SECURITY SUMMIT

14-15-16 marzo 2023

Security Summit

Clusit Associazione Italiana per la Sicurezza Informatica

ASTREA Advanced Security, Training Research, Events Agency

Scelta consapevole dell'architettura di servizio cloud adeguato alla realtà aziendale: i fattori imprescindibili da considerare

Roberto Obialero, CD Clusit - CISO, BL Manager S2E

Andrea Cerro, BU Director Cybersecurity S2E

Giorgio Rocca, CISO, Banca Progetto

15 marzo 2023 orario 9:20-10

Roberto Obialero

CONSIGLIO DIRETTIVO CLUSIT

TEAM LEADER DI PROGETTI DI RICERCA

CISO (CHIEF INFORMATION SECURITY OFFICER)

MANAGER BL CYBERSECURITY, ADVISORY & COMPLIANCE

Andrea Cerro

BUSINESS UNIT DIRECTOR

ENTERPRISE SECURITY SERVICES

Giorgio Rocca

CISO – BANCA PROGETTO

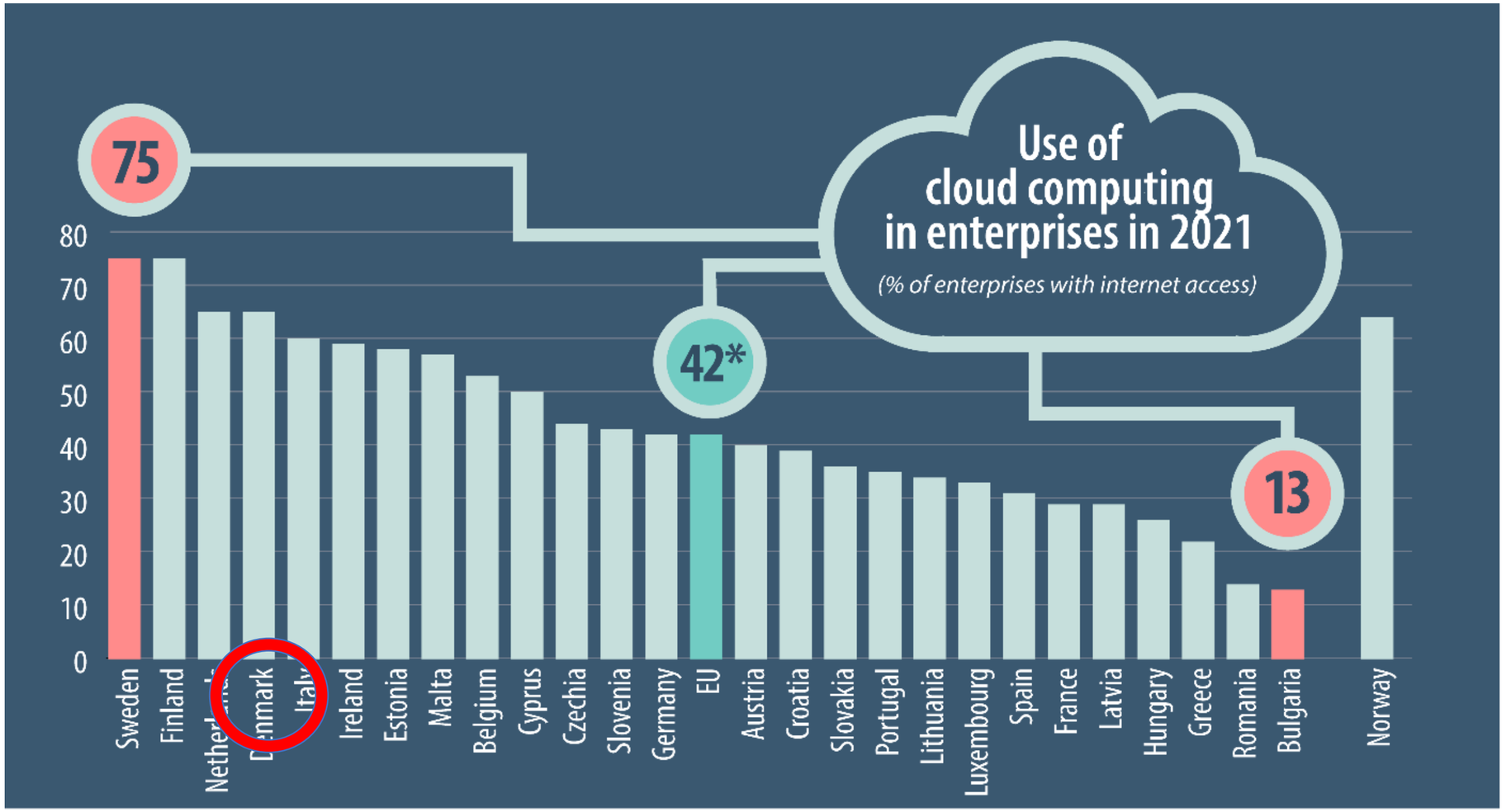
STEERING COMMITTEE CYBERSECURITY HUB CETIF

CISO CLOUD CLUB CSA (CLOUD SECURITY ALLIANCE)

