# WEBINAR

## Ochrona Active Directory przed cyberatakami oraz odtwarzanie na wypadek awarii przy wykorzystaniu narzędzi Semperis.

16 marca, godz. 12.00

QDP

semperis

Rozpoczynamy punktualnie o 12.00

# WEBINAR

## Ochrona Active Directory przed cyberatakami oraz odtwarzanie na wypadek awarii przy wykorzystaniu narzędzi Semperis.

**16 marca, godz. 12.00**


Paweł Żuchowski *CTO, QDP*
Calum Field *Senior Solution Architect, Semperis*
Robert Głowacki *Dyrektor Handlowy, QDP*
Krzysztof Rocki *Regional Director CEE, Semperis*


QDP semperis

QDP
Efektywność i bezpieczeństwo IT

semperis

# Agenda

- O firmie QDP
- O firmie Semperis
- Nowe wyzwania bezpieczeństwa
- Dlaczego warto zabezpieczać Active Directory
- NIST Cybersecurity Framework
- Działania przed/podczas/po ataku
- Sesja pytań i odpowiedzi

W trakcie prezentacji zaplanowaliśmy pokazy DEMO rozwiązań.

QDP
Efektywność i bezpieczeństwo IT

semperis

**QDP Sp. z o.o.** (wcześniej **Quest-Dystrybucja**) to dostawca i integrator rozwiązań przeznaczonych do optymalizacji zarządzania systemów IT oraz utrzymania cyberbezpieczeństwa.

Przedstawiciel wiodących na rynku producentów oprogramowania: **IDERA, Micro Focus, IPG Group, Semperis, CybeReady, Cymulate, Sasa Software, Broadcom, Secret Double Octopus, Yubico, ApiOmat/Easy Software, InfoBay** oraz dostawca usług dotyczących produktów **Quest Software/One Identity**.

Dzięki bezpośredniej współpracy z producentami  spółka zapewnia wsparcie w zakresie wdrożenia i użytkowania oferowanego oprogramowania.

QDP
Efektywność i bezpieczeństwo IT

semperis

Oferujemy rozwiązania informatyczne oraz wsparcie technologiczne i usługi integratorskie w zakresie:

- cyberbezpieczeństwa informatycznego
- zarządzania bazami danych i infrastrukturą Microsoft
- monitorowania systemów
- zarządzania tożsamością i dostępem
- automatyzacji procesów
- bezpiecznej komunikacji

semperis

NA POCZATEK

# O firmie Semperis

KKR

INSIGHT PARTNERS

Microsoft Partner
Enterprise Cloud Alliance
Microsoft Accelerator Alumni
Microsoft Co-Sell

