VARGROUP ORACLE

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

inspiring innovation

COME CAMBIANO LE STRATEGIE DI CYBERSECURITY NELL'ERA DEL CLOUD?

Michele Barbiero, Var Group

Fabrizio Zarri, Oracle

Milano, 12.03.2019

Il Cloud insicuro

Uno dei maggiori rischi che corre una azienda oggi è quello di non evolvere al passo con i tempi

Il Cloud non è più un’opzione

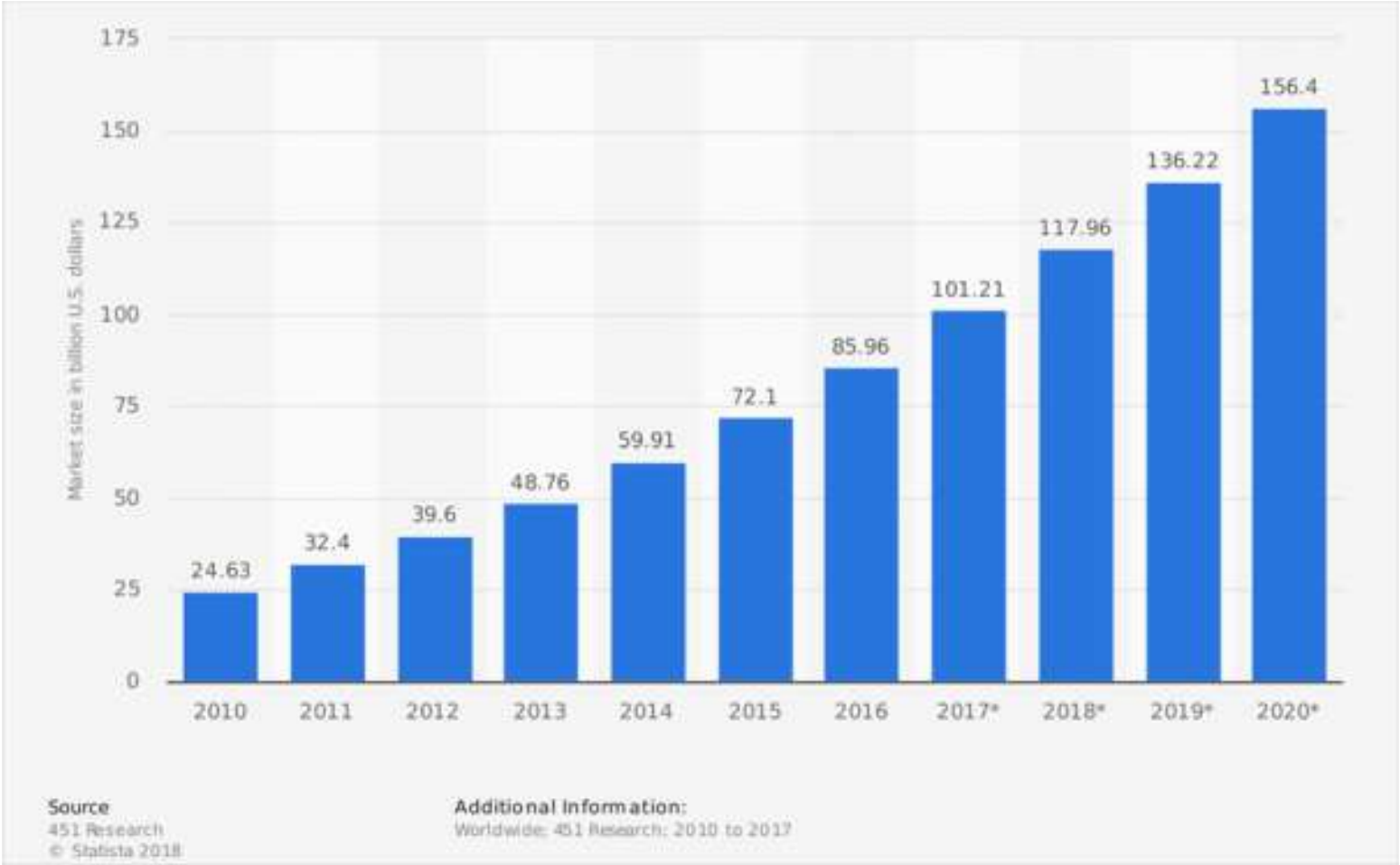
Il Cloud costringe ad un approccio differente alla security. Sottovalutarlo può essere deleterio.

Cloud - Crescita

- In 15 months, 80% of all IT budgets will be committed to cloud solutions
- 73% of companies are planning to move to a fully software-defined data center within 2 years
- 49% of business are delaying cloud deployment due to a cybersecurity skills gap

Source: Twitter

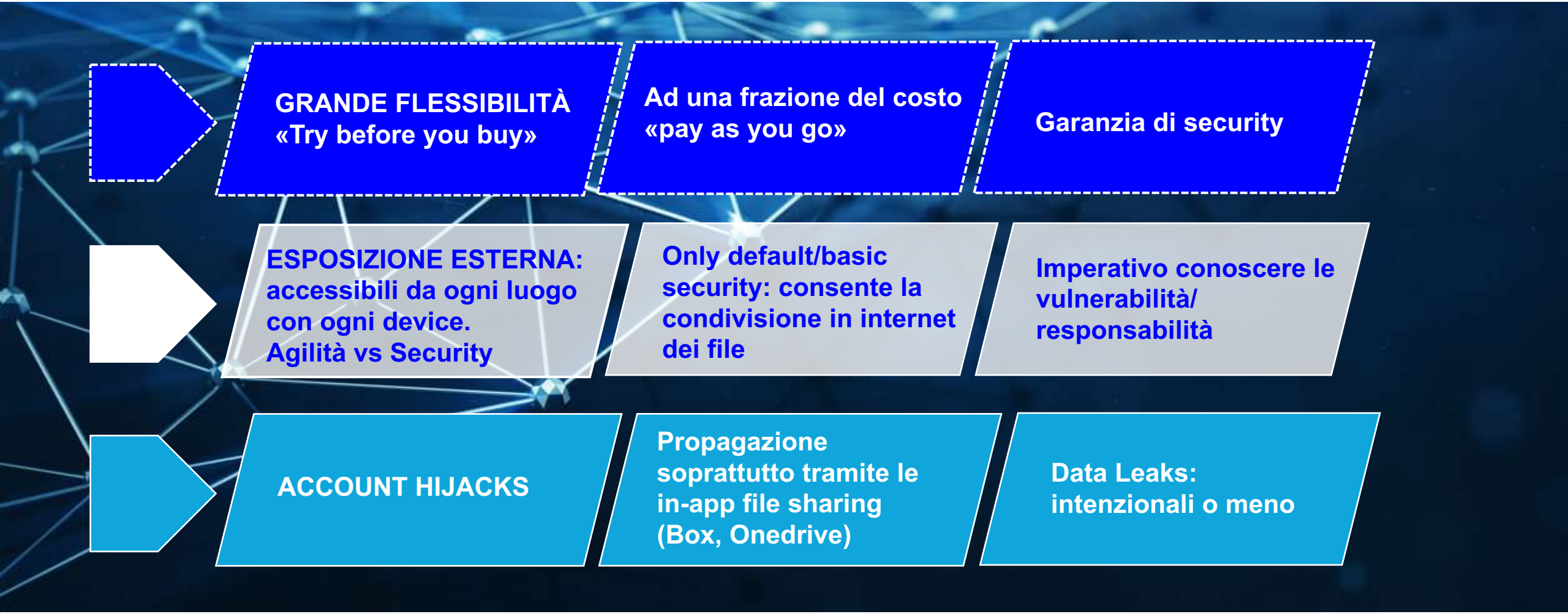
Size of the cloud computing and hosting market market worldwide from 2010 to 2020 (in billion U.S. dollars) **