AGENDA

- ANALISI DEL CONTESTO
- CLOUD SECURITY – NORMATIVE & BEST PRACTICES
- UTILIZZO CONSAPEVOLE DEI SERVIZI DI SICUREZZA
- CASE STUDIES

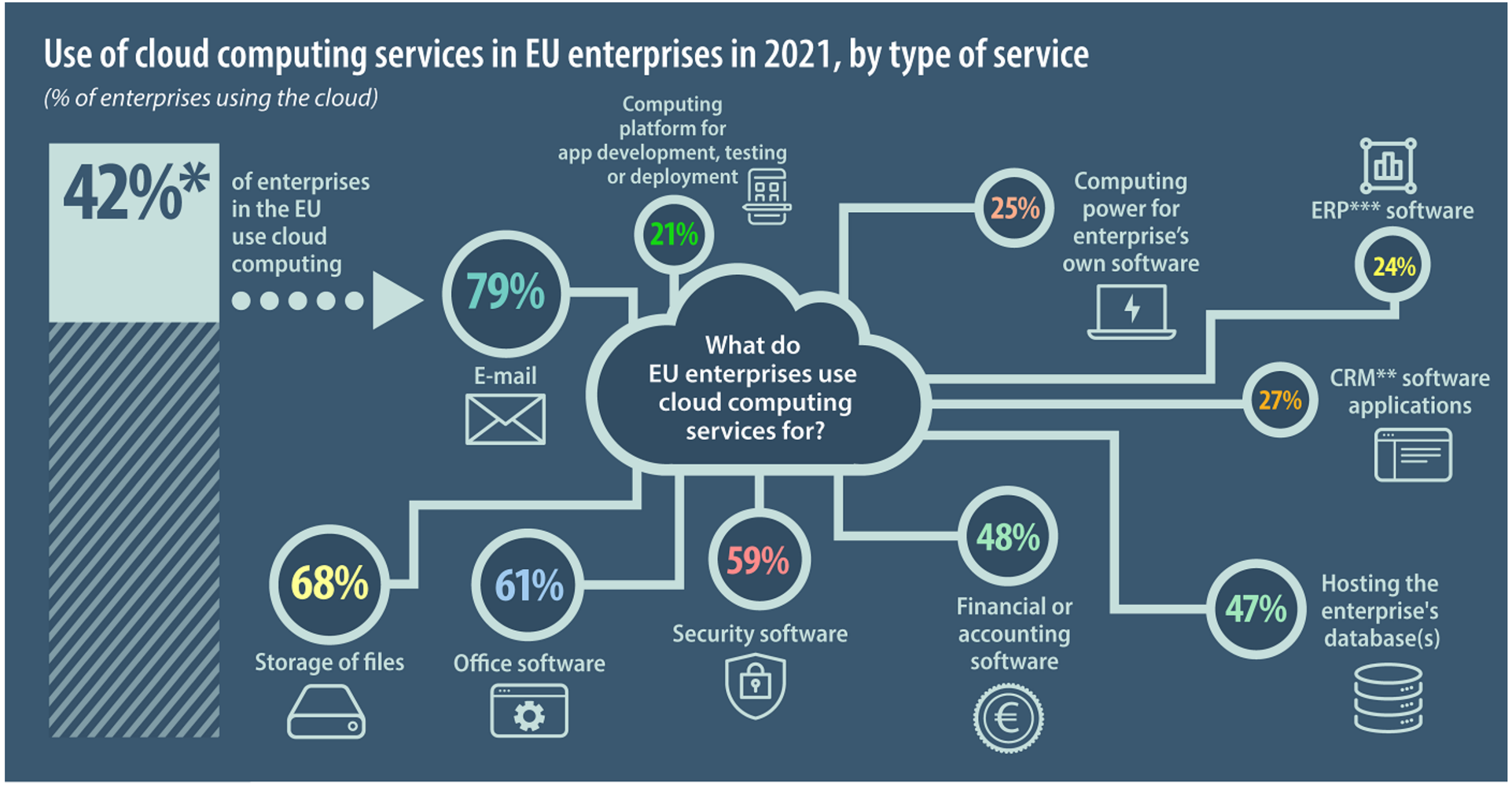
ANALISI DEL CONTESTO - STATISTICHE UE ADOZIONE SERVIZI CLOUD



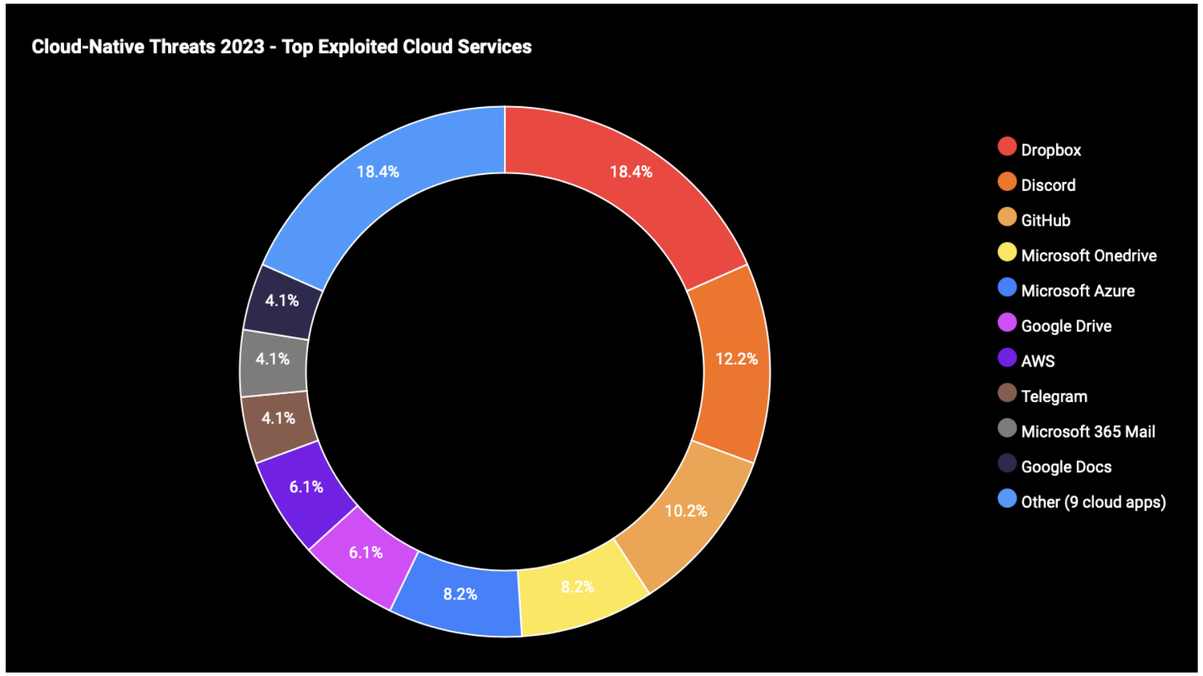
*Poland: data temporarily not available. As a result, the EU aggregate has been estimated.