Inc.5000 Nº 4 2022 IND SECURITY

500 Technology Fast 500 2022 NORTH AMERICA Deloitte.

Inc. 5000 Vet100 SIVMF AMERICA'S FASTEST GROWING VETERAN OWNED BUSINESSES 2022

Inc. Best Workplaces SECURITY 2022

CYBER SECURITY EXCELLENCE AWARDS WINNER 2023

CISO CHOICE AWARDS

BLACK UNICORN AWARDS 2022 FINALIST

THE CHANNEL CO. CRN CLOUD 100 2023

THE CYBER TOP 20

GLOBAL INFOSEC AWARDS WINNERS CYBER DEFENSE MAGAZINE 2021

2022 GLOBEE AWARDS GOLD WINNER INFORMATION TECHNOLOGY

QDP
Efektywność i bezpieczeństwo IT

semperis

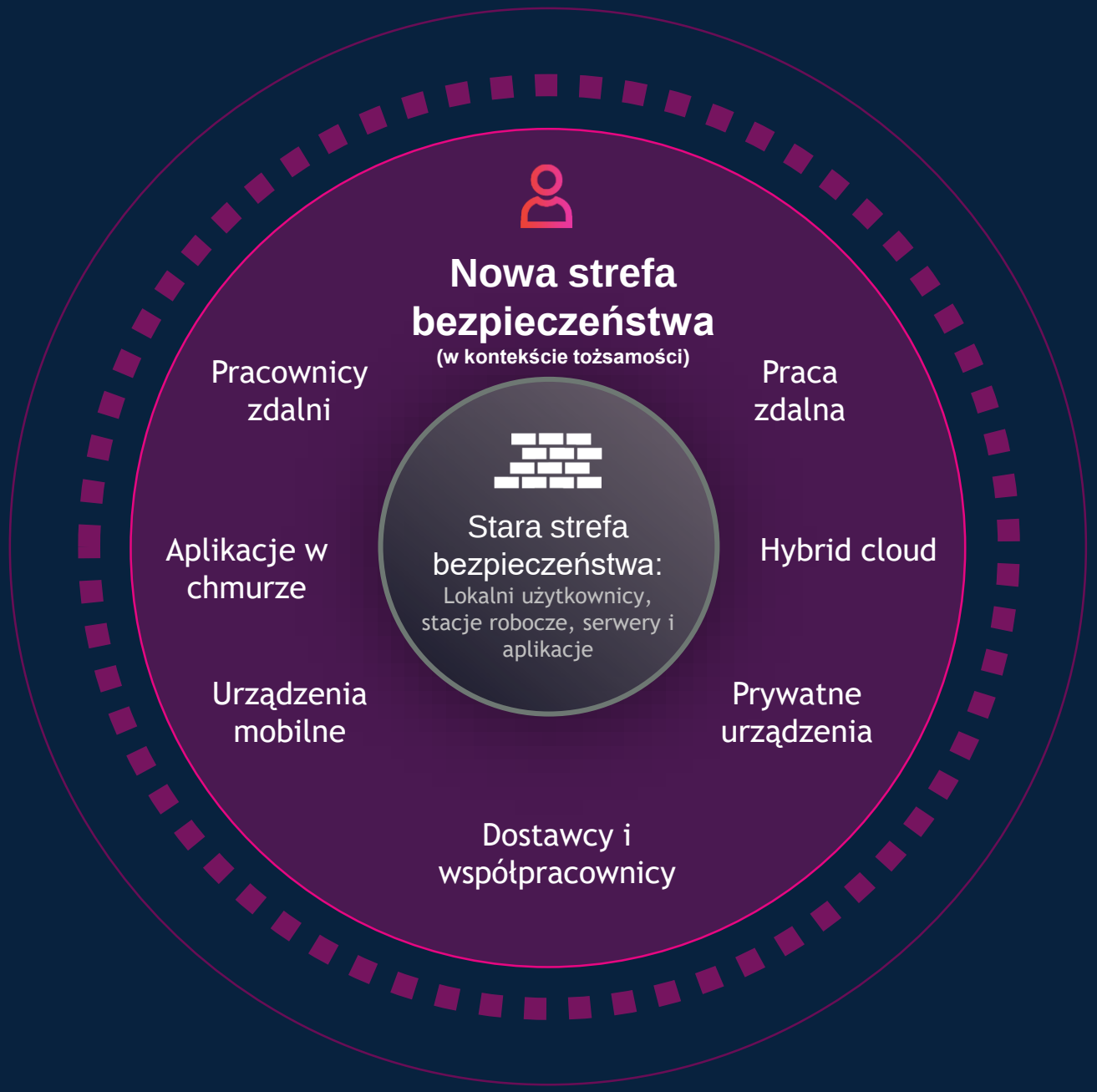
# Zaczynamy od małej awarii ☺

semperis

WYZWANIA BEZPIECZEŃSTWA

# Zabezpiecz środowisko podlegające zmianom i rozwijające się

1. Utrzymuj bezpieczeństwo w dotychczasowym środowisku
2. Otwórz się na cyfrowa transformację
3. Konsoliduj i automatyzuj bezpieczeństwo

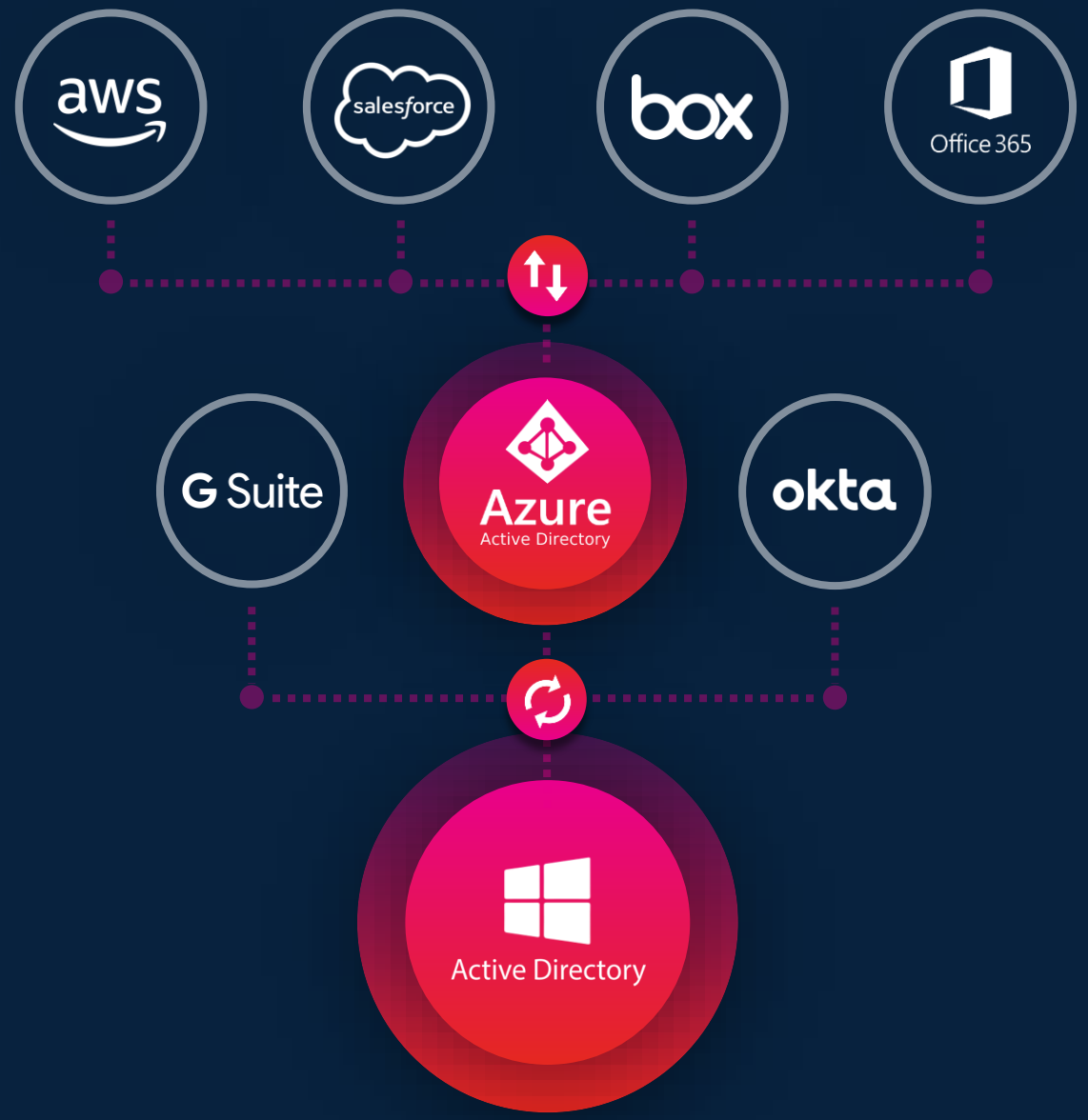


semperis

KLUCZE DO KRÓLESTWA

# Jeżeli AD nie jest bezpieczne, nic nie jest bezpieczne

- 80% wszystkich włamań jest opartych na kradzieży tożsamości
- Poziom bezpieczeństwa AD ciągle się obniża
- Rozwiązania chmurowe rozszerzają się poza AD
- Model Zero trust zakłada integralność rozwiązania hybrid AD




**90% przedsiębiorstw używa AD jako podstawowa platforma tożsamości**

semperis

PRZYKŁADY ATAKÓW

# AD na celowniku atakujących

Usługa Active Directory stała się w ostatnich latach głównym celem ataków.
Lokalna usługa AD jest coraz częściej wykorzystywana jako pierwszy krok w ataku na środowiska chmurowe.