inspiring innovation

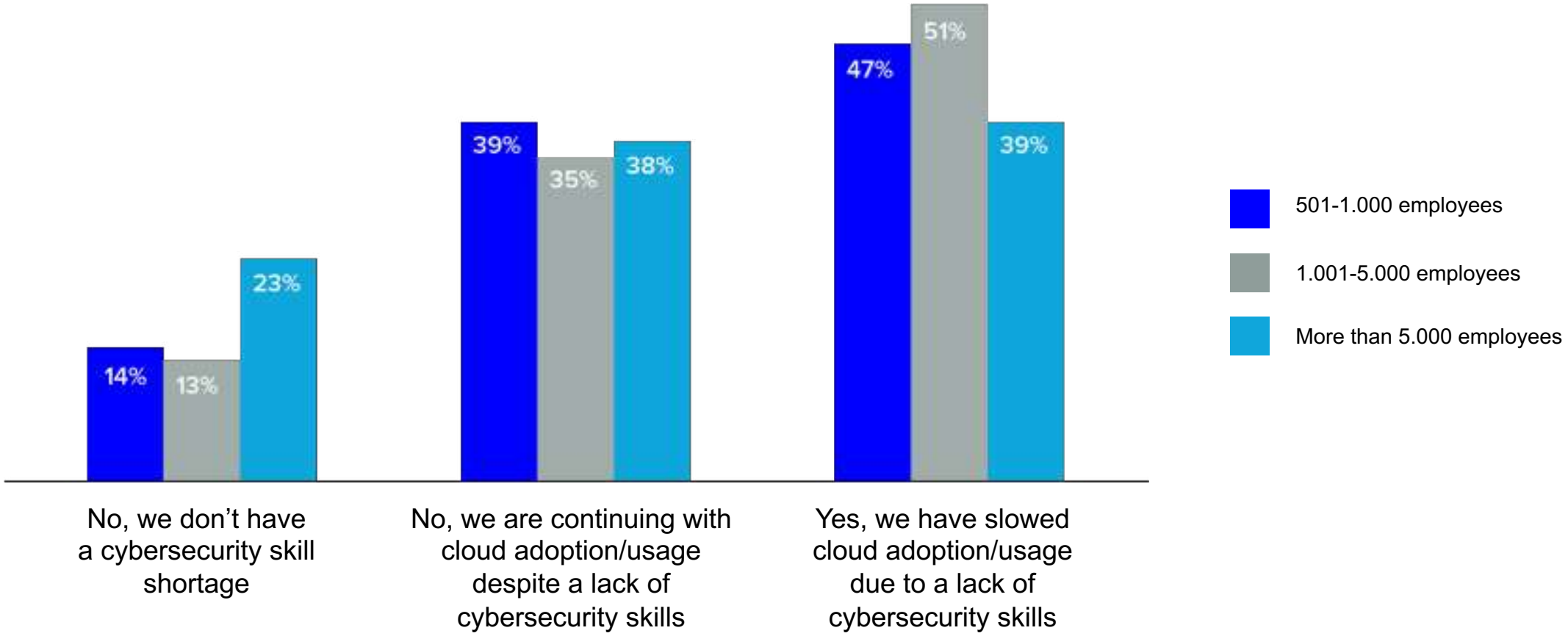
VARGROUP

Rischi e vettori di attacco



VARGROUP

Is a shortage of cybersecurity skills affecting your organization’s usage of cloud computing?



IL 65% DEI PROFESSIONISTI

sottostima i danni derivanti
da attacchi in Cloud. Le aziende NON
prendono la sicurezza in Cloud seriamente

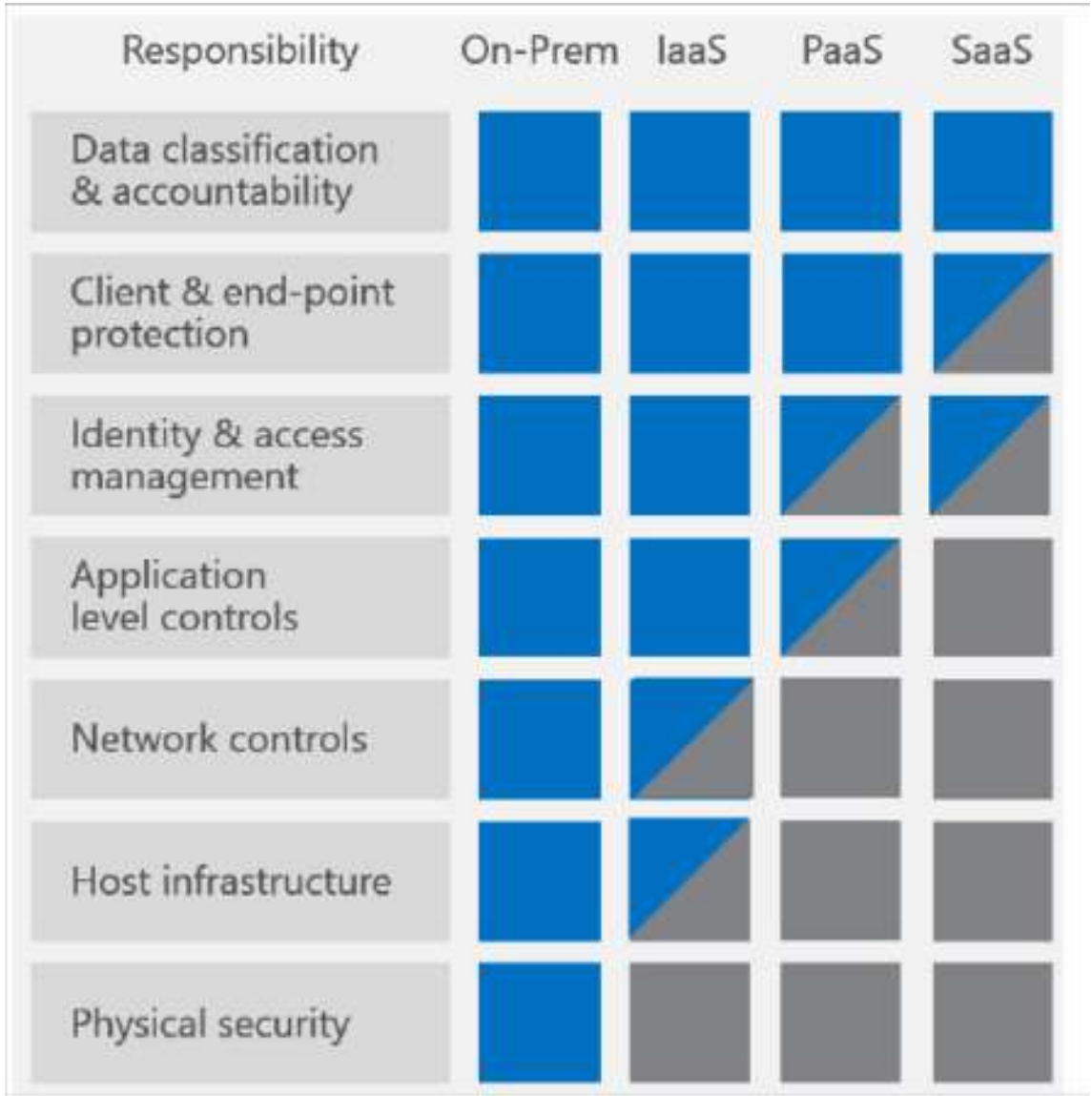
UN BUON 30% DEGLI INTERVISTATI

ritiene che la sicurezza in Cloud sia
responsabilità del Cloud Service Provider

FONTE: Studio Dome9 2018.

VARGROUP

Condivisione delle responsabilità in Cloud



Se due corpi interagiscono tra loro, si sviluppano due forze, dette comunemente azione e reazione: come grandezze vettoriali sono uguali in modulo e direzione, ma opposte in verso.

Il terzo principio della dinamica NON trova applicazioni in due casi reali nella vita di tutti i giorni

Nei rapporti familiari dove, tipicamente, ad una azione dell'uomo corrisponde una reazione della donna spropositata, spesso illimitata nel tempo e ove le azioni correttive richieste possano essere onerosissime.

Nella cybersecurity, dove un attacco talvolta non mirato, a basso costo e a basso rischio per l'attaccante, comporta un **impatto spesso spropositato**, di lunga durata e che richiede azioni correttive oltremodo onerose.

Identity Hijack

Quale può essere «..un attacco talvolta non mirato, a basso costo e a basso rischio per l'attaccante»
L'Identity Hijack!

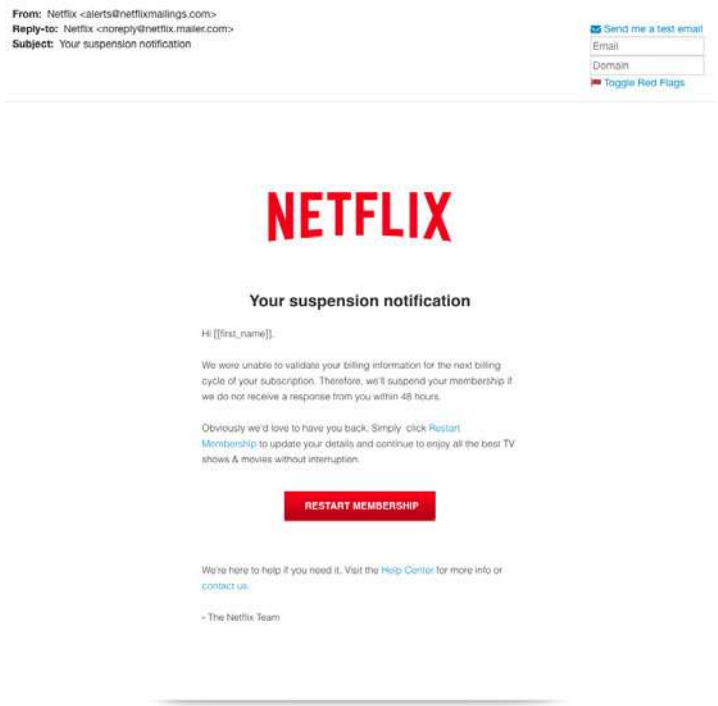
Come avviene un Hijack dell'account?
Phishing – Spyware - Social engineering - …

Ci si può difendere?

Storicamente siamo piuttosto proni a questo tipo di attacchi…

Training

Il training, passaggio fondamentale.



