La ciberseguretat a Catalunya

Setembre 2018

Informe tecnològic

ACCIÓ

Generalitat de Catalunya

La ciberseguretat a Catalunya: Informe tecnològic

ACCIÓ
Generalitat de Catalunya

Realització
sOwlers i Unitat d'Estratègia i Intel·ligència Competitiva d'ACCIÓ

Col·laboració
Secretaria de Telecomunicacions, Ciberseguretat i Societat Digital

Barcelona, setembre de 2018

Índex

1. Definició de ciberseguretat i importància per a la indústria

Definició de ciberseguretat

QUÈ ÉS LA CIBERSEGURETAT?

La ciberseguretat engloba el conjunt de mesures físiques, lògiques i administratives destinades a la protecció digital de les empreses, persones i sistemes, siguin dispositius, aplicacions o dades davant d'atacs digitals que puguin comprometre'n la confidencialitat, disponibilitat i/o integritat

EN QUÈ CONSISTEIX?

Els **sistemes ciberfísics** equipats amb la tecnologia d'Internet requereixen conceptes i tecnologies fiables per assegurar que la seguretat, la privacitat i la protecció del coneixement estan garantits. Per tant, són crucials unes **comunicacions fiables i segures**, juntament amb una identitat sofisticada i una gestió d'accés de les màquines.

Sobre aquests actius, es defineixen i s'implementen diferents capes de protecció a diferents nivells així com de prevenció i resiliència. D'aquesta manera, es combinen diferents mesures per poder prevenir i mitigar atacs de forma efectiva.

QUINA IMPORTÀNCIA TÉ?

Avui en dia les empreses tenen una gran presència digital, sigui exposada públicament a través d'Internet com internament amb la utilització de sistemes informàtics per gestionar les dades i processos interns. No ser capaç de protegir-se efectivament contra les noves amenaces exposa les empreses actuals a la pèrdua d'informació confidencial, a un impacte negatiu sobre la marca pròpia o a la incapacitat de desenvolupar l'activitat empresarial i a la vulneració de lleis específiques com el nou reglament de protecció de dades, l'incompliment del qual comporta sancions severes

Font: Mapeig Industria 4.0 i Palo Alto Networks

Importància de la ciberseguretat per a la indústria

EL CIBERCRIM ESTÀ EN EXPANSIÓ:

- El cost mundial dels danys produïts pel cibercrim costarà al món 6 bilions de dòlars americans el 2017, molt per sobre dels 3 bilions comptabilitzats el 2016.
- El 49 % dels directius espanyols reconeix que a les seves empreses manca una estratègia integral en ciberseguretat.
- Les empreses es veuen obligades a parar les seves operacions una mitjana de 17 hores a l'any a causa de ciberatacs.
- Durant el 2017, un 29,4 % dels equips d'usuari van patir un ciberatac almenys una vegada.
- Durant el 2017, programes d'antivirus van classificar com a maliciosos o falsos més de 199.400.000 URL.

PRINCIPALS IMPACTES NEGATIUS D'UN CIBERATAC PER A LES EMPRESES:

El 40 % dels ciberatacs causen la interrupció de les operacions i la facturació

Un 39 %, pèrdua d'informació confidencial i implicacions legals

El 32 % té un impacte negatiu sobre la qualitat dels productes

El 29 % dels ciberatacs causa danys a la propietat física

I el 22 %, danys en la vida humana

Sota el Reglament general de protecció de dades (GDPR) 2016/679, de 4 de maig de 2016, les empreses es fan responsables en un major grau de les dades que els seus usuaris volen compartir explícitament amb elles. Aquestes dades, en molts casos de caire personal, poden resultar d'interès per als cibercriminals o altres empreses, per treure'n profit econòmic mitjançant la venta o l'aprofitament econòmic i comercial d'aquestes. Casos recents com el de Cambridge Analitica ha fet central la privacitat de les dades que posseeixen les empreses sobre els seus usuaris i la protecció i l'ús d'aquestes.

Font: Elaboració pròpia a partir de Mapeig Indústria 4.0 i Palo Alto Networks

Importància de la ciberseguretat per a la indústria

el Periódico

Uber reconeix el robatori de les dades de 57 milions d'usuaris i conductors

LA VANGUARDIA

RANSOMWARE

Una nueva ola de ciberataques que empezó en Ucrania se extiende por el mundo

• El virus utilizado, de tipo Petya, sería un ransomware como el Wannacry que afectó a medio mundo en mayo

ABC

España bate su récord en ciberataques: 120.000 incidentes en 2017

• Según el Instituto Nacional de Ciberseguridad de España, los ataques en internet han crecido un 140% en tan solo dos años

Font: Notícies de premsa

El negoci del cibercrim

Agents	Motivacions	Vectors d'amenaça	Impacte
Estats / Nacions	• Competició global • Seguretat nacional • Frau	• Cibercampanyes de llarga durada • Persones infiltrades • Proveïdors terceres parts	• Pèrdua propietat intel·lectual • Disrupció infraestructures crítiques • Pèrdues monetàries • Legislatiu
Cibercriminals	• Enriquiment il·lícit • Frau • Suplantació identitat	• Robatoris individuals d'identitat • Esquerdes de dades i robatori propietat intel·lectual • Persones infiltrades • Via proveïdors tecnològics	• Pèrdua d'identitat • Pèrdues dineràries • Pèrdua propietat intel·lectual • Privacitat • Legislatiu
Ciberterroristes / *Hackers* individuals	• Ideològiques • Polítiques • Privació de drets • Crear el caos	• Vulnerabilitats oportunístiques • Persones infiltrades • Via proveïdors tecnològics	• Desestabilitzar, pertorbar i destruir actius d'institucions financeres • Legislatiu
Hacktivistes	• Causa política abans que guany personal • Ideològiques	• Organitzacions que s'interposen a la seva causa • Persones infiltrades • Proveïdors terceres parts	• Disrupció d'operacions • Desestabilització • Vergonya / Imatge • Relacions públiques • Legislatiu

* Els cibercriminals són els principals agents que ataquen les indústries

Font: EURECAT / PwC

PRINCIPALS MOTIUS DARRERE DELS CIBERATACS:

41 %	27 %	26 %	26 %	24 %	20 %	11 %
Segrest d'informació	Amenaça interna	Polític	Competició	Ciberguerra	Usuaris indignats	Desconegut

EXEMPLES MÉS HABITUALS DE VIES DE MONETITZACIÓ QUE UTILITZEN ELS CIBERCRIMINALS:

- Clonació de targetes de crèdit
- Transferències bancàries
- Frau en assegurances o serveis mèdics
- Suplantació d'identitat a la xarxa per fins comercials
- *Crime As A Service* / *Pay per Installs* (PPI)
- Robatori de criptomonedes
- Venta d'informació a terceres parts:
  - Propietat intel·lectual
  - Informació confidencial

Font: Raconteur.net

Ecosistema de la ciberseguretat en la indústria

Es defineixes **tres pilars fonamentals** per tal de construir una defensa sòlida dins de les organitzacions contra la pèrdua intencionada o no de dades:

PERSONES

L'element humà dins de la ciberseguretat és essencial per tal d'evitar comprometre les infraestructures i sovint és el més difícil de controlar.

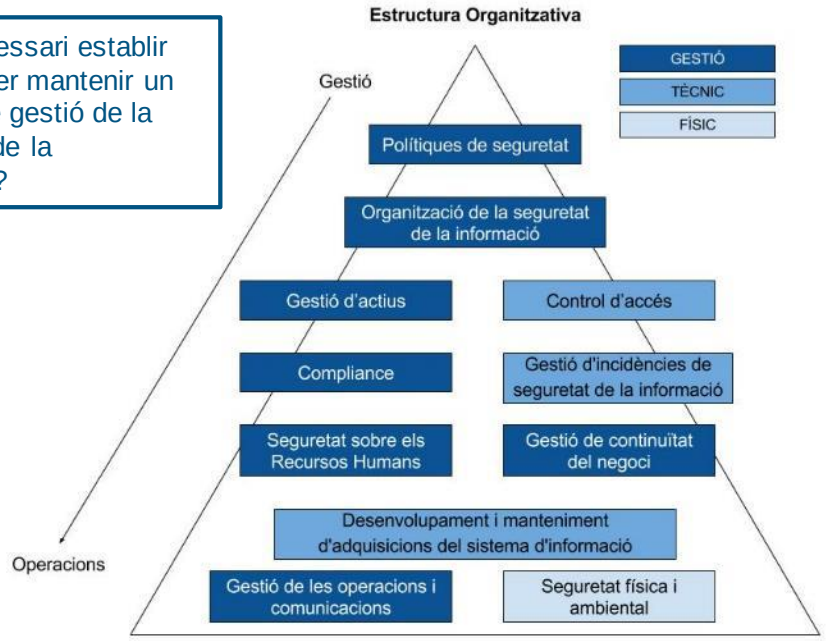
POLÍTICA

Juntament amb els procediments, són l'element vertebrador de l'organització. Serveixen de guia per als col·laboradors i per definir com s'emmagatzema, s'intercanvia i s'assegura la informació .

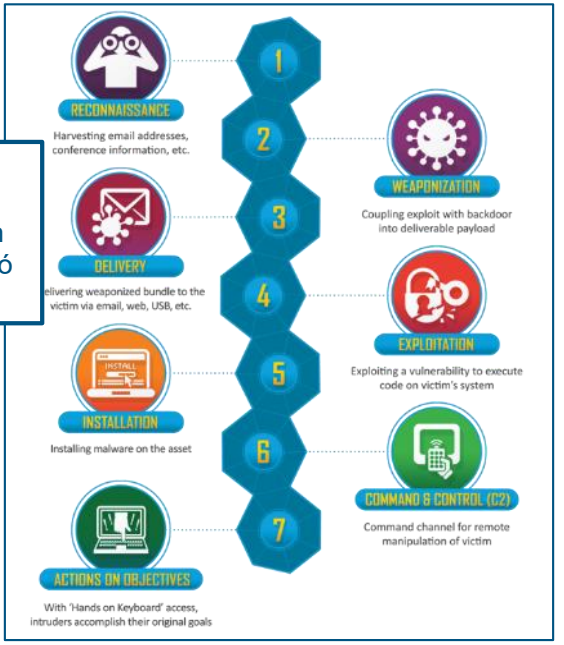
TECNOLOGIA

És un component vital per a la ciberseguretat d'una organització. Hauria de ser habilitador i protector dels actius.

