Faccia a faccia con la Cybersecurity

SOC ed approccio Continuous Monitoring

Roberto Obialero, GPPA, GCFA, ISO 27K LA - ADS
Matteo Galimberti, Senior Manager KPMG Advisory
Simone Campera, IT Security & Compliance Manager – Amplifon
Fabio Bucciarelli, CISSP, GCFA, CEH – Regione Emilia Romagna

Oracle Community For Security

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

C4S PUBBLICAZIONI DI SECURITY

ROSI RETURN ON SECURITY INVESTMENT

Return on Security Investments
È un supporto decisionale rivolto a quanti sono in posizioni di responsabilità sul settore ICT delle organizzazioni, e devono allocare in modo prudente delle risorse scarse nell'ambito della Sicurezza.

FSE SECURITY

Fascicolo Sanitario Elettronico
Una disamina degli aspetti di compliance e delle misure di sicurezza nell'ambito sanitario ed in particolare per la realizzazione del Fascicolo Sanitario Elettronico e del Dossier Sanitario

PRIVACY ON CLOUD&MOBILE

Privacy on Cloud and Mobile
Due studi separati su cosa deve fare un'azienda italiana titolare dei trattamenti in logica privacy, prima, durante e dopo l'adozione di servizi Cloud o l'uso di dispositivi Mobile

SICUREZZA E SOCIAL MEDIA

Sicurezza e social media
Una guida per le aziende che vogliono comprendere gli aspetti di sicurezza dei social media; per sapere che le ciliege hanno il nocciolo.

100 GIORNI SICUREZZA INFORMAZIONI

I primi 100 giorni del Responsabile della Sicurezza delle Informazioni
Una serie di raccomandazioni per il neo assunto o neo incaricato Responsabile della Sicurezza delle Informazioni; per riuscire a fare prima le cose più importanti od urgenti.

FRODI ICT

Le frodi nella rete
Questo documento parla del duplice ruoto dell'IT, da una parte come misura di contrasto e dall'altra, quando mal configurato o mal progettato ne permette l'attuazione

MOBILE ENTERPRISE SICUREZZA IN MOVIMENTO

Mobile Enterprise: sicurezza in movimento
Indicazioni per un percorso aziendale per la creazione della Mobile Enterprise per un utilizzo consapevole dei dispositivi mobili e del cloud in azienda.

SOC ed approccio Continuous Monitoring

#ISCMSOC

URI: https://iscmsoc.clusit.it/

SOC e Continuous Monitoring faccia a faccia con la Cybersecurity

- Perchè questo titolo?
- A chi si rivolge
- Perché adottare processi e soluzioni di Continuous Monitoring?
- Autori
- Download
- Altri lavori disponibili

SOC ed approccio Continuous Monitoring

Editor e team leader

Giovanni Belluzzo, Security Manager, Responsabile Risk & Internal Audit - CISA, CISM - InfoCert.
Fabrizio Bulgarelli, Partner - Head of RAS and IT Services - RSM
Francesca Gatti, Coordinatrice del GdL Osservatorio Sicurezza e Compliance, Segretario Generale e Tesoriere - CISA, CIGIT – AUSED
Roberto Obialero, Senior Cybersecurity Advisor - ADS Gruppo Finmatica; CTS Clusit
Alessandro Vallega, Security Bus.Dev.; CD Clusit; Coordinatore Community for Security - Oracle
Mauro Verderosa, CISSP - Identity and Access Management Specialist, CEO at PSYND & founder of Swiss-CyberSecurity.ch

