



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

CUS PUBBLICAZIONI DI SECURITY



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.



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 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

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



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.



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

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 



Licenza Creative Commons: Attribuzione Condividi allo stesso modo 3.0

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

SOC e Continuous Monitoring faccia a faccia
con la Cybersecurity

Perché questo titolo?

A chi si rivolge

Perché adottare processi e soluzioni di
Continuous Monitoring?

Autori

Download

Altri lavori disponibili



Cover illustrated by Lorenzo Della Giovanna.

Oracle Community For Security



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 Cecon; 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

| | |
|---|----|
| ISCM introduzione..... | 12 |
| Perché adottare processi e soluzioni di Continuous Monitoring? | 12 |
| Come funzionerebbe..... | 12 |
| Principali benefici | 13 |
| Normative e Standard di riferimento..... | 13 |
| Guida pratica Normative-Framework-Standard | 14 |
| Prerequisiti organizzativi e tecnologici del Continuous Monitoring..... | 15 |
| Politica di Log Management..... | 15 |
| Sinergia tra diverse funzioni interne..... | 15 |
| Maturità Cybersecurity | 15 |
| Gestione delle vulnerabilità | 15 |
| Analisi dei rischi | 16 |
| Approccio orientato alla difesa..... | 16 |
| Team dedicato alla gestione operativa della sicurezza | 16 |
| Commitment aziendale | 17 |

**... cosa troverete
nella pubblicazione**

SOC ed approccio Continuous Monitoring

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

| | |
|--|----|
| Vulnerability Management..... | 18 |
| Applicazione del Continuous Monitoring al processo di Vulnerability Management | 18 |
| Gestione delle priorità nell'attività di remediation e piani di rientro | 20 |
| Applicazione ai processi di rilevazione di violazione delle policy aziendali e degli attacchi | 23 |
| Integrazione con i processi di analisi dei rischi e di gestione degli incidenti di sicurezza | 25 |
| Rischi di Cybersecurity e Progetto CM (Continuous monitoring)..... | 26 |
| Integrazione del processo di analisi del rischio e incident management | 27 |

SOC ed approccio Continuous Monitoring

Sezione III - Utilizzo nell'ambito dei servizi SOC

Strumenti di attuazione e gestione dei processi di Continuous Monitoring: la struttura

| | |
|---|----|
| SOC..... | 28 |
| SOC e processi di gestione - Generalità..... | 28 |
| Modello Organizzativo del SOC..... | 28 |
| Strumenti di sicurezza in gestione al SOC..... | 29 |
| Processo di gestione degli alert..... | 29 |
| Differenze e complementarità negli obiettivi tra i due strumenti di gestione operativa: | |
| SOC e NOC..... | 30 |
| Gli Operation Center..... | 30 |
| Il Network Operation Center..... | 31 |
| Il Security Operation Center..... | 31 |
| Organizzazione e competenze necessarie per garantire l'operatività di un SOC..... | 32 |
| Tematiche HR in ambito SOC..... | 33 |
| Peculiarità e differenze di un servizio interno aziendale rispetto ad uno rivolto ai clienti esterni..... | 35 |
| Principali rischi e minacce..... | 38 |
| Funzionalità e caratteristiche da tener conto se ci si affida ad un SOC esterno..... | 44 |

| | |
|--|----|
| SIM versus SIEM: dalla centralizzazione nella raccolta dei singoli eventi sino alla loro presentazione in forma correlata..... | 46 |
| Selezione delle fonti di informazioni da raccogliere e pianificazione del loro periodo di conservazione..... | 48 |
| Informazioni disponibili per le varie tipologie di asset..... | 49 |
| Dispositivi di sicurezza..... | 49 |
| Sistemi operativi..... | 50 |
| Applicazioni web o web service..... | 50 |
| Selezione delle tipologie di eventi da raccogliere, da analizzare e da correlare..... | 51 |
| Operazioni preliminari..... | 51 |
| Cancellazione delle tracce..... | 52 |
| Mantenimento dell'accesso..... | 53 |
| Esfiltrazione dei dati..... | 53 |
| Monitoraggio del livello di servizio tramite definizione di indicatori KPI ed acquisizione di statistiche..... | 53 |
| Definizione di una baseline nel ciclo normale di attività del sistema informativo sotto monitoraggio..... | 56 |

