FESR MARCHE
PROGRAMMA OPERATIVO REGIONALE
POR 2014-2020

MARCHE
Fondi strutturali e di investimento europei

www.europa.marche.it

REGIONE MARCHE

WEBINAR

CYBERSECURITY PER L'INDUSTRIA 4.0

MERCOLEDÌ 14 APRILE 2021
ORE 17:00-18:30

i LABS
SMART AND DIGITAL SOLUTIONS
INDUSTRY
INFORMATION
INNOVATION

IBM Qradar

Il Laboratorio di Cybersecurity si dota di un prodotto leader di mercato in ambito sicurezza informatica per supportare le aziende della PMI marchigiana, nella gestione delle minacce informatiche in continua evoluzione

Premessa

Paolo Baldelli

p.baldelli@vargroup.it

p.baldelli@apra.it

VAR Group

Digital Security BU

Solution Team Leader

VAR Group S.p.A. è Platinum Partner di IBM e relativamente a progetti in ambito Cyber Security integra diverse soluzioni software IBM, progetti che vengono indirizzati dalla Digital Security Business Unit (BUDS) del Gruppo.

Apra S.p.A. è l'azienda controllata VAR Group che opera sul territorio marchigiano, costituendone la Filiale tecnico-commerciale in ambito Infrastruttura e Sicurezza.

Alcune informazioni introduttive

- Gli attacchi sono in costante aumento, in particolar modo quelli di tipo «Ransomware» dove l'Italia è purtroppo tra le più colpite in Europa
- **Qualunque tipologia di azienda è un target.** Non contano dimensioni o mercato di riferimento
- Dietro agli attacchi informatici ci sono vere e proprie organizzazioni criminali che hanno un solo obiettivo: **fare soldi nel modo più semplice possibile**
- Le tipologie di attacco informatico si stanno evolvendo molto velocemente, indirizzando tecniche sempre più innovative e sofisticate
- **I sistemi tradizionali di difesa, tra i quali firewall e antivirus, da soli non sono più sufficienti per proteggere il sistema informatico di un'azienda**

Il periodo di emergenza sanitaria che stiamo vivendo inoltre ha accelerato il processo di trasformazione del modo di lavorare, introducendo inevitabilmente maggiori fattori di rischio in ambito Cyber Security.

Cosa fare ?

Prevenzione

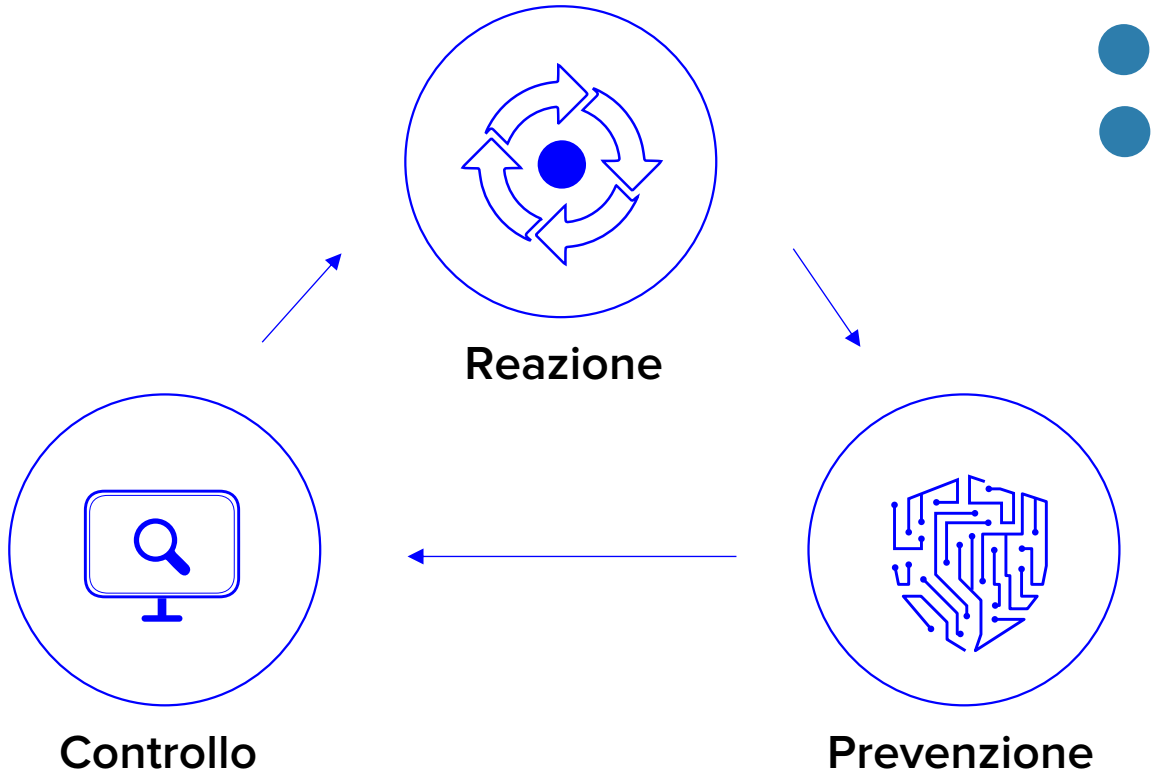
- ✓ Individuare asset e processi più critici
- ✓ Definire delle misure di sicurezza commisurate ai rischi
- ✓ Aumentare la visibilità su endpoint e network aziendali
- ✓ Patch Management
- ✓ Formazione continua sui dipendenti aziendali