ec.europa.eu/eurostat

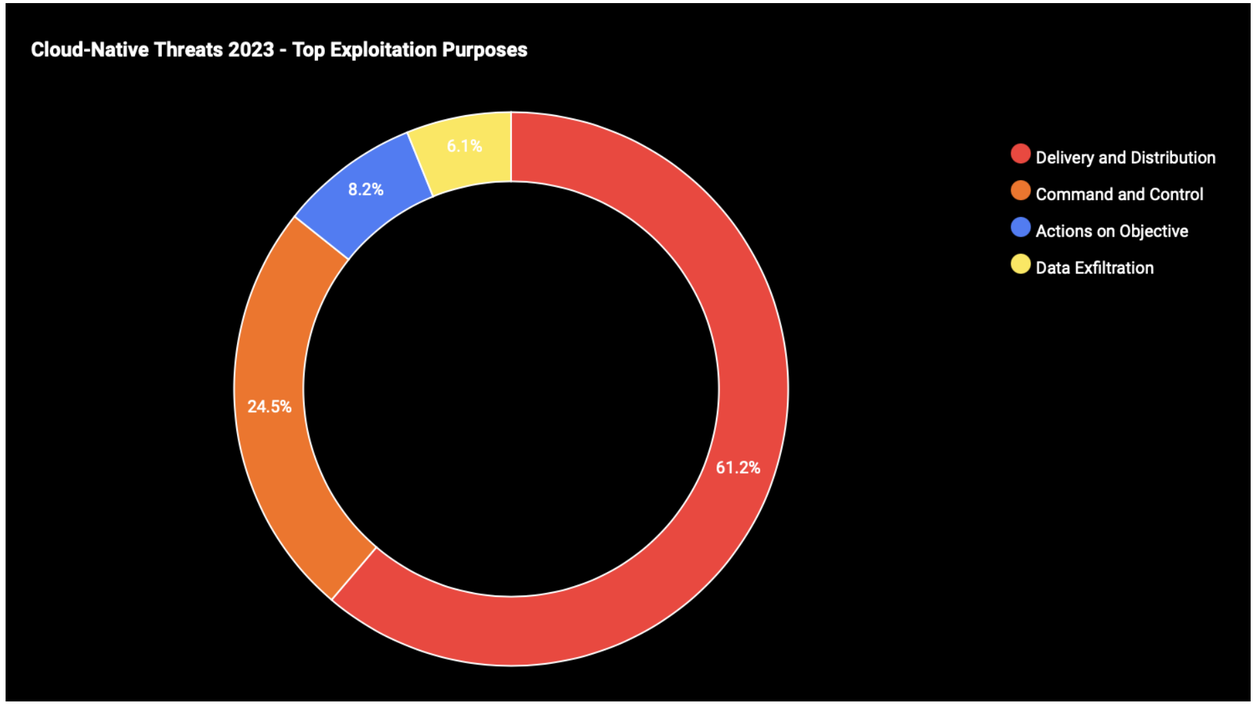
ANALISI DEL CONTESTO - TIPOLOGIA SERVIZI CLOUD ADOTTABILI



ANALISI DEL CONTESTO - INCIDENTI DI SICUREZZA SU SERVIZI CLOUD 1/2



Source https://www.hackmageddon.com/2023/03/06/cloud-native-threats-in-2023/



ANALISI DEL CONTESTO - INCIDENTI DI SICUREZZA SU SERVIZI CLOUD 2/2

Multiple cloud vendors impacted by PostgreSQL vulnerability that exposed enterprise databases

Emma Woollacott 16 August 2022 at 12:40 UTC
Updated: 05 September 2022 at 10:31 UTC

Heatwave forced Google and Oracle to shut down computers

20 July 2022

Argomenti

Comunicazione rivolta a tutta la community di LastPass.

Recentemente, vi abbiamo comunicato che un soggetto non autorizzato ha ottenuto l'accesso al servizio di archiviazione cloud di terze parti utilizzato da LastPass per conservare le copie di backup dei dati di produzione. Nell'ottica della trasparenza che da sempre ci contraddistingue, desideriamo aggiornarvi sulle attività investigative in corso.

ANALISI DEL CONTESTO – SERVIZI CLOUD & SHARED RESPONSIBILITY MODEL

1 Microsoft Azure, https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility.
2 Amazon Web Services, https://aws.amazon.com/compliance/shared-responsibility-model.

CLOUD SECURITY & NORMATIVE

VINCOLI NORMATIVA GDPR

- RESPONSABILE TRATTAMENTO > DPA
- SUPPORTO GESTIONE DIRITTI INTERESSATO
- SUPPORTO GESTIONE DATA BREACH
- TRASFERIMENTO DATI ALL'ESTERO
- SICUREZZA DEL TRATTAMENTO
- PRIVACY BY DESIGN
- REGISTRO TRATTAMENTI

VINCOLI NORMATIVA NIS2

- GESTIONE INCIDENTI
- SICUREZZA DELLA SUPPLY CHAIN

CLOUD SECURITY & BEST PRACTICES 1/2

Categoria controllo ISO/IEC 27001:2022	Controllo ISO/IEC 27001:2022
Controlli organizzativi	5.2 Ruoli e responsabilità per la sicurezza delle informazioni
