektive aktivitete të dyshimta.

Në mënyrë tipike, këta tregues vijnë nga shitësi e tools-eve - zhvilluesit e një IDS do të nxjerrin grupe të reja të nënshkrimeve që janë të dobishme për të gjithë bazën e tyre të konsumatorëve, të cilat mund të zbulojnë një gamë të gjerë të shfrytëzimeve dhe sulmeve. Por, këto nënshkrime dhe mund dhe nuk mund të përputhen me veprimtarinë e një sulmuesi që ka në shënjestër në fakt organizatën. Më të vlefshme për organizatat janë treguesit që reflektojnë taktikat aktuale, teknikat dhe procedurat (TTPs) e sulmuesit.

Një ekip i zbulimit të kërcënimeve është i ngarkuar me detyrën e analizimit të provave të lëna prapa nga sulmet e suksesshme apo të dështuara dhe detyrën e zhvillimit të kundërmasave për të zbuluar dhe, shpesh, për të parandaluar sulmet e ardhshme. Për këtë ekip, asgjë nuk është më e dobishme se të dhënat reale për sulmet aktuale, sidomos për ata sulme që janë investiguar plotësisht, dhe për të cilët treguesit kryesorë janë dokumentuar në një bazë të dhënash që përditësohet vazhdimisht. Sistemi i gjurmimit të incidenteve mund t’i shërbejë këtij qëllimi.

Analistët e zbulimit të kërcënimeve mund të shqyrtojnë rregullisht një incident tickets - si për sulmet e suksesshme ashtu dhe për false positives - dhe përdorimin e informacionit në lidhje me zbulimin e kërcënimeve për të përmirësuar nënshkrimet dhe rregullat e tyre. Për shembull, do të ishte e dukshme nga një ticket incident që përshkruan veprimtarinë e atij që realizon një kërcënim në qoftë se një komandë dhe kontrolli i host-it nuk ishte prekur nga një kërcënim i caktuar më parë, apo një aktor kërcënimi ka migruar në mënyrë të qartë në një të ri. Ose, në qoftë se një version i përditësuar i një backdoor është përdorur në një sulm të ri, dhe një investigues e zbulon atë, mostrën e tij, ose raportin e analizën për mostrën, mund të bashkangjitet në një ticket incident dhe të shqyrtohet nga ekipi i zbulimit të kërcënimeve.

Disa ekipe të zbulimit të kërcënimeve madje mund të konfigurojnë bazën e tyre të të dhënave të aplikacionit, të tillë si MITRE’s *CRITs tool*, që të marrë automatikisht të dhëna të caktuara nga një sistem i gjurmimit të incidenteve, në mënyrë që ata të mund të vendosin shpejt tregues të rinj që janë zbuluar gjatë investigimit të incidenteve.

### Raportim i përmirësuar

Menaxherët e riskut shpesh kanë problemin e mungesës së të dhënave reale të disponueshme nëpërmjet të cilave mund të marrin vendimet në lidhje me riskun. Darril Gibson (2011, p. 6), në librin e tij mbi menaxhimin e riskut në sistemet e informacionit, thotë që ‘… incidentet e sigurisë së mëparshme janë një burim i shkëlqyer të dhënash. Si evidencë të risqeve, të cilët tashmë kanë ndodhur, ata ndihmojnë në justifikimin e kontrolleve. Ata tregojnë problemet që kanë ndodhur si dhe tregojnë trendin e mundshëm të ngjarjeve të ardhshme’. Sidoqoftë, Gibson (2011, p. 20) gjithashtu thekson që “dobësia nga një incident i sigurisë do të zgjidhet në mënyrën e duhur pas incidentit”. Në praktikë, punonjësit janë ndonjëherë të prirur ta lënë jashtë incidentin dhe ta harrojnë atë sa më shpejt të jetë e mundur.

Mirëmbajtja e një baze të dhënash të qëndrueshme me informacion të detajuar mbi incidentet mund të ndihmojë në zgjidhjen e këtij problemi për menaxherët. Kryerja e kërkimeve dhe gjenerimi i raporteve automatike për gjithë incidents tickets lejojnë pamje të burimeve të të dhënave të targetuara, aplikacioneve dhe platformave. Kjo do të sigurojë një pasqyrë në të cilën vektorët e sulmeve dhe mjetet janë me interes të lartë, ashtu si dhe kontrollet dhe masat mbrojtëse që janë më efektive në ndalimin ose ngadalësimin e këtyre sulmeve. Së fundmi, teknologjitë më të dukshme që mund të sigurojnë CSIRT dhe grupet e sigurisë, nëpërmjet logs-eve dhe ndërfaqësve të aplikacioneve (APIs), mund të identifikohen.

