
CYBERSEC 2022 臺灣資安大會
CHANGE NOW
數位轉型 資安升級
SEP. 20-22 臺北南港展覽二館

SentinelOne®

守護駭客首要攻擊目標—偵測與攔阻針對AD的攻擊行為

王澄鋸 博士

掃描QRCode，填寫議程問券

憑完成畫面即可與工作人員兌換精美品牌禮品喔!

Attivo Networks is Now a SentinelOne Company

ATTIVO EXPANDS IDENTITY EXPOSURE VISIBILITY FOR HYBRID ENVIRONMENTS

EXPOSURE VISIBILITY FOR ACTIVE DIRECTORY & AZURE AD

Gain continuous insight into on-premises AD and Azure AD risk exposures, over-provisioning and misconfigurations for domains, users and devices across hybrid environments.

LEARN MORE

Identity Visibility | Identity Security | Deception

SentinelOne Completes Acquisition of Attivo Networks

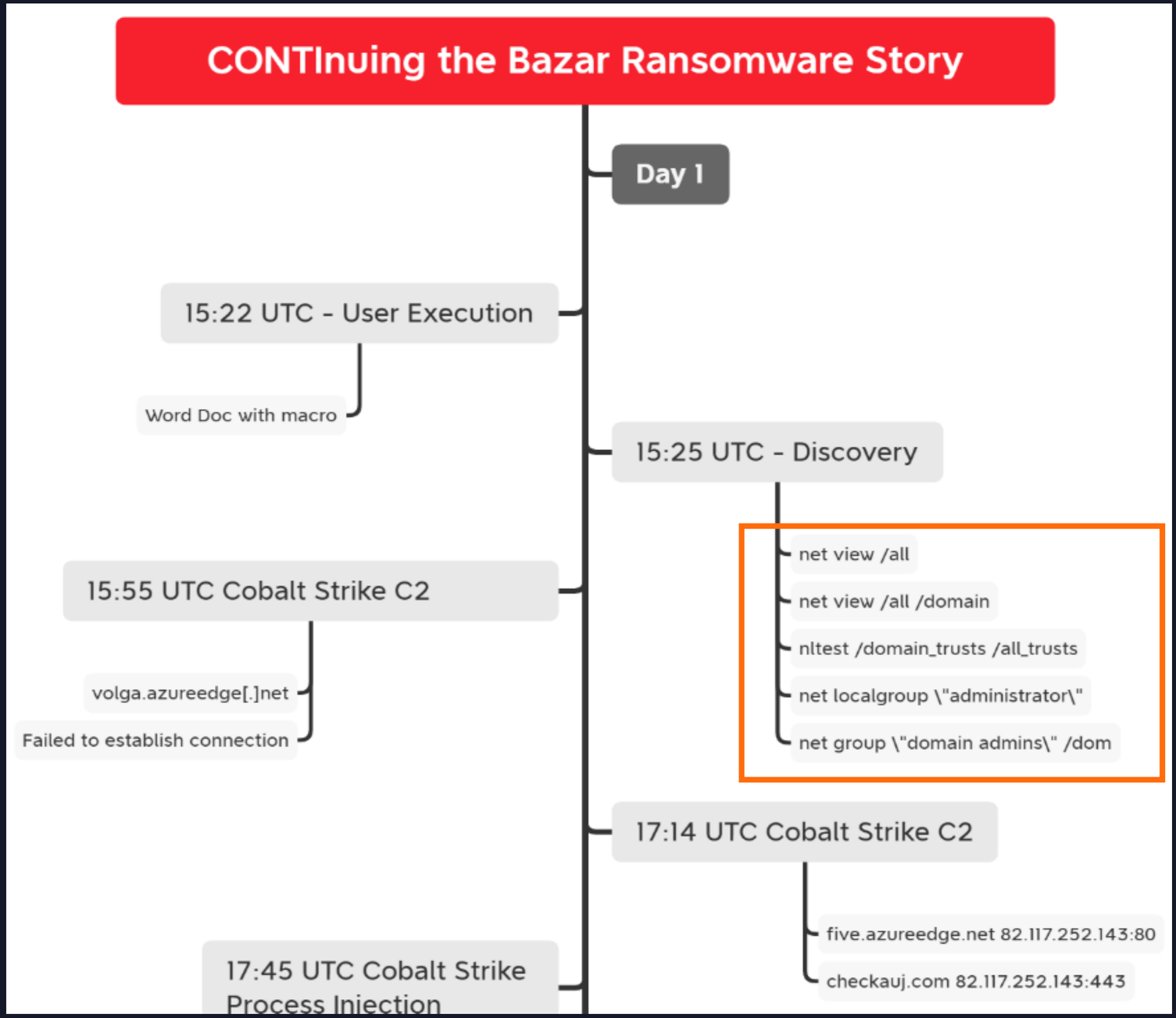
Mountain View, Calif. – May 4, 2022 – SentinelOne (NYSE: S), an autonomous cybersecurity platform company, that it has completed the acquisition of Attivo Networks. SentinelOne previously announced the agreement to ac Networks on March 15, 2022.