On és necessari establir requisits per mantenir un sistema de gestió de la seguretat de la informació?



El *Kill Chain* modela l'aproximació a la prevenció d'una amenaça en cadascun dels actius d'una organització segons l'estadi de la intrusió



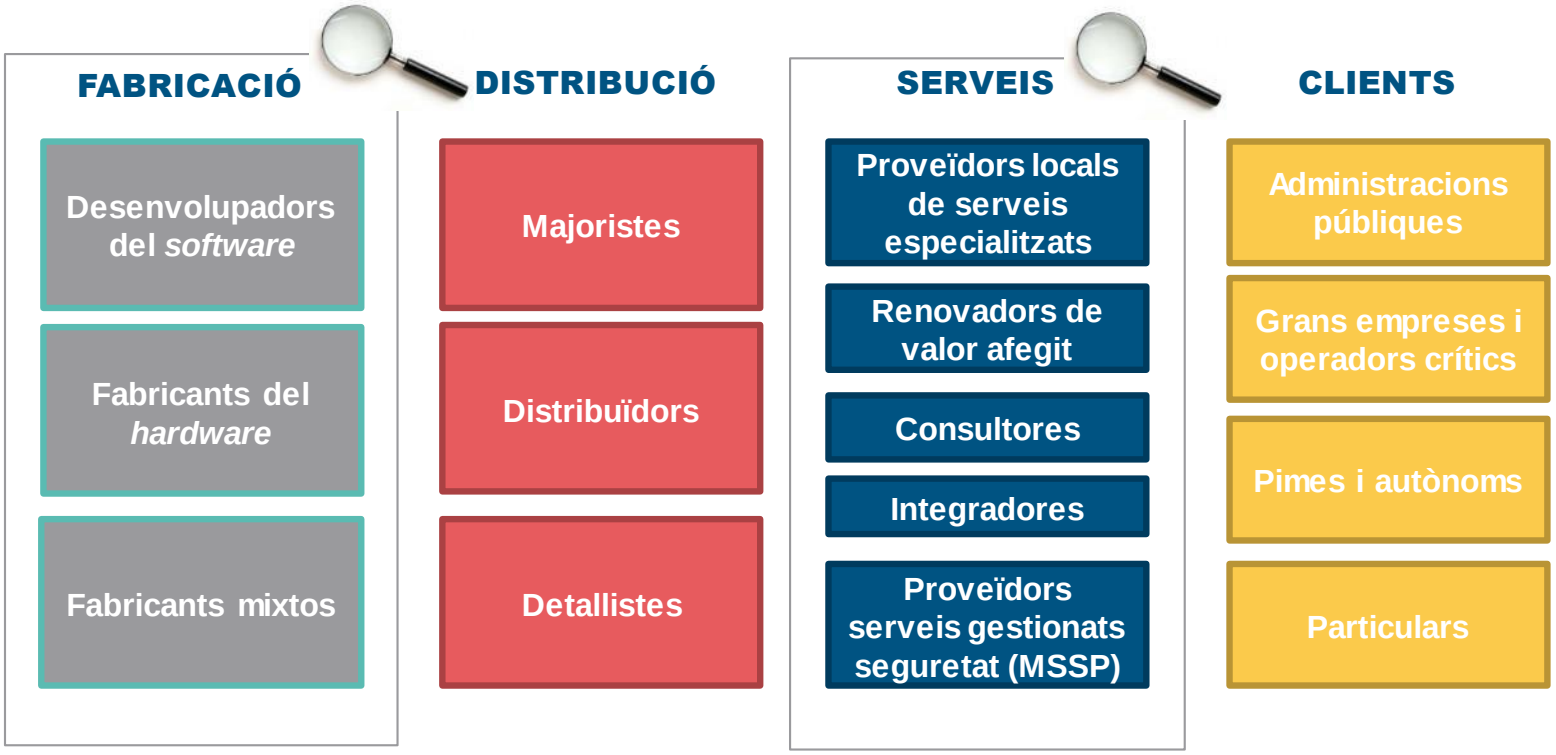
Font: Compass Cyber Security / Brain Book (Technology definitions, News, Reviews and Updates

2. Empreses líders en ciberseguretat

Empreses líders mundials en ciberseguretat

CADENA DE VALOR

La **cadena de valor** de la ciberseguretat és el model en què trobem les principals activitats i els vincles de relació entre les diferents parts de la cadena.



Font: INCIBE

FABRICACIÓ

S'hi emmarquen **els agents de fabricació i desenvolupament de solucions** de ciberseguretat, que giren entorn de les següents categories:

- Antifrau
- Antimalware
- Auditoria tècnica
- Certificació normativa
- Contingència i continuïtat
- Control d'accés i autentificació
- Compliment legal
- Intel·ligència de seguretat
- Prevenció de fuga d'informació
- Protecció de les comunicacions
- Seguretat dels dispositius mòbils

SERVEIS

Serveis de valor afegit entorn de les següents categories:

- Auditoria de seguretat, planificació i serveis d'assessorament
- Certificació de la normativa
- Contingència i continuïtat
- Compliment legal
- Formació i conscienciació
- Gestió d'incidents
- Implantació de solucions
- Seguretat en el núvol
- Suport i manteniment

Font: INCIBE

Empreses líders mundials en ciberseguretat

Nota: L'ús d'aquestes marques és merament informatiu. Les marques esmentades en el present informe pertanyen als seus respectius titulars i, en cap cas són titularitat d'ACCIÓ. Aquesta és una representació il·lustrativa parcial de les principals empreses que formen part de l'ecosistema del sector de la ciberseguretat a Catalunya, però hi pot haver altres empreses que no hagin estat incorporades a l'estudi.

Font: Cybersecurity Ventures

Empreses líders mundials en serveis de ciberseguretat

HERJAVEC GROUP
Information Security Services

EY
Security Awareness Training

BAE SYSTEMS
Cybersecurity Risk Management

IBM
Enterprise IT Security Solutions

SERA-BRYNN CYBER RISK MANAGEMENT
Cyber Risk Management

Booz Allen
Cybersecurity Solutions & Services

Raytheon
Cyber Security Services

CLEARWATER COMPLIANCE
Risk Management and Compliance

Telos
Risk Management and Compliance

Font: Elaboració pròpia de Cybersecurity Ventures

Principals actors en el mercat de la fabricació

mimecast	*E-mail Security*	Proporciona gestió de correu electrònic basada en núvol per a Microsoft Exchange, incloent-hi l'arxivament, la continuïtat i la seguretat. En unificar els entorns de correu electrònic dispars i fragmentats en una solució integral que sempre està disponible des del núvol, Mimecast minimitza el risc i redueix el cost i la complexitat.
KnowBe4 Human error. Conquered.	*Security Awareness Training*	Know Be4 s'ha convertit en la plataforma d'entrenament de conscienciació "*Awareness*" de seguretat i simulació de *phishing* més popular del món. Milers de comptes empresarials l'utilitzen, un 25 % dels quals són bancs i cooperatives de crèdit.
cisco	*Threat Protection & Network Security*	Les innovacions de seguretat de Cisco ofereixen tallafocs altament segurs, serveis web i serveis de correu electrònic per tal de permetre la mobilitat i el teletreball. Els productes de seguretat de Cisco inclouen: Control d'accés i política, Protecció avançada de *malware*, Seguretat per correu electrònic, Tallafocs, Seguretat en xarxa, Sistema de prevenció d'intrusions de nova generació (NGIPS), Gestió de la seguretat, Clients de seguretat VPN i *endpoint* i Seguretat web.
SOPHOS	*Anti-Virus & Malware Protection*	Sophos ajuda les organitzacions a mantenir les seves dades segures i deté la creixent quantitat d'amenaces complexes. Proporcionen una gamma completa de productes d'extrem final de xarxa (*Endpoint*), encriptació, correu electrònic, web i NAC.
LOCKHEED MARTIN	*Cybersecurity Solutions & Services*	D'origen aeroespacial i militar, Lockheed Martin és un dels contractistes de defensa més grans del món. En l'àmbit de la ciberseguretat, operen des d'un dels seus quatre segments de negoci, que comprèn el 27 % de les seves ventes netes.
FORCEPOINT	*Insider, Cloud & Network Security*	Forcepoint està transformant la ciberseguretat centrant-se a entendre la intenció de la gent a mesura que interactua amb dades crítiques i la propietat intel·lectual en qualsevol entorn en què resideixi. Els sistemes permeten a les empreses capacitar els empleats que gestionen dades confidencials, protegint la propietat intel·lectual i simplificant les polítiques de conformitat.
thycotic	*Privileged Account Management*	Thycotic desplega solucions de seguretat informàtiques, fiables i intel·ligents, que permeten a les empreses controlar i monitorar les credencials de comptes privilegiats i la identitat per l'accés dels administradors i usuaris finals.
Symantec.	*Cyber Threat Protection*	Empresa líder mundial en el disseny de protecció contra les amenaces cibernètiques tant de les empreses com dels usuaris individuals. També ofereix serveis i protecció en serveis *cloud.*
Check Point SOFTWARE TECHNOLOGIES LTD	*Cyber Threat Protection*	Check Point és un proveïdor global de solucions de seguretat IT. Amb el temps, la companyia ha desenvolupat, comercialitzat i suportat una àmplia gamma de *hardware* i *software* combinats i productes de *software* que cobreixen tot tipus d'aspectes de seguretat d'IT, incloent-hi seguretat de xarxa, seguretat *endpoint*, seguretat de dades i gestió de seguretat.

