SECURITY SUMMIT

Verona, 10 ottobre 2023

Security Summit

Clusit Associazione Italiana per la Sicurezza Informatica

ASTREA Advanced Security, Training Research, Events Agency

Come ottimizzare la Resilienza Informatica

Luca Bechelli, CS Clusit

Giacomo Giarola, Associate Sales Engineer, NinjaOne

10 ottobre Verona 2023 orario 11.30-12.10

Luca Bechelli

COMITATO SCIENTIFICO CLUSIT

PARTNER @P4I – GRUPPO DIGITAL360

Giacomo Giarola

ASSOCIATE SALES ENGINEER, NINJAONE

ninjaOne®

Come ottimizzare la Resilienza informatica

Gestione unificata dell'IT

Clusit
Associazione Italiana per la Sicurezza Informatica

SECURITY SUMMIT
VERONA

Che cos'è la Resilienza informatica?

- Tecnologia
- Strumenti
- Processi
- Persone

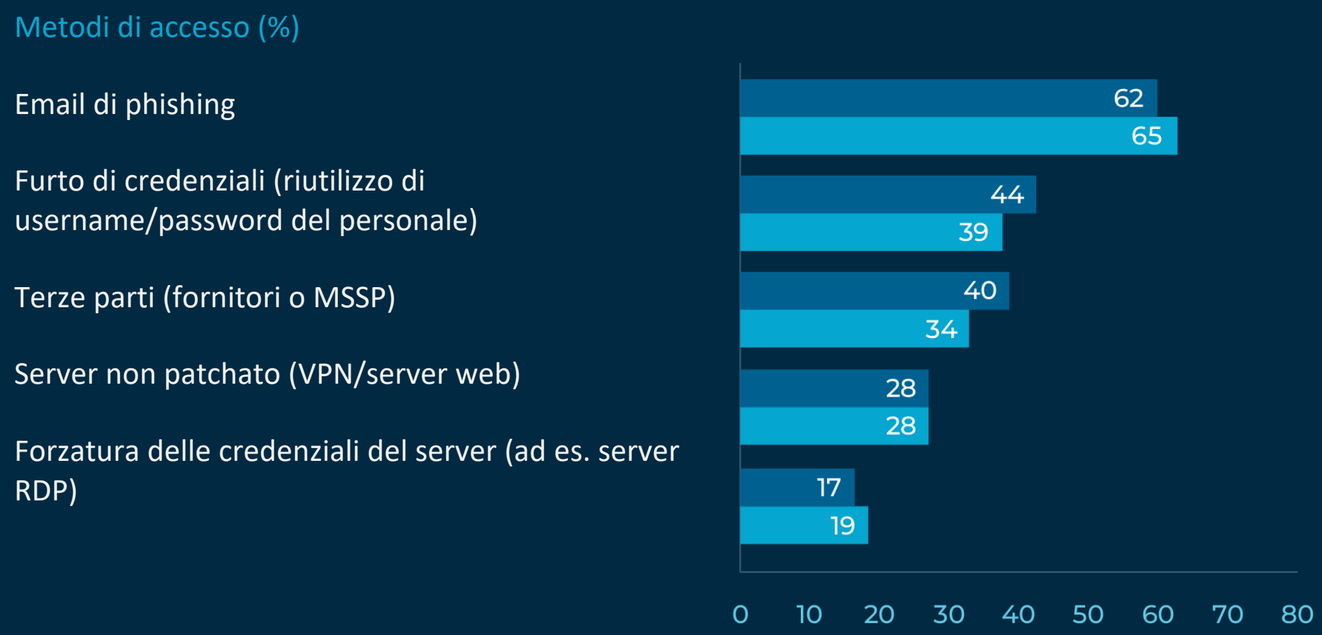
Statistiche sulla Sicurezza informatica

Punti chiave:

- 51% violazione significativa dei dati
- il 61% ha pagato un riscatto
- 74% CSIRP incoerente

Come fanno gli aggressori ad accedere?