**SOLARWINDS**
2020

**BALTIMORE**
2019

**SINGHEALTH**
2018

**MONDELEZ**
2017

**TARGET**
2013

**NTT COMMUNICATIONS**
2020

**NORSK HYDRO**
2019

**MAERSK**
2017

**SONY**
2014

**SAUDI ARAMCO**
2012

semperis

Fundamenty bezpieczeństwa tożsamości

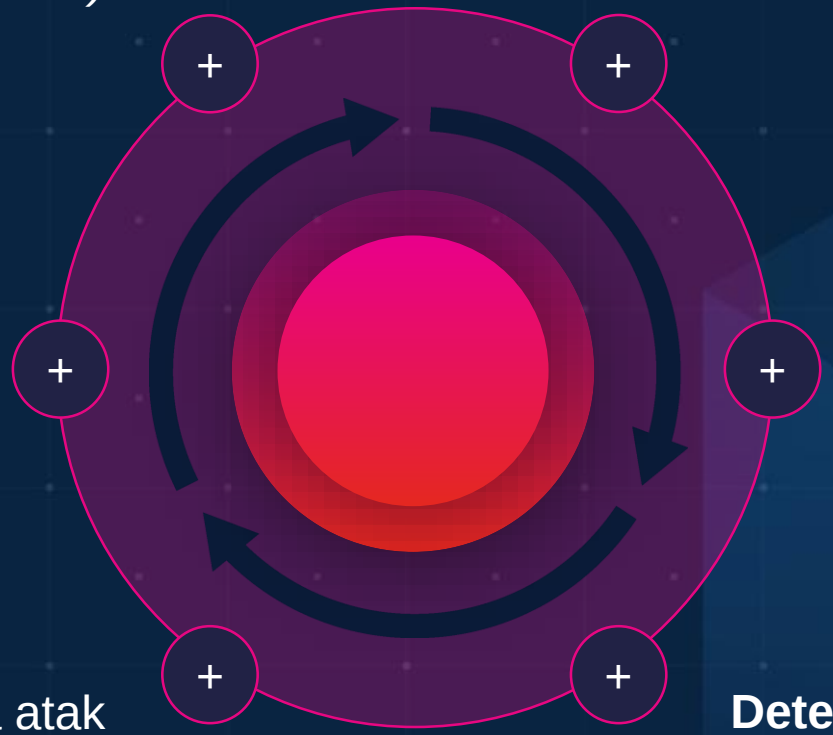
# Co należy zrobić aby zabezpieczyć środowisko Active Directory?

semperis

# NIST Cybersecurity Framework

*(Weryfikacja & Analiza)*

**Identyfikacja:** ryzyka



**Przywracanie:** po ataku

**Ochrona:** usługi

**Reagowanie:** na atak

**Detekcja:** ataku

semperis

Przed atakiem | Podczas ataku | Po ataku

Kryminalistyka i dochodzenie

Monitorowanie i wykrywanie IOE & IOC

Identyfikacja


Odzyskiwanie po awarii (Cyber-First)

Ocena podatności

Zabezpieczenie

Automatyczne naprawianie

Wykrywanie zagrożeń i ich widoczność

IOC oznacza Indicator of Compromise
IOE oznacza Indicator of Exposure

semperis

PURPLE KNIGHT

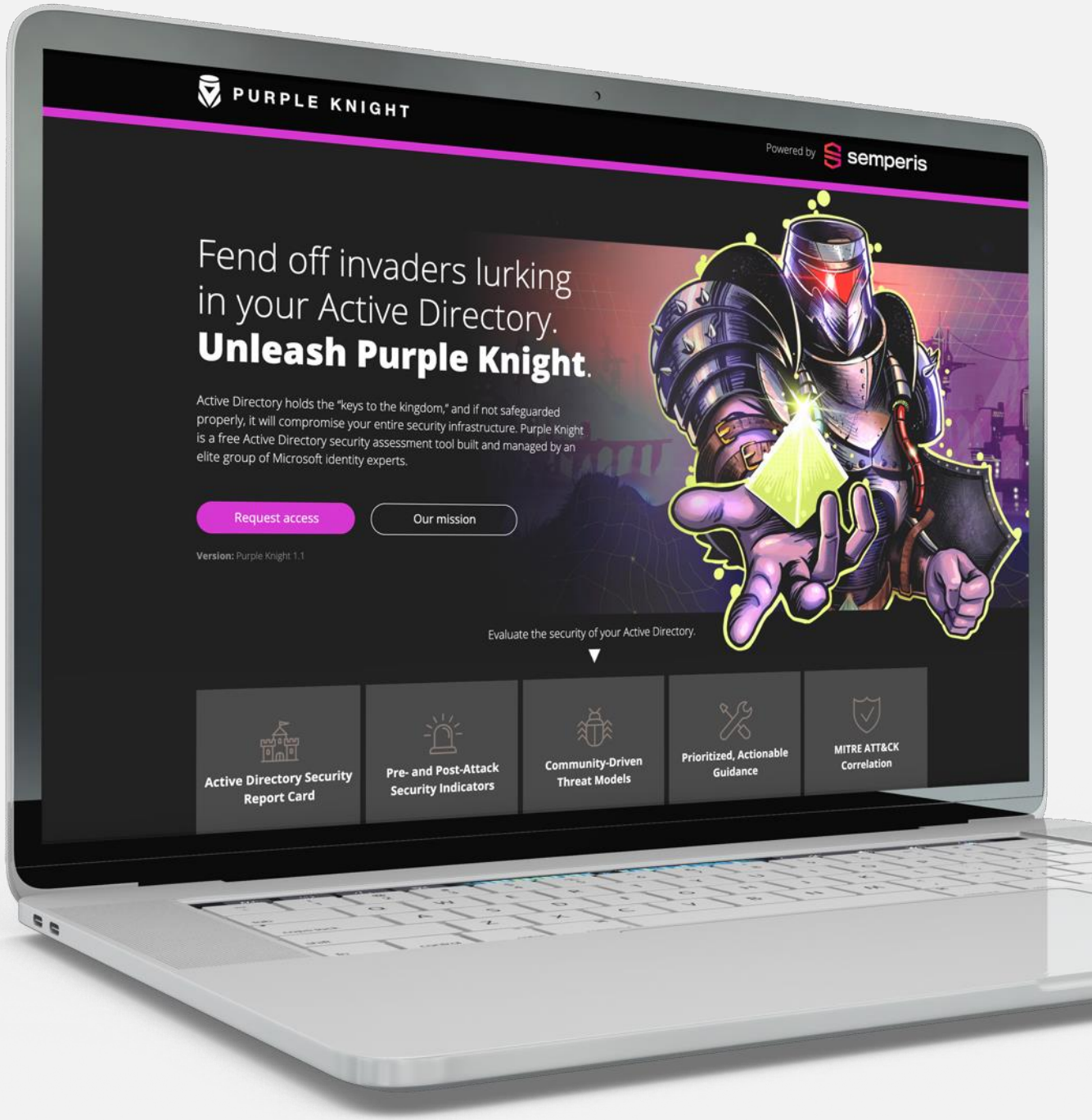
# Na szybko oceń poziom bezpieczeństwa AD