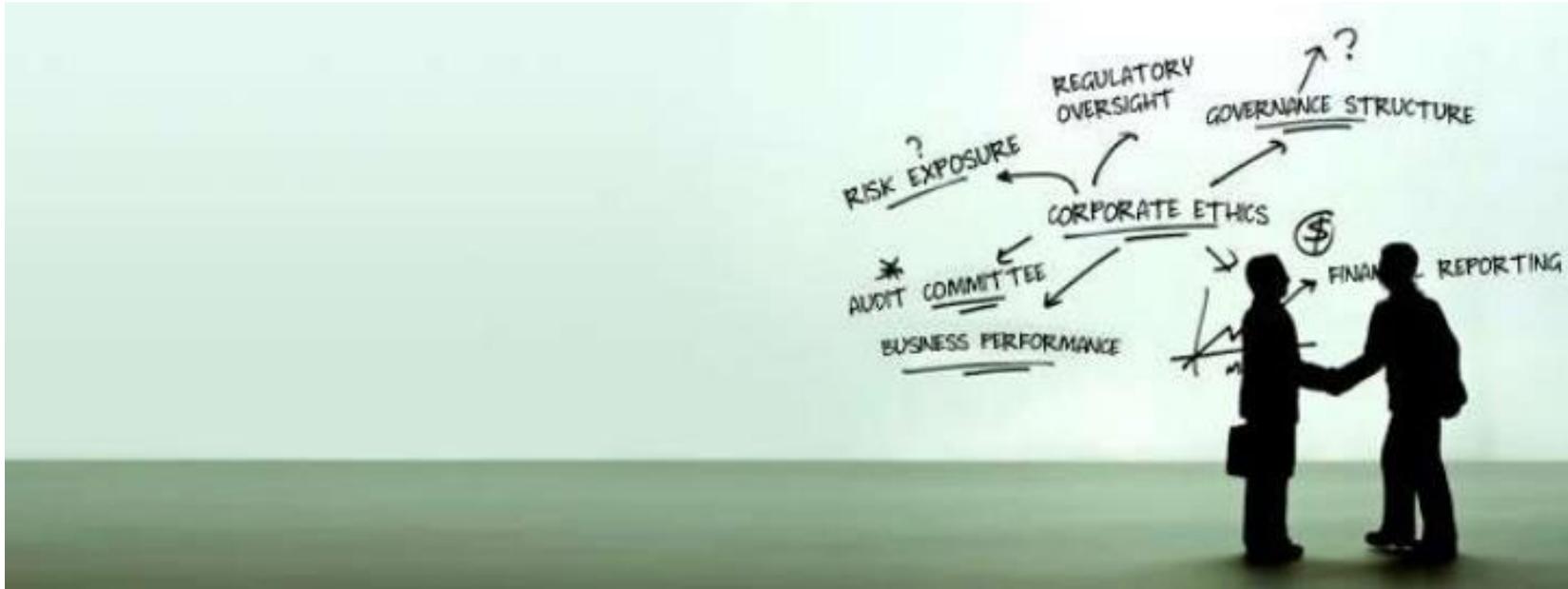
SOC ed approccio Continuous Monitoring

Sezione IV - Integrazione con ulteriori misure organizzative e tecnologiche

| | |
|---|----|
| La nuova frontiera: soluzioni tecnologiche basate sul Machine Learning | 59 |
| Consolidamento del processo di analisi e possibili servizi fruibili da parte di altri reparti ICT..... | 63 |
| SIEM come parte di un framework..... | 63 |
| Ausilio della piattaforma SOC nelle investigazioni di tipo Digital Forensics | 64 |
| Cos'è la Digital Forensics | 64 |
| Utilizzo del SIEM all'interno del processo di analisi forense | 65 |
| Integrazione con sistemi di incident response | 66 |
| Evoluzione del servizio attraverso integrazione con strumenti di Threat Intelligence ed Active Defence | 67 |
| Soluzioni di Threat Intelligence | 67 |
| Usecase: Collective Intelligence Framework | 69 |
| Quali sono i servizi offerti da CERT/CSIRT/ISAC | 70 |
| L'importanza dell'adozione di pratiche di information sharing con strutture analoghe. 73 | |
| Approfondimento sul Traffic Light Protocol | 74 |
| Direttiva (UE) 2016/1148 del Parlamento Europeo e del Consiglio, 6 luglio 2016... 74 | |
| Divulgazione Coordinata e Responsabile delle Vulnerabilità Informatiche | 75 |
| Introduzione alla divulgazione responsabile delle vulnerabilità | 76 |
| Benefici e vincoli del meccanismo | 76 |
| Iniziativa Olandese del Manifesto | 77 |