Ma non sufficiente…

Visibilità

Le soluzioni Cloud non forniscono a chi si occupa di security la VISIBILITÀ indispensabile per il controllo dei criteri di sicurezza:

Definizione → Implementazione → Applicazione → Verifica

Le soluzioni Cloud non forniscono gli strumenti per la protezione delle applicazioni o la prevenzione della perdita dei dati

Shared Responsibility: Visibility and Identity

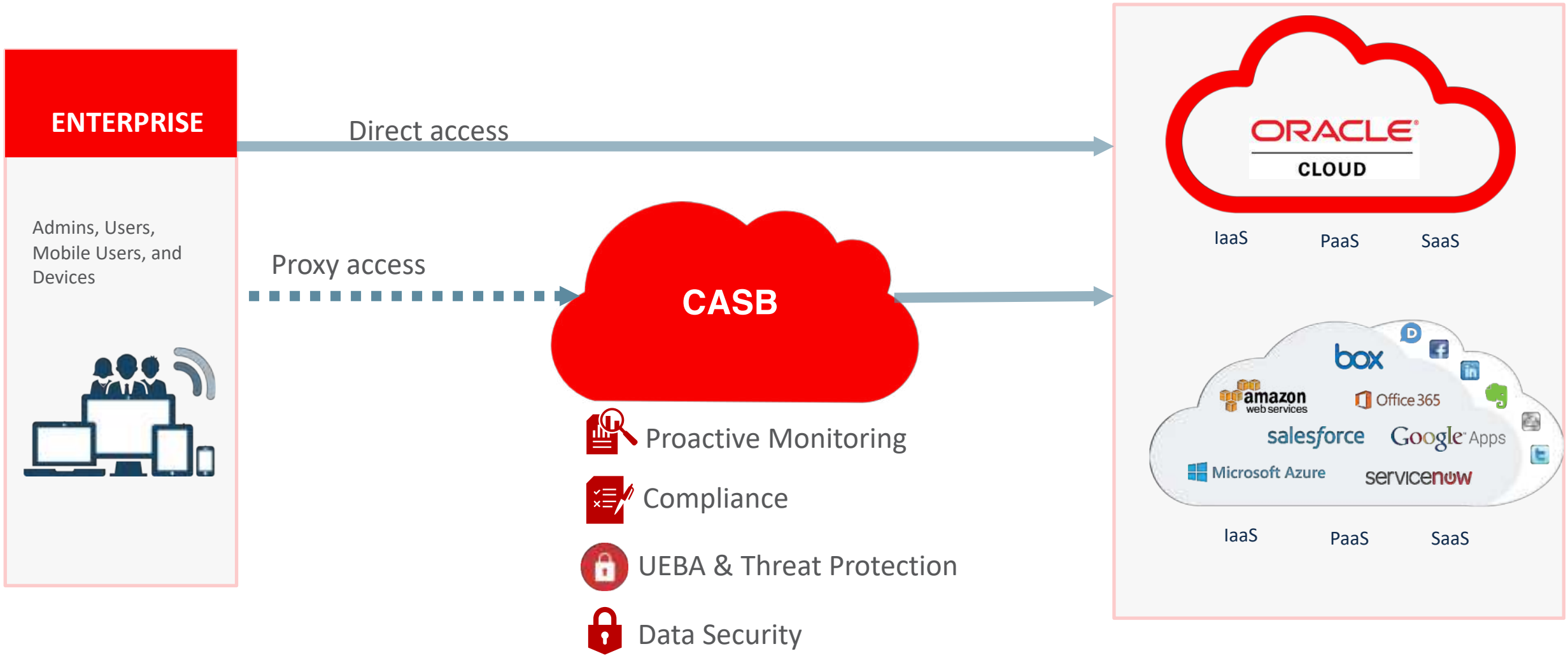
CASB (Cloud Access Security Broker)

- Visibility
- Threat Protection
- Compliance
- Data Security

IDaaS (Identity as a Service)

- Adaptive Auth
- User Management
- Access Mgmt (SSO)
- Provisioning
- MFA (OTP)
- Cloud Directory

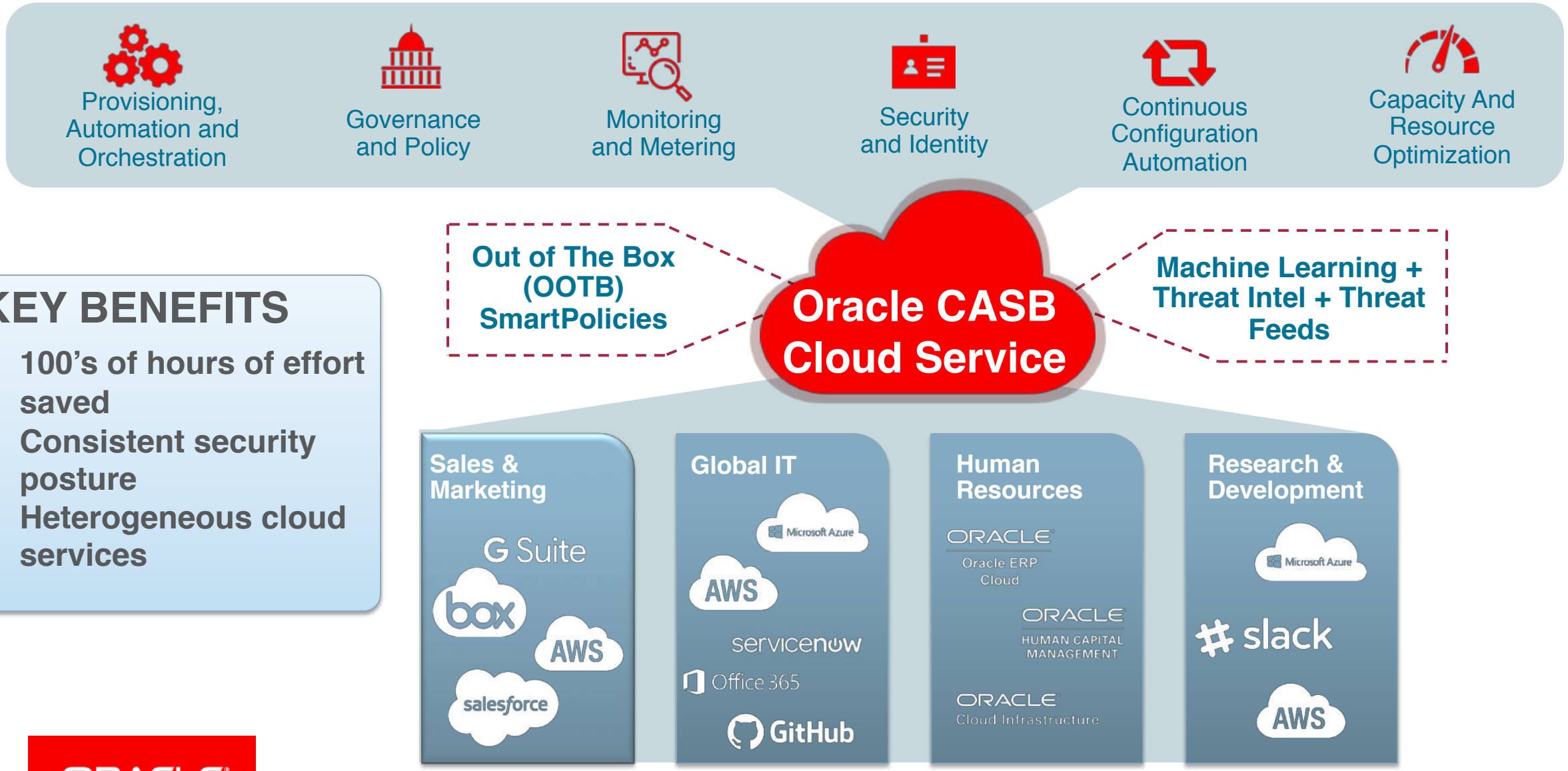
Cloud Access Security Broker (CASB)



*"**CASBs** are becoming as important **to cloud** as **firewalls** became **to data centers**"*

- Steve Riley, Gartner analyst

CASB: Shared Responsibility in Heterogenous Cloud



KEY BENEFITS

- 100's of hours of effort saved
- Consistent security posture
- Heterogeneous cloud services

Threats Detected by Oracle CASB (2018)

March 2018

Customer: Digital Media Company (> 1K users)

Threat Pattern: Abuse of compute resources

Details:

- User typically uses CPU instances
- User launches GPU instance at odd hour

CASB Action: Risk event raised

01

August 2018

Customer: Biotech Company

Threat Pattern: Brute force – Token Validation Replay

Details:

- "Low-volume", "Low-velocity" transactions in highly active systems
- Increase attacks with significant token errors from specific country

CASB Action: Risk event raised

03

02

June 2018

Customer: Government ERP Cloud Customer (>1K employees)