Controlli organizzativi	5.19 Sicurezza delle informazioni nelle relazioni con i fornitori
Controlli organizzativi	5.20 Indirizzare la sicurezza delle informazioni nelle relazioni con i fornitori
Controlli organizzativi	5.21 Gestire la sicurezza delle informazioni nella filiera di fornitura per l'ICT
Controlli organizzativi	5.22 Monitoraggio e riesame dei servizi dei fornitori
Controlli organizzativi	5.23 Sicurezza delle informazioni per l'utilizzo di servizi cloud
Controlli organizzativi	5.24 Pianificazione e preparazione per la gestione degli incidenti relativi alla sicurezza delle informazioni
Controlli organizzativi	5.25 Valutazione e decisione sugli eventi relativi alla sicurezza delle informazioni
Controlli organizzativi	5.26 Risposta agli incidenti relativi alla sicurezza delle informazioni
Controlli organizzativi	5.28 Raccolta di evidenze
Controlli organizzativi	5.29 Sicurezza delle informazioni durante le interruzioni
Controlli organizzativi	5.30 Pianificazione della continuità della sicurezza delle informazioni
Controlli organizzativi	5.34 Privacy e protezione dei dati personali

CLOUD SECURITY & BEST PRACTICES 2/2

Controlli tecnologici	8.6 Gestione della capacità
Controlli tecnologici	8.8 Gestione delle vulnerabilità tecniche
Controlli tecnologici	8.9 Gestione delle configurazioni
Controlli tecnologici	8.14 Ridondanza delle strutture di elaborazione delle informazioni
Controlli tecnologici	8.15 Raccolta di log
Controlli tecnologici	8.16 Attività di monitoraggio

ISO/IEC 27017:2015

Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

ISO/IEC 27018:2019

Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

QUANTO SONO SICURI ED INTEGRABILI I SERVIZI IN CLOUD ?

