ANDORRA DIGITAL

ANC-AD
Agència Nacional
de Ciberseguretat d'Andorra

Informe de Ciber-Intel·ligència

Investigació proactiva per anticipar-se a les amenaces cibernètiques

TLP:WHITE

GENER 2024

FITXA DEL DOCUMENT

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	23/01/2024	24/01/2024

Registre de canvis			
Versió	Pàgines	Data de modificació	Motiu del canvi

Propietari del document	ANC-AD

ÍNDEX

1. METODOLOGIA 3
2. INTRODUCCIÓ 5
3. INICIS I ANTECEDENTS DE LA CIBERINTEL·LIGÈNCIA 6
4. AGÈNCIES D'INTEL·LIGÈNCIA GOVERNAMENTALS 7
4.1. Agències d'intel·ligència a nivell internacional 7
4.2. Agències d'intel·ligència espanyoles 8
5. TÈCNIQUES D'INVESTIGACIÓ DE CIBERINTEL·LIGÈNCIA 9
6. APLICACIÓ DE LA CIBERINTEL·LIGÈNCIA EN UNA ORGANITZACIÓ 11
6.1. Servei de ciberintel·ligència estratègica 11
6.2. Servei de vigilància digital 12
6.3. Servei d'intel·ligència d'amenaces 13
6.4. Servei de *Threat Hunting* 14
6.5. Servei d'investigació i anàlisi de fraus 15
6.6. Servei d'intel·ligència de vulnerabilitats 15
7. PARÀMETRES DE MONITORATGE D'UNA ORGANITZACIÓ 17
8. CONCLUSIONS 19
9. CLÀUSULA DE CONFIDENCIALITAT 20

1. METODOLOGIA

Aquest informe aplica els principis de Traffic Light Protocol (TLP). Es tracta d'un esquema creat per fomentar un millor intercanvi d'informació de caràcter delicat (però no classificada) en l'àmbit de la seguretat de la informació. A través d'aquest esquema, d'una forma àgil i senzilla, s'indica fins a on pot circular la informació més enllà del receptor en qüestió, i aquest ha de consultar a l'ANC-AD (Agència Nacional de Ciberseguretat d'Andorra) [https://www.anc.ad/] quan la informació necessiti ser distribuïda a tercers.

CODI	QUAN EMPRAR-LO	COM COMPARTIR-LO
TLP:RED	S'ha d'utilitzar TLP:RED quan la informació està limitada a persones concretes, i podria tenir impacte en la privacitat, reputació o operacions si és mal utilitzada.	Els receptors no han de compartir informació designada com TLP:RED amb cap tercer fora de l'àmbit on va ser exposada originalment.
TLP:AMBER	S'ha d'usar TLP:AMBER quan la informació requereix ser distribuïda de manera limitada, però suposa un risc per a la privacitat, reputació o operacions si és compartida fora de l'organització.	Els receptors poden compartir informació indicada com TLP:AMBER únicament amb membres de la seva pròpia organització que necessiten conèixer-la, i amb clients, proveïdors o associats que necessiten conèixer-la per a protegir-se a si mateixos o evitar danys. L'emissor pot especificar restriccions addicionals per a compartir aquesta informació.
TLP:GREEN	S'ha d'emprar TLP:GREEN quan la informació és útil per a totes les organitzacions que participen, així com amb tercers de la comunitat o el sector.	Els receptors poden compartir la informació indicada com TLP:GREEN amb organitzacions afiliades o membres del mateix sector, però mai a través de canals públics.
TLP:WHITE	S'ha d'utilitzar TLP:WHITE quan la informació no suposa cap risc de mal ús, dins de les regles i procediments establerts per a la seva difusió pública.	La informació TLP:WHITE pot ser distribuïda sense restriccions, únicament subjecta a controls de Copyright.

2. INTRODUCCIÓ

Les amenaces cibernètiques, en la seva evolució constant, generen diàriament formes noves de programari maliciós, emergeixen actors d'amenaces i es divulguen vulnerabilitats, que representen riscos significatius per a les organitzacions. És imperatiu mantenir-se informat sobre aquestes novetats per enfortir la postura de ciberseguretat d'una entitat. La ciberintel·ligència es destaca com la disciplina clau en aquest escenari, i exerceix un paper estratègic fonamental en l'àmbit de la ciberseguretat.

Si contrastem amb la ciberseguretat defensiva i ofensiva, l'enfocament de la qual és mitigar incidents i posar a prova sistemes de seguretat respectivament, la ciberintel·ligència s'orienta a identificar de manera proactiva qualsevol element nou potencialment perillós al ciberespai. El seu valor diferencial radica en la capacitat d'anticipar-se a les amenaces emergents.