Attivo Networks is a leading identity security and lateral movement protection company with a rapidly growing business serving

Conti Ransomware

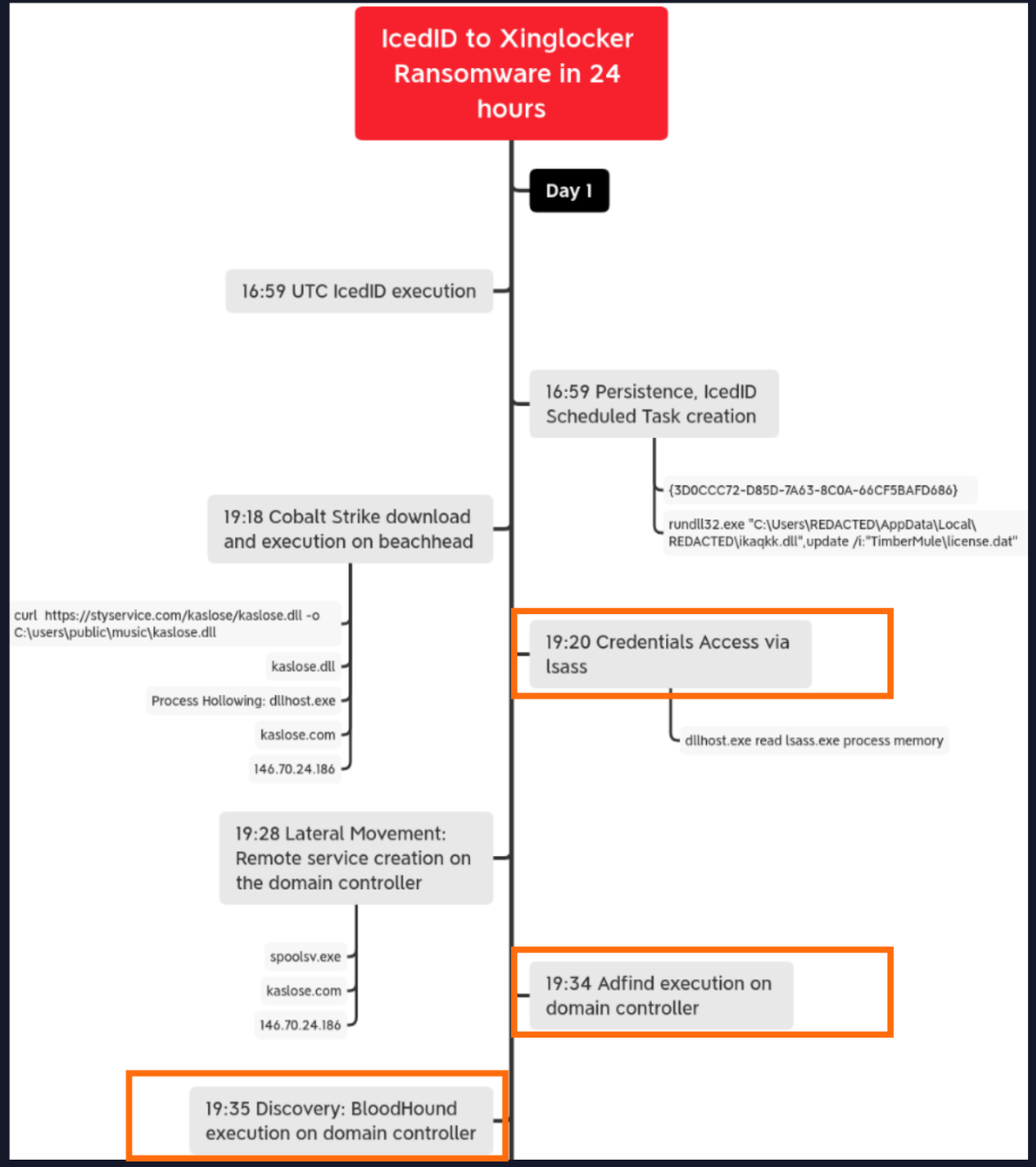
Courtesy of:
https://thedfirreport.com

- 初步成功入侵後 3 分鐘就開始攻擊AD



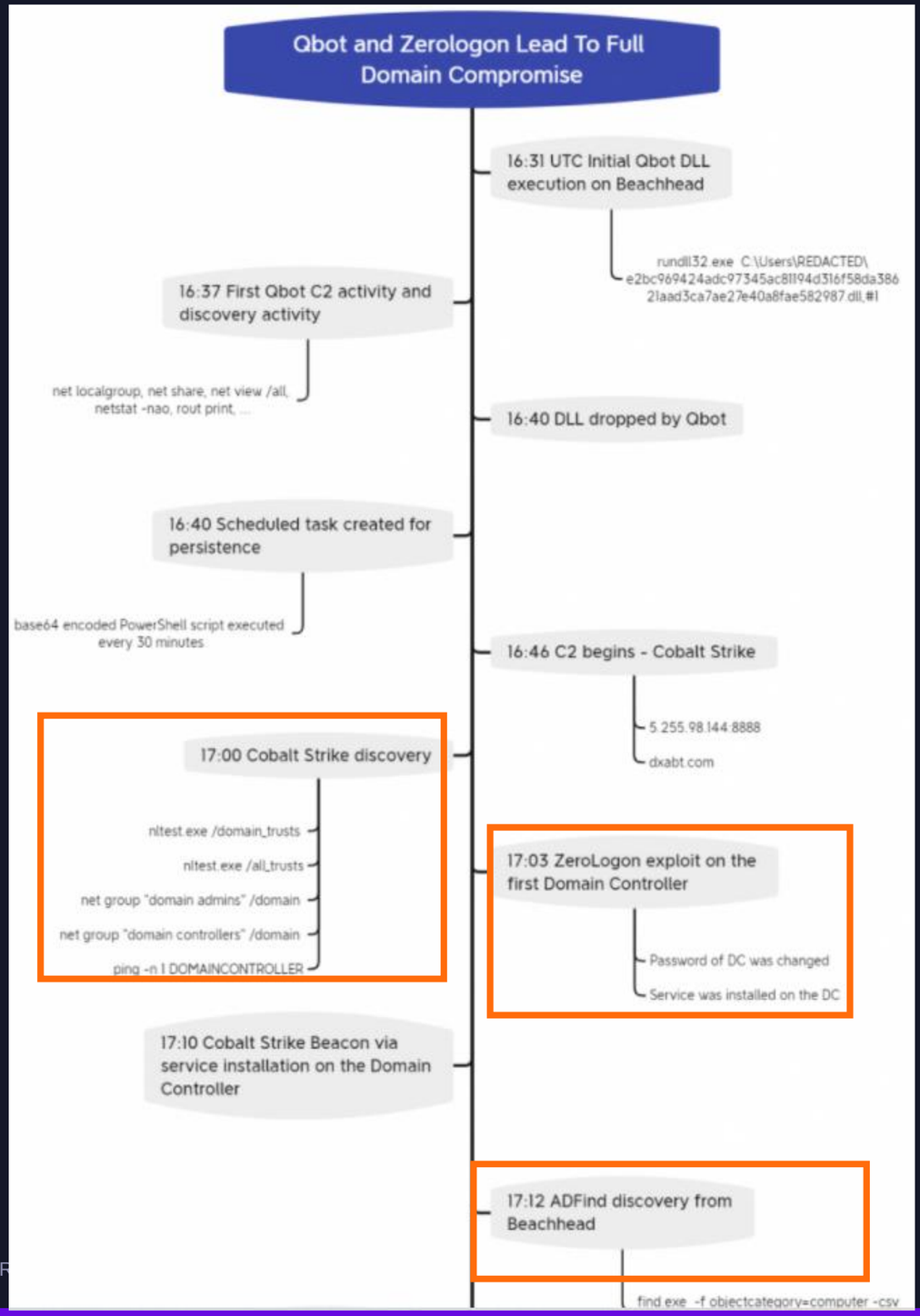
Xinglocker Ransomware

- 初步成功入侵後 3 小時開始提取身份憑證
- 24 小時內對AD目標(Xinglocker)發動攻擊



Nation-State Epsonage

- 初步成功入侵後 30 分鐘開始對身份憑證和AD發動攻擊
- 初步成功入侵後 1 個小時開始數據外洩。



攻擊者對準了身份憑證以及 AD

65%

的用戶在多個不同帳號上使用
相同**密碼**

(Google 2019 security survey)

60%

駭客入侵歸屬於
身分憑證盜竊

(Verizon 2021 Data Breach Investigation Report)

81%

駭客入侵利用
已被盜或易破的**密碼**

(Verizon 2021 Data Breach Investigation Report)

50%

企業在過去兩年遭受過
AD 攻擊

(EMA Research AD is Under Siege 2021)

42%

針對AD的攻擊是
成功的

(EMA Research AD is Under Siege 2021)

86%

受問券調查的企業計劃
增加 AD 安全的經費

(EMA Research AD is Under Siege 2021)

Gartner: 到 2023, 75% 的雲端安全事故是由於
管理不善的 identities, access, and privileges

SentinelOne

收購之前的Attivo ADAssessor

AD
保護和評估

AGENTLESS SCANNING AND REMEDIATION SOLUTION

On-Prem or Cloud

收購之前的Attivo ADSecure DC

AD
增強型保護

AGENT FOR DC

Cloud

收購之前的Attivo EDN, 包含ADSecure EP

身份偵測與回應 **Identity Detection & Response**

AGENT FOR WORKSTATIONS

Hide Credentials, AD info, Visualize Threatpaths

收購之前的Attivo Botsink 網路欺敵，主動防禦系統

實時接戰駭客攻擊
網路欺敵

HARDWARE BASED PLATFORM TO CREATE AND MANAGE DECOYS

Create thousands of real decoys across entire infrastructure

偵測與攔阻針對 AD 的攻擊行為

SentinelOne

身份保護 Identity Protection

ID Attack Surface Management & Identity Threat Detection & Response (ITDR)

Access Management

Identity Attack Surface Management

Identity Detection & Response (ITDR)