DIPENDE DA DIVERSI FATTORI …

- APPROCCIO ED INFO FORNITE DA CLOUD PROVIDER
- PERIMETRO DI EVENTUALE CERTIFICAZIONE
- SERVIZI DI SICUREZZA OFFERTI
- DIRITTO DI AUDIT
- CONSAPEVOLEZZA DEL CLOUD CUSTOMER
- PROPENSIONE ALLA SPESA

UTILIZZO CONSAPEVOLE DEI SERVIZI DI SICUREZZA

COMPRENDERE PIENAMENTE IL MODELLO DI RESPONSABILITÀ CONDIVISO

AVER BEN CHIARO IL CONTESTO DI APPLICAZIONE ED USO

CONOSCERE QUALI SERVIZI DI SICUREZZA E PROTEZIONE OFFRE IL CLOUD PROVIDER

ESSERE PARTE ATTIVA NELLA:

- PROTEZIONE DEI DATI
- GESTIONE DELLE IDENTITÀ E DEGLI ACCESSI
- IMPLEMENTAZIONE DELLA BUSINESS CONTINUITY E DELLE STRATEGIE DI DISASTER RECOVERY
- ADOZIONE ED APPLICAZIONE DEL DEVSECOPS

BRIEF CASE SU VALUTAZIONE OPPORTUNITÀ ADOZIONE SERVIZIO CLOUD

Third-party sources. We may combine personal information we receive from you with personal information we obtain from other sources, such as:

- **Public sources**, such as government agencies, public records, social media platforms, and other publicly available sources.
- **Data providers**, such as information services and data licensors that provide demographic and other information.
- **Marketing partners**, such as joint marketing partners and event co-sponsors.

website you visited before browsing to the Site (via referral information), navigation paths between pages or screens, information about your activity on a page or screen, access times and duration of access, and whether you have opened our marketing emails or clicked links within them.

Communication interaction data such as your interactions with our email, text or other communications (e.g., whether you open and/or forward emails) – we may do this through use of pixel tags (which are also known as clear GIFs), which may be embedded invisibly in our emails.

International data transfer

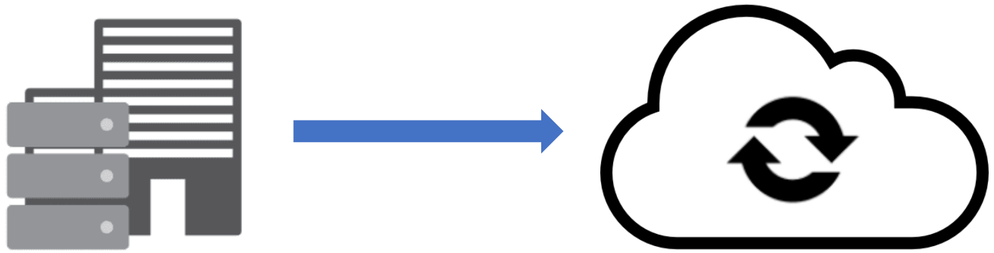
We are headquartered in the United States and may use service providers that operate in other countries. Your personal information may be transferred to the United States or other locations where privacy laws may be different from those in your state, province, or country.

Users in the EEA and the UK should read the important information provided in the Notice to European users below about transfer of personal information outside of the EEA and UK, as applicable.

CASE STUDIES: MIGRAZIONE IN CLOUD DEL SOC AS A SERVICE DI S2E

PERCHÈ MIGRARE AL CLOUD?

- RINNOVARE L'HARDWARE
- RIDURRE I TEMPI DELLE MANUTENZIONI E VELOCIZZARE GLI UPGRADE INFRASTRUTTURALI
- FACILITARE LO SVILUPPO DI NUOVE FUNZIONALITÀ
- AUMENTARE RISORSE E PERFORMANCE
- AUMENTARE RESILIENZA E DISPONIBILITÀ



