ICT Security in European Enterprises. Examples of ICT Security Solutions

Florin-Domnel GRAFU,
ROMATSA, Bucureşti, România
florin.grafu@romatsa.ro

Cristina LEOVARIDIS,
SNSPA, Bucureşti, România
cristina.leovaridis@comunicare.ro

Abstract
Lucrarea de faţă îşi propune să ofere o imagine statistică de ansamblu asupra situaţiei actuale a digitalizării şi a utilizării securităţii sistemelor TIC în companiile europene, cu accent pe propunerea implementării unor meteode de protecţie a datelor companiilor. După o analiză secundară de date statistice recente furnizate de instituţii europene cu privire la nivelul digitalizării, dar mai ales al preocupării pentru securitatea TIC în companiile europene, în care se evidenţiază comparaţia dintre România şi media UE, articolul continuă cu o prezentare a unor soluţii pentru implementarea tehnică a securităţii cibernetice în companii. Va fi expus un set de tehnologii care fac posibilă detectarea ameninţărilor cibernetice şi a atacurilor legate de securitatea IT.

Cuvinte cheie: securitate cibernetică, centru pentru operaţiuni de securitate, digitalizare.

1. Introducere

În contextul digitalizării accelerate din ultimii ani a întreprinderilor europene, se pune din ce în ce mai acut problema asigurării securităţii sistemelor TIC. O imagine statistică de ansamblu asupra nivelului de digitalizare a întreprinderilor europene, urmată de o prezentare statistică a situaţiei preocupărilor legate de securitatea cibernetică în cadrul companiilor, comparativ între ţara noastră şi media UE, am considerat a fi absolut necesare. Instrumentele tehnice utilizate pentru detecţia şi combaterea incidentelor la nivelul securităţii cibernetice sunt expuse sumar în cea de-a doua parte a acestui articol şi constau în analiza SOC-ului şi a SIEM-ului.

Dovadă a importanţei acordate de instituţiile europene protecţiei datelor în format digital sunt şi documentele oficiale europene elaborate în ultimii cinci ani, precum "The EU's Cybersecurity Strategy for the Digital Decade" [1] şi "Network and Information Security 2 (NIS2) Directive" [2], ce includ recomandări şi măsuri pentru un nivel comun ridicat de securitate a reţelelor şi a sistemelor informatice în Uniune. Pe plan naţional, implementarea Legii NIS intră în responsabilitatatea Directoratului Naţional de Securitate Cibernetică (DNSC), autoritatea românească în competenţele căreia intră securitatea reţelelor şi sistemelor informatice [3].

2. Digitalizare şi securitate TIC în companiile europene – o perspectivă statistică

În 2023, majoritatea covârşitoare (93,9%) a organizaţiilor europene cu peste 10 angajaţi europene aveau conexiune în bandă largă fixă la Internet, peste trei sferturi (78.1%) aveau website şi aproape două treimi (60.9%) foloseau cel puţin un tip de social media: peste jumătate (58.9%) foloseau reţelele de socializare (Facebook, LinkedIn etc.), o treime (31.5%) website-uri de multimedia content sharing (YouTube, Flickr, SlideShare,

Instagram, Pinterest, Snapchat), şi doar 1 din 10 (10.2%) foloseau bloguri corporative (Twitter) [4].

Referitor la integrarea e-business (utilizarea TIC de către întreprinderi pentru a rula, integra şi îmbunătăţi procesele lor de afaceri, pentru a împărtăşi şi a face schimb de informaţii în interior, pentru a analiza date sau pentru a comunica cu partenerii de afaceri şi clienţii), peste 4 din 10 întreprinderi au apelat la aplicaţii software de planificare a resurselor (ERP - enterprise resource planning), un sfert (25.8%) au folosit aplicaţii de managementul relaţiilor cu clienţii (CRM - customer relationship management), iar peste 1 din 10 (15.3%) au folosit software-uri de Business Intelligence (BI). Puţin sub jumătate din organizaţiile europene (45.2%) au apelat la serviciile de cloud (în loc să-şi extindă propria infrastructură IT, întreprinderile pot cumpăra resurse de calcul găzduite de terţi pe internet, iar aceasta include acces flexibil, la cerere, la servicii precum software, putere de calcul, capacitate de stocare etc.). În 2023, puţin peste un sfert (28,2 %) dintre întreprinderile europene peste 10 angajaţi au efectuat analize de date prin intermediul propriilor angajaţi (mai precis, au utilizat tehnologii, tehnici sau instrumente software pentru analiza datelor interne sau a datelor din surse externe şi pentru a extrage modele, tendinţe şi perspective din date pentru a formula concluzii, predicţii şi a lua decizii mai bune cu scopul de a-şi îmbunătăţi performanţa - creşterea producţiei, reducerea costurilor). Sub 1 din 10 (8%) din întreprinderile europene au apelat la inteligenţa artificială (sisteme care utilizează tehnologii precum: *text mining*, recunoaşterea vorbirii, generarea limbajului natural, învăţarea automată, învăţarea profundă pentru a culege şi/sau utiliza date pentru a prezice, recomanda sau decide, cu diferite niveluri de autonomie, cea mai bună acţiune de realizat anumite obiective specific etc.; sistemele de AI pot fi bazate exclusiv pe software sau încorporate în dispozitive) [4].