Vengono utilizzati cinque metodi di accesso.
Questi sono testati e diffusi dalle reti di ransomware, ma non sono impossibili da contrastare.



I principi fondamentali devono ancora essere rispettati

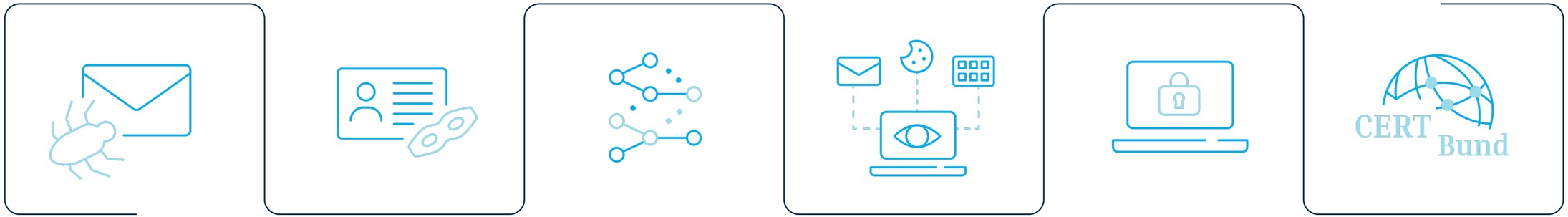
- Il gasdotto Colonial è stato colpito attraverso un **account** inattivo **senza MFA**
- L'attacco ai servizi sanitari irlandesi è riconducibile a un **documento Excel dannoso**
- Il gruppi di ransomware LockBit ha avuto accesso al governo degli Stati Uniti tramite **RDP esposto**
- Acer colpita da una richiesta di ransomware tramite una **vulnerabilità di Exchange non patchata**