CASE STUDIES: MIGRAZIONE IN CLOUD DEL SOC AS A SERVICE DI S2E

LE SFIDE CON CUI CI SIAMO DOVUTI CONFRONTARE

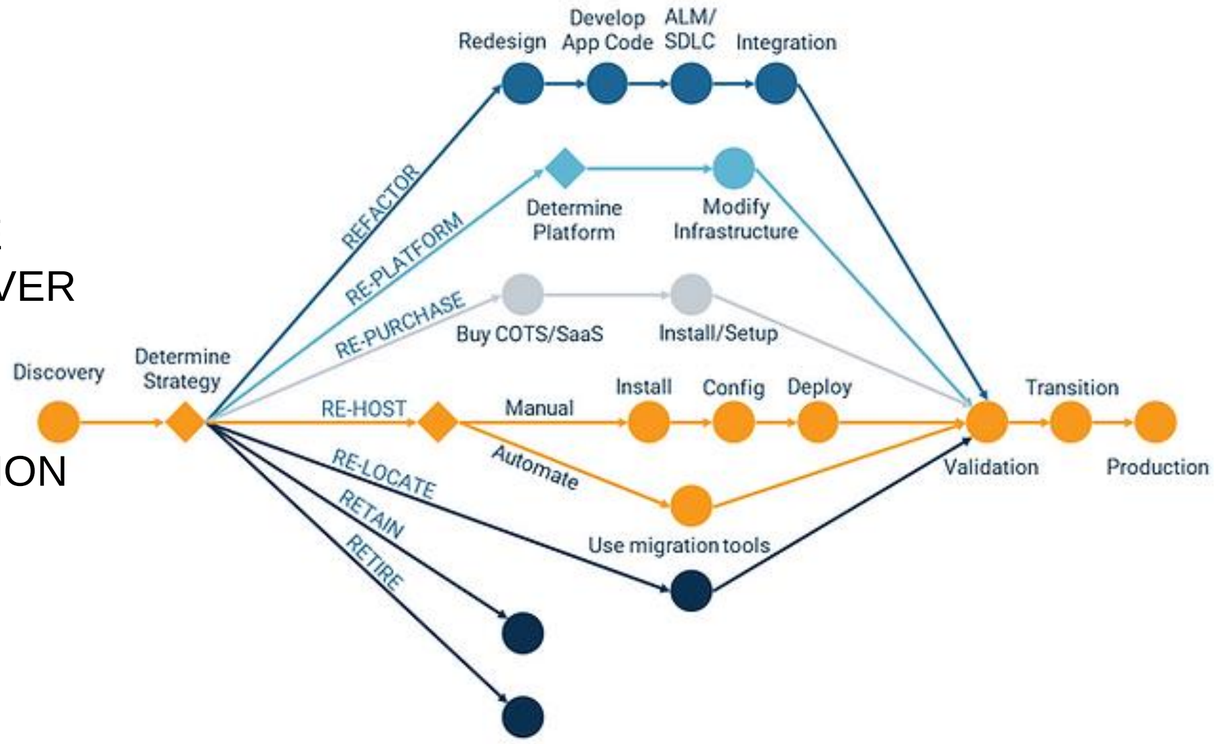
- SCELTA DEL CLOUD PROVIDER
- ADOZIONE STRATEGIE DI MIGRAZIONE
- MANTENIMENTO OPERATIVITÀ SOC
- GESTIONE DELLA SICUREZZA DEI DATI DEL SOC OSPITATI ALL'INTERNO DEL CLOUD PROVIDER

CASE STUDIES: MIGRAZIONE IN CLOUD DEL SOC AS A SERVICE DI S2E

ADOZIONE STRATEGIE DI MIGRAZIONE:

RE-PLATFORM: È UNA STRATEGIA CHE PREVEDE ALCUNE OTTIMIZZAZIONI DURANTE LA MIGRAZIONE UTILIZZANDO DEI PLATFORM SERVICES DEL CLOUD PROVIDER AL FINE DI AVVANTAGGIARSI RAPIDAMENTE DELLE FUNZIONALITÀ NATIVE DEL SERVIZIO SENZA DOVER MODIFICARE L'APPLICAZIONE CHE SI STA MIGRANDO.

RE-FACTORING: TRASFORMARE UN'APPLICAZIONE NON CLOUD IN UN'APPLICAZIONE CLOUD-NATIVE.
RIGUARDA TUTTA L'APPLICAZIONE: I COMPONENTI, IL CODICE DELL'APPLICAZIONE E I DATI STESSI.
È GUIDATA DALLA NECESSITÀ DELLE AZIENDE DI AGGIUNGERE FUNZIONALITÀ, SCALABILITÀ O PRESTAZIONI CHE ALTRIMENTI SAREBBERO DIFFICILI DA OTTENERE NELL'AMBIENTE ESISTENTE.



CASE STUDIES: MIGRAZIONE IN CLOUD DEL SOC AS A SERVICE DI S2E

COSA ABBIAMO OTTENUTO MIGRANDO AL CLOUD?

- **SICUREZZA AVANZATA**: RISPETTO DEGLI STANDARD E CERTIFICAZIONE DEI SISTEMI UTILIZZATI. INTEGRAZIONE NATIVA E GRANULARE DEL RISPETTO DELLE COMPLIANCE. PROTEZIONE DEI DATI MEDIANTE POLITICHE DI ACCESSO BASATE SUL LEAST PRIVILEGE E CRITTOGRAFIA DEI DATI IN TRANSITO E AT REST

- **SCALABILITÀ**: I SERVIZI SONO IN GRADO DI SCALARE IN FUNZIONE DEL CARICO A CUI DEVONO RISPONDERE SINGOLARMENTE.