Provisioning Identities	Connecting Identities	Controlling Identities	Securing Identities	
IGA	**IAM**	**PAM**	**ID ASM**	ITDR
• Identity Life Cycle Management • Access Requests • Entitlement Provisioning	• Authentication • Authorization • SSO • MFA	• Control privileged Identities • Just in Time Access • Least Privilege Access	• AD Database Vulnerabilities • Attack Paths • Credential Exposures • Least Privileges	• Domain Enumeration/Exploitation • Identity Privilege Escalation • Credential Protection • Cloud Entitlement

收購之前的Attivo ADAssessor

AD
保護和評估

AGENTLESS SCANNING AND REMEDIATION SOLUTION

On-Prem or Cloud

收購之前的Attivo ADSecure DC

AD
增強型保護

AGENT FOR DC

Cloud

收購之前的Attivo EDN, 包含ADSecure EP

身份偵測與回應 **Identity Detection & Response**

AGENT FOR WORKSTATIONS

Hide Credentials, AD info, Visualize Threatpaths

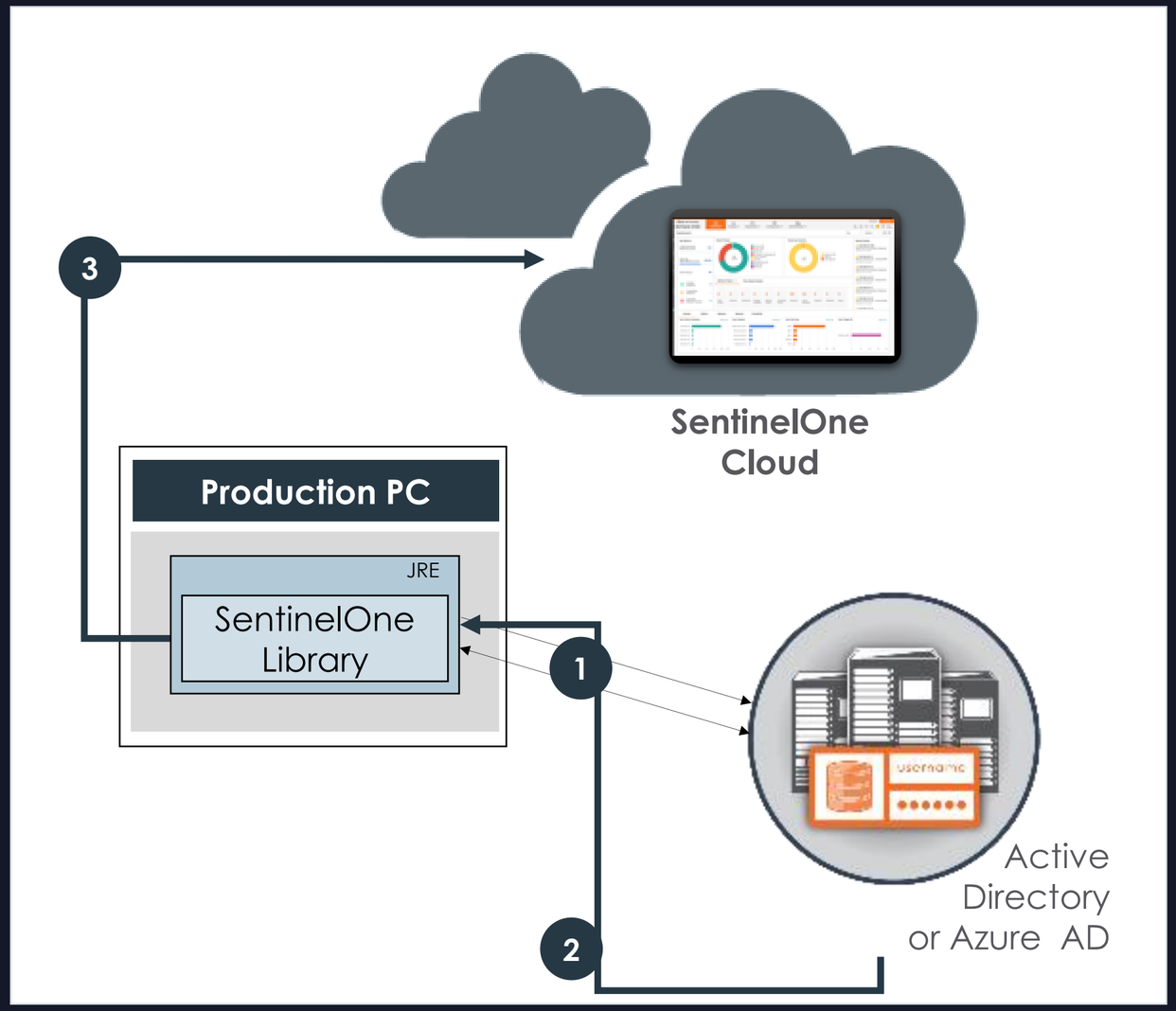
收購之前的Attivo Botsink 網路欺敵，主動防禦系統

實時接戰駭客攻擊
網路欺敵

HARDWARE BASED PLATFORM TO CREATE AND MANAGE DECOYS

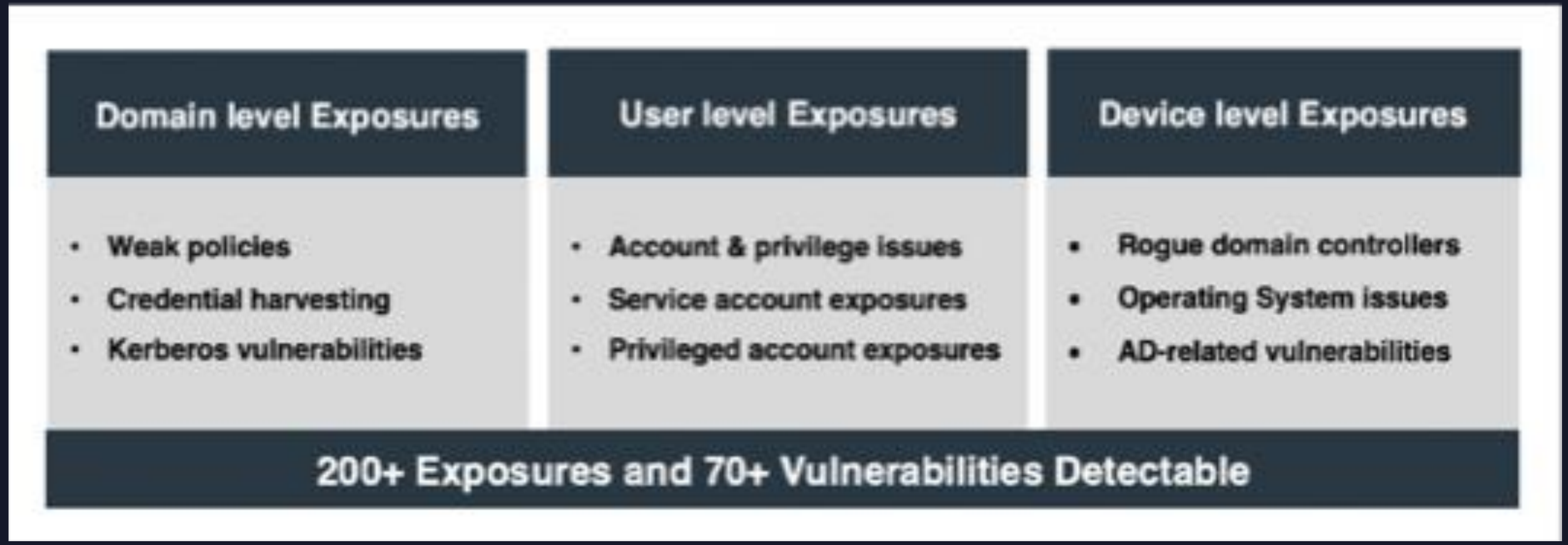
Create thousands of real decoys across entire infrastructure

AD 評估和保護



- Lightweight Library Installs on ONE PC
- On-prem AD, Azure AD, or Multi-cloud
- Management Console on Public Cloud
- Raise an alert if a weakness is discovered or an attack is detected
- On-prem version HW requirement change from ONE PC to ONE Server
- Agentless Scanning and Remediation