Me këto të dhëna reale, menaxherët e riskut mund të marrin vendime më të informuara. Kjo situatë gjithashtu mund të favorizojë CSIRTs dhe grupet e sigurisë- menaxherët mund të vendosin që këta ekipe kanë burime të pamjaftueshme dhe vendosin t’i mbështësin ata duke iu ofruar staf shtesë, tools-e ose trajnime.

## Praktikat më të mira për një gjurmim efektiv të incidenteve

Një gjurmim efektiv i incidenteve duhet të ndjekë një proces formal, duke përfshirë stafin e duhur dhe duke marrë të dhëna nga cdo rast. CSIRTs duhet të marrin në konsideratë faktin se si të dhëna nga incidente të vecanta mund të lidhen së bashku kështu këto modele dhe trende në të dhëna mund të kontribuojnë si në misionin e përgjigjes ndaj incidenteve ashtu dhe në gjendjen e përgjithshme të sigurisë në organizatë.

### Ndërtimi i proceseve IR në tools-et e gjurmimit.

Zakonisht CSIRT-et e zhvilluar e ndajnë procesin e përgjigjes ndaj incidenteve në faza dhe përdorin këto faza për të udhëhequr punën e investiguesve, analistëve dhe operacioneve IT të stafit. SANS rekomandon një process me gjashtë faza si pjesë e kursit të tyre SEC504 - përgatitja, identifikimi, kontrolli, eradication, recovery, dhe mësimet e nxjerra (Skoudis, 2010, fq 14.). Në mënyrë të ngjashme, NIST rekomandon përgatitjen, zbulimin & analizën, frenimi, eradication, recovery dhe veprimtaria pas incidentit (Cichonski et al, fq. 21). Secila nga këto faza zakonisht përfshin disa detyra, shumë prej të cilave janë të varura nga rezultati i një detyre të mëparshme.

Cdo detyrë duhet të përfshijë punën e një pjesëtari specifik të ekipit ose një nga shumë punët që kryejnë një rol të vecantë. Gjatë fazës së identifikimit, psh, një alarm duhet të shpërndahet me përparësi, që nënkupton që vlefshmëria e tij duhet të përcaktohet dhe një rradhë veprimesh gjithashtu. Ky mund të jetë hapi i parë në procesin e përgjigjes ndaj incidenteve. Pas shpërndarjes së alarmit, një kompromis i konfirmuar mund të dërgohet në një ekip analizues për të përcaktuar shkalla e aktivitetit të sulmuesit dhe prezencën në rrjet; në rastin e një false positive, alarmi fillestar mund të dërgohet në ekipin e operacioneve të sigurisë, ose në ekipin e zbulimit të kërcënimeve për të gjetur shkakun burim dhe për të përditësuar nënshkrimet e përdorura në sistemet e zbulimit.

Zakonisht është e mundur të ndërtohen këto lloj workflows nëpërmjet tools-eve të gjurmimit të incidenteve. Incidenti dhe të dhënat e lidhura me të ruhen në një njësi më vete, zakonisht ticket. Investiguesit bëhen task owners, dhe mund të krijohen si përdorues individual ose grupe. Ekipet mund të krijohen që të trajtojnë faza të veçanta dhe listat e detyrave apo tickets mund të ndërtohen në mënyrë që këto ekipe të shqyrtojnë vetëm ato informacione që kanë nevojë dhe kërkojnë vëmendjen e tyre.

Së fundmi, progresi i investigimit nëpërmjet procesit IR mund të projektohet si një lëvizje logjike e tickets nëpërmjet një seri hapash të përsëritur. Në fillim të një investigimi, një ticket mund të lindë në rradhët e ekipit të identifikimit dhe hetuesi i caktuar mund të shqyrtojë treguesit ose provat që e iniciuan atë. Ata mund të caktojnë një detyrë për të mbledhur të dhëna nga një makinë e dyshuar. Ose, pas kërkimit të tickets të kaluara, ata menjëherë mund të arrijnë në përfundimin se ka ndodhur një shkelje dhe dërgojnë një ticket në ekipin e kontrollit. Ky ekip do të marrë ticket dhe do të fillojë veprimet në lidhje me kufizimin e lëvizjeve të sulmuesit.

