Clusit Associazione Italiana per la Sicurezza Informatica

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

Streaming Edition 2021

ASTREA Advanced Security, Training Research, Events Agency

Sessione

Approccio alternativo al Data Loss Prevention

Giuseppe Marullo,
OT Security Architect,
Exprivia S.p.A.

Ran Norman
CTO & Co-Founder,
ITsMINE™

Data 16 Marzo 2021 orario 11.20-12.00 CET – Streaming Edition

#securitysummit #streamingedition

Giuseppe Marullo

OT Security Architect

Exprivia S.p.A.

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT
Streaming Edition
16-17-18 marzo 2021

exprivia

Ran Norman

CTO & CO-FOUNDER

ITSMINE™

SECURITY MANAGEMENT COMPLIANCE SUMMIT
Streaming Edition
16-17-18 marzo 2021

ITsMine™

Agenda

- Cosa è il DLP
- A cosa serve
- Ciclo di implementazione del DLP
- Caratteristiche di un progetto DLP
- Challenge
- Un nuovo approccio
- Come funziona ITSMINE
- Live Demo
- Q&A

DLP…

Cosa è in realtà il DLP

- E’ lo strumento principe per avere visibilità sul ciclo di vita del dato
- Consente di sapere come si comportano gli utenti e aiuta a profilarli
- Aiuta gli utenti a migliorare i comportamenti pericolosi
- Limita l’accesso ai dati ai soli soggetti autorizzati

A cosa serve

- Aiuta a dimostrare compliance circa le leggi e i regolamenti sulla privacy
- Identifica e aiuta a proteggere la proprietà intellettuale e altri asset «intangibili»
- Limita gli effetti dei data breach

Ciclo di implementazione del DLP

- Preparazione
  - Motivazioni per l'implementazione di un sistema DLP(legali, protezione IP etc)
  - Data discovery e inventory
  - Creazione delle policy iniziali
- Implementazione in modalità silente
  - Implementazioni delle policy(in modalità silente)
  - Fine tuning
- Modalità esplicita
  - Implementazione delle policy (in modalità visibile)
  - Fine tuning
- Enforcing delle policy
  - Implementazione delle policy (in modalità enforcing)
- Audit periodico

Caratteristiche di un progetto DLP

- Necessità di un forte commitment da parte del management
- Definire quali sono i dati da proteggere non è semplice
- I tempi di implementazione sono medio-lunghi

Challenge

- L’aspettativa è che il DLP blocchi e prevenga sempre i data breach. Per arrivare a questo risultato ci vuole tempo e impegno non indifferente.
- Il sistema quindi è il più delle volte passivo, fornisce solo allarmi
- La gestione degli allarmi va fatta da personale dedicato, con conoscenza dei processi di business

Un nuovo approccio

- « Look ma! No Agent!»
  - L’agent viene installato al volo so se vengono rilevate violazioni, poi viene rimosso dopo poche ore
- Capacità di mantenere il controllo sul dato anche quando lascia il perimetro aziendale
- Basato su behavioral analysis per gli utenti
- Self-training in caso di violazioni per gli utenti
- Profilazione degli utenti per individuare i ‘distratti’, i ‘malevoli’ e anche perché no, i supereroi difensori del dato

Come funziona ITSMINE

- Viene effettuata un analisi comportamentale sugli utenti con generazione di report che forniscono visibilità completa, molto dettagliati (vedi demo)
- i folder contenenti i dati da proteggere vengono scansionati e ne viene analizzato il pattern di utilizzo per identificare quelli che potrebbero essere più interessanti a un potenziale attaccante.
- Vengono utilizzati le attività degli utenti, le permission, le caratteristiche degli utenti e dei gruppi.

Come funziona ITSMINE

- L’algoritmo è dinamico e sempre aggiornato
- Nei folder più importanti vengono predisposte delle software mines (vedi demo)
- I file più importanti vengono protetti tramite la funzione File GPS (vedi demo)
- Se viene rilevata una minaccia, ITSMINE colleziona tutte le evidenze per analisi forensi, determina la natura e il livello di rischio e infine agisce di conseguenza (vedi demo)

LIVE DEMO

Ran Norman

Q&A

Giuseppe Marullo
giuseppe.marullo@exprivia.com
+39 348 521 92 73

Ran Norman
ran@itsmine.io
+972 (53) 332.3362

Riferimenti

Tre uomini e una gamba(1997)

- https://it.wikipedia.org/wiki/Template:PD-Italia

LEGGE 22 aprile 1941, n. 633

- https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1941-04-22;633!vig=

exprivia

future. perfect. simple.

wwww.exprivia.it

Grazie per l’attenzione