SOC ed approccio Continuous Monitoring

Autori e contributori

Elena Agresti; Senior Information Security Expert, Global Cybersecurity Center - GCSEC Global Cybersecurity Center
Davide Ariu; - Pluribus One
Domenico Billè; Security Solution Specialist – Oracle
Manfredi Blasucci; IT Security Manager - Auchan Retail Italia
Gianluca Bocci; Security Professional Master - Poste Italiane
Claudio Brisa; IT and Physical Security at Creval Sistemi e Servizi GCV – Creval
Fabio Bucciarelli; IT Security Manager - Regione Emilia Romagna
Giancarlo Butti; Internal Auditor - Europrivacy
Dario Carnelli; Advisory - Codd&Date Suisse
Alessandro Cavaliere; Security Analyst - ADS Gruppo Finmatica
Marco Ceccon; Advisory Practice Manager - Sinergy SpA, Lutech Group
Domenico Cuoccio; Responsabile Ufficio Qualità e Sicurezza dei Sistemi Informativi InnovaPuglia
Elena Esposito; Metropolitan operative center manager - Manpower
Valentina Falcioni; Channel Marketing Specialist – Oracle
Enrico Ferretti; Managing Director – Protiviti
Matteo Galimberti; Senior Manager IT Advisory, Information Risk Management - KPMG Advisory S.p.A.
Michele Gallante; Security Consultant – Alfagroup
Carlo Guastone; Vicepresidente Business Development - Sernet spa
Francesco Iorfida; Manager – EY
Andrea Longhi; Consulente Direzionale – ConsAL
Andrea Mariotti; Associate Partner – EY
Paola Meroni; Information Security Expert - Vodafone Automotive
Giuseppe Russo; Master Principal Sales Consultant & Chief Technologist – Oracle
Corrado Salvemini; Resp. Sicurezza delle informazioni - Carrefour Italia
Marco Sanseverino; Security Manager – KPMG
Fabio Saulli; Principal Security Consultant – Alfagroup
Erika Sciunzi; Principal Sales Consultant – Oracle
Giulio Spreafico; Consulente e Auditor di Sistemi Informativi – AIEA
Enrico Toso; IT Regulatory Risk Specialist - DB Consorzio

SOC ed approccio Continuous Monitoring

Sezione I - Presupposti e contesto di applicazione

… cosa troverete nella pubblicazione

SOC ed approccio Continuous Monitoring

Sezione II - Applicazione ed integrazione con i processi di Security Governance

SOC ed approccio Continuous Monitoring

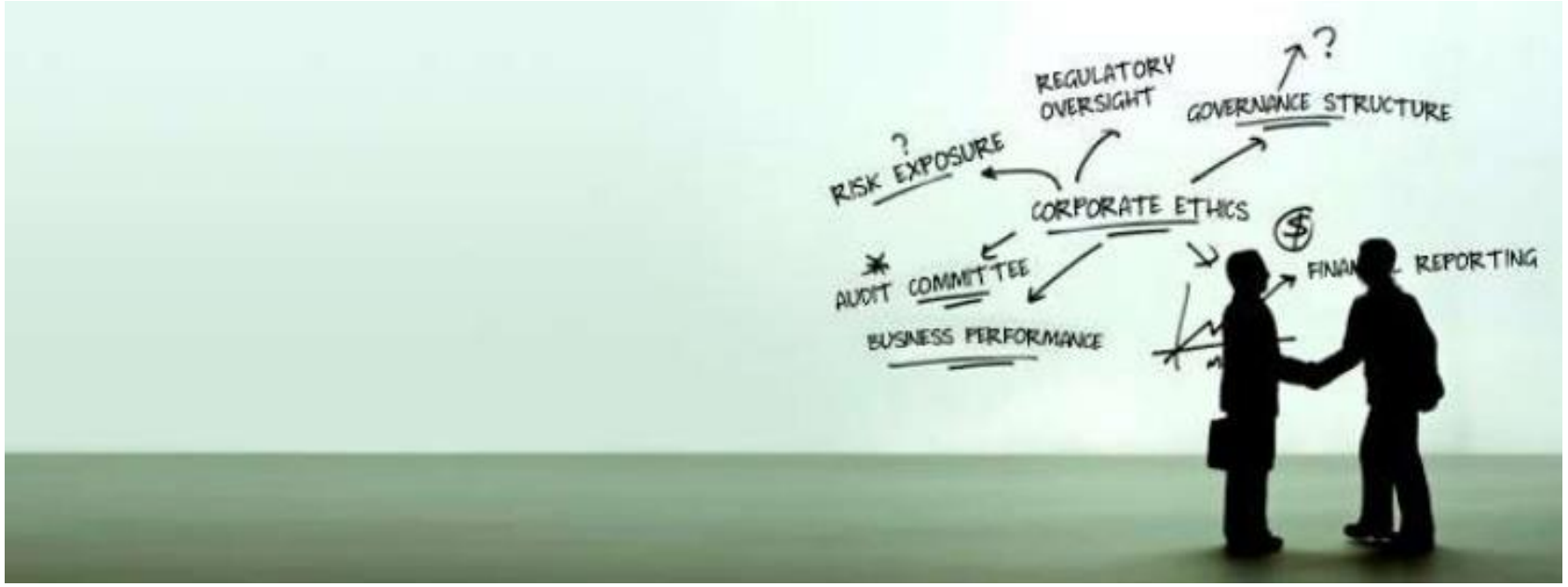
Sezione III - Utilizzo nell'ambito dei servizi SOC