Tempistica dall'accesso iniziale al Contenimento

Violazione – giorno 1

Scoperta – giorno 200

Contenimento – giorno 270



Fase 1
Infezione iniziale

Fase 2
Escalation dei privilegi

Fase 3
Movimenti laterale

Fase 4
Uscita dei dati

Fase 5
Crittografia

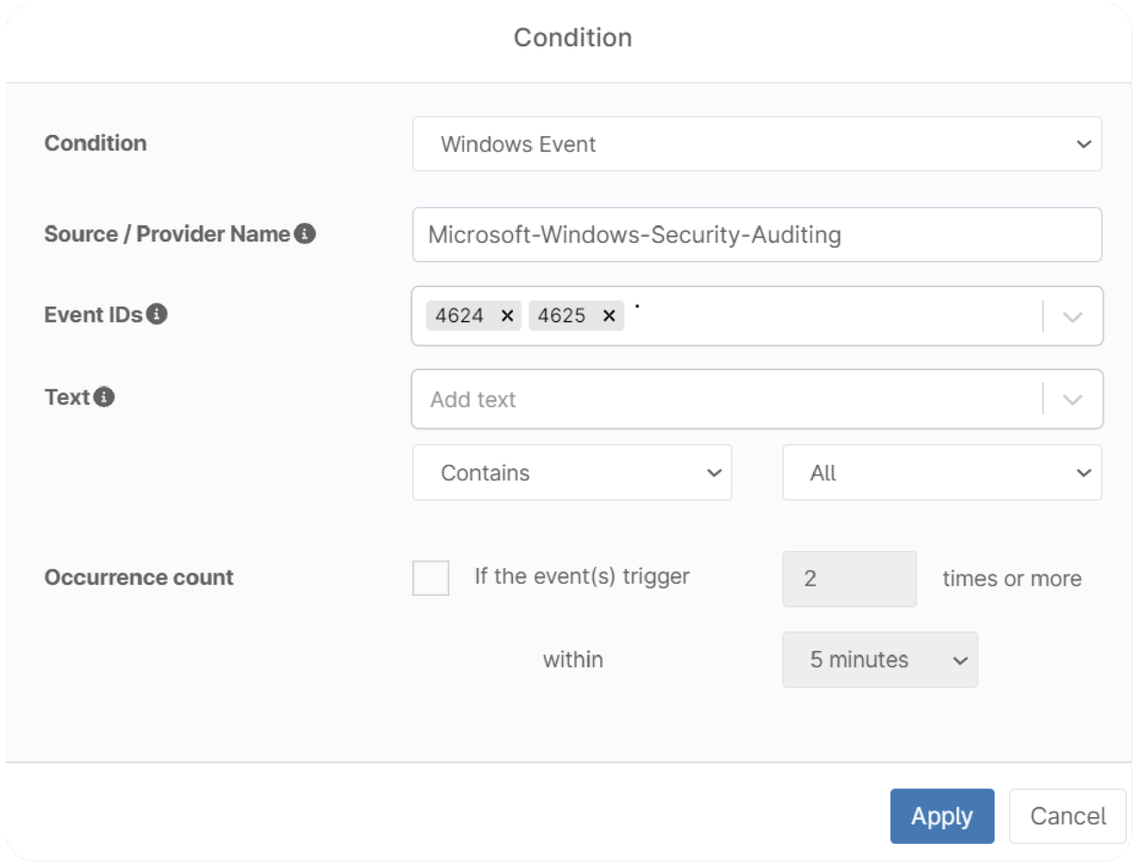
Fase 6
Risposta all'incidente

Raccomandazioni per il rilevamento

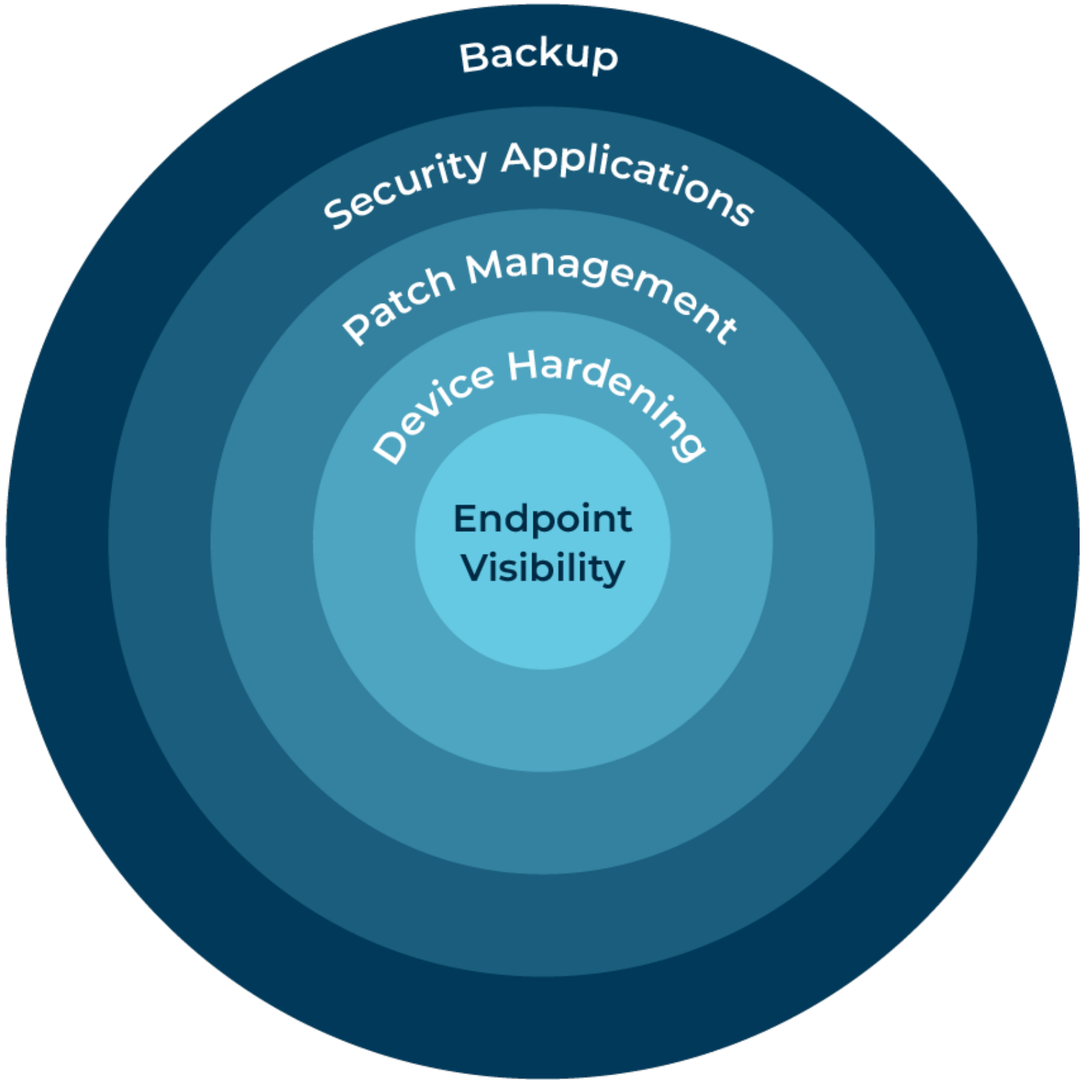
- Monitoraggio del PSR
- Uso insolito di CMD
- Download delle credenziali
- Attività pianificate sconosciute
- Ricognizione della rete
- Comando e controllo della comunicazione