**Purple Knight** to narzędzie do oceny bezpieczeństwa usługi Active Directory stworzone i zarządzane przez grupę ekspertów związanych z bezpieczeństwem systemów Microsoft (ponad 4000 pobrań)

2021 GLOBEE AWARDS SILVER WINNER
CYBER SECURITY GLOBAL EXCELLENCE AWARDS

**2021 GLOBEE® Winner**
Risk Management Solution
Innovation | Purple Knight

Learn more at **purple-knight.com** →

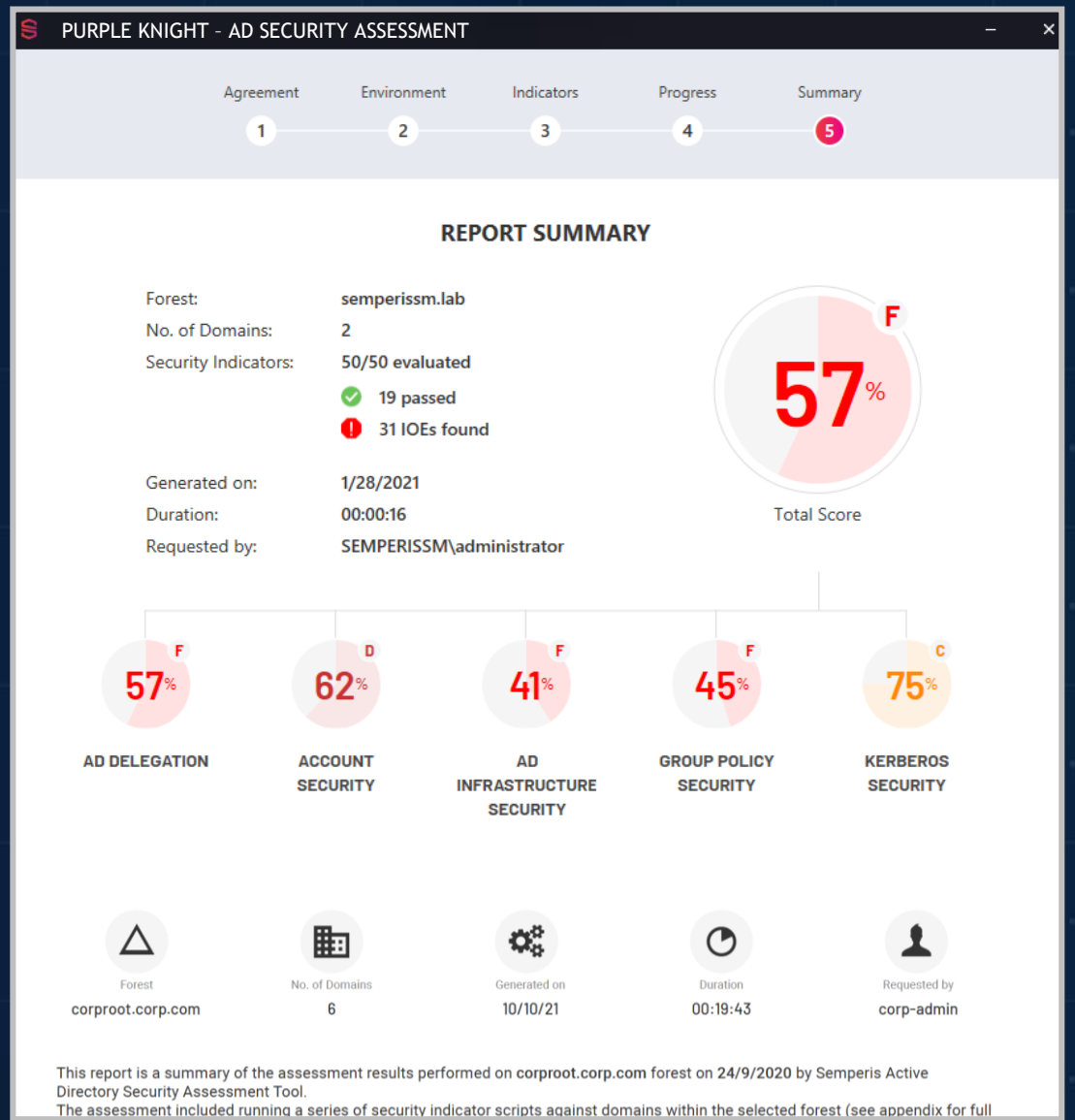


semperis

## KARTA RAPORTU BEZPIECZEŃSTWA

# Wykryj słabe punkty zanim zrobią to atakujący

- Wskaźniki bezpieczeństwa dla fazy przed i po ataku
- Modele zagrożeń tworzone przez społeczność
- Praktyczne wskazówki z określonym priorytetem
- Korelacja z frameworkiem MITRE ATT&CK
- Bez opłat, rozwijane przez społeczność



QDP
Efektywność i bezpieczeństwo IT

semperis

# Purple Knight Demo

semperis

Przed atakiem | Podczas ataku | Po ataku

Kryminalistyka i dochodzenie

Monitorowanie i wykrywanie IOE & IOC


Odzyskiwanie po awarii (Cyber-First)