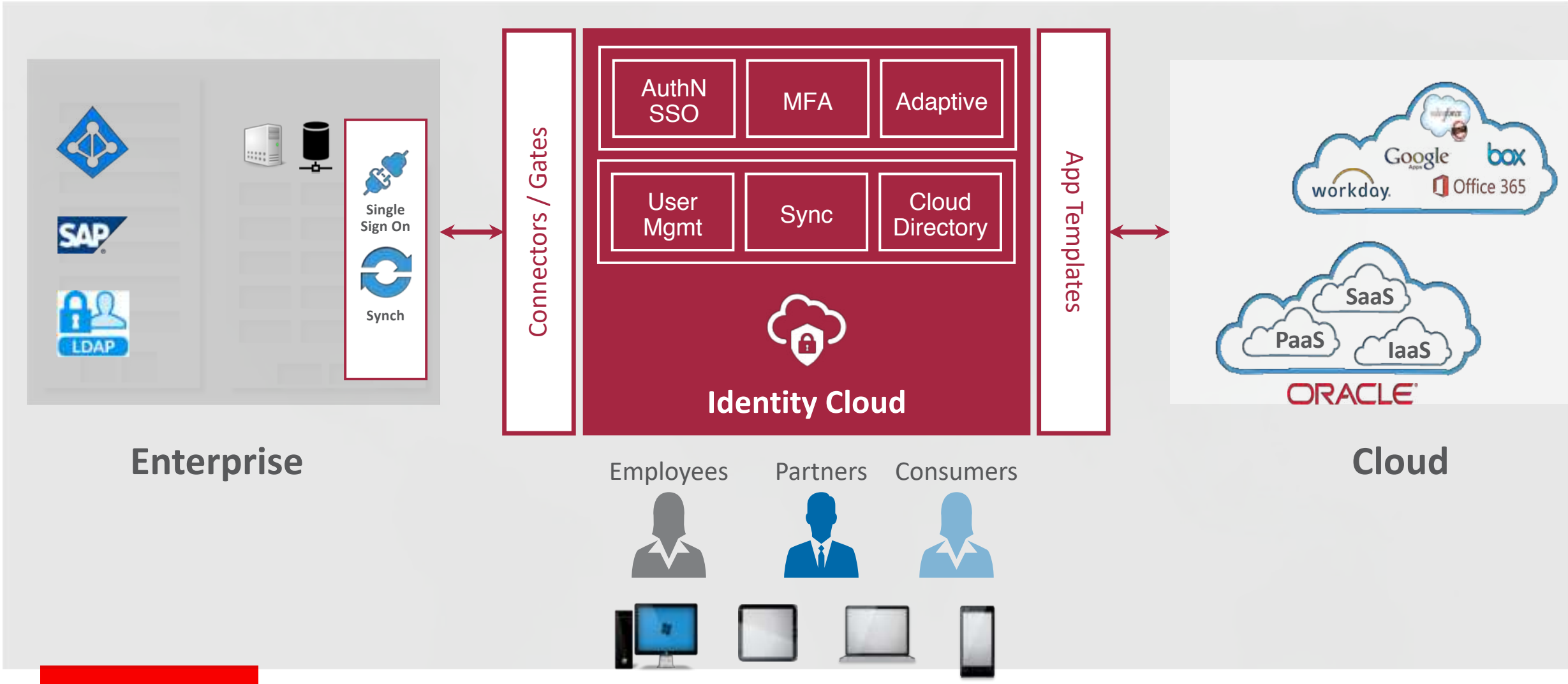
Threat Pattern: Configuration change

Details:

- System Security Options changed to disable payment data encryption

CASB Action: Admin notified, non-compliance prevented

IdaaS - Oracle Identity Cloud Service



Oracle Identity Cloud Service - Adaptive Security

Reputation Services
(IP/Mobile/Social Identity)

Adaptive Intelligence

ORACLE IDENTITY CLOUD SERVICE

Network

Location

Device

Time of access

External Risk/Threat feeds
(SIEM/UEBA/EMM)

User and App Context

Access Context

Oracle CASB Cloud Service

CASB

Remediate

Enterprise Resources protected by IAM/EMM/MDM

Security Ops Center

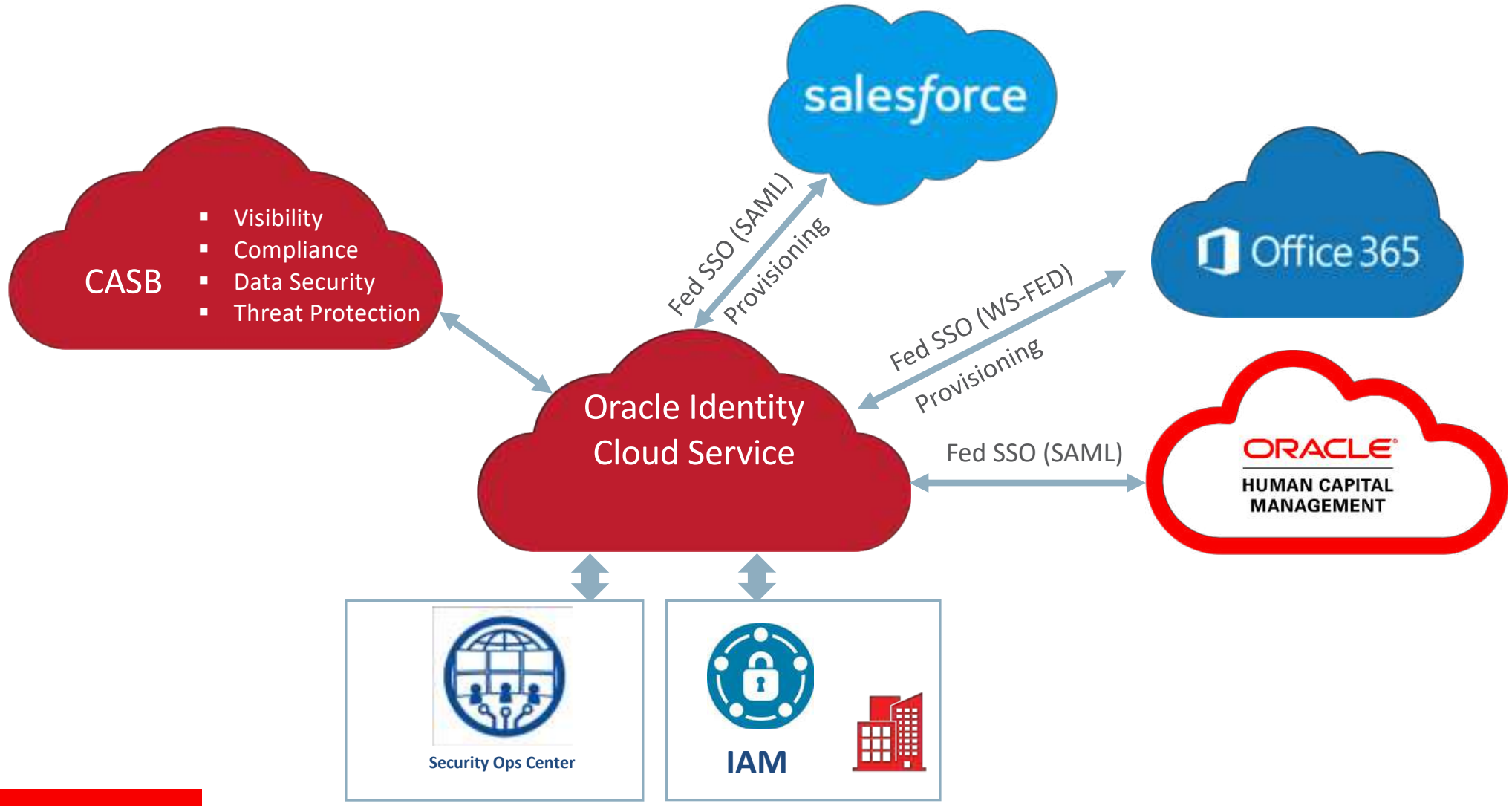
"Block/Challenge access if the user is coming from risky network/geo/untrusted devices"

"Prevent users from accessing sensitive apps & data, based on policies I can define"