Ca urmare a necesităţii asigurării securităţii cibernetice, conform ultimelor date furnizate de Eurostat, în 2022, 92% dintre întreprinderile din UE cu mai mult de 10 angajaţi au utilizat cel puţin o măsură pentru a menţine securitatea sistemelor TIC, mai precis integritatea, disponibilitatea şi confidenţialitatea datelor şi a sistemelor TIC; valorile indicatorului în România sunt apropiate de media europeană – 86% din întreprinderi au apelat la cel puţin o astfel de măsură. Firmele pot implementa o varietate de măsuri de securitate TIC pentru a preveni incidentele şi pentru a asigura integritatea, disponibilitatea şi confidenţialitatea datelor şi sistemelor lor TIC. Cea mai frecventă măsură utilizată pe plan european a fost autentificarea cu parolă puternică (82%), urmată de backup-ul datelor într-o locaţie separată sau în cloud (78%) şi de controlul accesului la reţea (65%) [5].

Sub jumătate (49%) dintre întreprinderi au utilizat reţele private virtuale (VPN) sau au avut fişiere jurnal pentru analize după incidente de securitate (45%). Cel mai rar au fost folosite tehnicile de criptare pentru date, documente sau e-mail-uri (36%), testele de securitate TIC (35%), evaluările riscurilor TIC (32%), combinaţii de două sau mai multe mecanisme de autentificare (31%) sau identificarea şi autentificarea utilizatorului prin metode biometrice (13%). Frecvenţa utilizării acestor măsuri diferă în funcţie de dimensiunea organizaţiei. Mai precis, autentificarea cu parolă puternică a fost utilizată de aproape toate întreprinderile mari europene (96%), de 90% dintre întreprinderile mijlocii şi de peste 8 din 10 întreprinderi mici (81%). Valori apropiate ale indicatorului au fost înregistrate şi pentru

salvarea datelor într-o locație separată: 93% dintre întreprinderile mari, 88% dintre întreprinderile mijlocii și 75% dintre întreprinderile mici au apelat la ea. Diferențe între organizații în funcție de dimensiunea lor sunt mai evidente în cazul măsurilor de securitate mai rar folosite: autentificarea printr-o combinație de cel puțin două mecanisme a fost utilizată de două treimi (64%) dintre întreprinderile mari, în timp ce ponderea celor mici care utilizează această măsură particulară a fost de peste două ori mai mică (28%). Indiferent de dimensiunea întreprinderii, identificarea și autentificarea utilizatorilor prin metode biometrice a fost cea mai puțin utilizată măsură de securitate TIC: de către doar o treime (29%) dintre întreprinderile mari și de doar 1 din 10 dintre cele mici (12%) [6].

Peste o treime (37%) dintre întreprinderile europene dețin documente care pun în aplicare măsuri, practici sau proceduri privind securitatea TIC, România înregistrând la acest indicator valori peste media UE (45%) și situându-se astfel în prima treime a clasamentului. Mai mult, în aproape un sfert (24%) din întreprinderi aceste documente sunt foarte actuale, fiind elaborate sau revăzute în ultimul an [5]. În țara noastră, o și mai mare parte din aceste documente au fost actualizate în ultimele 12 luni, mai precis în 4 din 10 întreprinderi (40%).