Bileta mund të kalojë përmes workflow, nga ekipi në ekip dhe nga rradha në rradhë, deri sa të përfundojë procesi. Përdorimi i workflow siguron se janë kryer në mënyrën e duhur, hapat e duhur, nga stafi i duhur.

### Gjurmimi i gjithë të dhënave të rëndësishme

Investigimi i incidentit përfshin mbledhjen, interpretimin, analizimin, dhe veprimin e të dhënave komplekse në shumë forma. Këto të dhëna mund të përshkruajnë sulmuesin, përdoruesin e shënjestruar, një sistem, të dhëna, një aplikacion, programe, kod, metoda komunikimi, rrjete, si dhe shumë aspekte të tjerë të një mjedisi kompjuterik ose operacionesh biznesi. Të dhënat që ruhen në sistemin e gjurmimit nuk duhet të mbeten vetëm në zgjedhjen e invstiguesit. Një investigator shpeshherë i konsideron disa të dhëna më të rëndësishme se disa të tjera, dhe si rezultat mund të humbasë materiale shumë kritike për një investigim të suksesshëm.

Modeli për një master incident ticket duhet të plotësohet në cdo hap me fushat që CSIRT, dhe organizata si e tërë, i shikon të rëndësishme. Disa fusha mund të përcaktohen si të domosdoshme, kështu ticket nuk mund të kalojë në hapin e rradhës pa regjistruar këto të dhëna. Shembuj të të dhënave të dobishme përfshijnë:

* Asetet të cilat janë komprometuar, si dhe ato për të cilat dyshohet për komprometim, vendndodhja e tyre gjeografike, pronari, sistemit operativ, modeli hardware dhe detaje, dhe treguesi i komprometimit që çoi në përfshirjen e tyre;
* Të dhënat që janë vjedhur apo dyshohet që mund të jenë vjedhur, vendndodhja e tyre gjeografike, pronari dhe niveli i klasifikimit;
* Informacion në lidhje me aktorin e kërcënimit, duke përfshirë llogaritë ose mjetet që janë përdorur, host-et në distancë nga të cilët është vepruar dhe motivi i mundshëm;
* Rezultatet e analizave, që nga teknikat e malware-ve ose mjeteve, provat e ligjshme dhe objektet e zbuluara;
* Lidhjet me njohuritë e brendshme, apo burimet e informacionit nga palët e treta

në lidhje me sulmuesit, mjetet, dobësitë, ose të dhënat e vjedhura.

Aksesi në disa fusha mund të kufizohet, në mënyrë që shpërndarja e hutuar e tyre mos e dëmtojë më tej organizatën. Një shembull do të ishin detajet e të dhënave të vjedhura nga një sulmues si numri i sigurimeve shoqërore, numri i kartës së kreditit, ose kredencialet.

Disa të dhëna mund të jetë e nevojshme të krijohen për eksport të thjeshtë, në mënyrë që ato të mund të përdoren për zbulim ose rehabilitim. Shembuj të tyre përfshijnë kodet hash të pjesëve të programeve malware, regjistrat e çelësave ose objekte të tjera endpoint, ose adresat IP të përdorura nga sulmuesit për drejtimin dhe kontrollin.

### Bërja e kërkimit më të thjeshtë

Disa çështje e ngadalësojë përparimin e një investigimi po aq sa dhe kërkimi. Kërkimi nga investiguesit i një pike kyce apo përpjekja për t'iu përgjigjur një pyetje duke përdorur shënime në letër, apo edhe dokumente (file) individuale në një kompjuter, mund të kërkojë minuta apo edhe orë. Për ta bërë këtë problem të parëndësishëm mund të përdoren algoritmet modernë të kërkimit.

Shumica e tools-eve të gjurmimit të incidenteve mund të konfigurohen për të indeksuar disa ose të gjitha fushat në një incident ticket. Qëllimi për të cilin një CSIRT duhet të synojë është që një investigues të jetë në gjendje të kërkojë për ndonjë informacion në ndonjë fushë të të gjitha tickets. Një investigues mund të dijë emri i domainit, për shembull, dhe do të dijë nëse është përdorur nga ndonjë sulm i njohur më parë.