Ocena podatności

Reakcja

Automatyczne naprawianie

Wykrywanie zagrożeń i ich widoczność

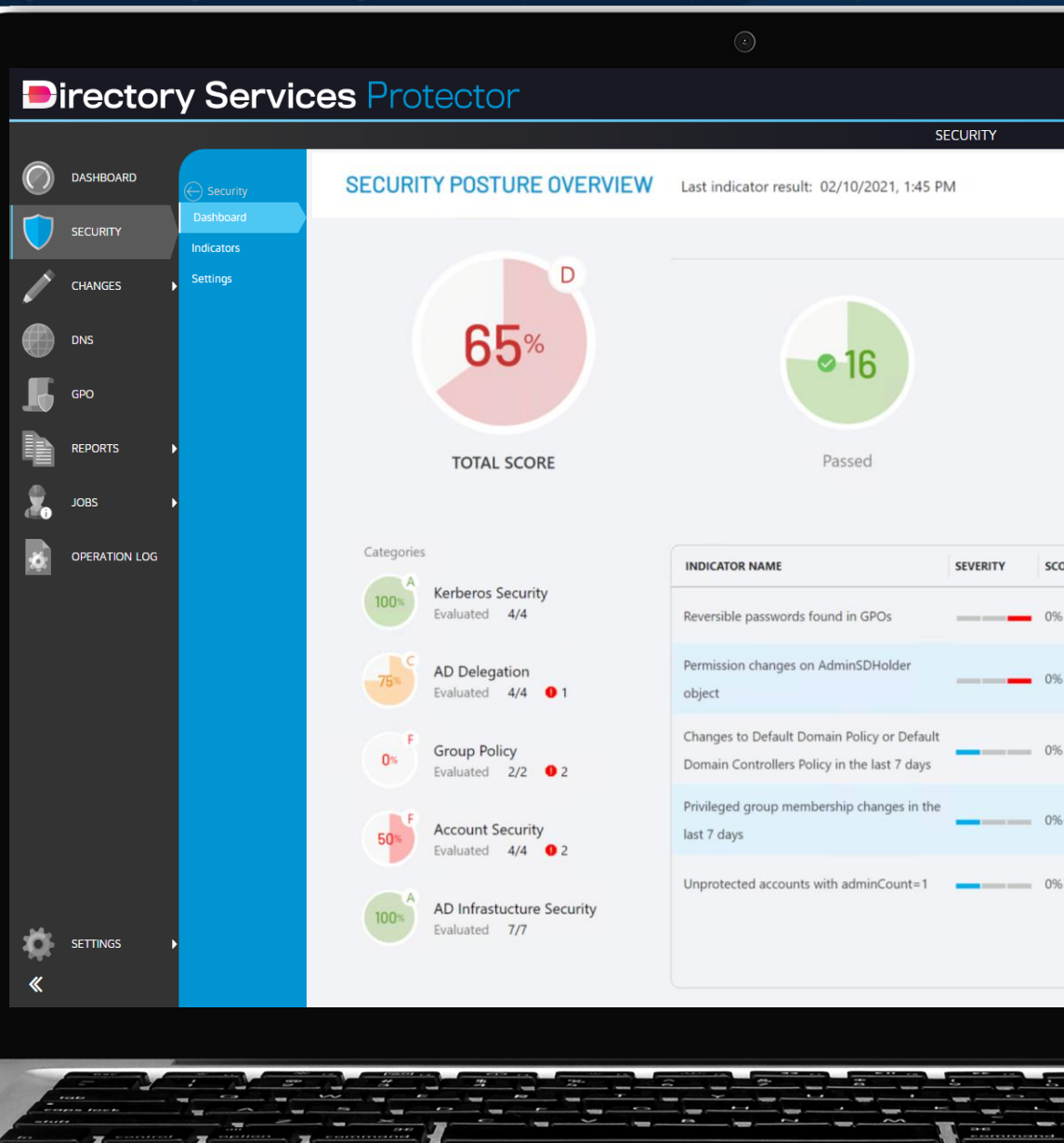
Wykrywanie

semperis

KOMPLEKSOWE ZABEZPIECZENIE

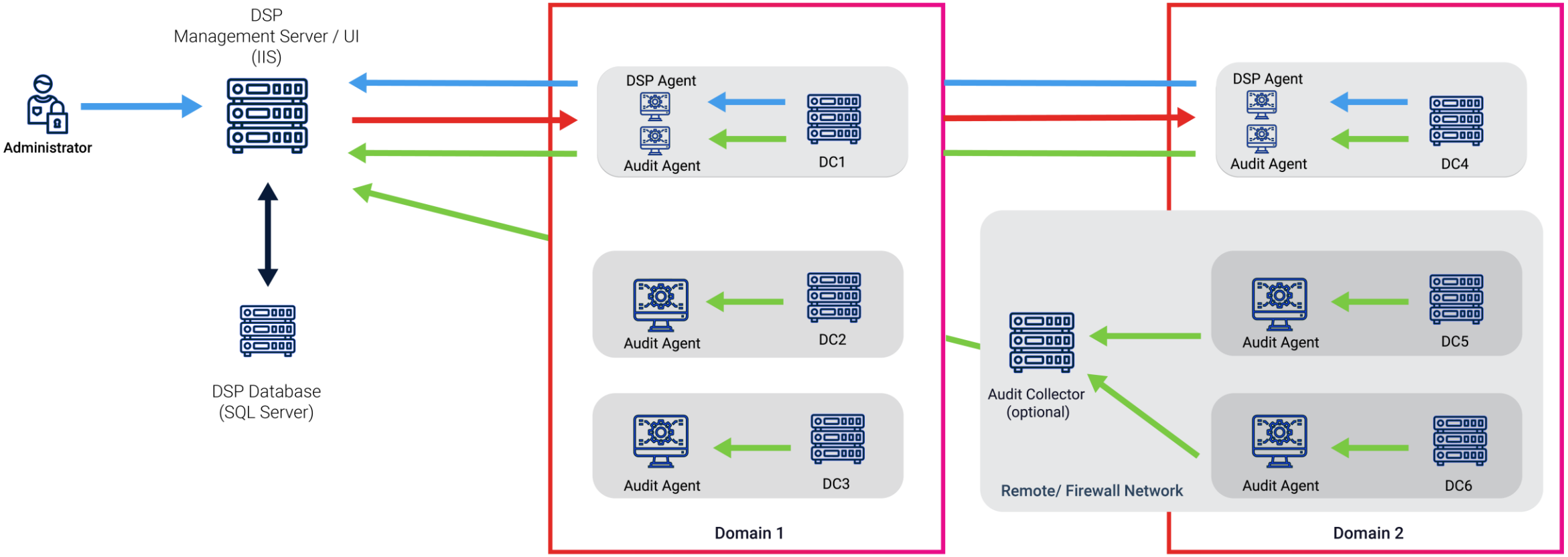
# Monitoruj, wykrywaj i reaguj

- Ciągła ocena podatności
- Monitorowanie odporne na manipulacje
- Alerty bezpieczeństwa w czasie rzeczywistym
- Automatyczna naprawa (wycofywanie złośliwych zmian)
- Raporty zgodności