Controllo

- ✓ Politiche di controllo sugli accessi
- ✓ Aumentare la capacità di riconoscimento degli attacchi
- ✓ Raccogliere maggiori evidenze che possano aiutare nella prevenzione e nel contenimento
- ✓ Monitoraggio H24

Reazione

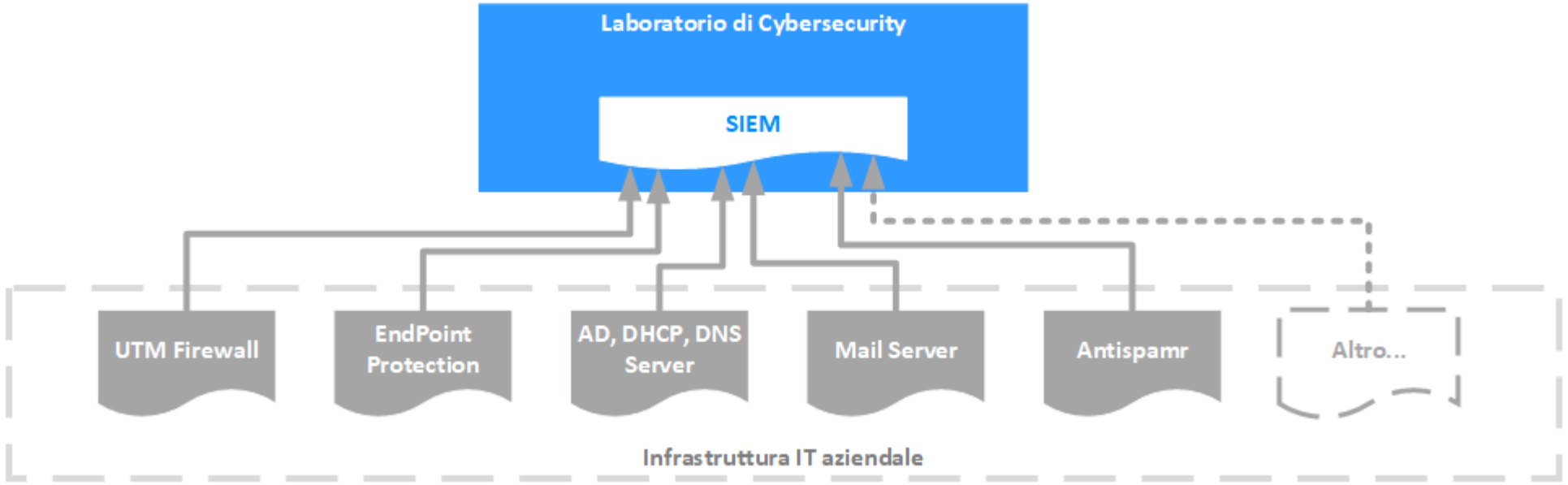
- ✓ Azioni di contenimento in emergenza
- ✓ Gestione degli eventuali incidenti
- ✓ Lesson learned



Una tecnologia in grado di cambiare l'approccio in ambito Cyber Security è il SIEM