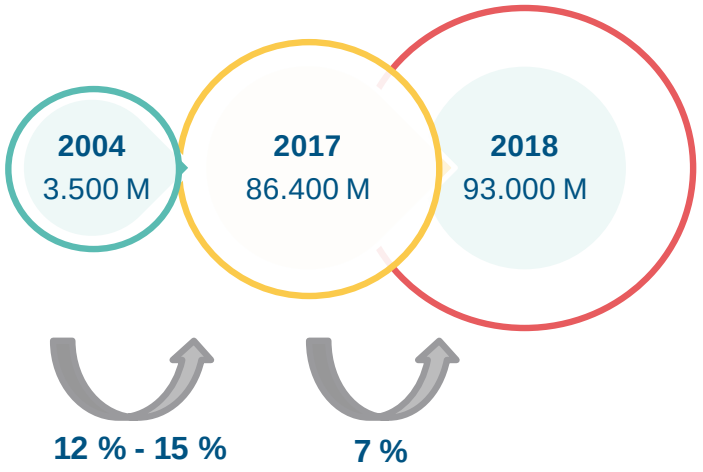
Font: Cybersecurity Ventures

3. Mercat mundial de la ciberseguretat

Mercat mundial de la ciberseguretat

DIMENSIÓ DEL MERCAT ACTUAL

- L'any **2004** el mercat global de la ciberseguretat estava valorat en 3.500 M US$. L'any **2017** va tancar assolint la xifra dels 86.400 M US$, el que suposa un creixement anual d'entre el 12 % i el 15 %. El **2018** s'espera un creixement de fins als 93.000 M US$.
- Aquest mercat, però, està concentrat en molts pocs països, especialment als EUA. I, en el cas d'Europa, especialment al Regne Unit.



DADES PROSPECTIVES

La ciberseguretat està en expansió

- Es preveu que la despesa acumulada global en ciberseguretat en el període 2017-2021 pugi a 1 bilió de dòlars americans (USD $1 \cdot 10^{12}$).
- Com a dada significativa, només en entrenament i conscienciació dels usuaris i col·laboradors per reconèixer i defensar-se contra ciberatacs (*awareness*) es preveu que la despesa global el 2027 serà de 10.000 M US$.
- Cal dir, però, que les dades sobre el que es gasten les empreses en ciberseguretat són cada vegada més difícils de rastrejar perquè es tracta d'informació sensible.

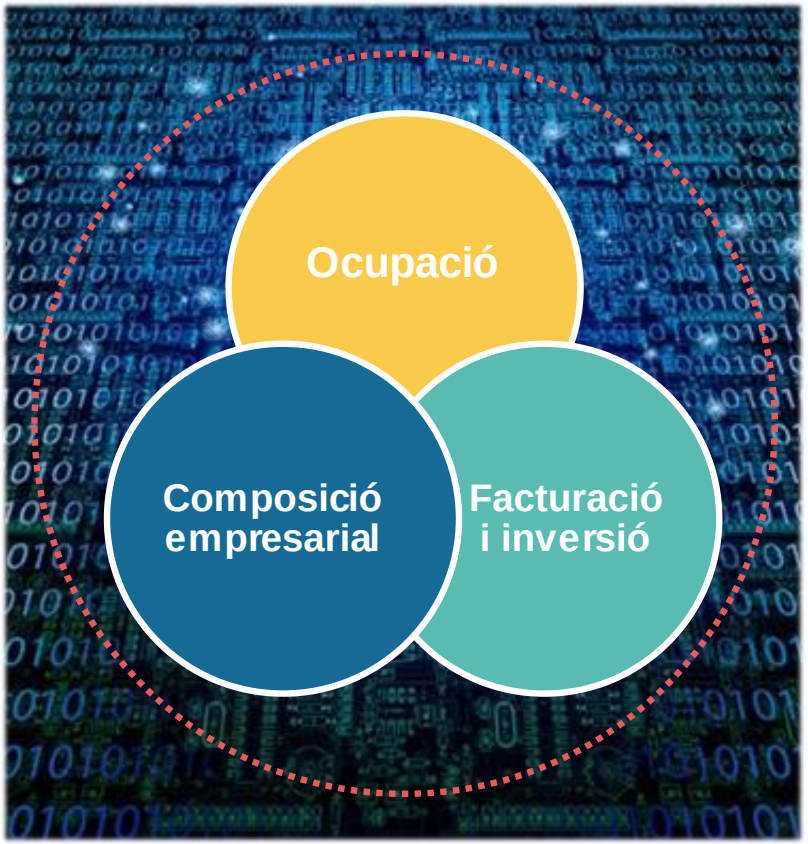
Font: Estadística Gartner / ACCIÓ / Cybersecurity Ventures

EL SECTOR A ESPANYA

- L'any 2014, **el sector de la ciberseguretat a Espanya** estava compost per un total de 533 empreses -*pure players* i empreses TIC- que proporcionaven feina a 5.808 persones. Pràcticament la totalitat d'aquesta força de treball (99,5 %) es concentrava en empreses del sector TIC. A més, 2.143 persones, **un 37 % dels empleats del sector, es dedicaven exclusivament al negoci de la ciberseguretat**.

- El mateix any, **la facturació total del sector de la ciberseguretat va ser de 598,2 milions d'euros**. Només el 14,8 % de les 533 empreses dedicades exclusivament al sector de la ciberseguretat van contribuir amb més del 50 % de la facturació total del sector.

- Finalment, **la inversió total realitzada per les empreses del sector durant el 2014 va ser de 79 milions d'euros**. Dins del sector de la ciberseguretat, la distribució de la inversió realitzada situava les empreses pertanyents al sector de Serveis TIC com les que més inversió havien dut a terme, amb 77,8 milions d'euros, un 98,5 % sobre el total invertit.



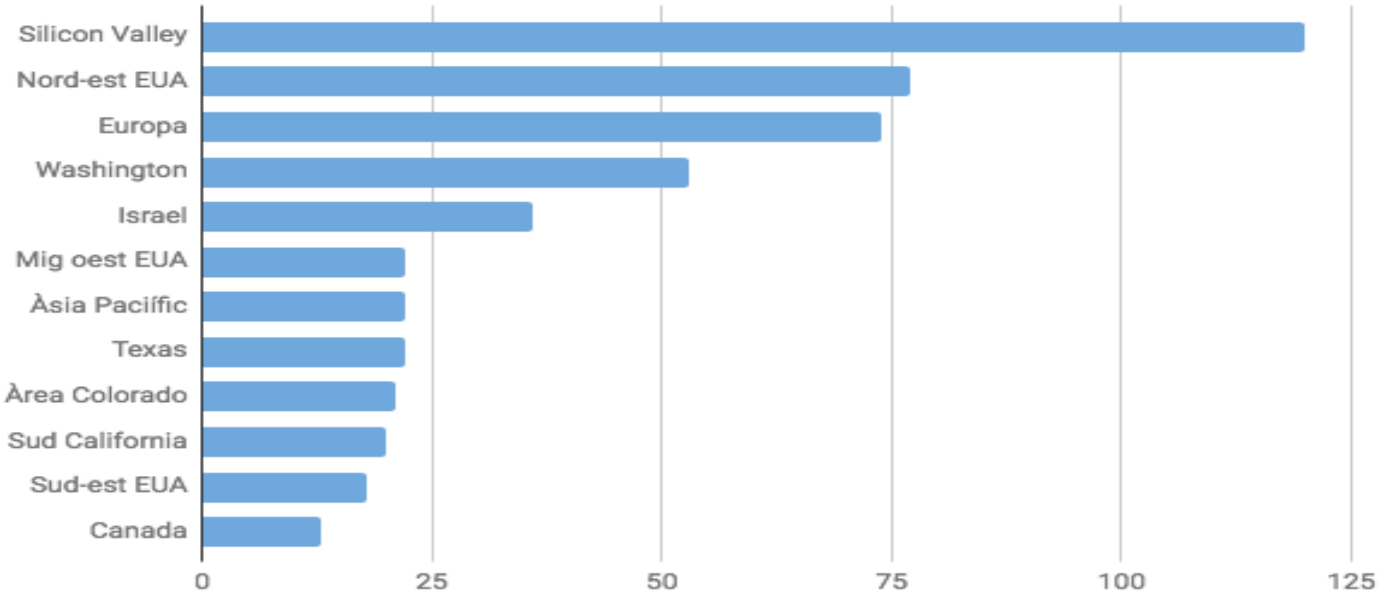
Font: Institut Nacional de Ciberseguretat (INCIBE)

4. Regions i *hubs* de rellevància al món

PRINCIPALS *HUBS* DE DESENVOLUPAMENT DE LA CIBERSEGURETAT

El mercat de la ciberseguretat està concentrat en molts pocs països, especialment als EUA amb diferents pols d'atracció com Silicon Valley (24 % *share* mundial), la regió nord-est que inclou Nova Anglaterra, Nova York i Nova Jersey (15 %) i Washington (10 %). Fora dels EUA, destaca el Regne Unit que concentra el 5 % del sector (32 % de les empreses europees), Israel amb un 7 % i The Hague Security Delta Cluster dels Països Baixos de referència en la ciberseguretat europea.