Peste jumătate (58%) din întreprinderile europene și-au conștientizat angajații în legătură cu responsabilitățile pe care le au în aspectele referitoare la securitatea TIC, și aici valorile indicatorului pentru România (62%) depășind media UE, ceea ce situează România în prima jumătate a clasamentului țărilor europene după acest criteriu (pe primul loc situându-se Irlanda și Cehia cu 75%). Pentru a realiza aceasta, 42% dintre întreprinderile europene au oferit angajaților săi instruire voluntară în domeniul securității TIC, 21% au introdus cursuri obligatorii pentru salariați în acest domeniu, iar 32% au inclus obligații de securitate TIC în contractele de muncă ale angajaților lor [5]. Și aici există diferențe în funcție de dimensiunea întreprinderii: ponderea întreprinderilor mari care conștientizează angajații cu privire la obligațiile lor în domeniul securității TIC a fost foarte mare (91%), acestea fiind urmate de cele mijlocii (76%) și de cele mici (54%).

Mai mult de una din cinci (22%) întreprinderi europene a experimentat în anul anterior incidente de securitate legate de TIC ce au dus la diferite consecințe, precum indisponibilitatea serviciilor TIC, distrugerea sau coruperea datelor sau dezvăluirea datelor confidențiale, România și din acest punct de vedere având o situație mai bună decât media UE – doar 19% din întreprinderile românești experimentând astfel de incidente. Incidentele de securitate TIC pot fi cauzate de atacuri rău intenționate din exteriorul sau din interiorul întreprinderii, sau de cauze non-malițioase, obiective, cum ar fi: defecțiuni hardware sau software sau acțiuni neintenționate ale propriilor angajați, aceasta a doua categorie fiind cel mai des raportată. Cea mai des înregistrată consecință generată de incidentele de securitate TIC a fost indisponibilitatea serviciilor TIC din cauza defecțiunilor hardware sau software (19% dintre întreprinderi). Mult mai rar a fost menționată (de doar 4% dintre organizații) indisponibilitatea serviciilor TIC din cauza atacurilor din exterior (de exemplu, atacuri ransomware, atacuri Denial of Service. Distrugerea sau coruperea datelor ca urmare a defecțiunilor hardware sau software a fost raportată de 4% dintre întreprinderi, în timp ce infectarea cu software cu scop rău intenționat sau intruziunea neautorizată care a dus la distrugerea sau coruperea datelor a fost raportată de 2% dintre întreprinderi. Cel mai rar, întreprinderile au raportat dezvăluirea de date confidențiale din cauza intruziunii, atacurilor

pharming sau phishing sau acțiunilor intenționate ale propriilor angajați (1%) sau din cauza acțiunilor neintenționate ale propriilor angajați (1%) [6].

Deși există un consens general la nivelul organizațiilor europene (71%) că securitatea cibernetică reprezintă o prioritate, punerea în practică a măsurilor de securitate TIC rămâne relativ dificilă: referitor la principalele provocări ale companiilor europene când trebuie să recruteze angajați cu competențe în cyber security, mai mult de jumătate dintre companiile care au căutat astfel de candidați au întâmpinat dificultăți cum ar fi găsirea de candidați calificați (45%), lipsa de candidați (44%), lipsa de conștientizare a rolului cybersecurity (22%), a schimbărilor tehnologice prea rapide și a nevoii permanente de instruire (19%), dar și a constrângerilor bugetare inclusiv din cauza costurilor foarte ridicate ale echipamentelor (16%) [7]. Mai mult, pregătirea analiștilor din companii, specializați în cybersecurity, pentru a executa fluxurile de lucru cu viteză și consecvență, poate fi o sarcină consumatoare de timp [8].

Toate măsurile pentru menținerea securității sistemelor TIC enumerate mai sus, pot fi realizate în cadrul companiilor prin intermediul soluțiilor expuse în cele ce urmează.

3. Soluții de securitate cibernetică pentru companii

Centrul de operațiuni de securitate (SOC) este un centru al unei instituții sau organizații specializate în monitorizarea și gestionarea securității informațiilor. SOC este punctul de întâlnire al sistemelor, proceselor și tehnologiilor legate de securitatea cibernetică. SOC este format dintr-o echipă dedicată de analiști și ingineri specializați în domeniul securității informațiilor. Această echipă monitorizează continuu rețelele, sistemele și aplicațiile pentru a detecta amenințările și atacurile cibernetice. SOC se bazează pe instrumente și tehnologii avansate pentru a detecta, verifica și răspunde la amenințări.