SOC ed approccio Continuous Monitoring

Sezione IV - Integrazione con ulteriori misure organizzative e tecnologiche

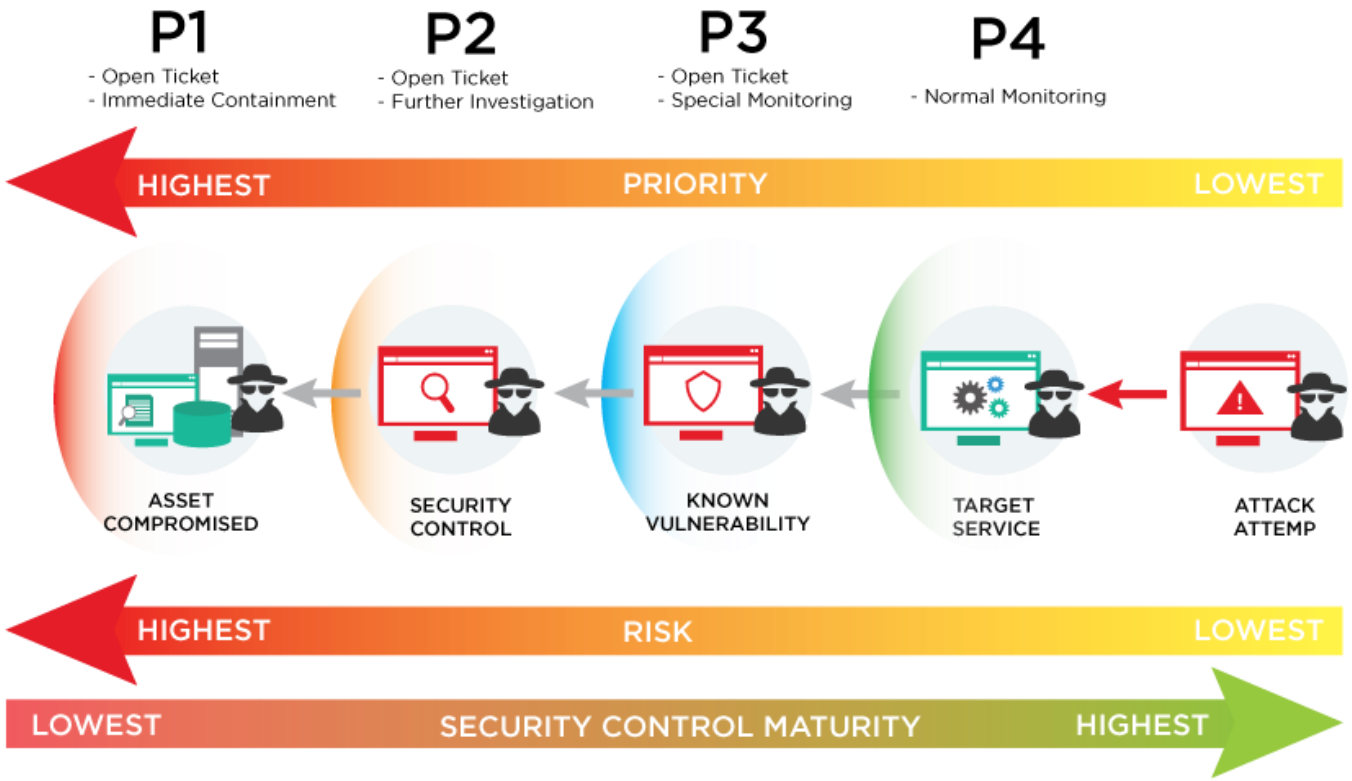
SOC ed approccio Continuous Monitoring

Integrazione del processo di analisi dei rischi



SOC ed approccio Continuous Monitoring

Integrazione del processo di analisi dei rischi



SOC ed approccio Continuous Monitoring

Integrazione del processo di incident management

SOC ed approccio Continuous Monitoring

…e se il SOC è esterno?

Punti focali:

- **Definizione del perimetro**: strutture, società coinvolte, infrastruttura tecnologica, etc
- **Definizione dei servizi "base"**: supporto 1° – 2° livello, reporting, KPI, etc
- **Definizione dei servizi "avanzati"** (on demand): threat intelligence, vulnerability assessment / management / penetration test, campagne phishing, asset inventory / management,
- **Definizione modalità operative**: SLA, procedure mitigazione / rientro, garanzie, penali, etc.
- **Definizione dei processi**: risk management, incident response, escalation, etc.