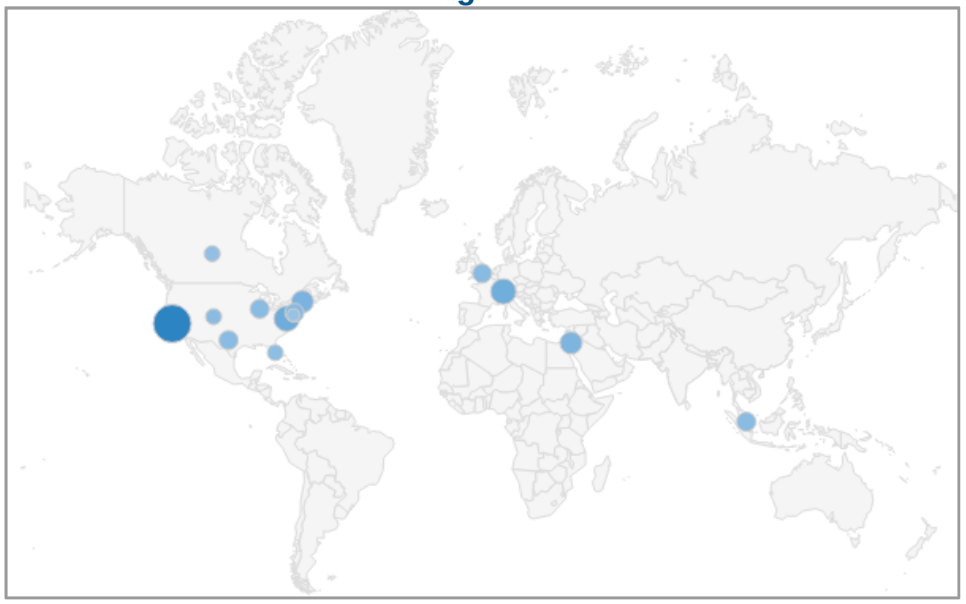
Nombre de *hubs* dedicats a la ciberseguretat



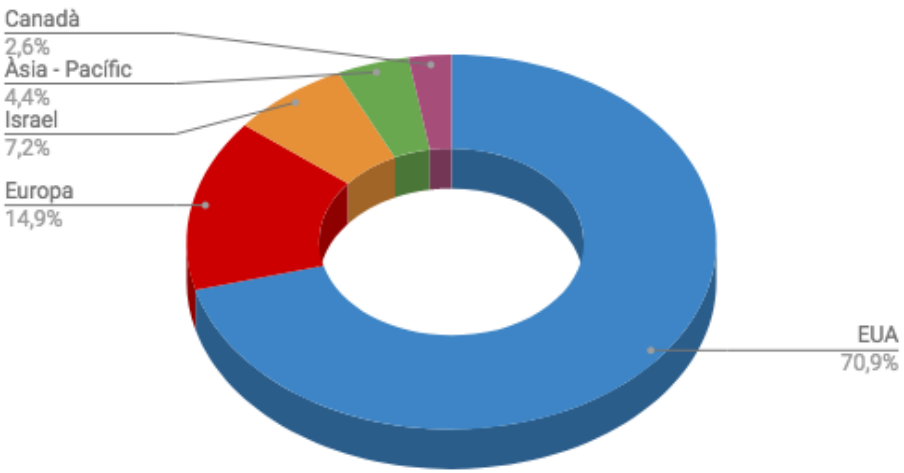
Font: Cybersecurity Ventures

PRINCIPALS *HUBS* DE DESENVOLUPAMENT DE LA CIBERSEGURETAT

Principals *hubs* de desenvolupament de la ciberseguretat al món:



Distribució de les 500 principals empreses del mercat de la ciberseguretat:



Com a **tendència**, el 2021 més del 80 % de les grans empreses a la **Xina** implementarà equips de seguretat de xarxa d'un venedor local. La recent aprovació de la legislació sobre seguretat cibernètica de la **Xina** contribuirà a un major desplaçament dels productes de seguretat fabricats pels EUA als proveïdors xinesos locals.

Font: Cybersecurity Ventures

5. Principals inversors mundials

Principals inversors mundials

New Enterprise Associates

Barkly Protect, Cloudflar, Cyvellance, Datavisor, Evident ID, Forter, IDFy, Nevis Networkniara, Qadium, Unifyld, Veriflow Systems, Illusive Networks, Yubico, Bitglass, Code42, Cyence, Datrium, Expel, Fugue, Hackerone, Niara, ThreatQuotient, Tigera, Virtu, ZeroFox, WireWheel

Andreessen Horowitz

Blue Box Security, DataGravity, CipherCloud, PagerDuty, Okta, Keybase, Pindrop Security, Sookasa, SignalFX, Illumio, Forward Networks, CoreOs, Bromium, Orchid, Lookout, Jumio, Tanium, Signifyd

Accel Partners

AirWatch, Code42 Software, Corelight, Demisto, Illumio, Netskope, Sansa Security, Shift Technology, Sookasa, Sysdig, Vectra Networks, Callsign, Core OS, CrowdStrike, ForeScout Technologies, Lookout, Pager Duty, SentinelOne, Simility, Sumo Logic, Tenable Network Security

Bessemer Venture Partners

Apperian, Bastille Networks, Claroty, CyberGRX, Defense.net, Endgame, LifeLock, PagerDuty, Team8, Virtu, Auth0, Capsule8, cloudLock, Dashlane, Distil Networks, Finjan Software, Nominum, PhishMe, ThreadTrack Security, Illustrative networks

Forge Point Capital

AlienVault, Appthority, Bay shore, Ironnet, Mocana, Prevoty, Reversinglabs, Solera

Adara Ventures

4IQ, AlienVault, Counter craft, Kompyte, loopup, Openbravo, Seedtag, Stratio

Font: CB Insights, Cesicat i pàginesweb de lesventure capital

Principals inversors mundials

SEED / ANGEL:

1 **MACH37** és la principal acceleradora de seguretat cibernètica centrada en el mercat americà. L'acceleradora està dissenyada per facilitar la creació de la pròxima generació de companyies de productes de seguretat cibernètica. El disseny dels programes de MACH37 fa èmfasi en la validació d'idees de producte i en el desenvolupament de relacions que produeixen una base de clients inicial i capital d'inversió.

2 **Y Combinator** és una empresa de capital risc en etapa "seed", fundada el 2005 per Paul Graham, Robert Morris, Trevor Blackwell i Jessica Livingston. Y Combinator s'especialitza en el finançament de *start-ups* en etapa inicial, principalment en l'àmbit del programari i serveis web.

3 **Cyber London (CYLON)** és un *hub* per a les empreses de seguretat cibernètica emergents. CYLON ofereix un programa accelerador de tres mesos que ofereix formació per construir i fer créixer companyies de seguretat cibernètica exitoses.

4 **Techstars** és un ecosistema global que permet als emprenedors aportar noves tecnologies al mercat des de qualsevol part del món. Conté desenes de programes de *mentoring* i milers de programes comunitaris a l'àmbit mundial, amb vocació d'acompanyar els emprenedors des de la fase d'idea fins a les primeres ofertes públiques de capital.

Font: CB Insights

Principals inversors mundials

SERIES A,B,C,D,E

1. NEA
2. ACCEL PARTNERS
3. ANDREESSEN HOROWITZ
4. BESSEMER VENTURE PARTNERS
5. KPCB KLEINER PERKINS CAUFIELD BYERS
6. NORWEST VENTURE PARTNERS
7. SEQUOIA
8. intel Capital
9. Google ventures
10. PALADIN CAPITAL GROUP
11. DELL Technologies CAPITAL
12. GENERAL CATALYST
13. BV Battery Ventures
14. .406 Ventures
15. LIGHTSPEED VENTURE PARTNERS

1 **New Enterprise Associates (NEA)** proporciona capital de risc per ajudar els emprenedors i líders empresarials a construir companyies transformadores i líders de la indústria a tot el món. La majoria de les seves inversions se centren en les primeres etapes de desenvolupament d'empreses que inverteixen una part significativa del seu capital en oportunitats de creixement a risc. NEA també inverteix en mercats fora dels EUA, incloent-hi la Xina i l'Índia. NEA aplica la seva experiència en la creació d'empreses a través de tres dominis clau: tecnologies de la informació, assistència sanitària i tecnologies energètiques

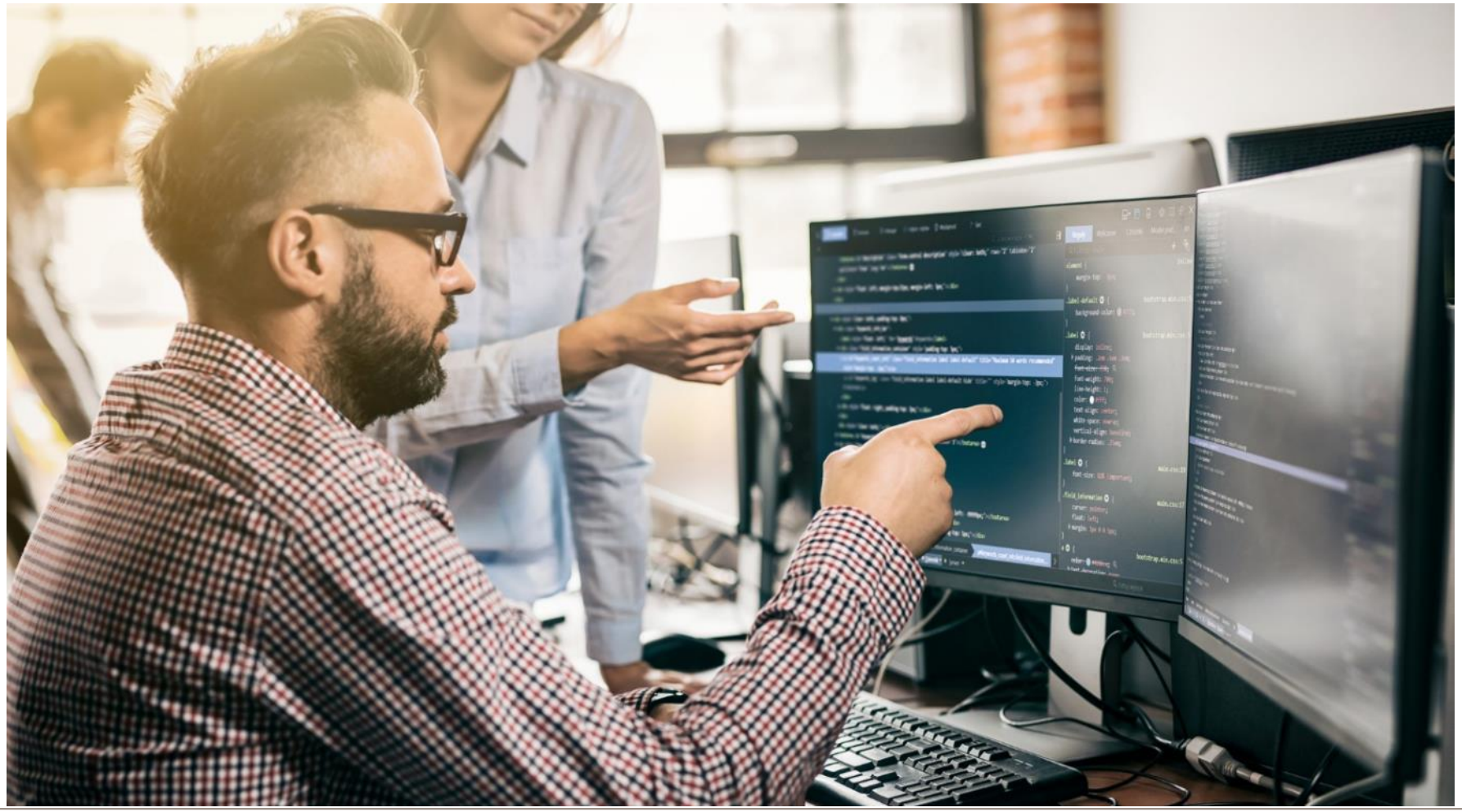
2 **Accel Partners** és una empresa de capital de risc que inverteix en diversos sectors, entre els quals s'inclouen la infraestructura de computadors i emmagatzematge, Internet i mitjans de consum, energia, *software* i serveis empresarials, serveis sanitaris i biotecnològics, mòbils, sistemes de xarxes, *retail*, seguretat, semiconductors i serveis tecnològics . Accel Partners té oficines als Estats Units, Londres, la Xina i l'Índia.