3.1. Ce este un SOC?

Un Centru de operațiuni de securitate (SOC) este o echipă centralizată de analiști de securitate responsabilă de monitorizarea, detectarea și răspunsul la amenințările de securitate cibernetică. SOC-urile folosesc de obicei o varietate de instrumente și tehnologii de securitate pentru a colecta și analiza date din întreaga infrastructură IT a unei organizații. Aceste date pot fi folosite pentru a identifica potențialele amenințări, pentru a investiga incidente și pentru a răspunde la atacuri. SOC-urile joacă un rol critic în protejarea organizațiilor împotriva atacurilor cibernetice [9].

3.2. Unele dintre principalele beneficii ale SOC în domeniul securității cibernetice

Monitorizarea și detectarea amenințărilor: SOC monitorizează și detectează amenințările cibernetice avansate și atacurile de securitate asupra sistemelor și rețelelor. Tehnologiile avansate și instrumentele de securitate sunt utilizate pentru a detecta amenințările din timp și pentru a limita impactul acestora.

Răspuns eficient la incident: Sunt implementate strategii de răspuns rapide și eficiente pentru a face față incidentelor de securitate. SOC ajută la analiza și clasificarea incidentelor și la luarea de măsuri de răspuns imediat pentru a investiga, a limita atacurile și a reporni în siguranță sistemele afectate.

Detectare și analiză: Datele și jurnalele de securitate din diverse surse sunt agregate și analizate în continuare pentru a identifica modele, comportamente neobișnuite și potențiale amenințări. Acest lucru permite organizațiilor să ia măsuri corective și să își îmbunătățească măsurile de securitate.

Reducerea timpului de recuperare: Cu monitorizarea continuă a securității și analiza eficientă, SOC poate reduce timpul de recuperare în urma atacurilor cibernetice. Permite verificarea rapidă și răspunsul la urgență pentru a reduce impactul atacurilor și a reduce timpul de nefuncționare.

Îmbunătățirea deciziilor strategice: SOC oferă rapoarte și analize periodice care ajută la înțelegerea situației generale de securitate și la evaluarea eficienței strategiilor și măsurilor de securitate luate [9].

3.3. Un set de tehnologii utilizate pentru a detecta amenințările cibernetice

Sistem de informare și management al incidentelor (Incident Information and Management System - SIEM): Un sistem de informare și management al incidentelor este utilizat pentru a colecta, analiza și monitoriza înregistrările evenimentelor și datele de securitate din mai multe surse. Tehnicile avansate de analiză și monitorizare sunt utilizate pentru a identifica modele neobișnuite și alerte atunci când sunt detectate activități suspecte.

Advanced Threat Detection (APT): Această abordare implică utilizarea de instrumente speciale și tehnologii sofisticate pentru a detecta amenințările avansate și atacurile țintite. Aceasta include analiza comportamentului utilizatorului și monitorizarea traficului de rețea pentru activități suspecte sau neobișnuite.

Analiza comportamentală: Tehnicile de analiză comportamentală sunt utilizate pentru a crea modele ale comportamentului normal al sistemelor și utilizatorilor. Tiparele neobișnuite și comportamentul anormal sunt monitorizate pentru potențiale amenințări, cum ar fi infiltrarea *hackerilor* și încălcările de securitate.

Fig. 1. Reprezentare logică a unui SIEM
Sursa : https://grcico.com/

Informații despre amenințări și informații despre securitate: sunt utilizate mai multe surse pentru a obține informații despre amenințări și informații despre securitate, cum ar fi baze de date publice, platforme de schimb de securitate și colaborări cu alte organizații din domeniul securității cibernetice. Aceste informații ajută la identificarea activităților cibernetice rău intenționate [9].

3.4. Principala importanță a SIEM în SOC

Colectarea datelor: Sistemul SIEM colectează date de securitate și jurnalele de evenimente din diverse surse din infrastructura de rețea și din diverse sisteme. Aceste date sunt agregate într-un singur loc pentru o analiză și monitorizare cuprinzătoare.

Analiză și verificare: Datele colectate sunt analizate folosind reguli și criterii specifice pentru a identifica tipare anormale, activități suspecte și amenințări de securitate. Tehnici avansate de verificare și analiză sunt utilizate pentru a se asigura că amenințările sunt validate și clasificate corespunzător.