SOC ed approccio Continuous Monitoring

L'esperienza di Amplifon: SOC as a service

Vantaggi:

- *Basso investimento iniziale: hardware e software sono del fornitore*
- *Scalabilità e flessibilità del servizio*
- *Servizio attivo 24x7*
- *Disponibilità di personale esperto*
- *Responsabilità scalate al fornitore tramite SLA*
- *Forte esperienza del fornitore, basata su più clienti e in segmenti di settore simili*
- *Minor rischio di collusione potenziale tra team di monitoraggio e attaccanti*

SOC ed approccio Continuous Monitoring

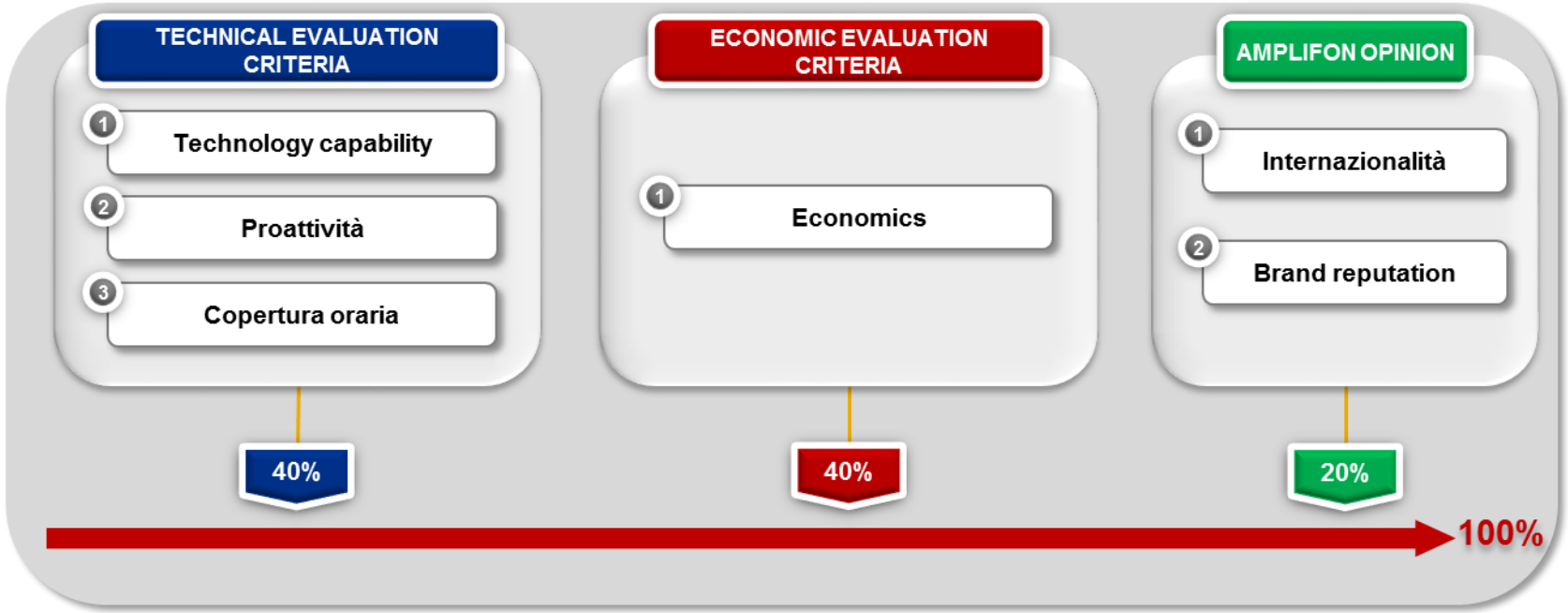
L'esperienza di Amplifon: SOC as a service

Svantaggi:

- *Mancanza di conoscenza diretta dell'ambiente monitorato*
- *Mancanza di personale dedicato a un singolo cliente*
- *Rischi dovuti all'esternalizzazione dei dati*
- *Informazioni non sempre (facilmente) a disposizione / fruibili*
- *Mancanza di personalizzazione*
- *Carenza di Governance*

SOC ed approccio Continuous Monitoring

L'esperienza di Amplifon: una nuova scelta



SOC ed approccio Continuous Monitoring

Il SIEM: dalla centralizzazione nella raccolte dei singoli eventi sino alla loro presentazione in forma correlata