3 **Andreessen Horowitz** és una empresa de capital de risc basada a Silicon Valley amb gestió de fons fins a 4.200 milions de dòlars. La firma inverteix en empreses emprenedores en cada etapa, des de la llavor fins a gran creixement.

4 **Bessemer Venture Parters** és una empresa de capital de risc amb oficines a Nova York, Silicon Valley, Boston, Mumbai i Herzliya. Bessemer inverteix principalment en oportunitats en primeres etapes, però també pot participar en finançament en fases finals i inclús, ocasionalment, també realitza inversions en fase inicial.

Font: CB Insights

6. Tendències en ciberseguretat



Principals tendències en ciberseguretat (I)

Segons un estudi de *Business Insights* elaborat per la Universitat de Barcelona i la consultora EY, **el 60 % de les empreses catalanes invertiran en ciberseguretat.** De la mateixa manera, el 83 % de les empreses admeten que estan immerses en processos de transformació digital. La ciberseguretat encapçala les preferències de les empreses catalanes dins els seus processos de transformació digital.

En el marc de una **societat globalitzada**, cada vegada més digital i connectada, la generació massiva de dades marca el paradigma de societat actual.

Les tendències en ciberseguretat es fonamenten en l'impacte que tenen les TIC en la societat actual.

- Una nova generació de components i sistemes: ***Internet of Things***
- La digitalització de la indústria, sensorització, robòtica i intel·ligència, en el concepte **Indústria 4.0**
- **Internet del futur**: la nova arquitectura de xarxa 5G, el *cloud* i *fog computing* i els serveis crítics
- Apoderament de les dades: ***big data* i intel·ligència artificial**
- Computació avançada i ***Cloud Computing***
- Tecnologies facilitadores a través de la innovació **en fotònica (quàntica) i nano-electrònica**
- Un nou sistema de computació i encriptació més segur, el ***quantum security***

Font: Elaboració pròpia / Mapeig Indústria 4.0 / Business Achievers

Principals tendències en ciberseguretat (II)

Pel que fa al **sector industrial**, les **ciberamenaces** són una tendència en augment arreu del món, que afecta totes les indústries. Els mateixos avenços tecnològics que han impulsat la productivitat i l'eficiència dels negocis són els que han fet les organitzacions vulnerables als ciberatacs.

Els factors que motiven aquest creixement tan gran del mercat de la ciberseguretat són els següents:

Les tendències industrials que requereixen ciberseguretat

El **desplegament de sistemes ciberfísics** en la producció, susceptibles als atacs cibernètics.

Els processos de **digitalització i migració** *online* penetren cada vegada més en les empreses i institucions

La complexitat de les **amenaces** augmenta ràpidament i de manera constant.

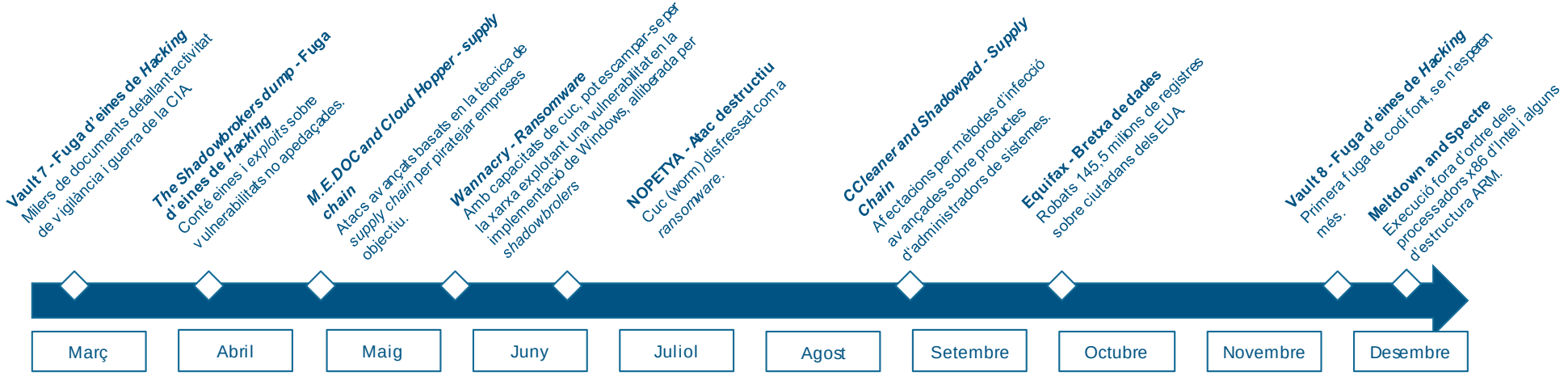
Les cadenes de producció cada vegada estan més **interconnectades.**

Hi ha una tendència cap a una **major obertura i accés a la informació** de les empreses.

Font: Elaboració pròpia / Mapeig Indústria 4.0 / Business Achievers

Tendències d'amenaces actuals i futures

ATACS MÉS IMPORTANTS DURANT EL 2017



TENDÈNCIES D'AMENACES

En els pròxims anys, s'espera que els atacs principals i més innovadors sorgeixin sobre les següents tècniques i objectius:

- **Atacs basats en *Ransomware*** utilitzant tècniques d'infecció avançades (*supply chain*) com "*watering hole*" o el compromís d'empreses de *software*. Exemples: *Wannacrya NoPetya, Bad Rabbit*.
- **Atacs basats en entorns mòbils.**
- IoHT (*Internet of Hackable Things*). Exemples com el cas de Mirai sobre "botnets".
- **Atacs als sistemes *Blockchain***, amb afectació sobre criptomonedes.
- **Atacs sobre caixers automàtics** (ATM).
- "***Lateral movement***", tècnica utilitzada per moure's dins d'una xarxa per trobar dades o actius que són l'objectiu final. Exemples: *Wannacry, NoPetya*.
- ***Fileless malware***: variants de virus que no escriuen als disc durs, en què els antivirus busquen constantment, sinó que utilitzen altres memòries com la RAM.

Font: Cybereason

7. Principals aplicacions per sector de demanda

Sectors en els quals la ciberseguretat té i pot tenir més aplicació

Indústria i medi ambient: el sector industrial sosté grans quantitats d'informació crítica com dades sobre patents i propietat intel·lectual. S'enfoquen cap a la protecció de dispositius i xarxes que conformen les *Smart Grid*, infraestructures crítiques, Indústria 4.0 i serveis amb cabuda dins del sector industrial, fonamentalment energètic.

Mobilitat: enfocat a la protecció de mitjans de transport aeri o terrestre, així com aviat als vehicles autònoms i/o connectats.

Serveis financers: en què s'inclou la divisió d'assegurances. La indústria posseeix molta informació sensible com comptes bancaris i informació financera. La ciberseguretat s'enfoca principalment a la defensa d'incidents derivats de la digitalització de serveis com la banca *online* o aplicacions *FinTech*.

El **sector TIC** o basat en la digitalització, és un sector transversal als anteriors que recopila les necessitats i pràctiques més habituals en matèria de ciberseguretat, que poden ser aplicades a la resta de sectors definits

Govern: basat en els organismes públics i administracions públiques i amb les seves corresponents vulnerabilitats derivades de la gestió de serveis públics electrònics. L'any 2015 la Generalitat va rebre prop de 216 milions d'atacs informàtics i va registrar més d'11.700 incidents de ciberseguretat.

Salut: inclou els serveis públics de sanitat i educació. Orientat a la protecció de dispositius mèdics interconnectats, patents o informació sensible. El 2015, tres de les set fugues de dades més importants van ser al sector mèdic.

Educació i formació: necessitat de formació i capacitació professional especialitzada en ciberseguretat.

Font: INCIBE i Smart Catalonia

Aplicacions per sector de demanda (I)

Indústria i medi ambient

Indústria: *Smart Grids*, Indústria 4.0, Infr. Crítiques, *Utilities*

Sistemes ciberresilients per infraestructures crítiques

Sistemes dissenyats per a la prevenció de la destrucció o pertorbació d'infraestructures estratègiques amb afectació a la disponibilitat dels serveis essencials.

Ciberseguretat en sistemes de control industrial: ICS/SCADA

Alts nivells de ciberseguretat per a sistemes altament complexos amb naturalesa multidisciplinària i aplicable a múltiples sectors. El cas de Stuxnet és un exemple per SCADA.

Protecció dels dispositius intel.ligents

Protecció de dispositius com sensors i actuadors que intervenen directament en els processos de fabricació i logística com autenticació, encriptació M2M i intrusió.

Mobilitat

Transport i Comunicacions: Cotxes intel·ligents, aviació, satèl·lits

Protecció de vehicles autònoms i connectats

Seguretat en els sistemes de control de vehicles inter-connectats i vehicles autònoms, així com de les xarxes dels sistemes intel·ligents que hi interaccionen.

Seguretat i protecció de vehicles aeris no tripulats: drons

Exposats a riscos de pèrdua de confidencialitat, integritat i disponibilitat de les dades, fet que fa del seu desenvolupament un repte per a la seguretat.