Alerte și alarme: Sistemul SIEM oferă alerte și alarme în timp real atunci când sunt detectate activități suspecte sau amenințări de securitate. Acest lucru ajută echipa SOC să răspundă rapid la amenințări și să ia măsuri pentru a reduce impactul negativ.

Investigarea și raportarea: SIEM facilitează investigarea și analiza ulterioară a incidentelor de securitate. Oferă un jurnal detaliat al tuturor activităților și incidentelor și permite crearea de rapoarte cuprinzătoare pentru a înțelege situația de securitate și a evalua performanța sistemelor de protecție.

Conformitate și audit: Sistemul SIEM ajută la respectarea standardelor și reglementărilor de securitate aplicabile, cum ar fi păstrarea datelor pentru o anumită perioadă, conform reglementărilor companiei [9].

4. Exemple de „Use Case-uri" în domeniul securității cibernetice

Problema 1: Răspuns la incident

O sală tehnică și echipamente actuale de înaltă tehnologie nu sunt necesare, nici măcar nu sunt suficiente pentru a preveni sau rezolva imediat incidentele. Elementele menționate sunt utile atunci când vine vorba de aspectele de „marketing" ale Centrului de operațiuni de securitate. Pentru a opera un SOC și în special în timpul răspunsului la un incident, oamenii joacă un rol cheie.

Soluția: oamenii

Abilitățile care se cer analiștilor SOC trebuie să corespundă cerințelor naturii muncii lor, care este foarte nișată. Abilitățile de bază care sunt necesare analiștilor SOC sunt următoarele:

Abilitati tehnice:

- Rețea (TCP/IP);
- Administrator de sistem (Linux, Windows);
- Analist malware (analiza comportamentală);
- Investigator criminalistic.

Abilități soft:

- Gândire analitică;
- Redactare;
- Comunicare;
- Lucru în echipă;
- Orientarea către client;
- Capacitatea de sinteză a rezultatelor obținute;
- Abilitatea de a lucra sub presiune.

Abilitățile de mai sus sunt cheia pentru stabilirea unei funcționalități de bază pentru SOC [10].

Problema 2: Cum să reacționați la evenimentele și incidentele de securitate

După cum s-a menționat mai sus, resursa umană este esențială. Dar organizația trebuie să fie sprijinită (în România, acest sprijin este oferit companiilor de către Directoratul Național de Securitate Cibernetică) pentru a putea răspunde în conformitate cu *Răspunsul* la incidentul de securitate IT.

Soluția: Procesul de răspuns la incident

Procesul de răspuns la incident urmează o abordare standard [10].