La ciberintel·ligència es percep com una evolució de les tasques tradicionals d'intel·ligència governamental, i s'adapta a l'entorn digital per reforçar les capacitats defensives. En incorporar les tecnologies avançades i combinar-les amb anàlisis de dades i una comprensió profunda de les tàctiques dels actors d'amenaces, aquesta disciplina contribueix significativament a enfortir les defenses, millorar la resiliència i salvaguardar els actius digitals crítics d'empreses i entitats governamentals en el complex entorn cibernètic actual.

Per això, en aquest informe, s'analitzarà com la ciberintel·ligència s'erigeix en un escut defensiu que permet la capacitat d'anticipació, no només amb la detecció d'amenaces existents, sinó també avançant-se a les noves que puguin sorgir.

Com es veurà tot seguit, la identificació prematura d'indicadors de compromís, el seguiment constant del web fosc i l'avaluació proactiva de vulnerabilitats, són components clau d'aquesta disciplina. En comprendre el panorama complet de les amenaces cibernètiques, la ciberintel·ligència es converteix en un pilar essencial per a la seguretat digital en una era on la innovació tecnològica va de bracet amb els desafiaments de seguretat.

3. INICIS I ANTECEDENTS DE LA CIBERINTEL·LIGÈNCIA

La intel·ligència, com a tasca orientada a la recopilació d'informació i anàlisi de dades, ha exercit un paper crucial a nivell geopolític al llarg de la història, i ha definit l'evolució de les nacions i els diferents governs que s'han succeït durant els últims segles. És a dir, la intel·ligència sorgeix de la necessitat política de tenir eines que permetessin avaluar riscos i facilitar la presa de decisions.

Per aquesta raó, en etapes crítiques a nivell històric com els processos de colonització o els diferents conflictes bèl·lics que s'han produït, on destaquen les dues guerres mundials o la guerra freda, les tasques d'intel·ligència per part dels diferents actors implicats va ser determinant.

Als seus inicis, com és evident, els mitjans per recaptar informació eren rudimentaris, i els elements encarregats de dur a terme aquesta tasca eren els espies i les xarxes d'informació. De fet, es té constància que ja a l'imperi romà o al xinès es feia una tasca important pel que fa a l'estudi de les intencions i les capacitats de les nacions enemigues.

Posteriorment, gràcies als avanços tecnològics, es van anar abastant objectius més ambiciosos com ara la intervenció de sistemes de comunicació o dur a terme tasques de reconeixement a distància.

I ja en el segle XX, quan la digitalització va començar a transformar la connectivitat global i les principals potències mundials van entendre la importància de disposar d'agències i serveis d'intel·ligència professionals dotats amb els recursos econòmics i tècnics que fossin necessaris, sorgeixen la CIA, l'FBI, la NSA, l'MI6, l'FSB, el Mossad, o l'MSS.

En ser organismes governamentals, la seva feina principalment ha consistit a vetllar pels interessos de les seves nacions respectives, sigui per protegir les seves infraestructures estratègiques d'atemptats o sabotatges, per contenir possibles accions terroristes i, fins i tot, per robar informació delicada de països enemics d'àmbits tan diferents com són el relacionat amb la carrera espacial o el desenvolupament armamentístic nuclear.

Més tard va succeir que, amb la consolidació d'Internet a nivell global, es va constatar que els riscos que van emergir del món cibernètic podrien tenir un impacte tan gran com els sabotatges o els atemptats físics. Així, amb la necessitat d'adaptar les tasques d'intel·ligència tradicionals al context nou, va sorgir la ciberintel·ligència.

Per altra banda, els ciberdelinqüents van entendre ben aviat que no només eren els governs els que podien ser un objectiu del qual treure un rèdit important. La xarxa, que ha suposat una revolució absoluta per a la humanitat amb beneficis nombrosos, també ha democratitzat els delictes.

Les empreses van començar a ser objectius de més ciberatacs. La digitalització va portar oportunitats i perills. La ciberseguretat va començar a concebre's com a necessària. I la ciberintel·ligència va deixar de concebre's únicament com una eina útil per a governs i nacions, fins que s'ha convertit en un dels elements clau de les estratègies i departaments de ciberseguretat de moltes entitats, on es treballa per anticipar-se a qualsevol amenaça que es pugui produir.