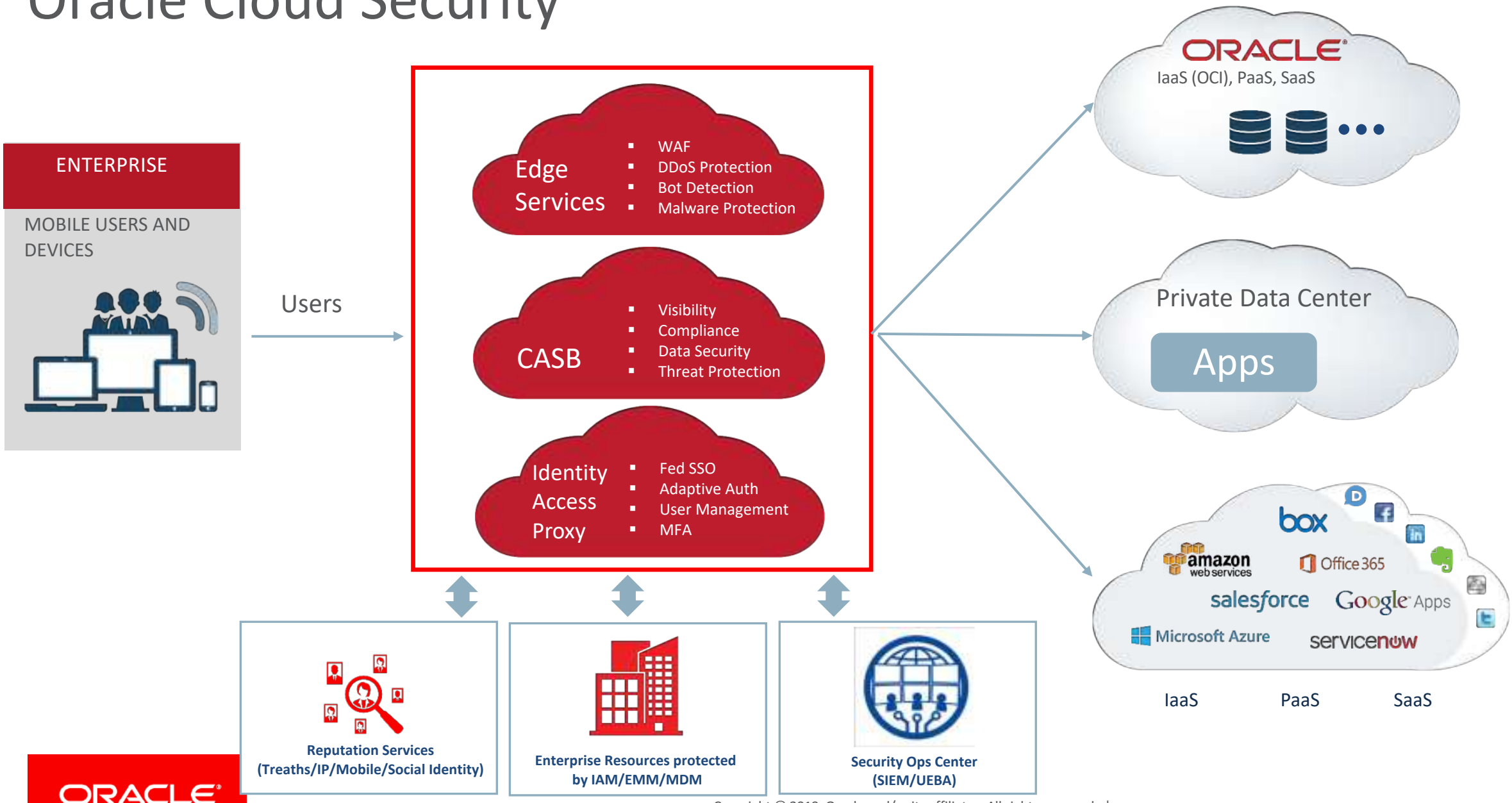
"Leverage external feeds and existing security tools to enforce better security"

ORACLE

IDCS Use-Case



Oracle Cloud Security



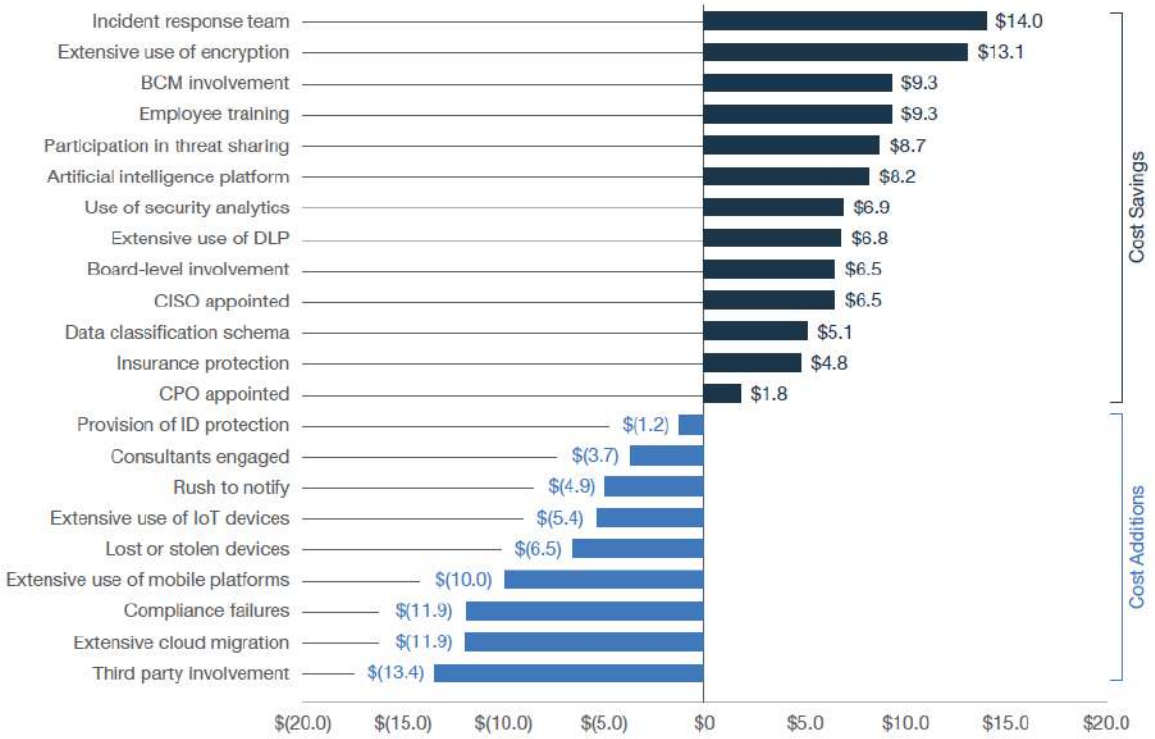
Cosa influenza il costo di un breach?

Factors that influence the cost of a data breach

Certain factors decrease or increase the cost of a data breach. Figure 12 provides a list of 22 factors that increase or decrease the per capita cost of a data breach.

Figure 12. Impact of 22 factors on the per capita cost of data breach

Measured in US$

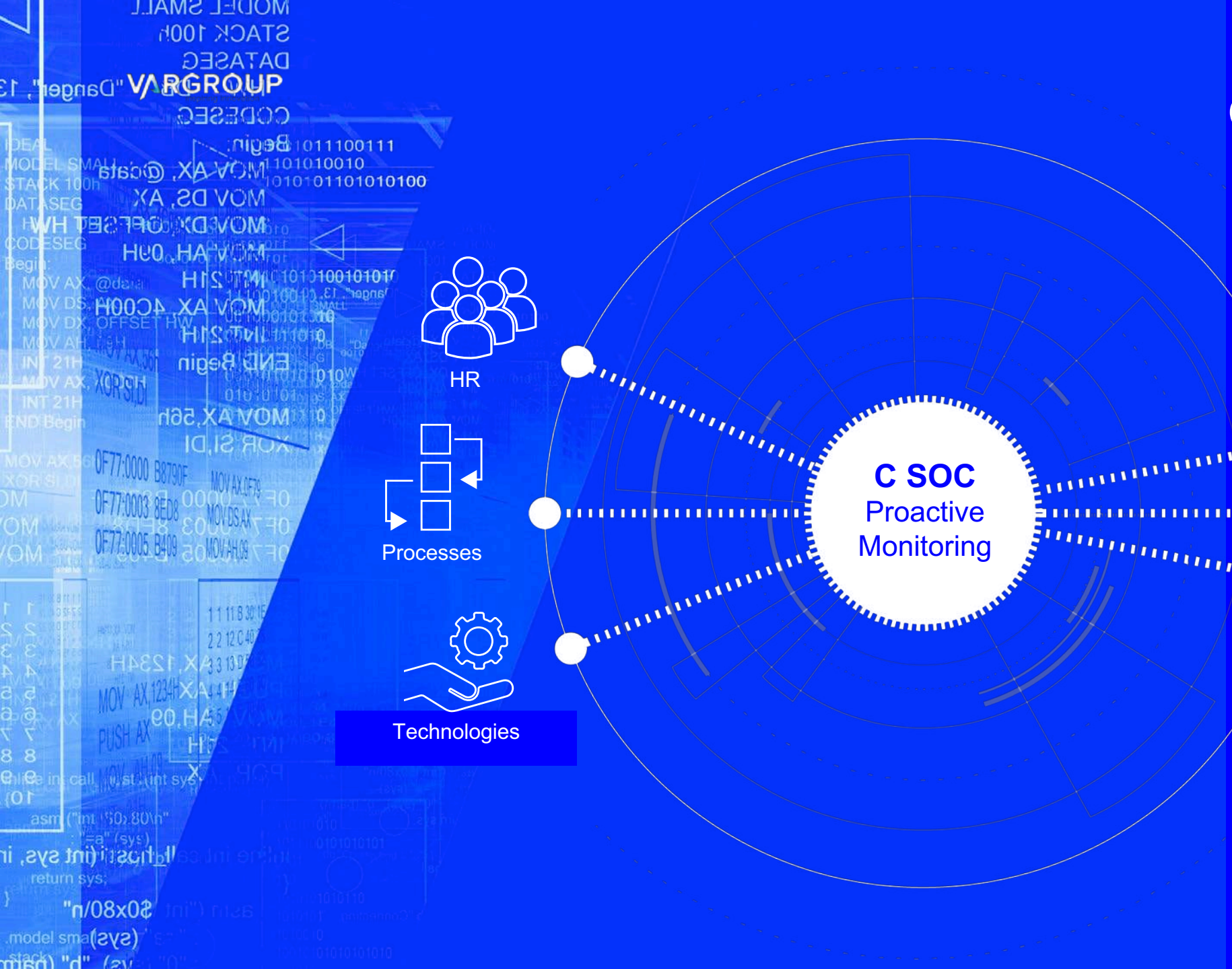


Costo medio di un breach per record: 140$

Ponemon Institute LLC
Attn: Research Department
2308 US 31 North
Traverse City, Michigan 49686 USA
1.800.887.3118
research@ponemon.org