Lejimi i përdoruesve për të etiketuar fjalë kyçe të veçanta në tickets mund të përmirësojë aftësitë e kërkimit. Nëse CSIRT ose fusha e sigurisë në përgjithësi i referohet një aktori kërcënimi duke përdorur një emër të koduar, emri i koduar mund të përdoret si një etiketë për një ticket incident në të cilin aktori dyshohet të jetë përfshirë. Ose, në qoftë se disa incidente përfshijnë vjedhjen e skicave skematike nga një organizatë, etiketimi 'skematike' mund të aplikohet për të gjitha tickets përkatëse. Sigurimi i një listë që gjeneron automatikisht etiketimet për investiguesit e bën funksionin e kërkimit edhe më të dobishëm.

### Rishikim i rregullt i incident tickets

Ndonjëhërë edhe pse anëtarët e CSIRT të një organizate mund të jenë jashtëzakonisht të aftë në përgjigjen ndaj incidenteve, mund të ndodhë që ata të mos jenë të organizuar mirë, ose të motivuar për të dokumentuar plotësisht gjithcka në çdo kohë. Si rezultat, drejtuesi i CSIRT mund të dëshirojë të shqyrtojë rregullisht përmbajtjen e një ticket të incidentit për tu siguruar që investiguesit janë duke ndjekur proceset e duhura.

Për shembull, një investigim i përsëritur i një incidenti që ndodh disa herë në javë

mund të bëhet rutinë apo i mërzitshëm për një investigues. Investiguesi mund të vazhdojë me

rrjedhën e punës, por pas disa rasteve, ai do të fillojë të plotësojë fushat e detyrueshme me

të dhëna jo të plota thjesht për të anashkaluar kërkesat e dokumentacionit dhe për ta kaluar ticket direkt. Në këtë situatë, një drejtues i CSIRT do të duhet të korrigjojë sjelljen e investiguesve, për të siguruar që të gjitha ticket e incidenteve të kenë të dhëna sa më të plota që të jetë e mundur, në çdo kohë. CSIRT shpejt do të mësojë që të dhënat e padobishme sot shpesh bëhen të dhëna kritike nesër.

Kjo gjithashtu mund të paraqesë një mundësi për të riparë politikat që diktojnë cilat të dhëna janë të detyrueshme dhe të qartësohet më mirë detyrimi i investiguesve për t’i paraqitur ato.

### Trajnimi i rregullt

Proceset komplekse të përgjigjes ndaj incidenteve dhe investigimet komplekse cojnë dhe në tools-e komplekse të gjurmimit të incidenteve. Investiguesit e rinj nuk mund të kuptojnë plotësisht karakteristikat e tools-eve ose implementimin e proceseve IR dhe procedurave në tool. Për këtë arsye duhet të bëhen trajnime të rregullta për ekipin në lidhje me përdorimin e drejtë të tools-eve, sidomos kur punonjës të rinj i bashkohen ekipit ose karakteristika të reja apo ndryshime zbatohen në lidhje me funksionalitetet e tools-eve.

Kjo gjithashtu iu jep pjesëtarëve të ekipit një mundësi për të bërë pyetje që mund të kenë qenë të paqarta në mendjet e tyre për disa kohë dhe një shans për të sugjeruar funksione të reja ose ndryshime që janë të nevojshme.

### Siguria operative

Një sulmues i zgjuar e di mirë objektivin e tij, dhe shumë prej tyre menjëherë do të gjejnë vendndodhjen e tools-eve dhe bazave të njohurive të përdorura nga ekipet e sigurisë së informacionit. Tools-et e gjurmimit të incidenteve do të jenë një element kyç me interes për një sulmues të tillë. Ata mund të dëshirojnë thjesht të dinë se çfarë organizata di në lidhje me ta; ata mund të duan të prishin aftësinë e organizatës për t'u përgjigjur me sukses ndaj incidenteve, të prishin të dhënat e regjistruara, ose modifikojnë të dhënat e ruajtura për të devijuar investigimin.