4. AGÈNCIES D'INTEL·LIGÈNCIA GOVERNAMENTALS

4.1. Agències d'intel·ligència a nivell internacional

Tot seguit, s'exposa breument algunes de les característiques més rellevants de les agències d'intel·ligència que s'han esmentat anteriorment:

- **CIA (Agència Central d'Intel·ligència):** amb seu als Estats Units, és una agència d'intel·ligència que opera a nivell global. La seva missió principal és la recopilació d'informació estratègica per assessorar el president i altres líders estatunidencs en la presa de decisions relacionades amb la seguretat nacional.

- **FBI (Oficina Federal d'Investigació):** tot i que no és exclusivament una agència d'intel·ligència, l'FBI juga un paper vital en la recopilació d'intel·ligència en el context de la seguretat interna dels Estats Units. Se centra en la investigació i el combat d'amenaces nacionals i internacionals, inclosos el terrorisme i l'espionatge.

- **NSA (Agència de Seguretat Nacional):** també és estatunidenca i està especialitzada en la recopilació i anàlisi de senyals d'intel·ligència (SIGINT), com a comunicacions electròniques i de ràdio. El seu enfocament principal és la seguretat cibernètica i la intercepció de comunicacions per protegir els interessos nacionals.

- **MI6 (Servei d'Intel·ligència Secret):** és l'agència del Regne Unit, responsable de la intel·ligència de l'exterior. Se centra en la recol·lecció d'informació d'interès per a la seguretat nacional britànica i la presa de decisions a nivell internacional.

- **FSB (Servei Federal de Seguretat):** successor de l'arxiconegut KGB, l'FSB opera a Rússia i es dedica a la seguretat interna i a la intel·ligència. Participa en la lluita contra el terrorisme, el crim organitzat i altres amenaces internes.

- **Mossad:** és l'agència d'intel·ligència d'Israel i és conegut per les seves operacions encobertes a nivell mundial i per, probablement, ser el millor en aquest camp. El seu enfocament abasta des de la contraintel·ligència fins a la recopilació d'informació sobre amenaces per a la seguretat d'Israel.

- **MSS (Ministeri de Seguretat de l'Estat):** la principal agència d'intel·ligència xinesa, encarregada de la seguretat interna i la contraintel·ligència. El seu enfocament inclou la vigilància d'activitats internes i externes que podrien afectar l'estabilitat del país.

Aquestes agències representen només una fracció de l'entramat complex d'organitzacions d'intel·ligència a nivell mundial. La seva importància radica en la seva capacitat per anticipar i abordar amenaces a la seguretat nacional, com també en la contribució a la presa de decisions estratègiques dels seus governs respectius.

4.2. Agències d'intel·ligència espanyoles

Espanya també disposa d'organismes que exerceixen rols molt importants en la protecció dels interessos nacionals i la seguretat del país. Si s'hagués d'esmentar un homòleg nacional a les agències enumerades anteriorment, seria:

- **CNI (Centre Nacional d'Intel·ligència):** és el servei principal d'intel·ligència d'Espanya. La seva missió abasta l'obtenció d'informació per prevenir i evitar amenaces a la seguretat nacional, tant internes com externes. A més a més, coopera estretament amb altres agències d'intel·ligència i seguretat a nivell internacional.

5. TÈCNIQUES D'INVESTIGACIÓ DE CIBERINTEL·LIGÈNCIA

La ciberintel·ligència és una especialitat heterogènia en què es combinen tècniques per abastar qualsevol camp d'investigació susceptible de contenir dades que puguin ser analitzades. Entre les tècniques més conegudes destaquen l'OSINT, el SOCMINT, HUMINT, SIGINT, GEOINT, TECHINT, FININT, CYBINT i el FISINT.

Tot seguit, s'aprofundirà en què consisteix cada una d'elles, però, grosso modo, conjuntament permeten estudiar tots els paràmetres amb els quals poder obtenir una visió completa sobre el panorama d'amenaces que poden afectar una organització.

- **OSINT (Intel·ligència de fonts obertes):** enfocada a la recopilació i anàlisi d'informació procedent de fonts públiques i accessibles per a qualsevol, com ara les xarxes socials, llocs web, fòrums, i altres fonts obertes en línia.

- **SOCMINT (Intel·ligència de mitjans socials)** se centra específicament en l'obtenció i l'anàlisi d'informació de mitjans socials. Això pot incloure el monitoratge de perfils, anàlisi de tendències, i avaluació de l'activitat i comportament en plataformes de xarxes socials.

- **HUMINT (Intel·ligència humana)** implica l'obtenció d'informació a través de fonts humanes, com ara informants, contactes, agents encoberts i altres mètodes que involucren la interacció directa amb els individus.

- **SIGINT (Intel·ligència de senyals)** se centra en la intercepció i anàlisi de senyals electrònics, com ara comunicacions en ràdio, senyals de satèl·lits i altres tipus de transmissions electròniques.