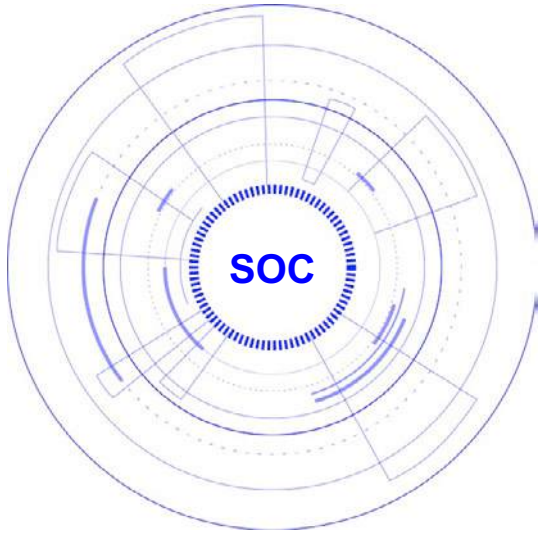
Complete copies of all country reports are available at www.ibm.com/security/data-breach

Cos’è un SOC

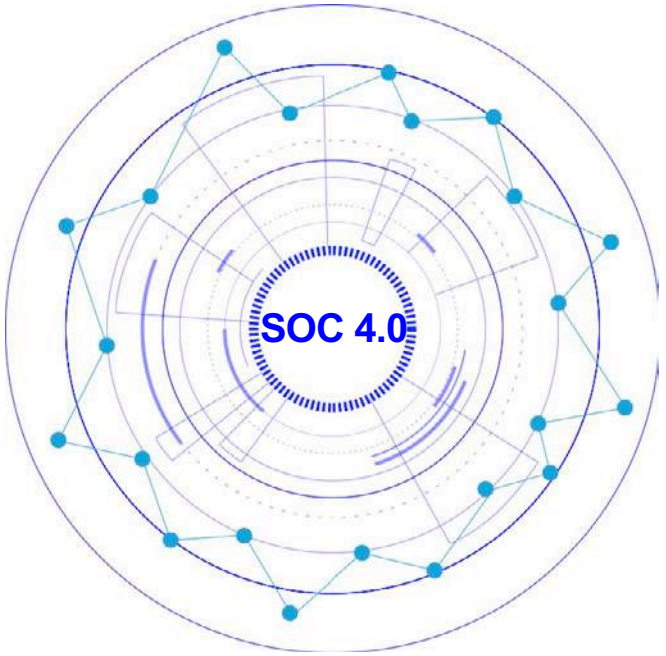

HR
Processes
Technologies
C SOC
Proactive
Monitoring
PREVENTION
REACTION
IDENTIFICATION

VARGROUP

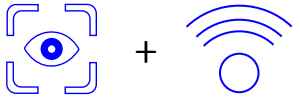
Cognitive SOC

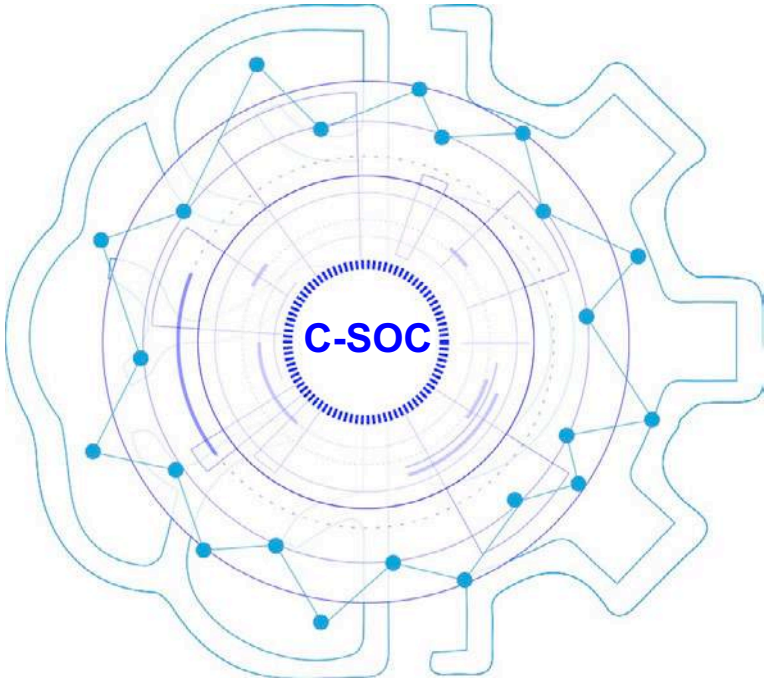


Security Operation Center



Security Operation Center 4.0





Cognitive Security Operation Center

Strategia di difesa

OBIETTIVI

Proteggere gli asset e le informazioni

Fornire l'analisi proattiva degli eventi intercorsi all'interno dell'infrastruttura IT

Individuare e rispondere agli incidenti di sicurezza

Fornire supporto alla business continuity

Garantire robustezza alla infrastruttura IT e ai servizi di business

SOLUZIONI

Monitorare, analizzare, correlare e segnalare gli eventi di sicurezza

Implementare meccanismi adeguati di risposta agli incidenti: Protect, Detect, Respond

Implementare le procedure di Incident Management e di Analisi Forense

Fornire supporto in caso di Crisis Operations

REQUISITI DI EFFICACIA

Supportare la compliance a standard, leggi e regolamenti

Proteggere le informazioni sensibili e garantire la privacy

Permettere all'Azienda di individuare e provare chi ha effettuato una operazione e quando

Gestire la sicurezza operativa in maniera efficace, efficiente e misurabile

Fornire una fotografia in real-time che sia reale (e non solo percepita) sul livello di sicurezza

Integrarsi con fonti di knowledge esterni che forniscono cybersecurity intelligence

Essere integrato con i servizi di business e in particolare supportare i processi di Risk Management

Sicurezza fisica

Sito di controllo operativo presso sede Yarix

- Controllo accessi fisici
- Videosorveglianza
- Presidio 24x7

Sito data center presso sede Var Group

- Data Center certificato ISO 27001 e basato sulle linee TIER 3
- Controllo accessi fisici
- Videosorveglianza
- Presidio 24x7

Organizzazione del servizio

Interazione diretta con
Team CERT Yarix:

- ✓ Incident management
- ✓ Forensic
- ✓ Ethical Hacking

monitoraggio degli eventi sulla Console del Sistema SIEM

gestione dell'Infrastruttura SIEM (manutenzione/aggiornamenti)

analisi su **eventi di sicurezza**, classificazione e assegnazione delle priorità

analisi dei **security bulletin** diramati da CERT nazionali o internazionali

stesura di **report** periodici

implementazione e gestione di tecnologie in ambito **Cyber Security** (es. SIEM)

analisi approfondita su alcuni specifici eventi di sicurezza

interventi di **ottimizzazione sull'infrastruttura SIEM** (es. attivazione di una nuova regola di correlazione o integrazione di nuovi Log Source)

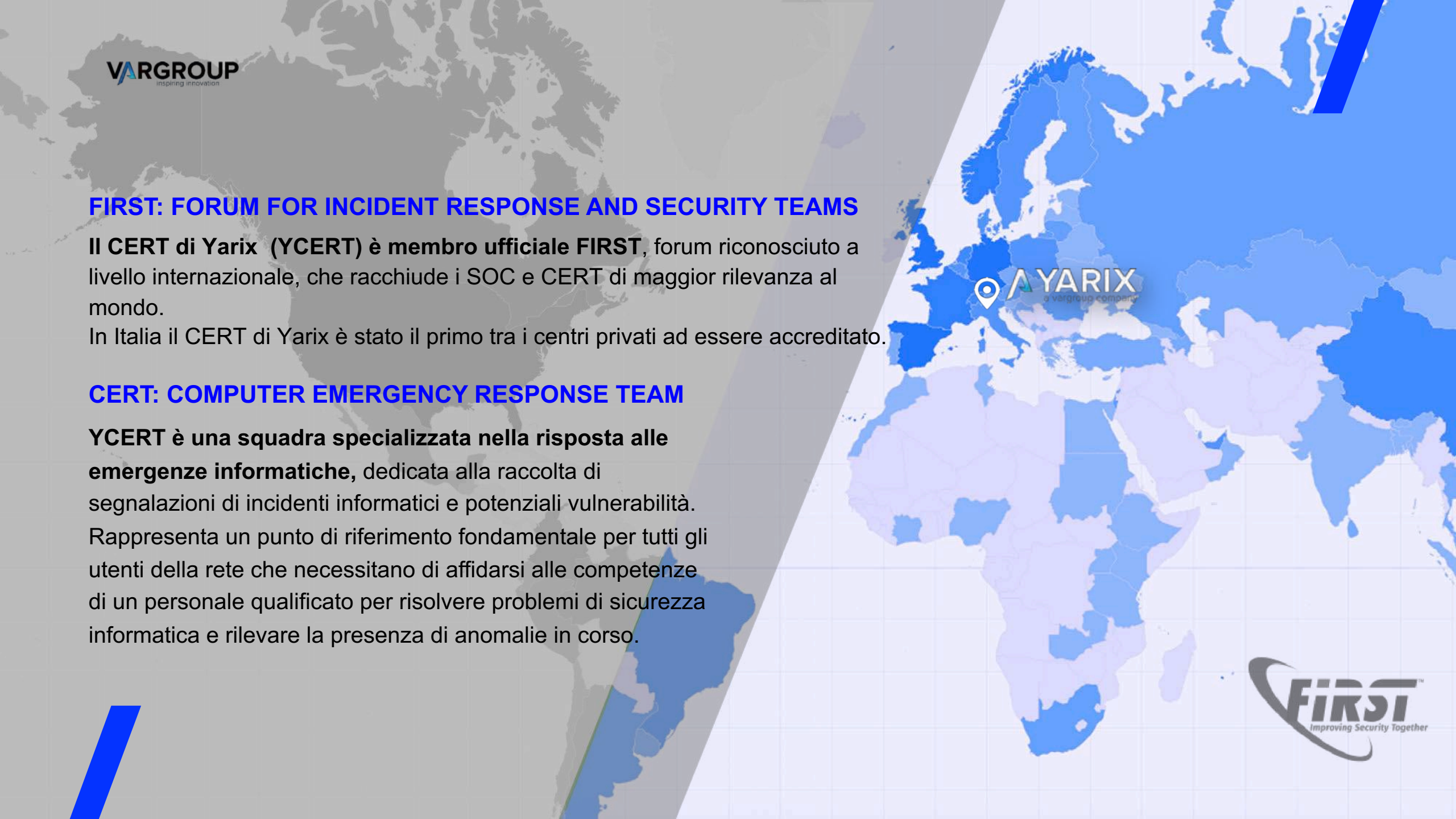
attività di **Security Assessment** (es. VA o PT)