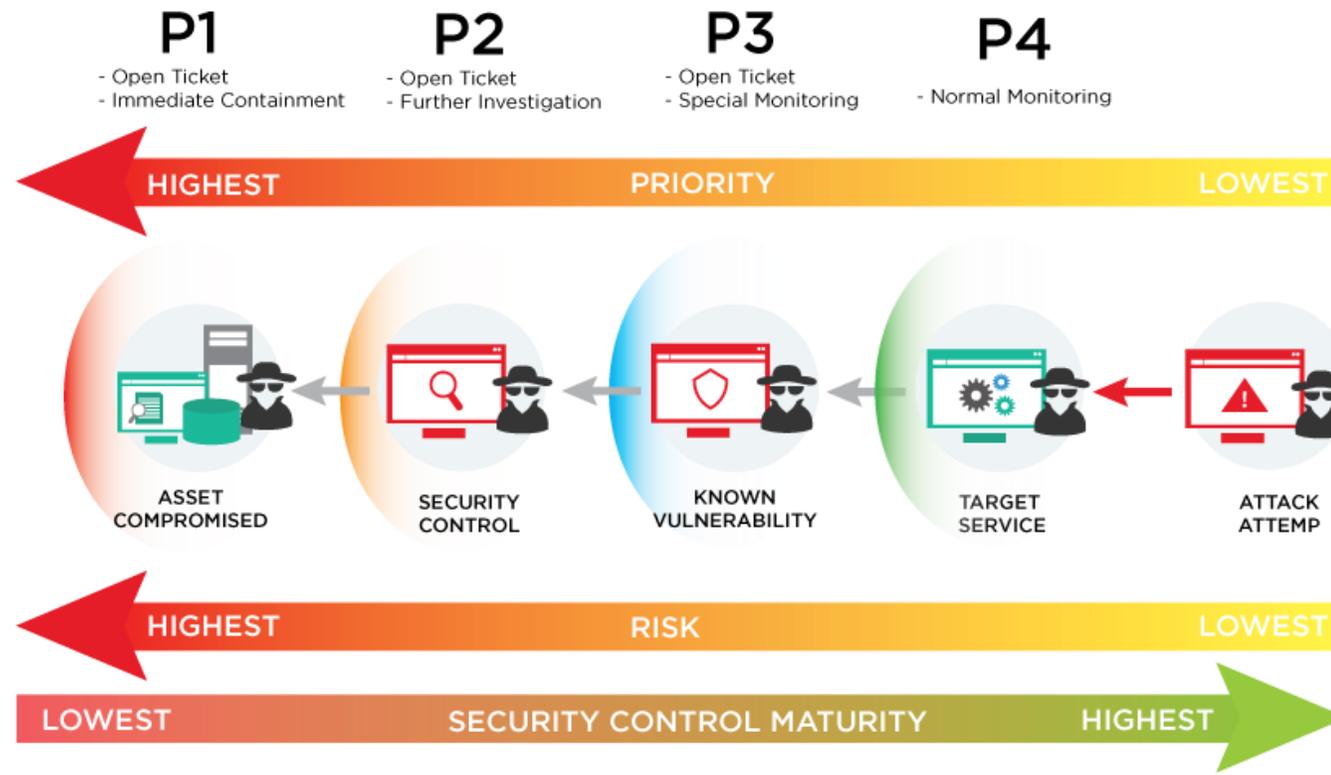
SOC ed approccio Continuous Monitoring

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

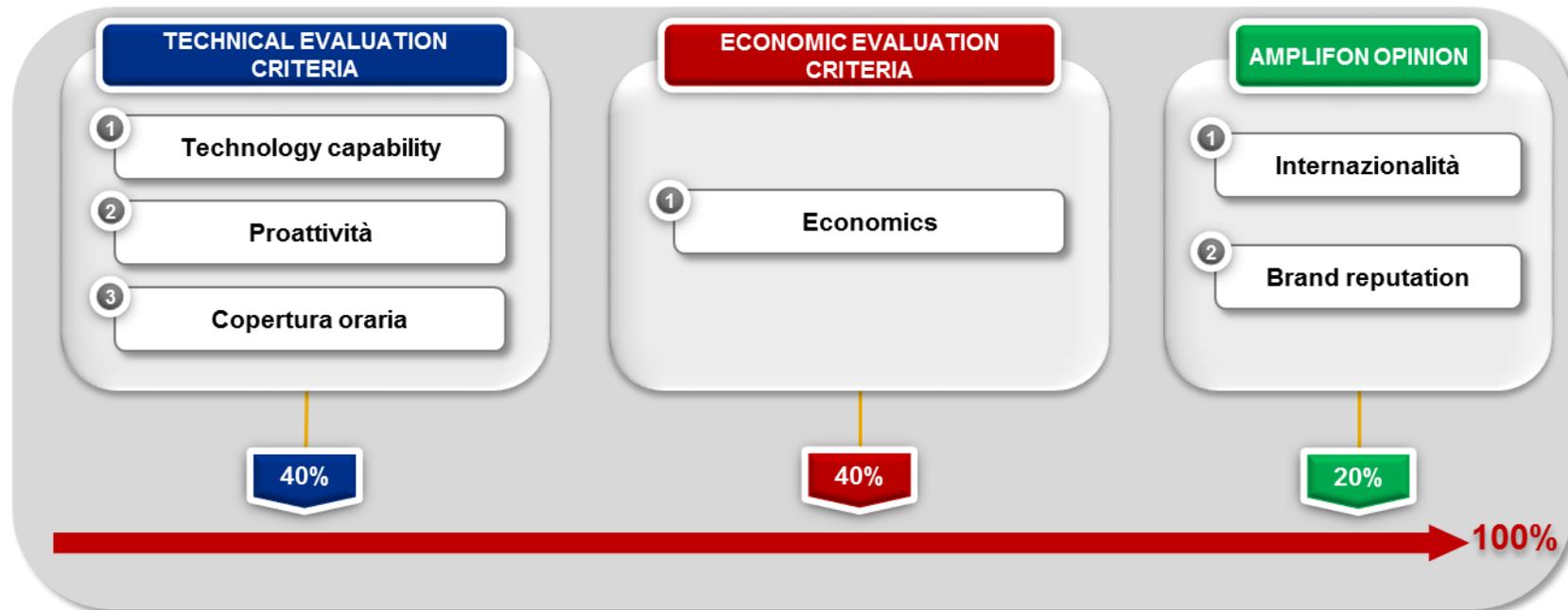
L'esperienza di Amplifon: SOC as a service