- **GEOINT (Intel·ligència geoespacial)** utilitza informació geoespacial, que inclou imatges i dades cartogràfiques, per analitzar i entendre més bé la ubicació i els patrons geogràfics relacionats amb les amenaces cibernètiques.

- **TECHINT Intel·ligència tècnica)** s'enfoca en l'obtenció i l'anàlisi d'informació relacionada amb tecnologies específiques, com ara maquinari, programari i sistemes, per comprendre més bé les capacitats i debilitats tecnològiques.

- **FININT (Intel·ligència financera)** analitza transaccions financeres i patrons econòmics per identificar possibles activitats delictives, incloses aquelles relacionades amb ciberdelictes i finançament d'operacions cibernètiques.

- **CYBINT (Intel·ligència cibernètica)** enfocada directament a la recopilació i anàlisi d'informació relacionada amb amenaces cibernètiques. Inclou la identificació de programari maliciós, anàlisi d'incidents de seguretat, i el monitoratge de l'activitat en línia.

- **FISINT (Intel·ligència de senyals físics)** s'ocupa de la recopilació i anàlisi d'informació procedent de radiacions electromagnètiques i altres signatures físiques.

- **COUNTERINT (Contraintel·ligència)** orientada a identificar i neutralitzar activitats de contraintel·ligència adreçades contra les mateixes operacions d'intel·ligència.

6. APLICACIÓ DE LA CIBERINTEL·LIGÈNCIA EN UNA ORGANITZACIÓ

Actualment, és molt difícil concebre una organització que no disposi d'actius digitals, és a dir, que tingui a Internet recursos i dades de gran valor per la seva implicació en el funcionament correcte de l'entitat, en el seu rendiment, o en la seva relació amb proveïdors i/o clients.

Alguns dels actius més transversals a qualsevol entitat serien:

- **Dades**: fa referència a la informació que una organització recopila, processa i emmagatzema. Això inclou dades de clients, dades financeres, informes interns, propietat intel·lectual, entre d'altres.
- **Sistemes i xarxes**: en aquest punt s'abasten des de servidors fins a xarxes i altres components tecnològics que permeten el funcionament de les operacions diàries i la connectivitat interna i externa de l'organització.
- **Programari**: correspon a les aplicacions, programes i sistemes operatius utilitzats per l'organització per dur a terme diverses funcions.
- **Maquinari**: fa referència als dispositius físics que es fan servir per processar, emmagatzemar i transmetre les dades que es gestionen, i que contemplen des de servidors, ordinadors, telèfons corporatius o dispositius d'emmagatzematge o equip de xarxa.
- **Presència en línia**: llocs web, botigues en línia, perfils a les xarxes socials i qualsevol altre actiu relacionat amb la presència en línia de l'organització.
- **Propietat intel·lectual**: abasta patents, marques registrades, drets d'autor i qualsevol altre actiu intangible que sigui propietat de l'organització i tingui un valor significatiu.
- **Infraestructura de TI**: la infraestructura tècnica que sosté les operacions de l'organització, inclosos centres de dades, serveis al núvol i altres recursos.
- **Relacions digitals**: correus electrònics, bases de dades de clients, i altres actius relacionats amb les interaccions digitals amb clients, proveïdors i altres parts interessades.

Si tenim en compte quins són els actius digitals que es volen protegir i salvaguardar, procedirem a explicar com ho fan cada una de les subespecialitats que conformen un servei de ciberintel·ligència.

6.1. Servei de ciberintel·ligència estratègica

La ciberintel·ligència estratègica es posiciona com una disciplina avançada dintre de l'àmbit de la ciberintel·ligència, orientada cap a la comprensió a llarg termini de les amenaces i tendències cibernètiques que podrien afectar la posició i l'estratègia general d'una organització. El seu enfocament s'allunya de la resposta immediata a incidents, i se centra a proporcionar una visió global i contextualitzada per donar suport a la presa de decisions a nivell executiu.

- **Anàlisi de tendències a llarg termini**: implica l'anàlisi de patrons i tendències cibernètiques al llarg del temps, que permet a l'organització anticipar desenvolupaments futurs i preparar-se per a escenaris possibles.

- **Avaluació del paisatge cibernètic**: fer una anàlisi detallada de l'entorn cibernètic global i regional, identificar actors claus, polítiques governamentals, i canvis en la legislació que podrien impactar en la seguretat cibernètica.

- **Comprensió d'amenaces emergents**: l'enfocament estratègic implica identificar amenaces emergents abans que es converteixin en problemes crítics, i permetre a l'organització anticipar i preparar-se per a vectors d'atac nous.