FIRST: FORUM FOR INCIDENT RESPONSE AND SECURITY TEAMS

Il CERT di Yarix (YCERT) è membro ufficiale FIRST, forum riconosciuto a livello internazionale, che racchiude i SOC e CERT di maggior rilevanza al mondo.
In Italia il CERT di Yarix è stato il primo tra i centri privati ad essere accreditato.

CERT: COMPUTER EMERGENCY RESPONSE TEAM

YCERT è una squadra specializzata nella risposta alle emergenze informatiche, dedicata alla raccolta di segnalazioni di incidenti informatici e potenziali vulnerabilità. Rappresenta un punto di riferimento fondamentale per tutti gli utenti della rete che necessitano di affidarsi alle competenze di un personale qualificato per risolvere problemi di sicurezza informatica e rilevare la presenza di anomalie in corso.



Accordo tra Polizia di Stato e Yarix

Treviso, 27 luglio 2016

Prevenzione e contrasto ai crimini informatici per la difesa delle infrastrutture critiche al centro dell'accordo tra Polizia di Stato e Yarix.

Un accordo importante e strategico che prende le mosse dalla necessità di garantire un'elevata sicurezza al Paese e al suo sistema economico e sociale, ormai fortemente dipendente dallo spazio cibernetico, mediante la **cooperazione mirata, di pubblica utilità, tra lo Stato ed i privati**, così come previsto dal Quadro Strategico Nazionale e dal Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica.

VARGROUP

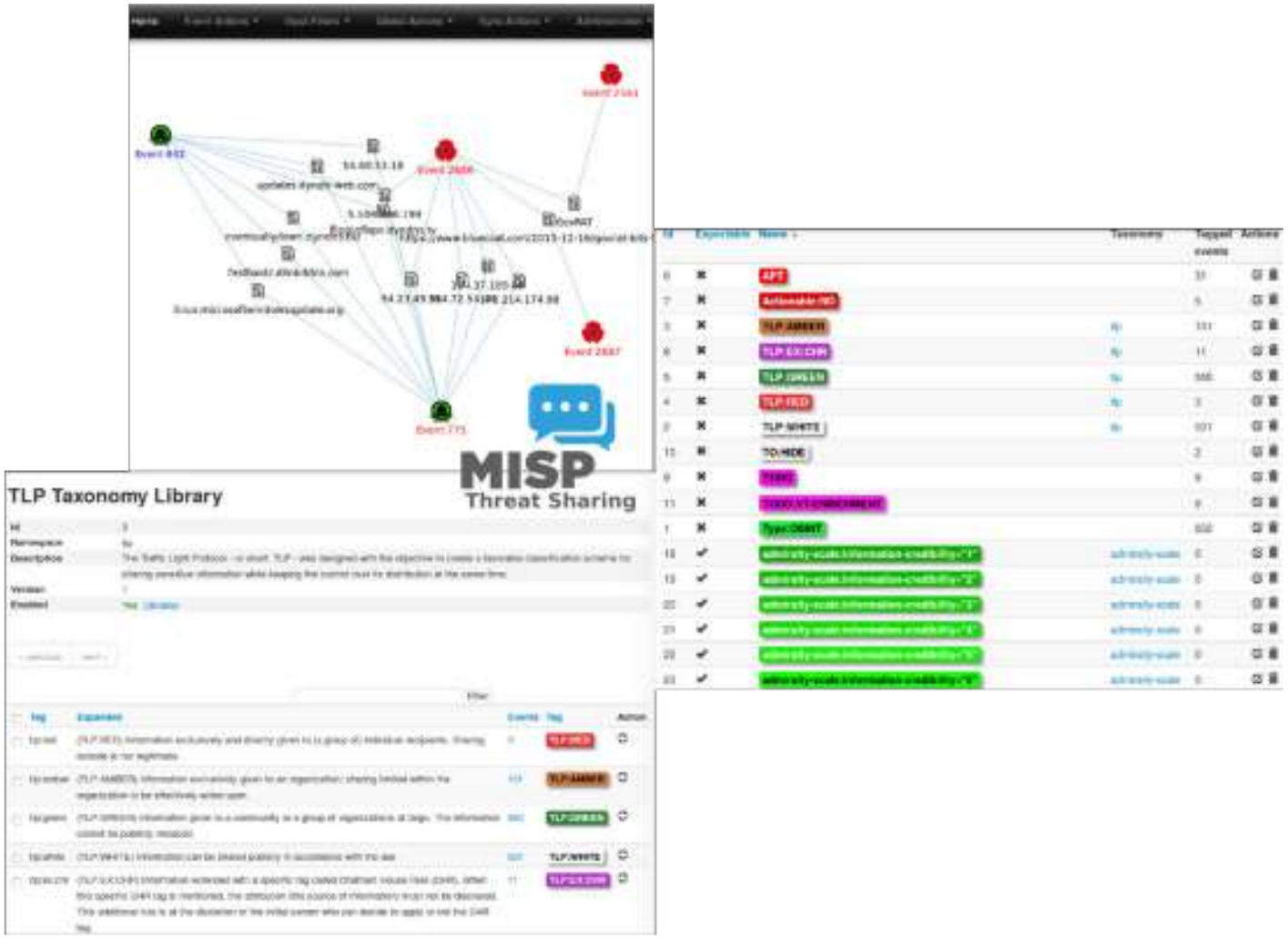
Integrazione dati Threat Intelligence

- ✓ Un database di IOC (IP, URL, hash, mutex, scam e-mail, nomi di dominio, etc…) ed indicatori per archiviare informazioni tecniche e non riguardo malware, attaccanti ed incidenti ➔ integrate nel SOC permettono di aggiungere **contesto** per individuare sistemi compromessi o identificare errori che si concretizzano in minacce
- ✓ Correlazione automatica tra attributi ed indicatori provenienti da malware, campagne o da attività degli analisti ➔ repository di IOC integrata nel SIEM per sollevare offense con elevata specificità
- ✓ Possibilità di condivisione secondo policy di disclosure definite e differenziate tra colleghi e partner ➔ sharing is caring!
- ✓ Tassonomia personalizzabile per classificare ed applicare tag ➔ attinenza personalizzata per ciascun ambito