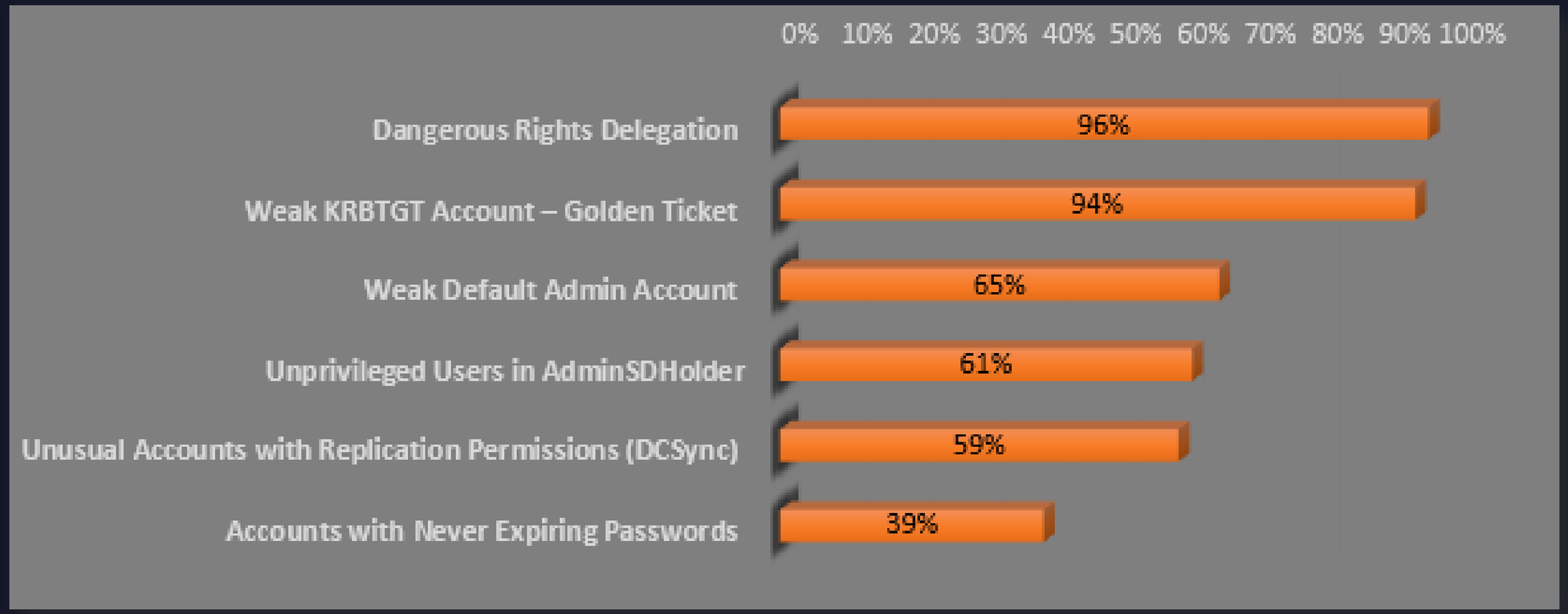
Ranger AD 掃描



- Visibility into AD Security hygiene issues and actionable alerts for key exposure at Domain, User, and Device levels
- Real-time Privilege AD escalation detection
- Granular access restriction to AD information without impacting business operation
- Continuous Insight into Identity and Service Account Risk related to credentials, privileged accounts, stale accounts, shared credentials, and Identity attack paths

最常發現的問題

Across the 200+ exposures and 90+ Vulnerabilities Evaluated



Ranger AD 偵測的攻擊

實時的可視性和偵測

- Detecting mass account lockouts, disables, and deletions
- Suspicious password changes on service or sensitive accounts
- Suspicious password changes for mass password reset / changes
- Detecting brute force – password spray attack
- Suspicious service creation on domain controller
- Use of default administrator account
- Reactivation of disabled privileged accounts
- SID history tampering