- **Integració amb l'estratègia empresarial**: implica entendre com les amenaces cibernètiques poden afectar directament els objectius comercials i la reputació de l'organització.

- **Avaluació de riscos a nivell executiu**: es proporciona informació detallada sobre els riscos cibernètics rellevants per a la presa de decisions a nivell d'alta direcció, i permetre l'assignació eficient de recursos i la priorització d'iniciatives.

- **Monitoratge d'actors estatals**: atès que la ciberintel·ligència estratègica s'enfoca envers un nivell més alt, inclou el monitoratge d'activitats cibernètiques fetes per actors estatals que podrien tenir implicacions geopolítiques significatives.

- **Col·laboració amb entitats externes**: sigui amb altres organitzacions, agències governamentals o entitats del sector per intercanviar informació i enfortir la postura col·lectiva contra amenaces cibernètiques compartides.

- **Escenaris d'amenaces**: la disciplina inclou la creació d'escenaris d'amenaces hipotètics que permeten a l'organització preparar-se per a situacions crítiques abans que passin.

6.2. Servei de vigilància digital

Es refereix a la pràctica de monitorar de manera activa i anticipada la presència en línia d'una entitat, sigui una organització, una persona o qualsevol entitat digital, amb l'objectiu d'identificar possibles amenaces, riscos o esdeveniments rellevants abans que es converteixin en problemes més grans. Aquest enfocament busca anticipar i prevenir possibles impactes negatius en la seguretat, reputació o integritat de l'entitat vigilada.

En el context de la ciberseguretat i la intel·ligència, la vigilància digital proactiva implica la recol·lecció sistemàtica i l'anàlisi d'informació en línia per identificar patrons, tendències o senyals d'alerta prematura. Això pot incloure:

- **Monitoratge de xarxes socials**: observació de converses i activitats a plataformes socials per detectar esments, comentaris o comportaments que puguin indicar amenaces o riscos.

- **Anàlisi de fòrums i comunitats en línia**: exploració de fòrums, comunitats i llocs web en línia on es discuteixen temes rellevants per a l'entitat, amb l'objectiu d'identificar possibles problemes o amenaces.

- **Investigació al web fosc**: per identificar possibles activitats il·lícites o dades compromeses relacionades amb l'entitat.

- **Seguiment d'activitats anòmales**: supervisió d'activitats inusuals o patrons de comportament estranys als sistemes, xarxes o plataformes digitals de l'entitat.

- **Anàlisi d'amenaces cibernètiques**: avaluació constant d'amenaces cibernètiques potencials, com ara programari maliciós, pesca o altres atacs, per tal d'anticipar o mitigar possibles riscos.

D'aquesta manera es pot entendre que la vigilància digital proactiva s'hagi convertit en una peça essencial per mantenir una estratègia defensiva sòlida a l'entorn digital actual, on les amenaces cibernètiques i els riscos per a la seguretat poden evolucionar ràpidament. En adoptar un enfocament proactiu, les organitzacions poden identificar i abordar possibles problemes abans que es converteixin en crisis significatives.

6.3. Servei d'intel·ligència d'amenaces

La intel·ligència d'amenaces no només identifica possibles riscos, sinó que també proporciona a les organitzacions les eines necessàries per anticipar i contrarestar proactivament les amenaces cibernètiques en un entorn dinàmic i que està canviant constantment.

La comprensió profunda de les amenaces permet a les organitzacions enfortir les seves defenses i mitigar els riscos de manera més efectiva. Les tasques que es duen a terme són:

- **Recol·lecció d'intel·ligència**: es fa una recopilació exhaustiva de dades procedents de fonts diverses, incloses fonts d'intel·ligència oberta (OSINT), intel·ligència de font tancada (CSINT) i dades internes de l'organització.

- **Anàlisi d'amenaces**: consisteix a examinar la informació recopilada per identificar patrons, comportaments i relacions que puguin indicar la presència d'amenaces cibernètiques. Això implica entendre les motivacions, eines i tàctiques dels actors maliciosos.

- **Avaluació de vulnerabilitats exposades**: aquesta tasca consisteix a avaluar les vulnerabilitats específiques que podrien ser explotades per atacants. Això permet a l'organització prioritzar l'aplicació de pedaços i enfortir les defenses en àrees crítiques.

- **Intel·ligència sobre actors d'amenaces**: es du a terme un seguiment dels grups i actors individuals que representen amenaces significatives per a l'organització. Això inclou la identificació de campanyes específiques i la comprensió dels seus objectius.