Protecció de sistemes de comunicació satèl·lit

Vulnerabilitats als sistemes de comunicacions globals que poden permetre a atacants remots inutilitzar per complet sistemes i serveis crítics com: serveis de emergències, militars, avions, etc.

Font: INCIBE

Aplicacions per sector de demanda (II)

Serveis financers

Finances i Assegurances: Banca *online*, *FinTech*

Big Data Analytics: detecció de frau en banca i assegurances

Permet, entre d'altres, la detecció i prevenció del frau en temps real, reduint els costos de monitoratge i d'investigació d'incidents.

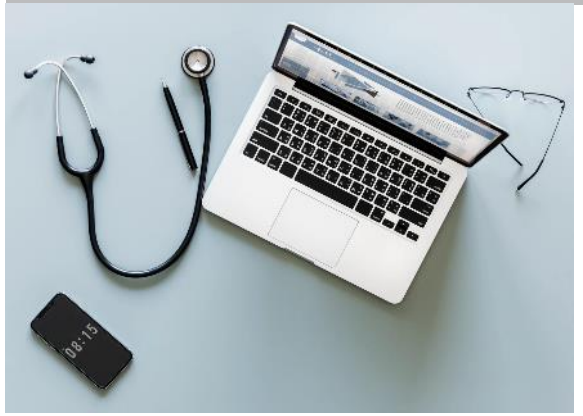
Gestió d'informació d'actes de seguretat (SIEM)

Detecció d'amenaces i resposta a incidents de seguretat a través de l'obtenció en temps real d'esdeveniments de seguretat i la seva anàlisi històrica.

Seguretat en els serveis *FinTech*

Basat en el desenvolupament de noves solucions de protecció de sistemes o aplicacions de pagament *on-line*, sistemes de *m-commerce* o mòbil, NFC, lectors de targetes per mòbils, etc. basats en l'autenticació d'usuari i solucions de prevenció del frau.

Salut



Sanitat i Farmàcia: eHealth, Farmàcia

Protecció de dispositius mèdics connectats

Dispositius connectats a la xarxa que necessiten assegurar-ne la confidencialitat, la integritat i el control, especialment els que no disposen de *software* personalitzat per al seu ús.

Encriptació per recerca mèdica i farmacèutica

Tendència de seguretat cap a l'encriptació apta per disposar de fonts d'informació de múltiples centres mèdics xifrats amb claus diferents que, sense la desencriptació de la informació, salvaguardin la confidencialitat dels pacients.

Emmagatzematge segur de dades mèdiques

La protecció de les dades personals i clíniques dels pacients requereix, no només un sistema d'emmagatzematge xifrat, sinó també mecanismes de transferència segurs que en garanteixin la ubiqüitat.

Font: INCIBE

Aplicacions per sector de demanda (III)

Educació

Formació: formació en seguretat, ocupació, *e-learning*

Cibereducació i laboratoris de ciberseguretat

La integració de l'educació amb la tecnologia i la ciberseguretat convergeix en la cibereducació. Es tracta d'una modalitat educativa a partir de diferents competències i disciplines com ara: interacció, retroalimentació, gamificació, simulació, etc. aplicades a la formació en ciberseguretat.

Govern

AAPP: *e-Government*, defensa i participació

Distribució de ciberintel·ligència

Basat en l'intercanvi d'informació entre organismes públics i privats provinent de l'anàlisi de ciberamenaces.

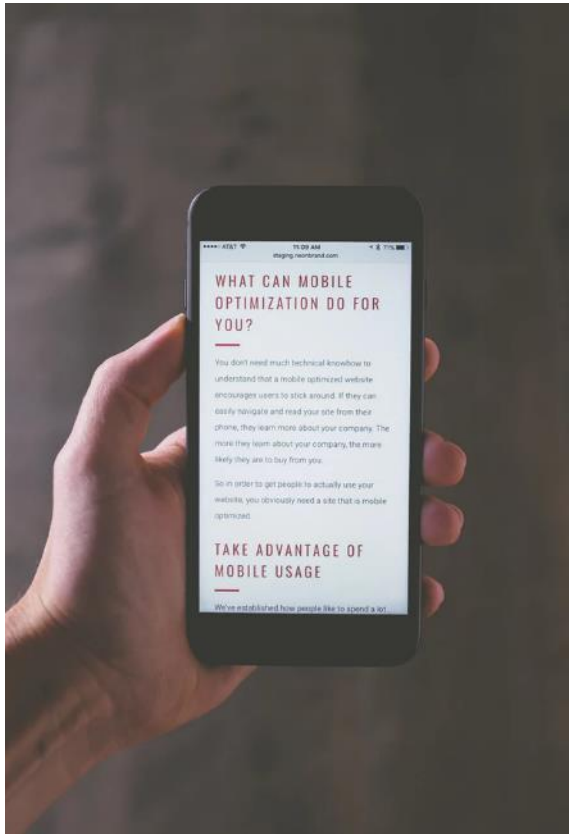
Simulació d'incidents i ciberexercicis

Entorns d'entrenament que simulen escenaris i incidents per posar a prova la capacitat tecnològica i de recursos d'una organització.

Font: INCIBE

Aplicacions per sector de demanda (IV)

TIC



Digitalització: *Internet of Things*, *Cloud Computing*, Serveis de seguretat

Serveis de seguretat en el núvol

Serveis generalment d'*outsourcing* de l'administració de la seguretat que aprofiten l'escalabilitat del model del *Cloud Computing* que permet a les organitzacions dimensionar els esforços de la seva capacitat actual

Hacking ètic

Cerca les vulnerabilitats de les xarxes d'una organització mitjançant la utilització de proves de penetració.

Encriptació en temps real

Mecanismes de protecció de la seguretat de les dades en les transaccions electròniques en què les dades es xifren abans de ser emmagatzemades i es desxifren quan es baixen, abans de ser utilitzades.

Internet of Things

Els dispositius connectats actualment no tenen una seguretat suficient, i requereixen solucions de ciberseguretat, tant en entorns empresarials com individuals i governamentals.

Encriptació homomòrfica

Permet que la informació codificada sigui compartida amb terceres parts i sigui utilitzada en càlculs i processos computacionals, sense que els sistemes implicats puguin interpretar-ne la informació.

Certificació de confiança digital

Comprova, materialitza i dona visibilitat del nivell de ciberseguretat que implementa un proveïdor sobre un servei determinat mitjançant l'emissió de segells de confiança digital.

Font: INCIBE

8. La ciberseguretat a Catalunya

Principals conclusions del mapeig

La ciberseguretat a Catalunya

352 empreses

5.898 treballadors vinculats a la ciberseguretat

Facturació de 806 M d'€ directament vinculats a la ciberseguretat

La ciberseguretat representa un 0,36 % del PIB català

El 37,5 % de les empreses té menys de 10 anys

El 95 % de les empreses són PIMES

El 41,5 % de les empreses facturen més d'un milió d'euros i el 49 % factura menys de 500.000 €

El 6,5 % de les empreses tenen filials a l'estranger

El 35 % les empreses són exportadores

Font: elaboració pròpia en base a Orbis, INCIBE, directoris d'ACCIÓ i Barcelona&Catalonia Start-up *hub*. Per les dades de facturació i treballadors s'han fet estimacions en base a línies de negoci de les empreses.

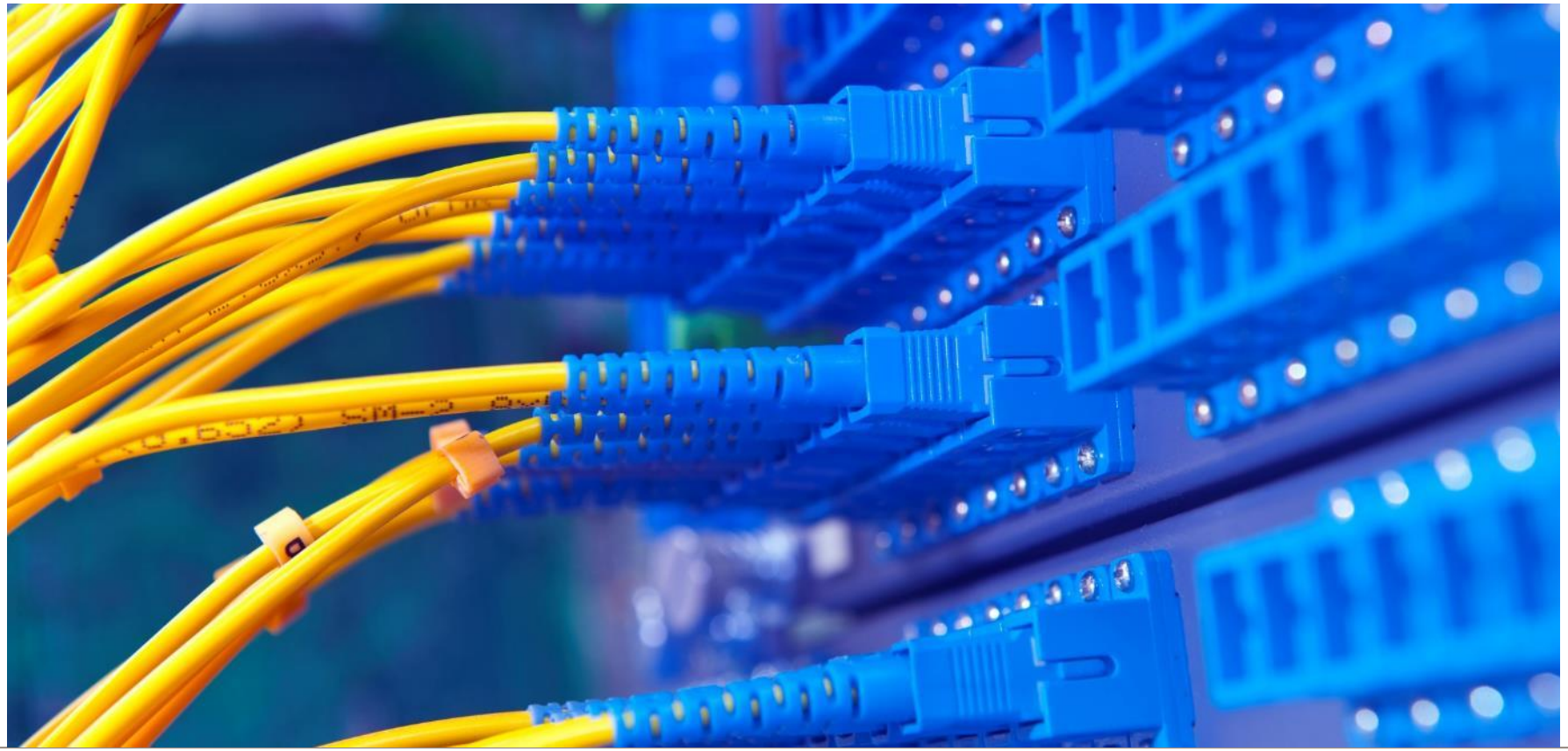
Ecosistema de la ciberseguretat a Catalunya

*Il·lustratiu parcial

Nota: L'ús d'aquestes marques és merament informatiu. Les marques esmentades en el present informe pertanyen als seus respectius titulars i, en cap cas són titularitat d'ACCIÓ. Aquesta és una representació il·lustrativa parcial de les principals empreses que formen part de l'ecosistema del sector de la ciberseguretat a Catalunya, però hi pot haver altres empreses que no hagin estat incorporades a l'estudi.