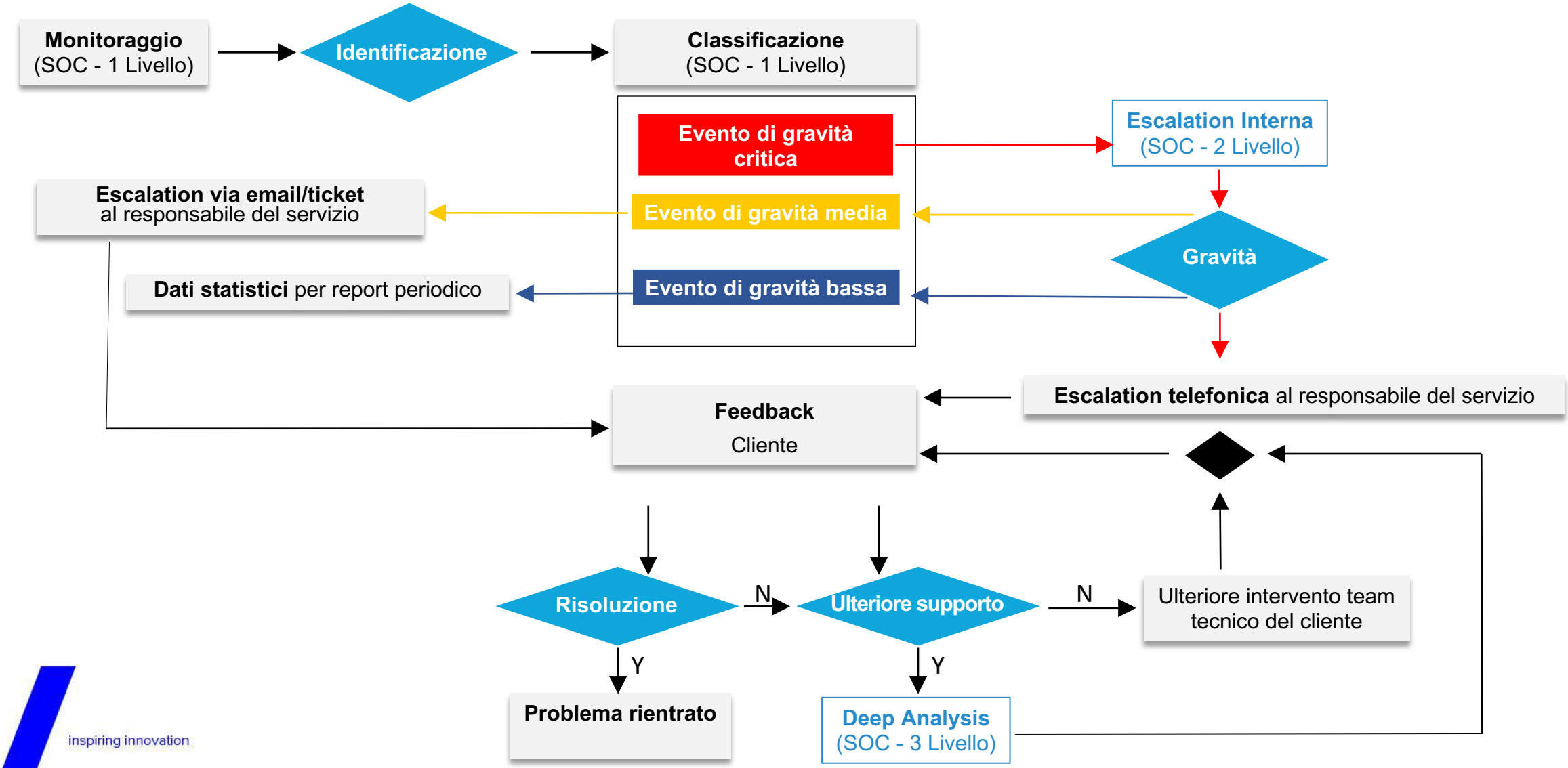
Integrazione dati Threat Intelligence

L'elenco degli IOC, forniti anche dalla Cyber Intelligence Division, sono integrati in near real time all'interno del SIEM, consentendo al SOC di:

- ✓ **individuare o fermare** il transito di dati, la visualizzazione di pagine, l'arrivo di mail sospette
- ✓ **salvaguardare la salute delle rete** aziendale e/o individuare quelle risorse ormai corrotte/compromesse che vanno quindi isolate e messe in sicurezza



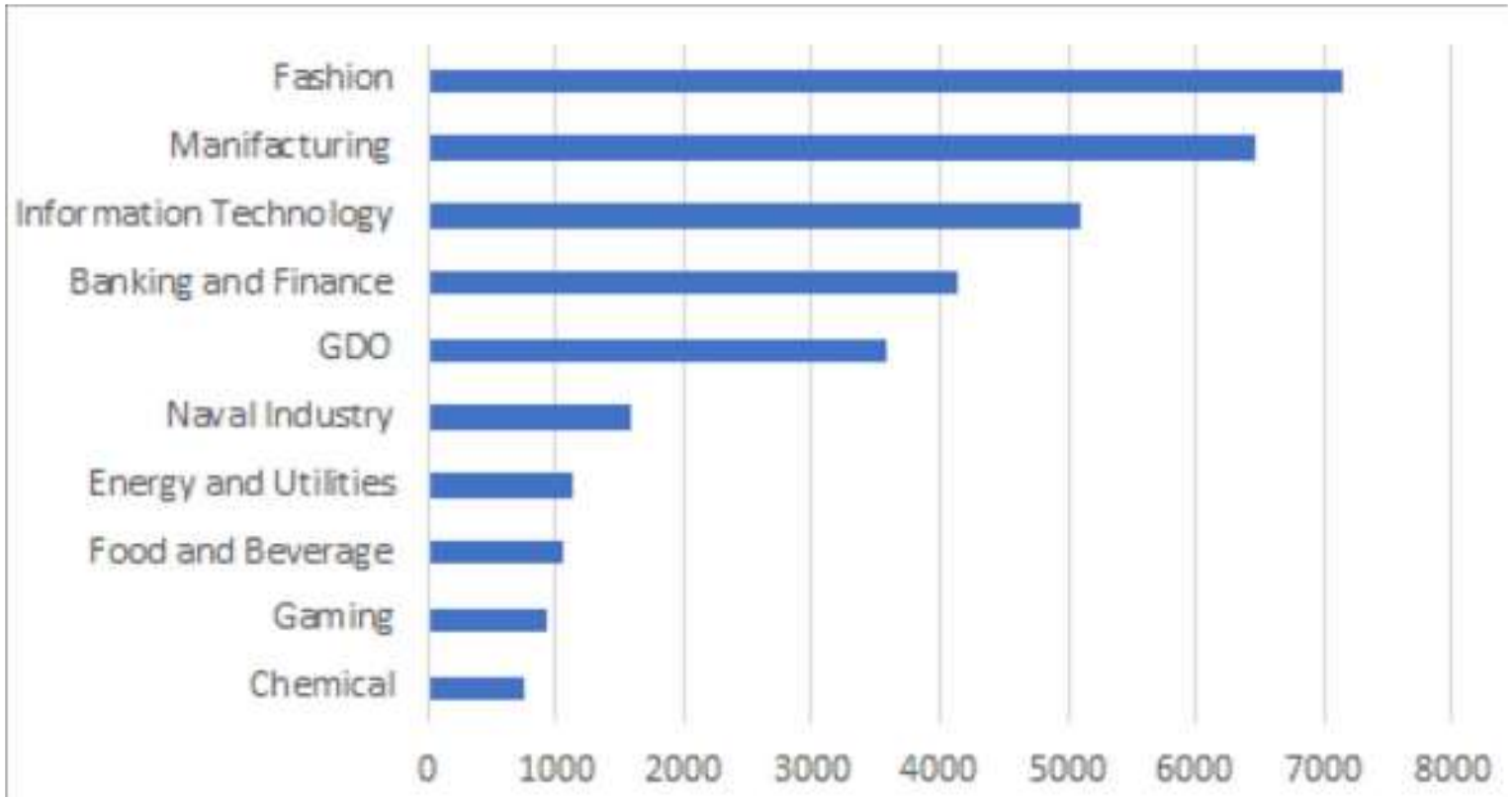
Esempio di workflow implementato



VARGROUP

SOC statistics

Casi per industry gestiti 2018



40.000 +
Managed Cases

12.000 +
Security Events Notified

3.000 +
True Positives

VARGROUP

SOC 4.0

VARGROUP

Minacce

ATTACCHI INTERNI

- ✓ **63%**: incidenti nel 2015 causati da impiegati malintenzionati
- ✓ Azienda australiana per lo smaltimento delle acque reflue ha disabilitato le funzioni SCADA causando la fuoriuscita di **800,000 litri di liquame**

MALWARE DI STATO

- ✓ La rete elettrica ucraina è stata violata lasciando **un quarto di milione di persone al buio**
- ✓ Corea del Nord accusata di aver violato i **sistemi dei trasporti pubblici** della Corea del Sud
- ✓ Iran accusato di aver violato il **sistema di controllo di una diga** dello stato di New York

TERRORISTI, CYBERCRIMINALI e HACKTIVISTI

- ✓ Un membro di Al Qaeda ha lavorato in cinque diverse centrali nucleari
- ✓ Hacktivisti siriani accusati di aver violato un impianto statunitense per la purificazione delle acque, modificando le quantità di sostanze chimiche nell'acqua

Contrasto all’impersonificazione

Identifica i fingerprint nei segnali

Valida la loro integrità e autenticità

Identifica l’apparecchiatura compromessa e i dati falsificati

Utilizza algoritmi di machine learning istruiti per riconoscere alterazioni ai dati rilevati e modifica in tempo reale gli stessi

Utilizza algoritmi per ricostruire in real time lo stato reale di un sistema

Consente la conoscenza dello stato reale permettendo all’operatore di adottare tempestivamente le azioni correttive necessarie

Rileva injection di nuovi dati artificiali, riproduzione di dati storici e alterazioni in linea dei dati raccolti (es: moltiplicando il segnale per un fattore)

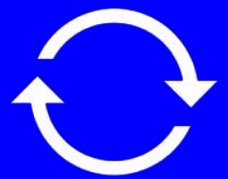
Ogni sistema fisico possiede un unico fingerprint

Algoritmi avanzati apprendono i fingerprint in oggetto

Connessione in modo non intrusivo nel sistema di monitoraggio esistente

Utilizzo del fingerprint per identificare i dati alterati e dare immediato allarme all’operatore dell’impianto

Ripristino dei valori reali dei dati alterati



VARGROUP


BLOCKCHAIN
CYBER INTELLIGENCE
PSD2
ANTI PHISHING
C SOC
PCI-DSS
ANTI-FRAUD
SECURITY ASSESSMENT
AI

www.vargroup.it