- **Creació de perfils d'amenaces**: que ajuden l'organització a entendre les tàctiques i procediments possibles als quals es podrien enfrontar en cas que es produïssin determinades circumstàncies.

- **Compartir intel·ligència**: la intel·ligència d'amenaces implica no només la protecció interna, sinó també l'intercanvi d'informació rellevant amb altres entitats del sector per enfortir la defensa col·lectiva contra amenaces compartides. Existeixen nombroses eines i plataformes operades per equips de ciberintel·ligència d'entitats diferents en què es comparteixen, per exemple, indicadors de compromís (IcO), informació sobre actors nous d'amenaça detectats, mostres de programari maliciós, TTP nous, etc.

- **Generació d'informes i alertes**: proporcionen informació de gran valor per als equips de seguretat. Aquests informes ajuden a la presa de decisions informades i a la implementació de mesures preventives.

6.4. Servei de *Threat Hunting*

És una disciplina proactiva dintre de la ciberdelinqüència que se centra en la cerca activa i continua d'amenaces cibernètiques ocultes o no detectades a la infraestructura d'una organització. A diferència de les estratègies de seguretat reactiva, el *Threat Hunting* adopta un enfocament perspicaç i orientat a la identificació primerenca d'amenaces possibles. Tot seguit, es detallen els aspectes claus d'aquesta especialitat:

- **Cerca activa i continua**: el *Threat Hunting* no espera que les alertes s'activin, sinó que, de manera proactiva i sistemàtica, s'encarrega de detectar comportaments anòmals a la xarxa o identificar activitat maliciosa.

- **Anàlisi de dades en temps real**: fa servir anàlisis avançades i eines especialitzades per avaluar dades en temps real, i permet una resposta ràpida a amenaces potencials.

- **Identificació d'IoC i TTP**: cerca indicadors de compromís coneguts i desconeguts, com també tàctiques, tècniques i procediments (TTP) utilitzats per actors maliciosos.

- **Col·laboració amb intel·ligència d'amenaces**: treballa en estreta col·laboració amb equips d'intel·ligència d'amenaces per incorporar informació rellevant en la cerca i assegurar una comprensió contextualitzada dels riscos possibles.

- **Desenvolupament d'hipòtesis**: els analistes de *Threat Hunting* desenvolupen hipòtesis sobre possibles amenaces basades en la comprensió profunda de la infraestructura i el comportament normal de la xarxa.

- **Disseny i implementació d'eines especialitzades**: per a la detecció proactiva d'amenaces, com ara sistemes de detecció d'anomalies i solucions d'anàlisi de comportament com les regles famoses YARA.

- **Investigació forense en temps real**: en cas d'identificar activitats sospitoses, es fa una investigació forense en temps real per comprendre la naturalesa i l'abast de l'amenaça.

- **Documentació i notificació**: documenta de manera exhaustiva les activitats de caça d'amenaces, i identifica IoC, TTP i qualsevol troballa rellevant. Aquests informes són valuosos per millorar les defenses i compartir intel·ligència amb altres equips.

- **Automatització de respostes**: en alguns casos, s'implementen respostes automatitzades per neutralitzar amenaces identificades, reduir el temps de resposta i mitigar l'impacte potencial.

6.5. Servei d'investigació i anàlisi de fraus

Aquesta especialitat dintre de l'àmbit de la ciberintel·ligència se centra en la detecció, investigació i mitigació d'activitats fraudulentes, tant en entorns digitals com fora de línia. Aquest servei exerceix un paper fonamental en la protecció de les organitzacions contra pràctiques il·lícites que podrien afectar la seva reputació, les finances i les operacions. Aquí es descriuen els aspectes claus d'aquesta disciplina:

- **Detecció proactiva de fraus**: implica l'adopció de mesures per identificar possibles activitats fraudulentes abans que generin un impacte significatiu. Això pot incloure el monitoratge constant de transaccions financeres i patrons de comportament inusual.
- **Anàlisi de patrons i tendències**: permet identificar comportaments anòmals que podrien indicar pràctiques fraudulentes.
- **Investigació en entorns digitals**: inclou la investigació en línia per rastrejar possibles senyals de frau al web, xarxes socials i altres espais digitals. Això pot involucrar la identificació de perfils falsos, activitats sospitoses o intents de pesca.
- **Anàlisi de transaccions financeres**: s'examinen detalladament en cerca d'irregularitats, patrons fraudulents o indicadors de compromís relacionats amb fraus financers.
- **Col·laboració amb entitats financeres**: s'estableix col·laboració amb institucions financeres i altres organitzacions per compartir informació sobre activitats fraudulentes i enfortir les defenses col·lectives.
- **Monitoratge d'activitats fora de línia**: també es fa un seguiment d'activitats fraudulentes que puguin succeir fora de l'àmbit digital, com ara el frau per correu, el robatori d'identitat o la manipulació de documents.
- **Desenvolupament de perfils de frau**: incloent els seus mètodes, tàctiques i possibles motivacions. Això facilita l'anticipació i prevenció d'intents futurs de frau.
- **Utilització d'eines forenses**: per recopilar evidència digital, cosa que facilita la presentació de proves en cas d'accions legals.
- **Implementació de mesures preventives**: basant-se en les troballes de les investigacions, es desenvolupen i apliquen mesures per evitar episodis futurs de frau. Això podria incloure la millora de polítiques de seguretat, la implementació de controls més estrictes i la conscienciació del personal.
- **Documentació**: s'elaboren informes detallats sobre les investigacions de frau, inclosa la documentació d'evidència, troballes clau i recomanacions per a l'acció.