Font: ACCIÓ, Barcelona & Catalonia Start-up Hub

9. Centres TECNIO i agents de l'entorn de la ciberseguretat



Centres TECNIO que treballen amb ciberseguretat

El **Centre Tecnològic de Telecomunicacions de Catalunya (CTTC)** és un centre públic d'R+D+i creat per la **Generalitat de Catalunya** a Castelldefels (BCN).

El **CTTC** rep fons de la **Generalitat**, dels contractes de transferència tecnològica a empreses i de projectes d'R+D competitius. La recerca, innovació i transferència tecnològica que fa el **CTTC** es basa en tecnologies dels nivells físic, d'enllaç i xarxa de sistemes de comunicacions, en els serveis i la infraestructura de xarxa, i en la geomàtica. Les activitats s'organitzen en 4 divisions: Sistemes, Xarxes, Tecnologies de Comunicacions i Geomàtica, i compten amb l'assessorament d'un comitè científic extern internacional.

En l'àmbit de la ciberseguretat han realitzat algunes publicacions en temes de *Security in Internet of Things, impact on security of Enabling SDN in VANETs i Detection of Malicious Users in Cognitive Radio Ad Hoc Networks*

El **Centre Easy** està especialitzat en intel·ligència artificial i *Machcrowd*, en tecnologies digitals intel·ligents i en la seva transferència a la indústria.

1. **Intel·ligència artificial *machcrowd***: la nostra investigació en recerca social consisteix en l'automatització d'alguns aspectes de la interacció dels usuaris amb l'objectiu de millorar i accelerar els resultats.

2. **Tecnologies digitals intel·ligents**: en relació amb aquest tema, el Centre és expert en monedes virtuals (un tipus de diners no regulat, digital, que és emès i controlat normalment pels seus desenvolupadors, i és utilitzat i acceptat pels membres d'una comunitat virtual específica) i en preservació digital (un esforç formal per assegurar que la informació digital de valor continua sent accessible i utilitzable). El **Centre Easy** connecta això amb la indústria.

3. **Indústria**: a través de col·laboracions com amb la Consultoria *Blue Room Innovation* i amb la gestió de l'únic Màster Oficial en Smart Cities a Europa.

Eurecat, Centre Tecnològic de Catalunya (membre de TECNIO), aplega l'experiència de més de 600 professionals que generen un volum d'ingressos de 42 milions d'euros anuals i dona servei a més de 1.000 empreses.

R+D aplicat, serveis tecnològics, formació d'alta especialització, consultoria tecnològica i esdeveniments professionals són alguns dels serveis que **Eurecat** ofereix tant per a grans com per a petites i mitjanes empreses de tots els sectors. Amb instal·lacions a Barcelona, Canet de Mar, Cerdanyola del Vallès, Girona, Lleida, Manresa, Mataró, Reus i Amposta i amb una seu a Brasil, participa en 160 grans projectes consorciats d'R+D+i nacionals i internacionals d'alt valor estratègic i té 73 patents i 7 *spin-off*.

El valor afegit que aporta **Eurecat** accelera la innovació, disminueix la despesa en infraestructures científiques i tecnològiques, redueix els riscos i proporciona coneixement especialitzat a mida per a cada empresa.

Font: Directori d'ACCIÓ

Centres TECNIO que treballen amb ciberseguretat

La **Fundació i2CAT** és una institució de recerca aplicada en l'àmbit d'Internet, tecnologies digitals avançades i societat digital. És l'entitat de recerca i innovació de Catalunya que participa en més projectes europeus TIC, en les línies d'*Internet of Things* (IoT), 5G, arquitectura de xarxes i gestió i tecnologies immersives i interactives, incorporant també noves àrees com les d'*open big data*, intel·ligència artificial i ciberseguretat.

La Generalitat de Catalunya, a través del lideratge de la Secretaria de Telecomunicacions, Ciberseguretat i Societat Digital, té una participació directa en la Fundació. Alhora, i2CAT disposa d'aliances estratègiques amb la IOT Catalan Alliance, CESICAT, CTTI i 5GBarcelona per tal de vertebrar projectes tractors i d'impacte en el teixit industrial i social.

La **Salle R&D** vol ser un centre tecnològic de referència en l'àmbit de les ciutats intel·ligents i del sector salut, impulsor de la transferència de tecnologia cap al teixit empresarial i de reconegut prestigi a l'àmbit nacional i internacional per l'excel·lència de la seva recerca i del seu desenvolupament.

La missió de la **Salle R&D** és impulsar l'ús de les TIC en el dia a dia convencional, aportant valor afegit i competitivitat a les empreses mitjançant la recerca aplicada i el desenvolupament de noves solucions innovadores i úniques.

Font: Directori d'ACCIÓ

Cybercat: centre de recerca de ciberseguretat a Catalunya

- Sis universitats públiques catalanes han creat **el primer Centre de recerca de ciberseguretat de Catalunya.** Les sis universitats aportaran al Cybercat els grups de recerca que actualment treballen en tecnologies de la seguretat i privacitat de la informació.
- **La missió** és impulsar la recerca en ciberseguretat i privadesa de la informació a Catalunya i enfortir la seva projecció internacional, així com reforçar i estendre la formació d'alt nivell en aquest àmbit i consolidar les relacions de recerca existents entre les sis universitats participants.
- **L'ambició** del centre és constituir-se com un centre de referència a l'àmbit nacional i internacional en la recerca en ciberseguretat i privadesa.

CYBER[SECURITY]CAT

Universitat Rovira i Virgili · Universitat Oberta de Catalunya · Universitat de Lleida · Universitat Politècnica de Catalunya · Universitat Autònoma de Barcelona · Universitat Pompeu Fabra Barcelona

Cybercat té diverses **línies de recerca en els següents àmbits del coneixement:**

Seguretat i privadesa en l'automòbil connectat	Privadesa en grans volums de dades	Privadesa al núvol	Privadesa en ciutats intel·ligents
Privadesa en xarxes socials	Privadesa en entorns col·laboratius	Privadesa en mineria de dades	Privadesa de la localització
	Automatització de dades	Seguretat i privadesa en la internet de les coses	

Font: Cybercat, Expansión

Agència de Ciberseguretat de Catalunya

Generalitat de Catalunya
Agència de Ciberseguretat de Catalunya

El passat juliol del 2017 el ple del Parlament de Catalunya va aprovar la Llei de creació de **l'Agència de Ciberseguretat de Catalunya, òrgan que substituirà el Centre de Seguretat de la Informació de Catalunya (CESICAT).**

L'Agència de Ciberseguretat de Catalunya s'encarregarà de prevenir, detectar, respondre i investigar incidents o amenaces a les xarxes de comunicacions electròniques i als sistemes d'informació públics, i de planificar, gestionar, coordinar i supervisar la ciberseguretat a Catalunya, minimitzar els danys i el temps de recuperació de les xarxes i els sistemes en cas de ciberatac i col·laborar amb els cossos policials i les autoritats judicials.

- L'objectiu és establir un servei públic de ciberseguretat que permeti garantir la protecció adient per als seus ciutadans, desenvolupant funcions com:
- Planificar, gestionar, coordinar i supervisar la ciberseguretat a Catalunya.
- Exercir les funcions d'equip de resposta a emergències (CERT) a Catalunya.
- Actuar com a suport, en matèria de ciberseguretat, de qualsevol autoritat competent per a l'exercici de les seves funcions públiques.
- Investigar i analitzar tecnològicament els ciberincidents i ciberatacs en els quals intervingui per raó de la seva competència.
- Col·laborar amb entitats públiques i privades per tal de fomentar la millora dels nivells de ciberseguretat a les infraestructures i les aplicacions, entre d'altres.
- Millorar el nivell de ciberseguretat de la ciutadania de Catalunya, organitzant les activitats de difusió, formació i conscienciació adients

Centre de Seguretat de la Informació de Catalunya

QUINA ÉS LA SEVA MISSIÓ?

El CESICAT és l'**organisme encarregat de garantir la protecció, prevenció i governança en matèria de ciberseguretat** de la Generalitat de Catalunya i el seu Govern.

Els seus **principals objectius** són:

- Establiment i seguiment dels programes de seguretat cibernètica sota la direcció estratègica de la Generalitat de Catalunya, en coordinació amb els òrgans públics de la Generalitat i en cooperació amb les autoritats locals de Catalunya, el sector privat i la societat civil.
- Dins de la Generalitat de Catalunya, el CESICAT realitza activitats de protecció contra ciberatacs, incidents de seguretat i prevenció en termes de seguretat cibernètica des d'un punt de vista organitzatiu, tecnològic i regulador. A més, garanteix la flexibilitat dels actius i les infraestructures TIC com a mecanisme per garantir la seguretat dels sistemes davant dels ciberatacs i reduir-ne els efectes.
- Establir un programa de sensibilització sobre seguretat cibernètica que permeti a Catalunya convertir-se en una societat més madura pel que fa a la gestió de la informació.
- Proporcionar un interlocutor per notificar i gestionar incidents de seguretat cibernètica.