# Architektura rozwiązania Directory Services Protector

semperis




Replication Data

Undo/Restore Data

Security Event Log Data

QDP
Efektywność i bezpieczeństwo IT

semperis

# Directory Services Protector DEMO

semperis

Przed atakiem | Podczas ataku | Po ataku

Kryminalistyka i dochodzenie

Monitorowanie i wykrywanie IOE & IOC

Odtwarzanie


Odzyskiwanie po awarii (Cyber-First)

Ocena podatności

Automatyczne naprawianie

Wykrywanie zagrożeń i ich widoczność

semperis

ODTWARZANIE (CYBER-FIRST)

# Skrócenie czasu odtwarzania z dni do godzin

- Pewny Backup (bez malware)
- Szybkie odtwarzanie
- Automatyzacja
- Odtwarzanie gdziekolwiek

PORÓWNANIE KOPII ZAPASOWYCH

# ADFR a inne kopie zapasowe Kontrolera Domeny

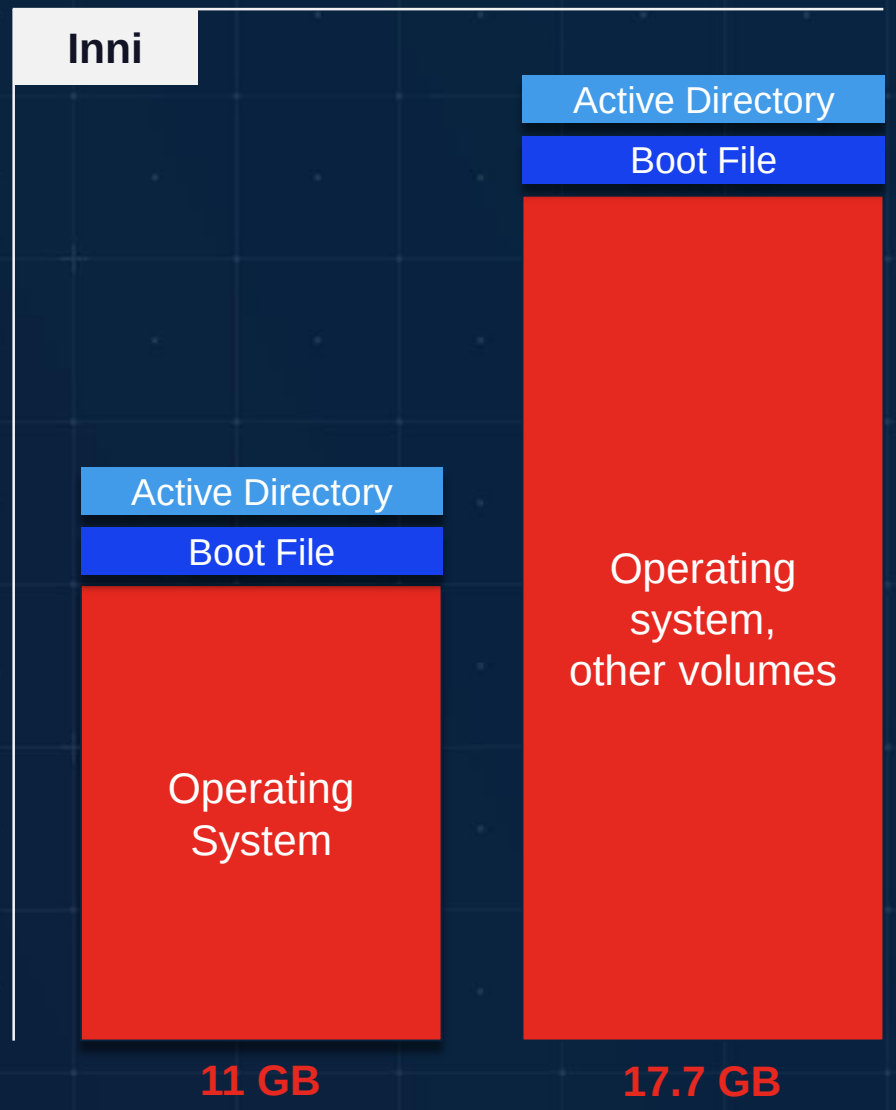
**ADFR**

**116 MB**
(500 MB przed kompresją)

- Active Directory
- Boot File

**Kopia zapasowa ADFR**

- ✓ Nie zawiera OS → brak malware rezydującego w OS
- ✓ Usunięte zależności źródłowego sprzętu → odtwarzanie gdziekolwiek
- ✓ Znacznie mniejsze
- ✓ Szybsze tworzenie kopii bezpieczeństwa i odtwarzanie
- ✓ Mniejsze wymagania dotyczące storage



# W jaki sposób mar

1. Pull the network cables from all DCs or otherw
2. Connect DCs to be restored to a private netwo private VLAN)

For each domain,

3. Nonauthoritative restore of first writeal
4. Auth restore of SYSVOL on that DC
5. Look for malware, etc. Forensic analysis
6. Reset all admin account passwords
7. Seize FSMOs
8. Metadata cleanup of all writeable DCs e
9. Configure DNS on the forest root DC
10. Remove the global catalog from each D

<Wait for GC to unhost...>

11. Delete DNS NS records of DCs that no longer ex
12. Delete DNS SRV records of DCs that no longer e
13. Raise the RID pool by 100K
14. Invalidate the current RID pool
15. Reset the computer account of the root DC twi
16. Reset krbtgt account twice

<seed forest at this point>

**Microsoft Whitepaper**: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/ad-forest-recovery-guide

learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/ad-forest-recovery-perform-initial-recovery