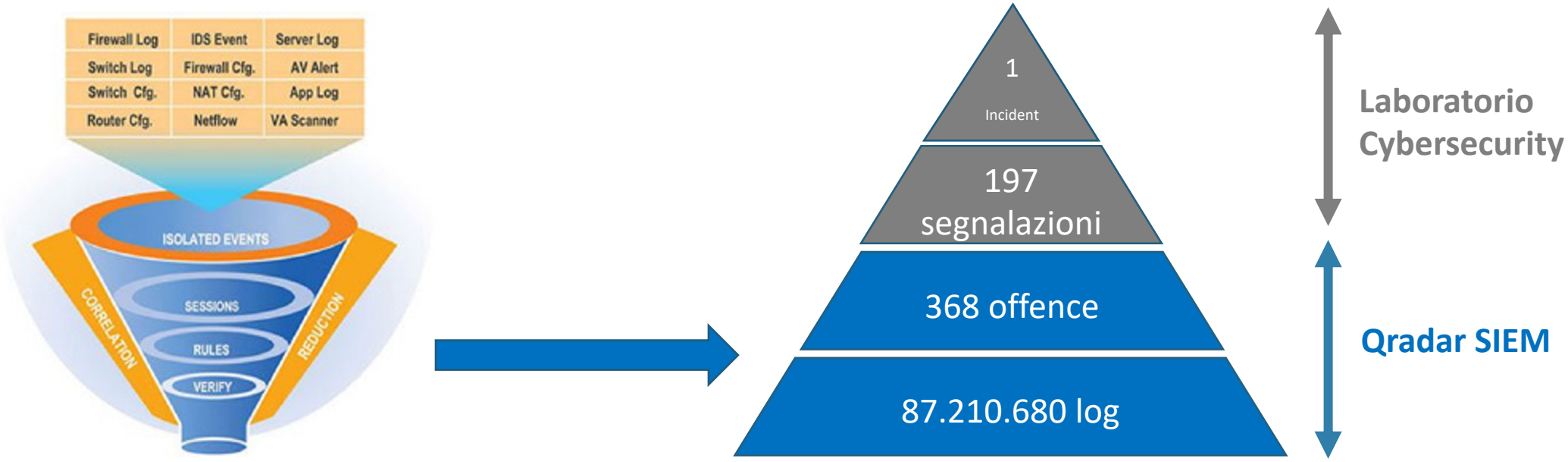
SIEM – Security Information & Event Management

Tecnologia in grado di ricevere i log da vari sistemi presenti in un'infrastruttura IT; di correlarli in modalità avanzata insieme anche ad informazioni di Intelligence; di mettere in evidenza cosa sta accadendo all'interno del sistema informativo di un'azienda, indirizzando adeguati livelli di prevenzione e controllo.



La piattaforma SIEM di IBM: Qradar

IBM® QRadar® Security Information and Event Management (SIEM) indirizza la possibilità di individuare e stabilire la priorità delle minacce in modo accurato e offre insight intelligenti che consentono di rispondere rapidamente per ridurre l'impatto degli incidenti. Accorpando i log provenienti dai sistemi sorgente in perimetro, QRadar è in grado di stabilire una correlazione tra tutte le varie informazioni e di raggruppare gli eventi correlati in singole offence al fine di accelerare l'analisi delle segnalazioni degne di nota.



Il valore aggiunto di IBM Qradar

Visibilità completa

Correlazione tra eventi provenienti dai vari sistemi sorgente + informazioni di Intelligence provenienti da IBM e dalle attività di ricerca del Laboratorio di Cybersecurity. Questo consente il rilevamento delle minacce in tempo reale.

Ottimizza le attività manuali

Centralizza in un'unica console tutti gli eventi di sicurezza relativi ad un'infrastruttura IT aziendale + attraverso il concetto di «offence» semplifica il lavoro di un analista di sicurezza che si potrà concentrare sugli eventi con priorità più alta.

Sopporto alla gestione delle conformità

Consente di rispondere alle necessità di compliance verso normative e standard di riferimento (es. GDPR e monitoraggio attività di Amministratori di Sistema), mettendo a disposizione regole e report pre-impostati

Un caso reale nelle Marche – Lube

Tra dicembre 2019 e gennaio 2020, durante delle attività di consulenza e analisi, sono emerse delle evidenze che potevano essere ricondotte ad una fase iniziale di compromissione. L'azienda ha deciso prontamente di dotarsi di una piattaforma SIEM gestita in H24 da un SOC.

Questa decisione ha consentito di verificare al meglio cosa stava succedendo: il SIEM Qradar ha iniziato a correlare informazioni rese disponibili dalle soluzioni di sicurezza che l'azienda aveva in casa e con il supporto dei Security Analyst del SOC, è stato possibile isolare in maniera mirata ed eliminare le compromissioni in atto, riuscendo a prevenire una possibile situazione di forte criticità che si sarebbe potuta manifestare nei mesi successivi.

Il progetto per il Laboratorio di Cybersecurity

- Il Laboratorio di Cybersecurity si sta dotando di una piattaforma SIEM IBM Qradar
- In qualità di IBM Platinum Partner, VAR Group metterà a disposizione un proprio specialista della Digital Security BU, certificato Qradar, per installare e configurare la piattaforma
- La piattaforma Qradar verrà consegnata al Laboratorio di Cybersecurity attraverso delle sessioni di formazione «training-on-the-job»
- A questo punto utilizzando anche altre tecnologie, il Laboratorio di Cybersecurity, potrà erogare dei servizi di consulenza sulla gestione delle minacce informatiche, indirizzati per la PMI marchigiana

PROGETTO FINANZIATO DA REGIONE MARCHE E FONDO EUROPEO DI SVILUPPO REGIONALE