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

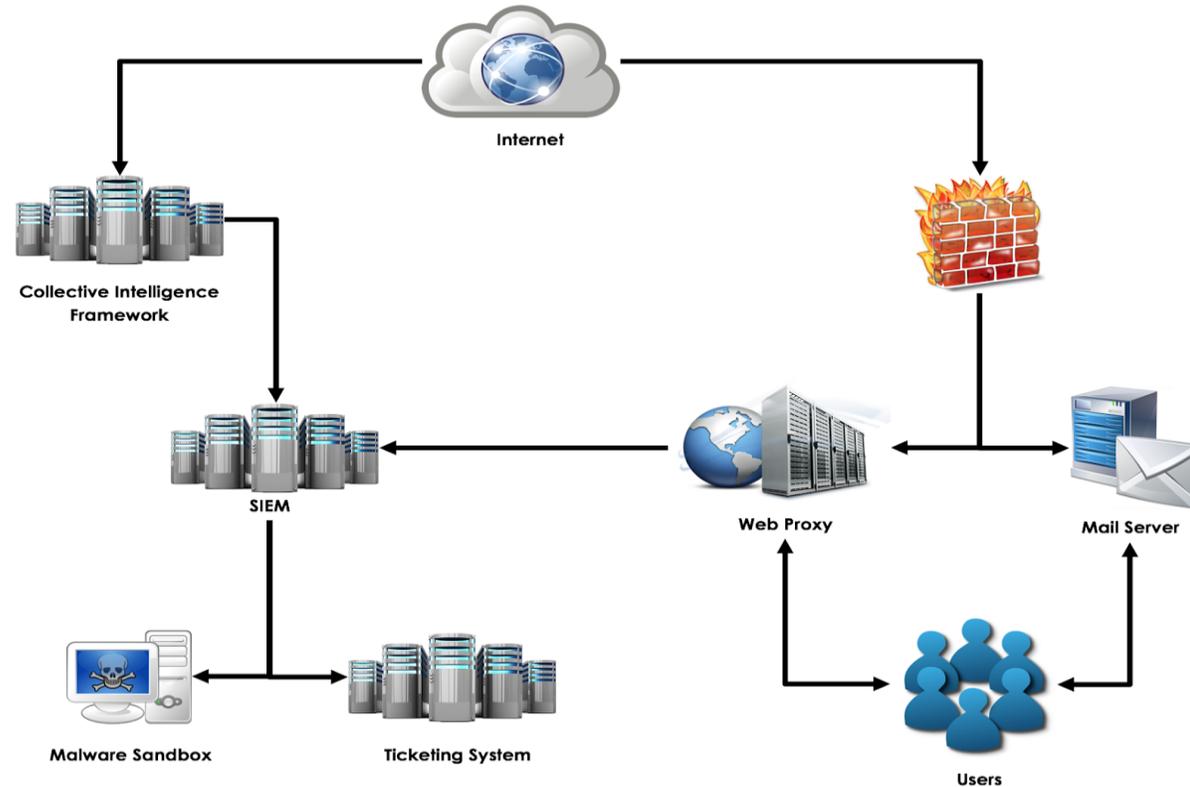
- Riconoscere in tempi stretti gli indicatori di attacco
- Rispondere adeguatamente a minacce con grande impatto
- Fornire ai SIEM solo informazioni utili e pulite