Active Directory

收購之前的Attivo ADAssessor

AD
保護和評估

AGENTLESS SCANNING AND REMEDIATION SOLUTION

On-Prem or Cloud

收購之前的Attivo ADSecure DC

AD
加強型保護

AGENT FOR DC

Cloud

收購之前的Attivo EDN, 包含ADSecure EP

身份偵測與回應 **Identity Detection & Response**

AGENT FOR WORKSTATIONS

Hide Credentials, AD info, Visualize Threatpaths

收購之前的Attivo Botsink 網路欺敵，主動防禦系統

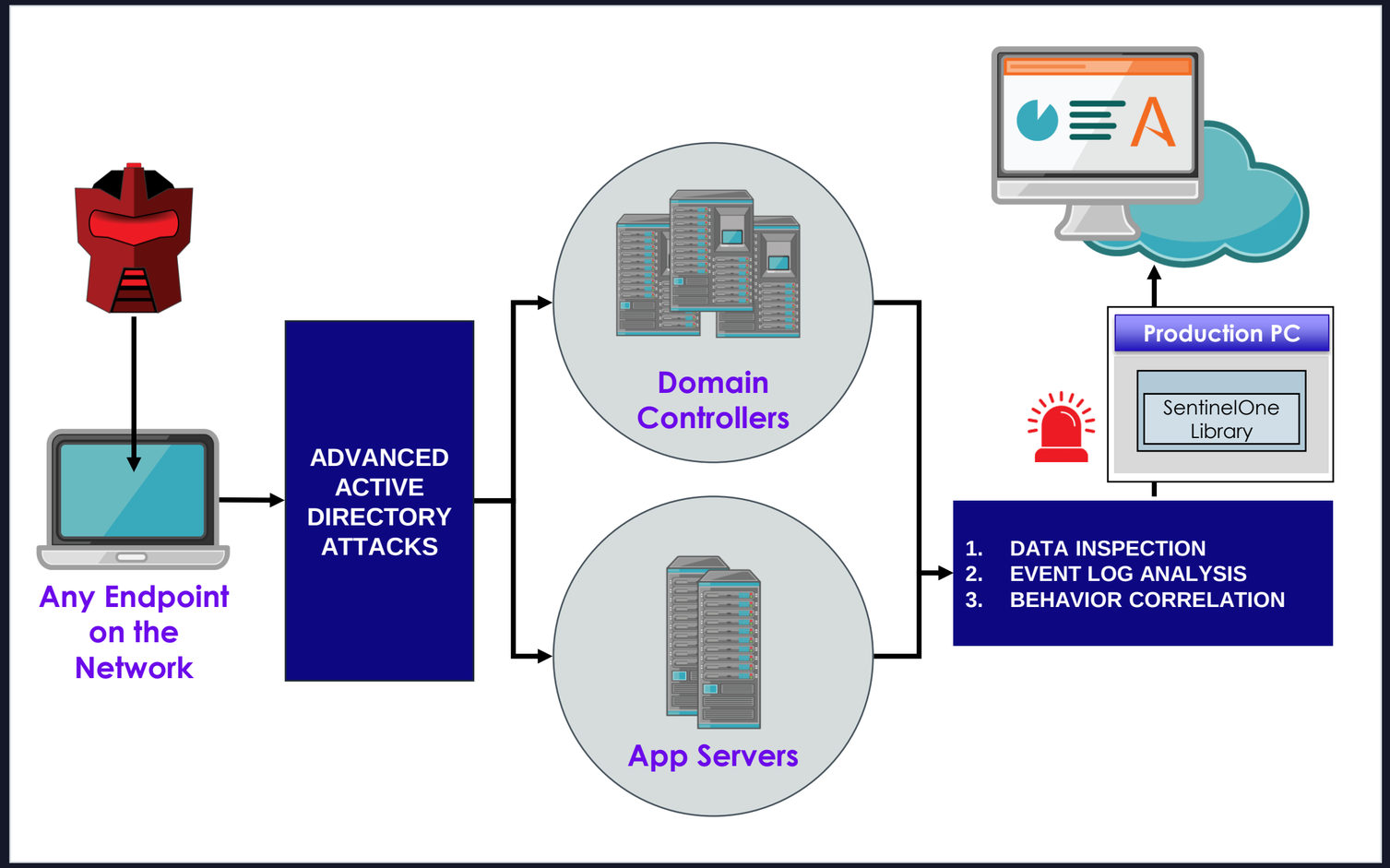
實時接戰駭客攻擊
網路欺敵

HARDWARE BASED PLATFORM TO CREATE AND MANAGE DECOYS

Create thousands of real decoys across entire infrastructure

偵測與攔阻針對 AD 的攻擊行為

AD Domain Controller的加強保護



- Install Agents on Domain Controllers and Critical Servers
- Lightweight Library Install on ONE PC
- Protects against comprehensive attacks to AD regardless of the attack source
- Protection without context knowledge on end-points
- Employs deep packet inspection and behavior analysis of AD logs

Ranger AD Protect 偵測並且阻擋

業界最強大的功能，最容易安裝和使用

- AD Recon attack using LDAP, SAMR, LSAR protocols
- Golden ticket attack
- Silver ticket attack
- Skeleton ticket attack
- Pass-the-ticket attack
- Pass-the-hash attack
- Overpass-the-hash attack
- Forged PAC attack
- DCSync attack
- DCShadow attack
- AS REP Roasting attack (Kerberoasting)