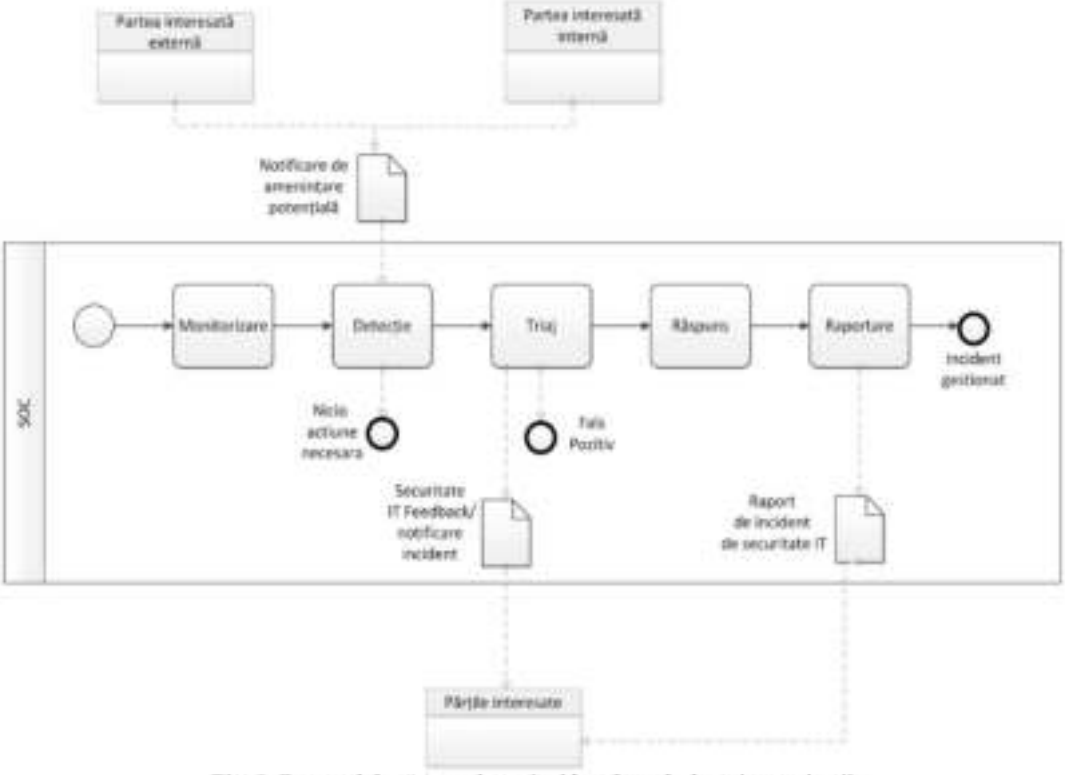

Fig. 2. Procesul de răspuns la un incident în cadrul unei organizații
Sursa : Eurocontrol, "ATM-ATM SOC Implementation v1.0"

5. Concluzii și discuții

Analiza secundară de date statistice realizată în prima parte a lucrării de față, pe baza datelor oficiale oferite de Eurostat și Comisia Europeană indică faptul că România se plasează, la majoritatea indicatorilor ce țin de securitatea cibernetică a companiilor, în prima parte a clasamentului țărilor europene, în cele mai multe cazuri valorile indicatorilor pentru România fiind peste media UE atunci când facem referire la aspecte pozitive (deținerea de către companii de documente care pun în aplicare măsuri, practici sau proceduri privind securitatea TIC, actualitatea acestora, conștientizarea angajaților în legătură cu responsabilitățile pe care le au vis-a-vis de securitatea TIC) sau sub media UE atunci când ne referim la aspecte negative (incidente de securitate cibernetică în companii, ce au dus la diferite consecințe).

Prin oferirea de cursuri de conștientizare a securității cibernetice, organizațiile trebuie să își responsabilizeze angajații să devină prima linie de apărare împotriva amenințărilor cibernetice. Angajații informați sunt mai bine pregătiți pentru a detecta și a răspunde eventualelor incidente de securitate. Existența unui SOC în interiorul unei companii crește rezistența acesteia la atacurile cibernetice; totodată, acest serviciu poate fi contractat și de la firme specializate în domeniu.

Anexă

Acronime

AI – Artificial Intelligence (Inteligență Artificială)
ATSEP – Air Traffic Safety Electronics Personnel (Personal electronist care asigură siguranța traficului aerian)
NIS - Network and Information Security (Securitatea Rețelei și a Informațiilor)
SIEM - Incident Information and Management System (Sistem de informare și management al incidentelor)
SOC – Security Operations Center (Centru de operațiuni pentru securitate)
TIC – Tehnologia Informației și a Comunicațiilor.

Referințe

[1] European Commission, "The EU's Cybersecurity Strategy for the Digital Decade," December 2020. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.

[2] European Commission, "Network and Information Security 2 (NIS2) Directive," Whitepaper, February 2023. [Online]. Available: https://www.dnv.com/cybersecurity/cyber-insights/nis2-directive/ .

[3] Directoratul Național de Securitate Cibernetică (DNSC), "Autoritatea competentă la nivel național pentru securitatea rețelelor și sistemelor informatice," 2024. [Online]. Available: https://dnsc.ro/pagini/ansrsi .

[4] Eurostat , "Digital economy and society statistics – enterprises. Statistics explained," January 2024. [Online]. Available: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_enterprises.

[5] Eurostat, "Digitalisation in Europe – 2023 edition," 2023. [Online]. Available: https://ec.europa.eu/eurostat/web/interactive-publications/digitalisation-2023#ict-security.

[6] Eurostat , "Statistics explained. ICT security in enterprises," December 2022. [Online]. Available: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_security_in_enterprises#ICT_security_in_EU_enterprises .

[7] European Commission , "Eurobarometer survey on cyberskills.," May 2024. [Online]. Available: https://europa.eu/eurobarometer/surveys/detail/3176.

[8] T. Driggs, "New Charlotte AI Innovations Enable Prompt Collaboration and Demystify Script Analysis," Crowdstrike Blog, 2024.

[9] M. Abu-Fadaleh, "All About SOC (Security Operation Centers)," Green Circle, 2024.

[10] Eurocontrol, "ATM-ATM SOC Implementation v1.0," Brussels, 2024.