via HTTPS criptati

- Esfiltrazione
- Monitoraggio dell'accesso ai file
- Manipolazione dei backup o del software AV



Un approccio a livelli alla sicurezza degli endpoint



Ottieni completa **VISIBILITÀ**

- Individuare e gestire i dispositivi non funzionanti
- Identificare quotidianamente le vulnerabilità note
- Avvisare in merito a attività legate alla sicurezza

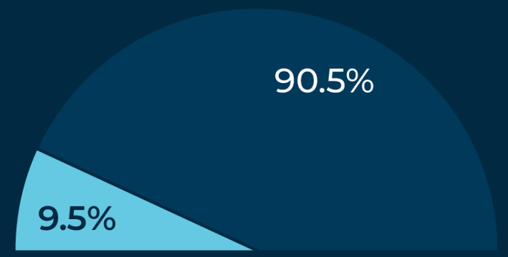
Hardening degli endpoint

- Riduci le vulnerabilità tradizionali
- Rafforza il sistema operativo
- Blocca account
- Rafforza le applicazioni

Applica le patch

- Identifica quotidianamente le vulnerabilità note
- Applica patch al sistema operativo, alle applicazioni, alle unità e al firmware
- Rimedia immediatamente le vulnerabilità critiche
- Distribuisci altre patch il più rapidamente possibile
- Convalida e riferisci i risultati delle patch