Duhet të merren masa për sigurinë operative për të mbrojtur konfidencialitetin,

integritetin dhe disponueshmërinë e tools-eve të gjurmimit. Duhet të bëhet backup i të dhënave cdo ditë dhe duhet të përfshijë si sistemin operativ, ashtu dhe aplikimin e gjurmimit dhe bazën e tij të të dhënave. Backup-et duhet të jenë të koduar, dhe aftësitë e rimëkëmbjes duhet të testohen rregullisht. (SANS CSC 8, 2015)

Tools-et e gjurmimit të incidenteve janë ndërtuar zakonisht nga software dhe si të tillë kërkojnë patching. Duhet të zbatohen dhe update të herë pas hershme. (SANS CSC 4, 2015)

Aksesimi në tools-et e gjurmimit duhet të kërkojë autentifikim të fortë për përdoruesit dhe administratorët. Në një arkitekturë klient / server, sesionet me aplikimin server duhet të jenë të koduar. (SANS CSC 17, 2015)

Mund të jetë e nevojshme për të vepruar me tools-et e gjurmimit të incidentit out-of-band në rastet kur dyshohet apo priten ndërhyrje. Tools-et mund të veprojë në një rrjet të veçantë fizik, për të cilën një klient i ndryshëm fizik është i lidhur ose me të cilin duhet të përdoret një lidhje VPN për aksesim.

## Tools-et e gjurmimit të incidenteve

Gjetja e një tool për gjurmimin e incidenteve mund të jetë një detyrë e vështirë. Një CSIRT mund të mos ketë burime financiare, apo aftësi për ta vendosur në funksionim ose mirëmbajtur një tool. Një rishikim i plotë i kërkesave të ekipit duhet t'i paraprijë çdo përpjekjeje për të projektuar, vendosur, apo përdorur një tool për gjurmimin e incidenteve.

### Software-t e bashkëpunimit

Shumë organizata përdorin spreadsheets, të tilla si Microsoft Excel, apo të tjerë software standalone gjerësisht të disponueshëm, kur bëjnë organizimin ad-hoc ose ndjekjen e aktivitetit. Edhe pse kjo është një praktikë e zakonshme, gjithsesi nuk është një mënyrë efektive për mbajtjen e të dhënave të investigimit të një incidenti. Ata janë zakonisht shumë kompleksë, me shumë të dhëna për të regjistruar, dhe nuk ofrojnë mundësi bashkëpunimi për shkak të natyrës asinkrone të ruajtjes së dosjeve (fileve) që mund të hapen vetëm nga një përdorues në një kohë të caktuar.

Software-t Wiki (të tillë si MediaWiki apo Atlassian Confluence), të cilët lejojnë menaxhim të përmbajtjes nga përdorues të shumtë në të njëjtën kohë, mund të jenë një fillim i mirë për CSIRT-et që dëshirojnë një sistem të gjurmimit të incidenteve që nuk kërkon një nivel të lartë mirëmbajtje dhe që janë të lehtë për t’u vendosur në funksionim. Wiki-t kanë tendencë për të përmbushur kërkesat e bashkëpunimit dhe kërkimit, por shumica prej tyre nuk ofron mundësi të kontrollit të workflow. Kjo nënkupton që një wiki software është i thjeshtë për t’u vendosur dhe nuk kërkon shumë përpjekje administrative për ta mbajtur funksional. Mund të shtohen llogari përdoruesish dhe më pas investiguesit mund të fillojnë të krijojnë faqe wiki për çdo incident, duke përdorur të forma dokumentesh falas ose template që iu mundësojnë investiguesve të dokumentojnë informacione specifike.

### Support and issue-tracking software

By default, shumë organizata gjurmojnë incidentet duke përdorur help desk ose support tickets. Kjo praktikë më së shumti ndodh në cështje të raportuara nga përdoruesit, të tilla si një problem performance, zhvillim i një çështje të sigurisë, pas një periudhe troubleshooting. Kuadri i tickets i pranishëm në help desk dhe software-t e shërbimit, të cilët lejojnë teknikë të shumtë për të përditësuar një ticket, për të ndjekur gjendjen e saj, dhe për të ecur nëpërmjet një workflow, i bëjnë këta lloj tools-e (të tilla si Remedy rapo ServiceNoë) tërheqës për qëllimin e gjurmimit të incidentit.