Selezione delle fonti di informazione e pianificazione del loro periodo di conservazione

Tipologia delle tipologie di eventi da raccogliere, da analizzare e da correlare

SOC ed approccio Continuous Monitoring

Ausilio della piattaforma SOC nelle investigazioni di tipo Digital Forensics

La Digital Forensics

- Collezione
- Esame
- Analisi
- Reporting

Utilizzo del SIEM all'interno del processo forense

- Raccolta e conservazione sicura degli eventi di tutti i dispositivi
- Strumenti di ricerca avanzata

Integrazione con sistemi di incident response

SOC ed approccio Continuous Monitoring

Evoluzione del servizio attraverso l'integrazione con strumenti di Threat Intelligence e Active Defense

La Threat Intelligence

- Secondo il NIST: «*l'insieme di dati raccolti, valutati ed applicati riguardanti minacce alla sicurezza, attori delle minacce, exploit, malware, vulnerabilità ed indicatori di compromissione*»

Benefici

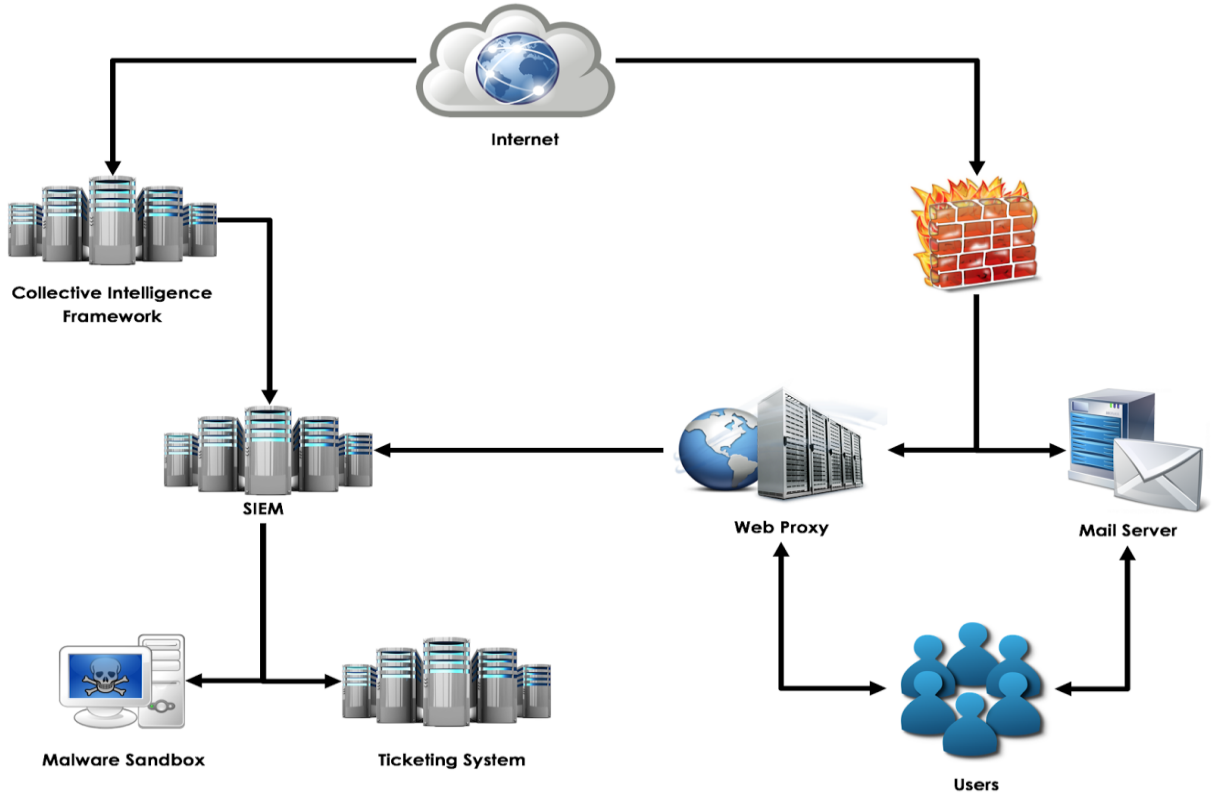
- Riconoscere in tempi stretti gli indicatori di attacco
- Rispondere adeguatamente a minacce con grande impatto
- Fornire ai SIEM solo informazioni utili e pulite

Condivisione della Threat Intelligence

- Necessità di linguaggi e protocolli comuni per facilitare lo scambio e il trattamento automatico delle informazioni