6.6. Servei d'intel·ligència de vulnerabilitats

Aquesta branca especialitzada en l'àmbit de la ciberintel·ligència que s'enfoca en la identificació, avaluació i gestió de vulnerabilitats en els sistemes i aplicacions d'una organització. Aquest servei exerceix un paper crucial en permetre que les entitats mantinguin

una postura de seguretat proactiva i mitiguin riscos potencials. Aquí es detallen els aspectes claus d'aquesta disciplina:

- **Identificació proactiva de vulnerabilitats:** implica la cerca constant i proactiva de vulnerabilitats en sistemes, xarxes i aplicacions, fins i tot abans que siguin explotades per actors maliciosos.
- **Recol·lecció d'intel·ligència d'amenaces:** es nodreix d'informació procedent de la intel·ligència d'amenaces per identificar les vulnerabilitats més rellevants i les tàctiques fetes servir pels actors maliciosos per explotar-les.
- **Anàlisi de pedaços i actualitzacions:** avalua de manera contínua els pedaços de seguretat i actualitzacions disponibles per a sistemes i aplicacions, i assegura que les vulnerabilitats conegudes siguin abordades de manera oportuna.
- **Avaluació de riscos:** classifica les vulnerabilitats segons la seva gravetat i risc potencial per a l'organització, i permet una assignació eficient de recursos per a la mitigació.
- **Escaneig i proves de penetració:** fa escanejos automàtics i proves de penetració per identificar activament vulnerabilitats en la infraestructura, incloses xarxes, servidors i aplicacions web.
- **Integració amb sistemes de gestió de vulnerabilitats:** per facilitar el seu seguiment i correcció.
- **Anàlisi d'impacte:** avalua l'impacte possible que una vulnerabilitat podria tenir en les operacions i la seguretat general de l'organització, i permetre decisions informades sobre la priorització de mitigacions.
- **Col·laboració amb equips de seguretat:** treballa en col·laboració estreta amb altres equips de seguretat, com ara el de *Threat Hunting* i Intel·ligència d'amenaces, per integrar la informació sobre vulnerabilitats en l'estratègia general de seguretat.
- **Desenvolupament d'estratègies de mitigació**: proporciona recomanacions i estratègies per mitigar les vulnerabilitats identificades, incloses la implementació de pedaços, la configuració segura de sistemes i la millora de polítiques de seguretat.
- **Alertes i notificacions**: proporciona alertes immediates sobre noves vulnerabilitats crítiques que podrien afectar l'organització, i permetre respostes ràpides i mesures preventives.
- **Auditories de seguretat**: per garantir que les polítiques i les pràctiques de seguretat siguin efectives i estiguin alineades amb les millors pràctiques de la indústria.

7. PARÀMETRES DE MONITORATGE D'UNA ORGANITZACIÓ

Quan es tracta de protegir els actius digitals d'una entitat, mitjançant la ciberintel·ligència es poden definir tots aquells paràmetres susceptibles de patir un ciberatac.

En aquest context, es poden monitorar diversos paràmetres per enfortir la seguretat d'una organització. Alguns exemples específics inclouen:

- **Dominis i subdominis**:
  - Registre i monitoratge de dominis nous que podrien ser utilitzats per atacs de pesca o altres activitats malicioses.
  - Anàlisi de subdominis per identificar punts d'entrada possibles per a amenaces.
- **Adreces IP:**
  - Identificació d'adreces IP associades amb activitats malicioses o amb historial de compromisos.
  - Monitoratge de canvis a les adreces IP de servidors crítics per detectar possibles atacs.
- **Bretxes de credencials:**
  - Monitoratge de bases de dades de contrasenyes compromeses al web fosc per detectar possibles bretxes de credencials de l'organització.
  - Anàlisis d'intens d'inici de sessió no autoritzats o activitats sospitoses en comptes d'usuari.
- **Indicadors de compromís (IoC):**
  - Identificació i seguiment d'indicadors de compromís, com ara hashes d'arxius maliciosos, adreces IP de comandament i control, i patrons de trànsit sospitosos.
  - Incorporació dels IoC coneguts a les defenses de l'organització per bloquejar o alertar sobre possibles amenaces.
- **Amenaces persistents avançades (ATP):**
  - Monitoratge d'activitats associades amb APT, com ara campanyes de pesca dirigida, infiltració sigil·losa i moviments laterals a la xarxa.
  - Anàlisi de tàctiques, tècniques i procediments (TTP) que fan servir actors avançats.
- **Activitat al web fosc:**
  - Investigació proactiva al web fosc per identificar discussions o plans relacionats amb l'organització.

  - Monitoratge de fòrums i mercats clandestins en línia per a la venda d'informació confidencial.

- **Anàlisi de programari maliciós:**

  - Estudi de programari maliciós conegut i desconegut per comprendre la seva funcionalitat i adaptar les defenses contra amenaces noves.

  - Monitoratge de la propagació i evolució de programari maliciós a la xarxa.

- **Avaluació de vulnerabilitats:**

  - Anàlisi constant de vulnerabilitats en sistemes i aplicacions per prioritzar l'aplicació de pedaços.

  - Identificació de possibles explotadors o amenaces associades a vulnerabilitats conegudes.

Aquests només són alguns exemples de paràmetres que es poden monitorar a través de la disciplina de ciberintel·ligència.

La combinació d'aquestes dades permet a les organitzacions construir una visió integral de les amenaces i enfortir proactivament les seves defenses cibernètiques.

8. CONCLUSIONS

La ciberintel·ligència, una disciplina crucial en l'àmbit de la ciberseguretat, s'ha convertit en un component essencial per a la defensa i la protecció de les institucions públiques i privades a l'actual panorama digital. En la seva essència, la ciberintel·ligència s'enfoca en la recopilació, anàlisi i aplicació d'informació relacionada amb amenaces cibernètiques, i permet una anticipació proactiva a possibles riscos.

En l'actualitat, les amenaces cibernètiques evolucionen de manera constant, amb nous programaris maliciosos, tàctiques d'atac i vulnerabilitats que sorgeixen diàriament. La ciberintel·ligència s'erigeix en un pilar estratègic en proporcionar la capacitat d'identificar i comprendre cada element nou potencialment perillós al ciberespai. A diferència de la ciberseguretat defensiva, que respon a incidents, i la ciberseguretat ofensiva, que avalua sistemes de seguretat, la ciberintel·ligència destaca pel seu enfocament preventiu i la seva habilitat per anticipar amenaces emergents.

Per a les institucions públiques i privades, la ciberintel·ligència representa un valor diferencial essencial. La capacitat d'anticipació no només permet la detecció prematura d'amenaces, sinó també la implementació proactiva de mesures per mitigar riscos i protegir actius digitals crítics. En aquest sentit, la disciplina es presenta com una evolució de les tasques d'intel·ligència tradicionals, que s'adapta a l'entorn digital i millora les capacitats defensives en un entorn cibernètic cada vegada més complex.

Al cor de la ciberintel·ligència hi ha la incorporació de tecnologies avançades, l'anàlisi de dades i una comprensió profunda de les tàctiques dels actors d'amenaces. En monitorar dominis, adreces IP, bretxes de credencials i altres indicadors de compromís, les institucions poden enfortir les seves defenses, millorar la resiliència i salvaguardar la integritat de les seves operacions.

En resum, la ciberintel·ligència emergeix com un escut anticipat, essencial per afrontar les complexitats del ciberespai. La seva rellevància no només radica en la identificació i mitigació d'amenaces actuals, sinó també en la capacitat de preparar i protegir les institucions contra les amenaces del futur. En un entorn on la innovació tecnològica avança a un ritme vertiginós, la ciberintel·ligència es presenta com a un component crític per garantir la seguretat digital i preservar la integritat de les operacions tant en l'àmbit públic com privat.

9. CLÀUSULA DE CONFIDENCIALITAT

Aquest document és propietat de l'Agència Nacional de Ciberseguretat d'Andorra. Tota la informació que conté és confidencial, aquesta informació s'actualitzarà regularment per reflectir els possibles canvis dels productes i no podrà ser copiada o revelada a terceres persones sigui totalment o en part, sense consentiment previ exprés de l'Agència Nacional de Ciberseguretat d'Andorra.