Megjithatë, pamundësia për shumë zgjidhje nga help desk që lejojnë përshtatjen e

fushave, menusë, dhe kërkimit mund të pengojë efektivitetin në gjurmimin e incidentit. Gjithashtu kalimi i të dhënave specifike për t’u përdorur në sistemet e monitorimit të sigurisë mund të jetë i vështirë, pasi nuk përbën zakonisht një rast të nevojshëm kur përdoret si zgjidhje help desk.

Bug ose cështjet e sistemeve të gjurmimit, të përdorura nga grupet e zhvillimit të software-ve, janë të ngjashme në koncept edhe në software-t help desk, kështu të dy llojet tentojnë të përdorin raste individuale ose tickets për të gjurmuar aktivitetet në zgjidhjen e disa problemeve teknike. Sidoqoftë, kërkesa e trashëguar që zhvilluesit kanë për custom workflows, tipin e problemeve dhe fushat e bën një issue tracking system, të tillë si Bugzilla ose Atlassian JIRA, një zgjedhje më të mirë se sa një tool për gjurmimin e incidenteve. zhvilluesit e natyrshme nevoja të ketë për flukset e punës doganore, llojet çështje, dhe fushat, e bën një sistem të përcjelljes çështje

Një CSIRT brenda një organizate, e cila ka një grup zhvillimi software-sh, mund të përdorë produktet e këtij grupi për të krijuar një software (instancë) të personalizuar për qëllimet e tij. Kjo e lejon CSIRT të vendosë një IR workflow, përdorues, rradhë (queues), dhe modele tickets me fusha custom që qëndrojnë të ndara nga ato të përdoruara prej zhvilluesve.

### Software-t e gjurmimit të incidenteve purpose-build

Sigurisht, të përpiqesh t’i shtosh aftësitë për gjurmimin e incidenteve një produkti i cili nuk është dizenjuar për këtë gjë, mund të jetë kohë-konsumuese dhe një përpjekje e dështuar për një CSIRT, vecanërisht kur software i dizenjuar vetëm për këtë qëllim është i disponueshëm. CSIRTs duhet të fillojnë më një tool purpose-built, nqs dhe burimet e tyre e mundësojnë këtë gjë, në mënyrë që të minimizojnë kohën e fillimit dhe të përshtatin punën. Fatkeqësisht, ka shumë pak tools-e purpose-built të disponueshme.

Best Practical’s RTIR është një tool për gjurmimin e incidenteve falas, open-source dhe web-based që përdoret nga disa CSIRTs. Ky tool nisi si një Request Tracker, një bug dhe issue tracking system, dhe karakteristikat për përgjigje ndaj incidenteve u shtuan më vonë si modul i vecantë. Kostoja e ulët e bën RTIR një pikë fillimi të mirë për CSIRTs që janë duke vendosur sistemin e tyre të parë të gjurmimit të incidenteve dhe që kanë gjithashtu buxhet të kufizuar. Tradeoff vjen nga burimet e operacioneve IT të nevojshme për të instaluar, përshtatur dhe menaxhuar aplikacionin dhe komponentët e tij, gjë e cila është e rëndësishme.

AIRT, ose Application for Incident Reponse Teams, është një tjetër tool për gjurmimin e incidenteve web-based ("Application for Incident Response Teams (AIRT)," n.d.). AIRT është relativisht i thjeshtë në karakteristikat dhe funksionalitetet në krahasim me RTIR; sidoqoftë ai është i përshtatshëm për një ekip të vogël që ka pak incidente për të gjurmuar në vit. Duket sikur nuk ka nevojë për mirëmbajtje, edhe pse software nuk është përditësuar që nga viti 2009, dhe lidhet me web serverat që janë të pasdisponueshëm.

Një alternativë komerciale është CyberSponse’s Security Operations Platform. Ky produkt pretendon të ofrojë gjithë karakteristikat e nevojshme për të realizuar një gjurmim efektiv të incidenteve dhe mund të përdoret relativisht shpejt nga një CSIRT. Klientët mund të vendosin tool-in on-premises ose në një mjedis hosted ("IR Team," n.d.). Megjithëse tool supozohet të jetë i pasur me funksionalitete, ai është relativisht i ri dhe i patestuar, si dhe kostoja e tij është pak e lartë, prandaj ai mund të jetë një pengesë për CSIRT-et me burime të kufizuara.