Active Directory

收購之前的Attivo ADAssessor

AD
保護和評估

AGENTLESS SCANNING AND REMEDIATION SOLUTION

On-Prem or Cloud

收購之前的Attivo ADSecure DC

AD
增強型保護

AGENT FOR DC

Cloud

收購之前的Attivo EDN, 包含ADSecure EP

身份偵測與回應 **Identity Detection & Response**

AGENT FOR WORKSTATIONS

Hide Credentials, AD info, Visualize Threatpaths

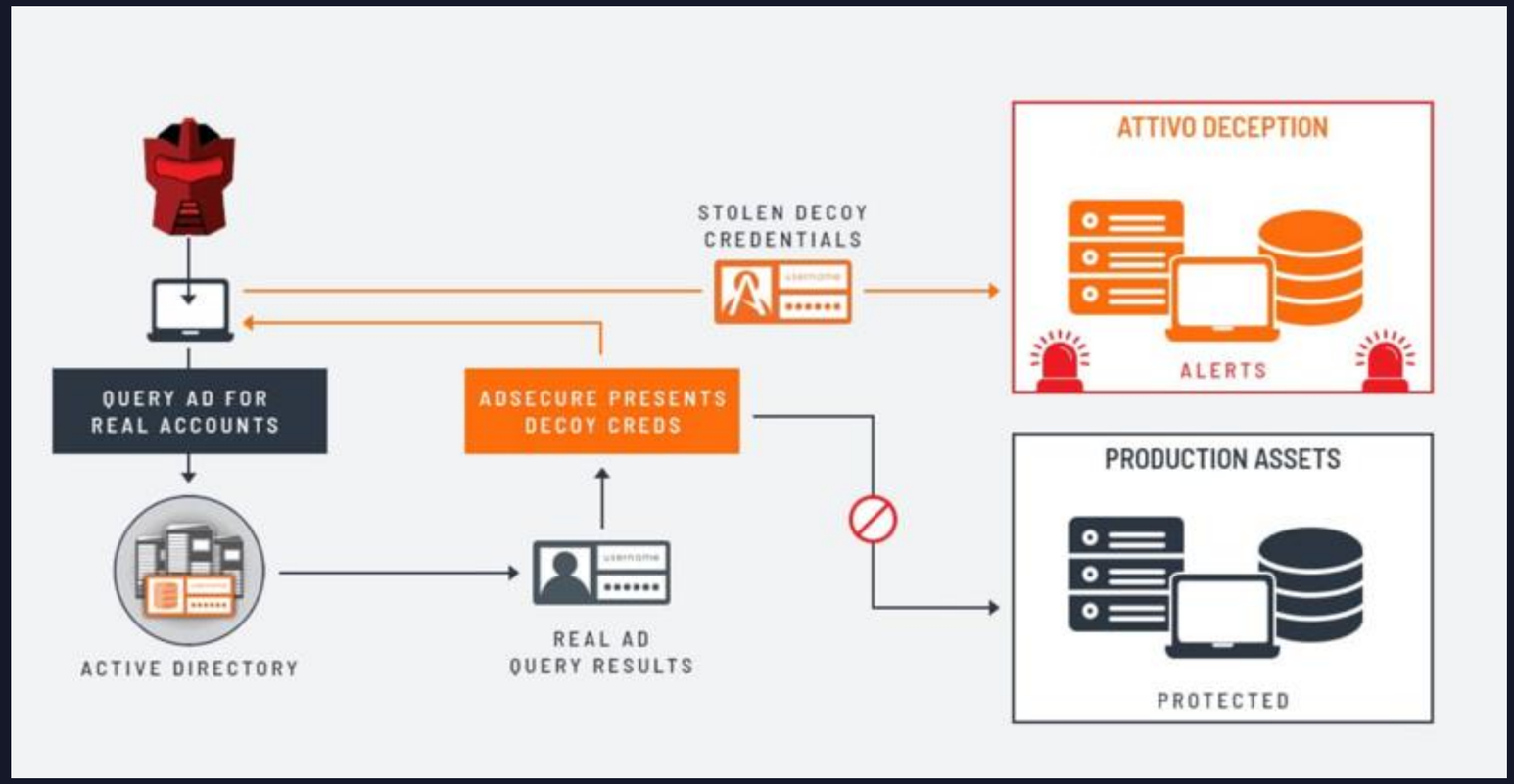
收購之前的Attivo Botsink 網路欺敵，主動防禦系統

實時接戰駭客攻擊
網路欺敵

HARDWARE BASED PLATFORM TO CREATE AND MANAGE DECOYS

Create thousands of real decoys across entire infrastructure

偵測/誤導端點上的AD攻擊



- Hides info, protect critical objects
- Returns deceptive objects
- Fake data steers attackers to decoys
- Telemetry for visibility & hunting

Cyber Kill Chain 的主動式防禦

對目標採取行動 – 第 7 步驟

攻擊方

- Collect User Credentials
- Privilege Escalation
- Internal reconnaissance
- Lateral Movement
- Collect and exfiltrate data
- Destroy systems
- Corrupt Data
- Modify Data

防守方

- Hide live Creds, show False Creds
- Hide sensitive users, show decoys
- Hide AD, Services, Shares - Derail
- Derail, allow into decoys, collect intel
- Allow collection of beaconed files, docs
- Destroy decoy systems, collect intel
- Corrupt decoy data, collect intel
- Modify decoy data, collect intel

兩類偵測和攔阻AD攻擊的比較

Attack Detection at Domain Controller

- Detect attacks affecting multiple AD objects
- Detect attacks from managed and unmanaged systems
- Detect attacks from IoT/OT devices
- Detect Attacks from Windows and non-Windows systems (Mac/Linux)
- Comprehensive attack detection and disruption

Active Directory

Detection from Endpoints

- Even more comprehensive attack detection and disruption
- Detect advanced attacks in real time
- Alert on unauthorized activities targeting AD
- Conceal sensitive or privileged AD objects, mislead with deceptive objects
- Gather adversary TTP’ s and IoCs
- Automated response

SentinelOne

端點上身份憑證的分層防禦

Cloaking, policy-based application access, credential lures, attack paths

Attack Surface Mgmt

Attack Surface Reduction
Find and remediate exposed credentials and attack paths

Decoy Credentials
Obfuscates credentials, misdirects attackers and gathers threat intelligence

Endpoint Credentials

Cloak Credentials
Hides credentials from attackers & their tools

Bind Credentials to Applications
Blocks unauthorized access to credential store

Privileged Cred & Accts

AD Query Misdirection
Detects unauthorized queries and delivers fake AD objects

Decoy Active Directory
Decoy AD environment to detect recon and gather threat intelligence

SentinelOne

Identity 還包含其他功能

- Active Directory Protection
- Active Directory Attack Detection
- Ransomware Protection ++
- Credential Theft Protection ++
- Credential-based Vulnerability Assessment & Visualization ++
- Real-time Recon Detection ++

收購之前的Attivo ADAssessor

AD
保護和評估

AGENTLESS SCANNING AND REMEDIATION SOLUTION

On-Prem or Cloud

收購之前的Attivo ADSecure DC

AD
增強型保護

AGENT FOR DC

Cloud

收購之前的Attivo EDN, 包含ADSecure EP

身份偵測與回應 **Identity Detection & Response**

AGENT FOR WORKSTATIONS

Hide Credentials, AD info, Visualize Threatpaths

收購之前的Attivo Botsink 網路欺敵，主動防禦系統

實時接戰駭客攻擊
網路欺敵

HARDWARE BASED PLATFORM TO CREATE AND MANAGE DECOYS

Create thousands of real decoys across entire infrastructure

偵測與攔阻針對 AD 的攻擊行為

SentinelOne

Questions?

掃描QRCode，填寫議程問券

憑完成畫面即可與工作人員兌換精美品牌禮品喔!

SentinelOne®

sentinelone.com