Abilitazione delle patch dei dispositivi



Percentuale di patch del dispositivo

Patch installate/totali

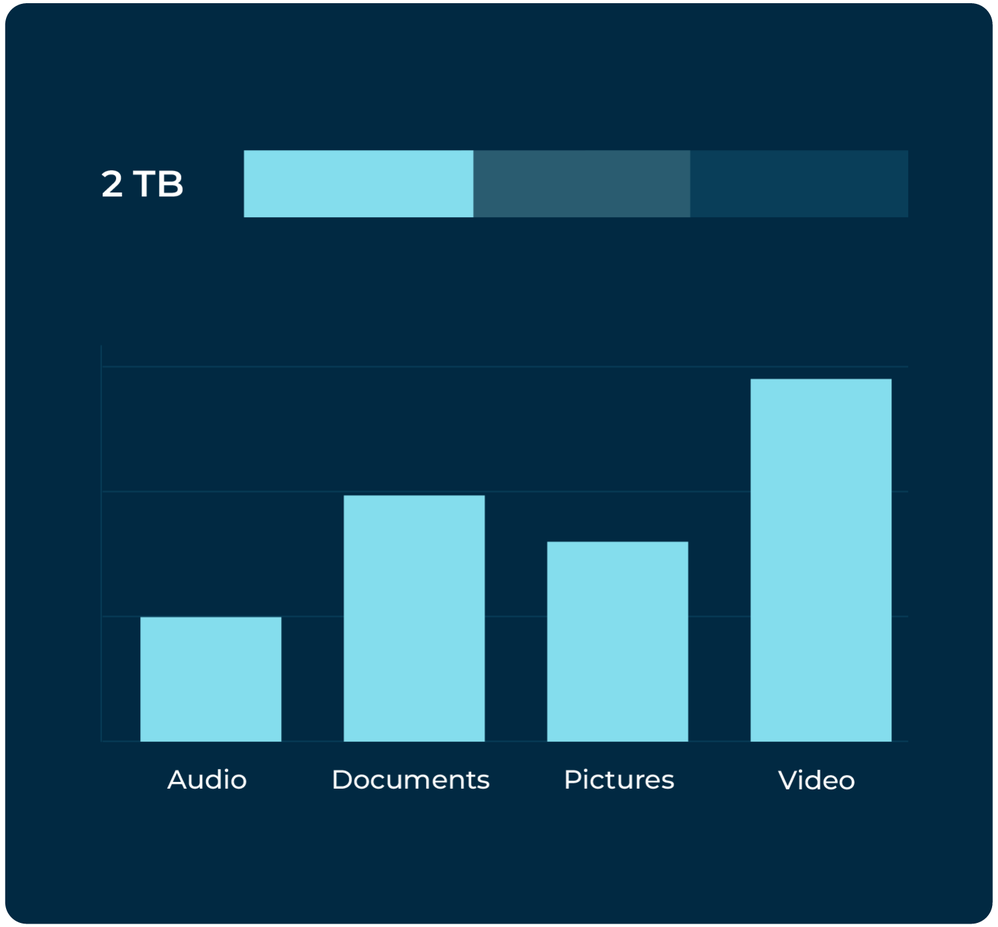
Totale	**484**
Installate	475
Approvate	5
In attesa	4
Fallite	0

Distribuisci
Applicazioni di sicurezza

- Identifica i dispositivi non protetti
- Individua gli endpoint e distribuisci automaticamente
- Monitoraggio della conformità
- Avviso e gestione da un unico pannello centralizzato

Esegui il backup di tutto

- Identifica gli endpoint con dati vulnerabili
- Esegui il backup di tutti gli endpoint
- Assicurati di seguire il modello 3-2-1
- Avviso e gestione da un unico pannello centralizzato



Conclusioni

- Monitoraggio e allerta precoce - tieni a mente i 270 giorni
- Il backup da solo non è sufficiente (ma è assolutamente necessario)
- Fondamenti di resilienza e sicurezza IT
- Carenza di talenti a livello globale (tutti si occupano di sicurezza)
- SOC interno o esterno come supporto aggiuntivo

La piattaforma di gestione unificata dell'IT

GESTIONE UNIFICATA

GESTIONE E MONITORAGGIO DA REMOTO

- MONITORAGGIO E AVVISI
- PATCH MANAGEMENT
- DISTRIBUZIONE SOFTWARE
- SCRIPTING E AUTOMAZIONE

AGGIUNTE

- ACCESSO REMOTO
- SICUREZZA DEGLI ENDPOINT
- BACKUP
- GESTIONE DEI TICKET
- DOCUMENTAZIONE

INTEGRAZIONI

Demo

Per iniziare la tua prova gratuita, visita il sito
ninjaone.com/it/prova-gratuita/

Q&A