SOC ed approccio Continuous Monitoring

Usecase: Collective Intelligence Framework



SOC ed approccio Continuous Monitoring

La nuova frontiera: tecnologie basate sul Machine Learning

Utilizzo conveniente per la soluzione di problemi in cui è complesso scrivere un algoritmo che ne contenga la soluzione

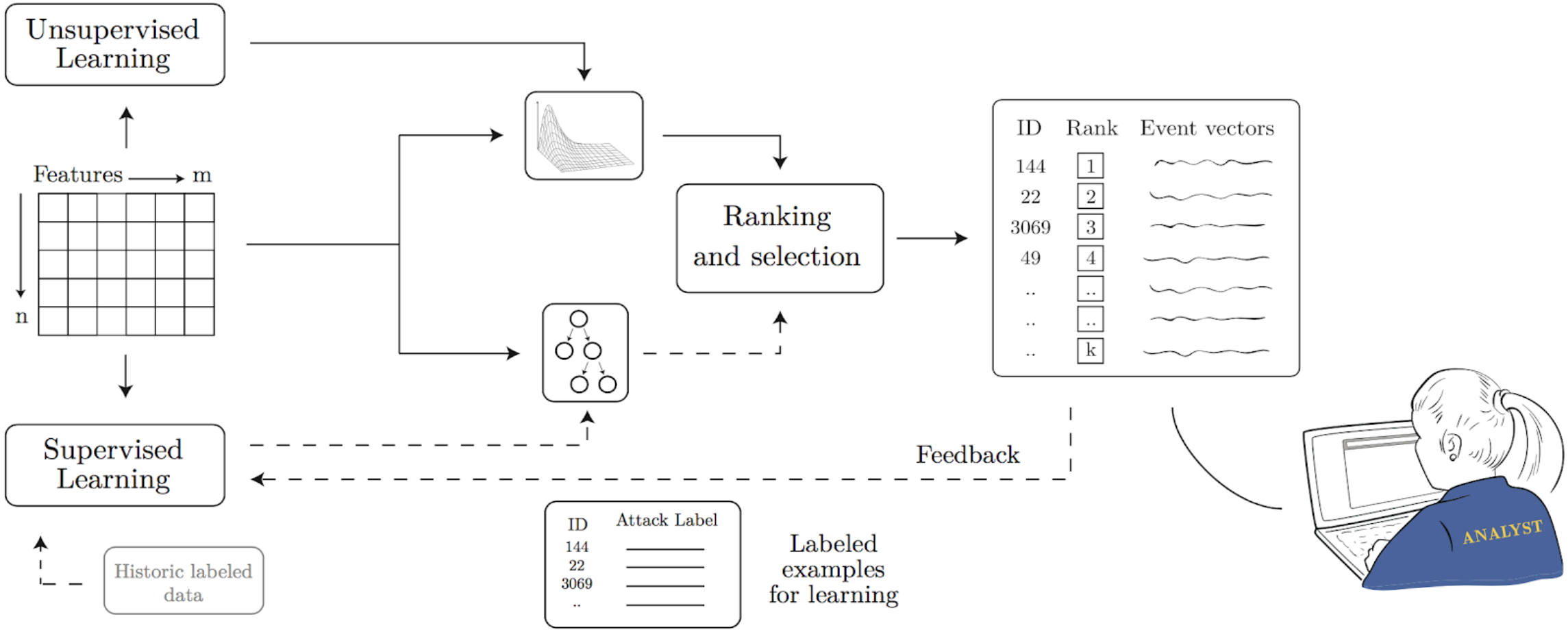
Benefici dell'utilizzo del ML in ambito cybersecurity

- Disponibilità di soluzioni che che consentono di generare, immagazzinare, e anche di analizzare elevati volumi di dati
- Può in parte compensare la mancanza di professionalità specifiche in ambito cybersecurity

Rischi dell'utilizzo del ML in ambito cybersecurity

- Utilizzo della tecnologia in ambiente ostile
- Tecnologia poco «trasparente»
- Sottovalutazione della necessità di dotarsi di personale formato

SOC ed approccio Continuous Monitoring



Fonte: K. Veeramachaneni, et al. “AI2: Training a big data machine to defend”
https://people.csail.mit.edu/kalyan/AI2/

Grazie per l’attenzione …

r.obialero@ads.it
matteogalimberti@kpmg.it
simone.campera@amplifon.com
fabio.bucciarelli@regione.emilia-romagna.it