- **RIDUZIONE DEI COSTI**: L'ARCHITETTURA DEL SOC È QUASI TOTALMENTE SERVERLESS. QUESTO HA PERMESSO DI AFFRONTARE SOLO I COSTI DOVUTI ALLE REALE RICHIESTE GESTATE E ABBATTERE I COSTI DI MANUTENZIONE E GESTIONE DELL'INFRASTRUTTURA

- **FLESSIBILITÀ ED AGILITÀ**: DISPONIBILITÀ DI COMPUTAZIONE E STORAGE INSIEME ALLE PRESENZA DI SERVIZI E PIATTAFORME GIÀ PRONTE HA PERMESSO DI VELOCIZZARE IL PROCESSO DI MIGRAZIONE E LE SUCCESSIVE NECESSITÀ EVOLUTIVE

CASE STUDIES: MIGRAZIONE IN CLOUD DEL SOC AS A SERVICE DI S2E

- **ALTA DISPONIBILITÀ E DISASTER RECOVERY**: L'UTILIZZO DEI MANAGED SERVICES DEL CLOUD PROVIDER CI HA PERMESSO DI OTTENERE L'ALTA DISPONIBILITÀ DEI SERVIZI E DELLE FUNZIONALITÀ DEL SOC. CONTEMPORAMENTE ABBIAMO SEMPLIFICATO ED OTTIMIZZATO LE PROCEDURE DI DISASTER RECOVERY FINALIZZATE ALLA BUSINESS CONTINUITY

- **SOSTENIBILITÀ**: S2E È UN'AZIENDA ESTREMAMENTE ATTENTA ALLA SOSTENIBILITÀ E L'IMPATTO ENERGETICO CHE I SUOI SERVIZI ED I SUOI DIPENDENTI POSSONO AVERE SULL'AMBIENTE. L'ADOZIONE DEL CLOUD CI HA PERMESSO DI ESSERE MAGGIORMENTE ATTIVI IN TAL SENSO

- **AUMENTO DELLA PRODUTTIVITÀ**: AVER ADOTTATO IL CLOUD CI HA PERMESSO DI POTER SPERIMENTARE ED INNOVARE PIÙ FACILEMENTE. QUESTO CI HA PERMESSO DI ESSERE PIÙ PRODUTTIVI ED EFFICACI.

CASE STUDIES: MIGRAZIONE IN CLOUD DEL SOC AS A SERVICE DI S2E

- **MIGLIORE AFFIDABILITÀ**: LE FUNZIONALITÀ DEL SOC SONO DISPONIBILI H24, 365 GIORNI L'ANNO. TUTTO IL PRIMO LIVELLO D'INTERVENTO È TOTALEMENTE AUTOMATIZZATO COSÌ COME LA GESTIONE DEI TICKET E LE PROCEDURE DI ESCALATION VERSO IL SECONDO ED IL TERZO LIVELLO D'INTERVENTO

- **RIDUZIONE DEI TEMPI DI RISPOSTA**: I TEMPI DI RISPOSTA AGLI INCIDENT SI SONO RIDOTTI GRAZIE AD UN'ARCHITETTURA A MICROSERVIZI SERVERLESS CHE ALLOCA LE RISORSE NECESSARIE AI SERVIZI CHE NE HANNO REALEMENTE BISOGNO

- **MIGLIOR LIVELLO DI AUTOMAZIONE**: ABBIAMO AUTOMATIZZATO LA RISPOSTA AGLI INCIDENT RIUSCENDO AD ESSERE AGNOSTICI RISPETTO ALLE TECNOLOGIE UTILIZZATE DAI NOSTRI CLIENTI. SIAMO IN GRADO DI RISPONDERE SIA AGLI INCIDENT PROVENIENTI DAI NOSTRI SISTEMI DI CONTROLLO CHE A QUELLI DEL CLIENTE, INDIPENDENTEMENTE DALLA TECNOLOGIA UTILIZZATA E DALLA PROVENIENZA