10. Casos empresarials de la ciberseguretat a Catalunya

Casos empresarials de ciberseguretat a Catalunya

La indústria maliciosa del cibercrim, amb models de negoci consolidats, afecta cada cop més tots els sectors industrials. Aprofitant la vulnerabilitat de les infraestructures industrials, **els cibercriminals intenten atacar aquestes empreses amb diferents objectius:** extorsió, robatori de dades, danyar els sistemes industrials, com SCADA i IoT.

Els cibercriminals coordinen i planifiquen atacs, creant campanyes d'infecció de *malware* vers la indústria 4.0, protegits sovint per la capacitat d'anonimat que faciliten les xarxes TOR o *dark web*.

Aquesta situació va motivar Blueliv i Aquae Security a unir esforços per buscar **mètodes per anticipar i predir atacs contra instal·lacions industrials.** Així doncs, han desenvolupat en col·laboració un sistema que permet replegar les dades d'amenaces, *malware* i servidors del crim que poden atacar actius tecnològics, plantes de producció, serveis, etc.

Mitjançant la tecnologia d'ambdues empreses i el *big data*, han aconseguit ser més responsives davant la gran varietat de ciberamenaces, **detectant futurs atacs i infeccions, dispositius compromesos, i reaccionar de forma immediata, dirigida i eficaç**. Ambdues empreses contribueixen amb la seva tecnologia a millorar els estàndards de protecció de la indústria 4.0 davant les innovadores i emergents ciberamenaces.

https://www.blueliv.com/

http://www.aquaesecurity.es/

AQUAE SECURITY

Blueliv.

Casos empresarials de ciberseguretat a Catalunya

LOGITEK és un exemple de la incorporació de tecnologies ***antimalware off line*** **o el** ***whitelisting*** **d'aplicacions a l'àmbit industrial**.

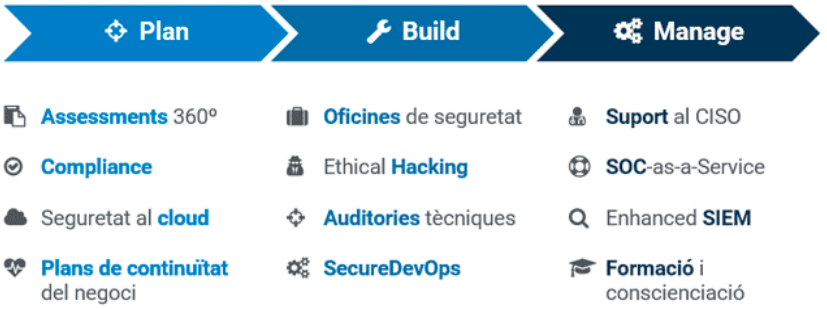
Aquestes funcionalitats permeten dotar de nivells de seguretat més alts els sistemes industrials. Per altra banda, potencien que es disposi de sistemes i dispositius que permetin documentar fàcilment tot l'inventari de xarxa, gestionar-les de manera centralitzada, conèixer les incidències associades als dispositius *hardware* i aplicacions *software* i monitorar el seu ús per diferents usuaris.

Més específicament, per gestionar l'accés extern a les xarxes s'incorporen solucions tipus IDS (*Intrusion Detection System*) i per tal de realitzar la segmentació i fortificar les xarxes s'utilitzen tècniques de DPI (*Deep Packet Inspection*) i IPS (*Intrusion Prevention System*)

Industrial Cybersecurity by LOGITEK
CIBERSEGURIDAD INDUSTRIAL

http://www.logitek.es/

IThinkUPC és la **consultora tecnològica i el proveïdor corporatiu de serveis informàtics de la UPC.** La consultora ajuda els seus clients a afrontar els reptes de la ciberseguretat amb garanties i amb un equip de **professionals qualificats que aporten una visió integral**.



IThink UPC
Digital Experts for your Business Agility

www.ithinkupc.com/

Casos empresarials de ciberseguretat a Catalunya

L'empresa neerlandesa de ciberseguretat **Brightsight ha obert la seva primera oficina fora del seu país d'origen a Sant Cugat del Vallès**. Aquest moviment ha suposat també l'adquisició de Bitwise, una empresa catalana dedicada a l'àmbit de la ciberseguretat. S'espera que aquesta inversió creï **40 llocs de treball** fins l'any 2020. Brightsight, com a especialista en avaluació de seguretat, ofereix **serveis de consultoria, formació i eines d'anàlisi úniques en l'àmbit de la ciberseguretat**, en el qual té molts anys d'experiència.

Les raons que ha donat la companyia per triar Catalunya com la ubicació del seu nou centre d'operacions són les següents:

"L'àrea està en plena expansió pel que fa a les noves tecnologies. Les persones que estudien i treballen a Barcelona tenen un elevat grau de formació i coneixement en aquests àmbits. A més, d'aquesta manera Brightsight mantindrà una relació més propera, eficient i interactiva amb els seus clients de l'àrea de Barcelona."

brightsight®
your partner in security approval

www.brightsight.com

Facebook, el conglomerat de xarxes socials, ha creat a Barcelona un **centre de detecció de notícies falses**, que s'ubicarà a la Torre Glòries. Aquest centre, que serà operat conjuntament amb l'empresa Competence Call Center (CCC) **donarà feina a unes 500 persones**. Aquests treballadors s'ocuparan principalment de controlar el contingut que es publica a Facebook, d'acord amb les normes de la mateixa xarxa social.


INVERSIONES

Facebook oficializa su aterrizaje en Barcelona con 500 empleos

La compañía luchará desde Glòries contra el abuso en la plataforma

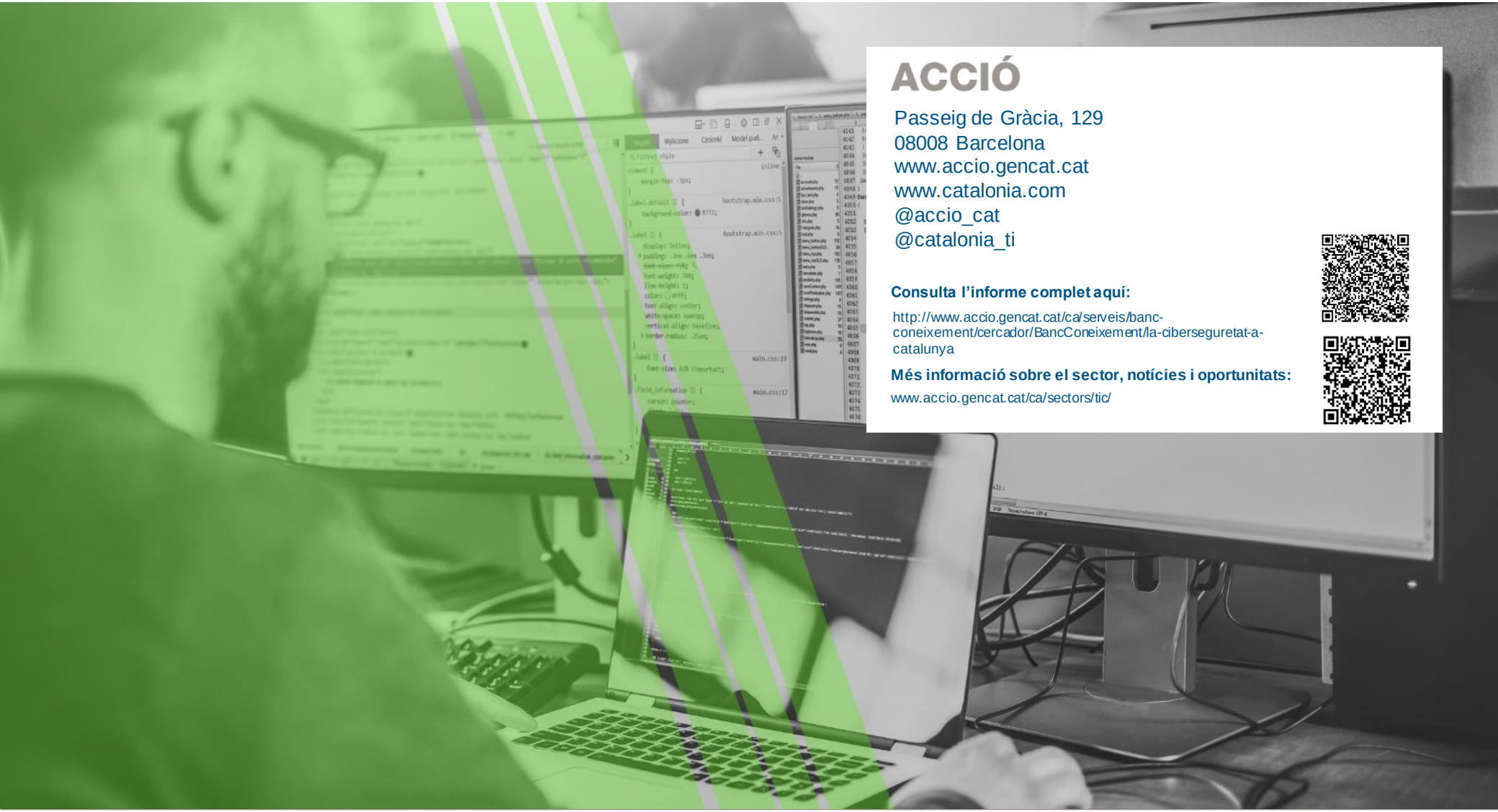
Más noticias

Raquel Mosquer pasa de robar cremas... a pecar 'Supervivientes'

Zaplana detenido

CCC
COMPETENCE CALL CENTER

www.facebook.com



ACCIÓ

Passeig de Gràcia, 129
08008 Barcelona
www.accio.gencat.cat
www.catalonia.com
@accio_cat
@catalonia_ti

Consulta l'informe complet aquí:

http://www.accio.gencat.cat/ca/serveis/banc-coneixement/cercador/BancConeixement/la-ciberseguretat-a-catalunya

Més informació sobre el sector, notícies i oportunitats:

www.accio.gencat.cat/ca/sectors/tic/