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 consentono di generare, immagazzinare, e anche di analizzare elevati volumi di dati

Può in parte compensare la mancanza di professionalità specifiche in ambito cybersecurity

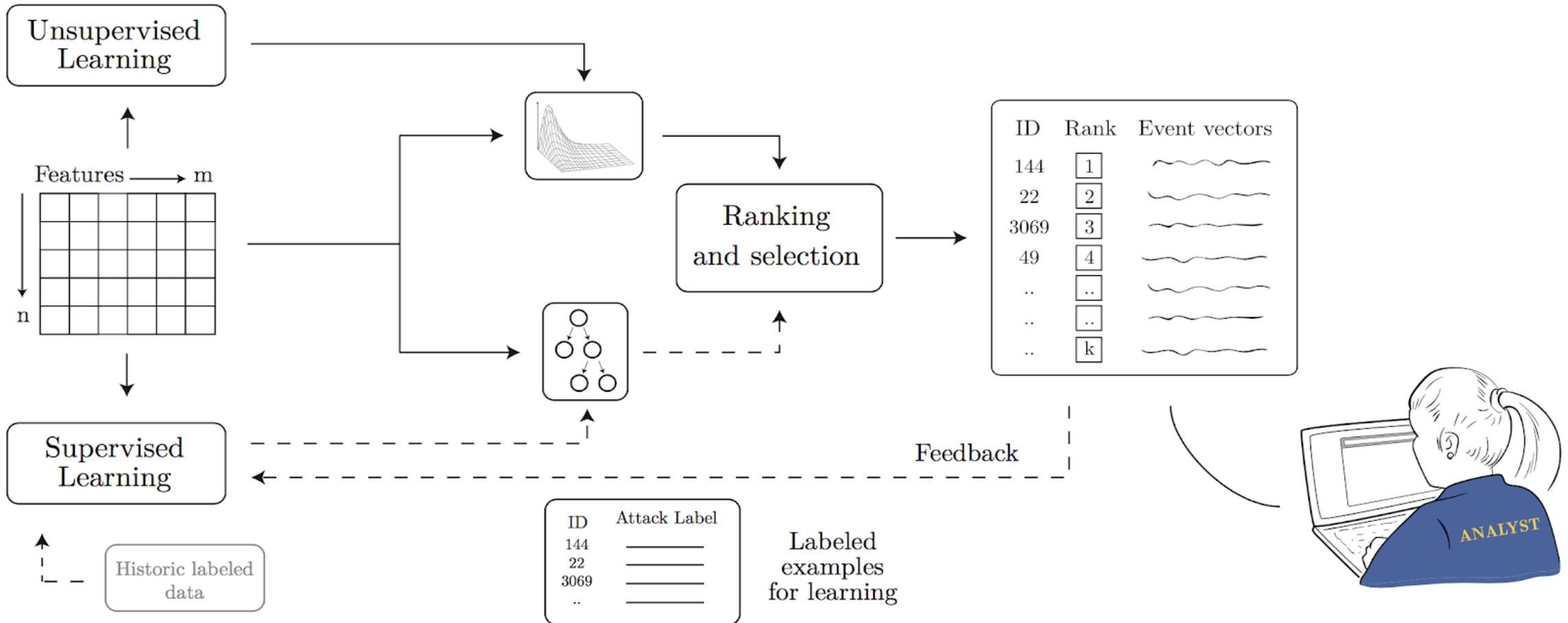
Rischi dell'utilizzo del ML in ambito cybersecurity

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