Filter by title

- Identity and Access
- Solutions and Scenario Guides
- Active Directory Domain Services
  - Active Directory Domain Services
  - What's new in Active Directory Domain Services
  - AD DS Getting started
  - AD DS Design and Planning
  - AD DS Deployment
  - AD DS Operations
    - AD DS Operations
    - AD Forest Recovery Guide
      - AD Forest Recovery Guide
      - AD Forest Recovery - Prerequisites
      - AD Forest Recovery - Steps for Recovery
      - AD Forest Recovery - Identify the Problem
      - **AD Forest Recovery - Perform Initial Recovery**
      - AD Forest Recovery - Procedures
      - AD Forest Recovery - FAQ
      - AD Forest Recovery - Recovering a single domain with multidomain forest
      - AD Forest Recovery - Virtualization
      - AD Forest Recovery - Windows Server 2003
    - Best Practices for Securing Active Directory
    - Active Directory Replication and Topology Management Using Windows PowerShell
    - Managing RID issuance
    - Active Directory Domain Services component updates
    - Active Directory accounts
    - Special identities
    - Active Directory security groups
    - Service accounts
    - Microsoft accounts

Download PDF

maintain the trust hierarchy in the forest. In addition, the forest root domain usually holds the DNS root server for the forest's DNS namespace. Consequently, the Active Directory–integrated DNS zone for that domain contains the alias (CNAME) resource records for all other DCs in the forest (which are required for replication) and the global catalog DNS resource records.

After you recover the forest root domain, repeat the same steps to recover the remaining domains in the forest. You can recover more than one domain simultaneously; however, always recover a parent domain before recovering a child to prevent any break in the trust hierarchy or DNS name resolution.

For each domain that you recover, restore only one writeable DC from backup. This is the most important part of the recovery because the DC must have a database that has not been influenced by whatever caused the forest to fail. It is important to have a trusted backup that is thoroughly tested before it is introduced into the production environment.

Then perform the following steps. Procedures for performing certain steps are in AD Forest Recovery - Procedures.

1. If you plan to restore a physical server, ensure that the network cable of the target DC is not attached and therefore is not connected to the production network. For a virtual machine, you can remove the network adapter or use a network adapter that is attached to another network where you can test the recovery process while isolated from the production network.
2. Because this is the first writeable DC in the domain, you must perform a nonauthoritative restore of AD DS and an authoritative restore of SYSVOL. The restore operation must be completed by using an Active Directory-aware backup and restore application, such as Windows Server Backup (that is, you should not restore the DC by using unsupported methods such as restoring a VM snapshot).
   - An authoritative restore of SYSVOL is required because replication of the SYSVOL replicated folder must be started after you recover from a disaster. All subsequent DCs that are added in the domain must resynchronize their SYSVOL folder with a copy of the folder that has been selected to be authoritative before the folder can be advertised.

**Caution**

Perform an authoritative (or primary) restore operation of SYSVOL only for the first DC to be restored in the forest root domain. Incorrectly performing primary restore operations of the SYSVOL on other DCs leads to replication conflicts of SYSVOL data.

- There are two options perform a nonauthoritative restore of AD DS and an authoritative restore of SYSVOL:
- Perform a full server recovery and then force an authoritative synchronization of SYSVOL. For detailed procedures, see Performing a full server recovery and Perform an authoritative synchronization of DFSR-replicated SYSVOL.
- Perform a full server recovery followed by a system state restore. This option requires that you create both types of backups in advance: a full server backup and a system state backup. For detailed procedures, see Performing a full server recovery and Performing a nonauthoritative restore of Active Directory Domain Services.

QDP
Efektywność i bezpieczeństwo IT

semperis

# Active Directory Forest Recovery DEMO

semperis

# Wykrywanie zagrożeń oraz reagowanie na incydenty

## PEŁNE WSPARCIE W PROCESIE

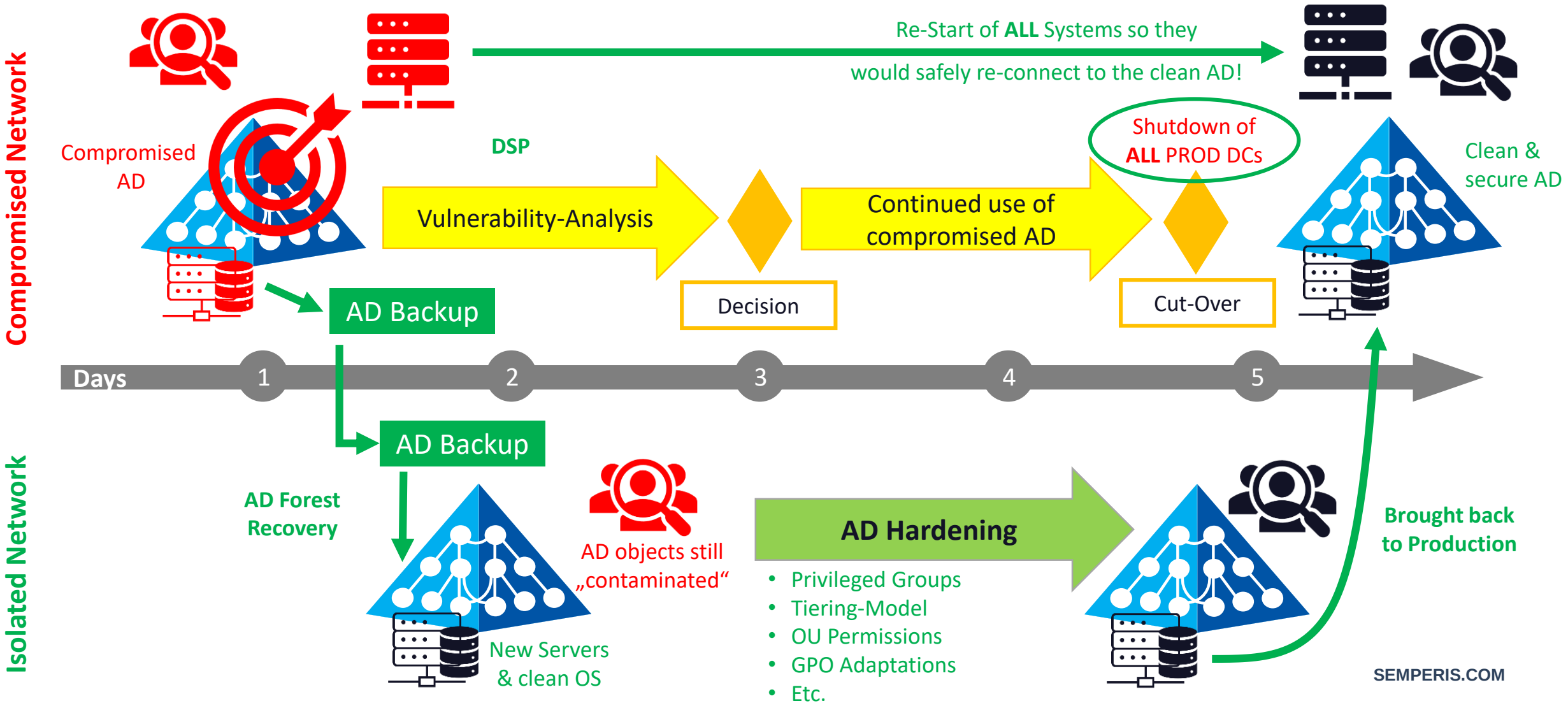
Semperis to nie tylko kolejny dostawca zabezpieczeń, ale rzeczywisty partner w całym procesie