CASE STUDIES: L'ESPERIENZA DI BANCA PROGETTO

BANCA PROGETTO

La prima Banca italiana in cloud aws

> 200 Dipendenti

> 150.000 Clienti

> 7 miliardi Portafoglio

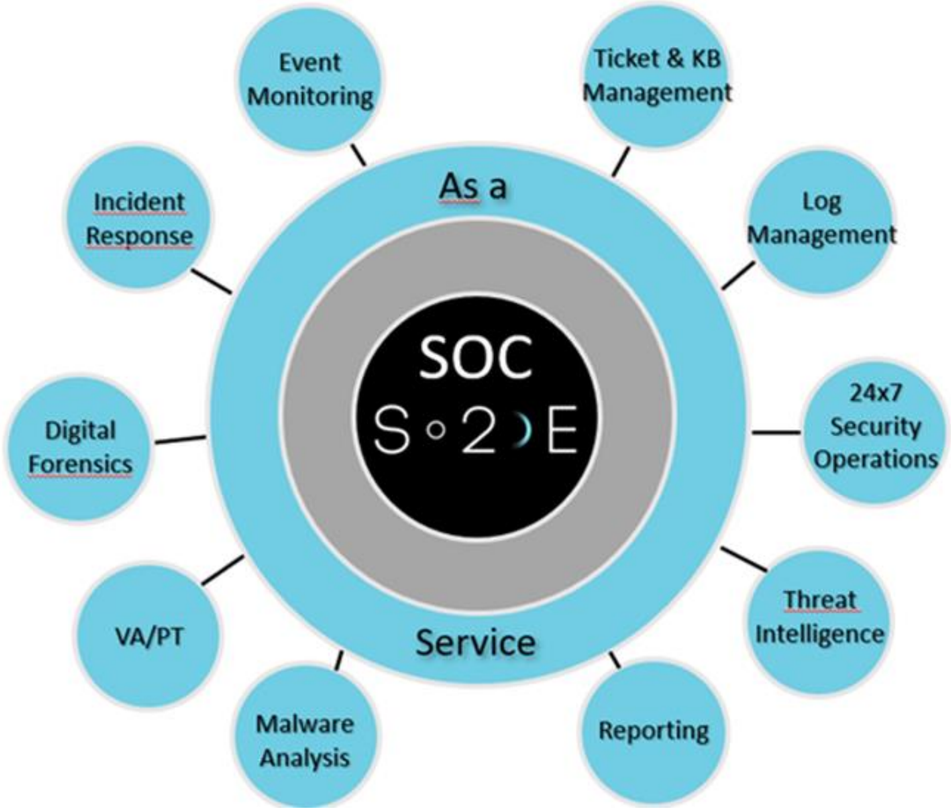
PROGETTOIMPRESE

PROGETTOQUINTO

CONTOPROGETTO

Cream
BANCA PROGETTO

2019



CASE STUDIES: I VANTAGGI PER BANCA PROGETTO

REAL DIGITAL TRANSFORMATION

ANCHE LA CYBERSECURITY DIVIENE PARTE DELLA TRASFORMAZIONE DIGITALE DELLA BANCA, CHE NON SI CONCRETIZZA CON IL SOLO TRASFERIMENTO IN CLOUD DELLE MACCHINE MA CON IL PIENO UTILIZZO DEI SERVIZI NATIVI.

INTEGRABILITY

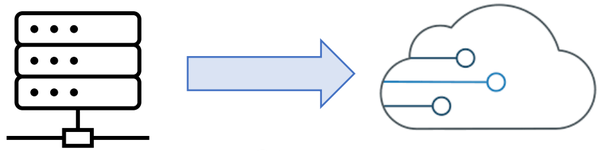
IL SIEM IN CLOUD PERMETTE UNA PIENA INTERAZIONE CON LE FONTI DATI CLASSICHE DI SECURITY OPERATION E CON STRUMENTI SPECIFICI DI SECURITY GOVERNANCE (ES. CLOUD SECURITY POSTURE) INTEGRANDOSI PERFETTAMENTE CON LA VISIONE CLOUDCENTRICA DELLA BANCA.

CHANGEABILITY

OLTRE AL CLASSICO CONCETTO DI SCALABILITA' VIENE GARANTITA LA POSSIBILITÀ DI ESEGUIRE CAMBIAMENTI ED IMPLEMENTAZIONI DEI SERVIZI IN TEMPI RAPIDI, AL MUTUARSI DEGLI SCENARI E DEI RISCHI NELL'ECOSISTEMA BANCA.

SECURITY BY DESIGN

L'EVOLUZIONE DEL SOC IN CLOUD APPLICA IL CONCETTO DI SECURITY BY DESIGN ALLA STESSA CYBERSECURITY PERMETTENDO DI MIGLIORARE LA CYBER RESILIENCE GENERALE DELLA BANCA.



Q&A

SU COSA POSSONO ESSERE D'AIUTO I TEAM SPECIALISTICI S2E?

- **DATA PROTECTION ADVISORY & COMPLIANCE: SERVIZI E PROGETTI CYBERSECURITY, NORMATIVE & BEST PRACTICES**
- **IDENTITY GOVERNANCE ADMINISTRATION: PRIVILEGED ACCOUNT MANAGEMENT, ACCESS MANAGEMENT**
- **CLOUD SECURITY: NETWORK AND APPLICATION PROTECTION, DEVSECOPS, SECURITY POSTURE AT SCALE**
- **SECURITY OPERATIONS: SOC AS A SERVICE, VA/PT, DIGITAL FORENSICS, OT SECURITY, INCIDENT RESPONSE**

VIENI A TROVARCI AL NOSTRO STAND!

CONTATTI: *ROBERTO.OBIALERO@S2E-PRO.COM* *https://bit.ly/3DCd4m5*

ANDREA.CERRO@S2E-MAIL.COM *https://bit.ly/3T3LN5l*