Przygotowanie → Wykrywanie i analiza → Odseparowanie, likwidacja i odzyskiwanie → Aktywność po incydencie

**Threat Research Team** (Wykrywanie IOE & IOC)

**24/7 Incident Response Team**

# Przykład z życia




SEMPERIS.COM

semperis

Przed atakiem → Podczas ataku → Po ataku

ForestDruid

forest druid powered by semperis

Download Forest Druid

RE-SYNC AD DATA

Unclassified privilege escalation relationships: 76

Hops from Tier 0: 1

Only Privilege Escalation

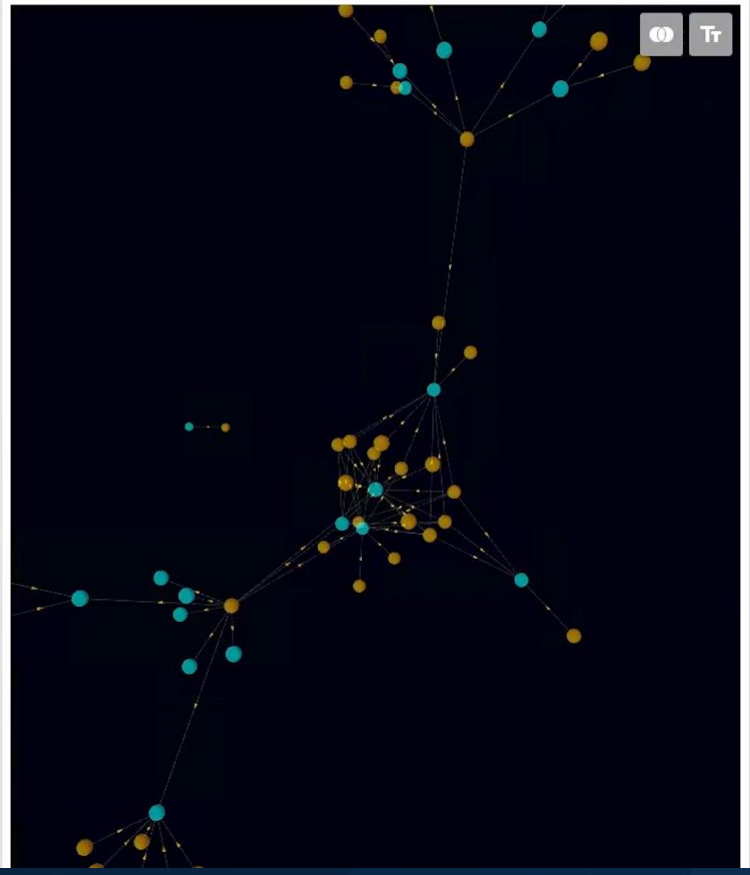
No target filtering

Classify as: TIER 0 RISKY EXPORT

Legend

Search

| Name | Type | Relation | Target Name | Target Type |
|---|---|---|---|---|
| ADOLFO_BURKE | user | Member | Domain Admins | group |
| AISHA_ARNOLD | user | Member | DnsAdmins | group |
| ALFONZO_BOONE | user | Member | Account Operators | group |
| ALYSON_JENKINS | user | GenericAll | NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS | foreignSecurityPrincipal |
| ALYSON_JENKINS | user | GenericAll | Enterprise Read-only Domain Controllers | group |
| ALYSON_JENKINS | user | GenericAll | Remote Desktop Users | group |
| ALYSON_JENKINS | user | GenericAll | Group Policy Creator Owners | group |
| ALYSON_JENKINS | user | GenericAll | DnsAdmins | group |
| ANTONE_JARVIS | user | Member | Administrators | group |
| BOBBI_BERGER | user | Member | Group Policy Creator Owners | group |
| Builtin | builtinDomain | Contains | Administrators | group |
| Builtin | builtinDomain | Contains | Account Operators | group |
| Builtin | builtinDomain | Contains | Print Operators | group |
| Builtin | builtinDomain | Contains | Backup Operators | group |
| Builtin | builtinDomain | Contains | Remote Desktop Users | group |
| Builtin | builtinDomain | Contains | Server Operators | group |
| DIANNA_MARTINEZ | user | Member | Server Operators | group |
| EDDY_MORIN | user | Member | Domain Admins | group |
| ELBERT_BEACH | user | Member | Group Policy Creator Owners | group |
| F127-D01-DC01 | computer | PrimaryGroup | Domain Controllers | group |
| F127-D01-DC02 | computer | PrimaryGroup | Domain Controllers | group |
| ForeignSecurityPrincipals | container | Contains | NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS | foreignSecurityPrincipal |
| GENEVIEVE_CARR | user | Member | Account Operators | group |



& IOC

purple knight powered by semperis

forest druid powered by semperis

Directory Services Protector

QDP
Efektywność i bezpieczeństwo IT

semperis

# Pytania ?

**Linki do produktów:**
Directory Services Protector - https://www.semperis.com/active-directory-security/
Active Directory Forest Recovery - https://www.semperis.com/active-directory-forest-recovery/
Purple Knight - https://www.purple-knight.com/
Forest Druid - https://www.purple-knight.com/forest-druid/

Blog Semperis - https://www.semperis.com/blog/
NIST Cybersecurity Framework - https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02122014pl.pdf
Active Directory Forest Recovery Guide - https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/ad-forest-recovery-guide

QDP
Efektywność i bezpieczeństwo IT

semperis

# Dziękujemy za uwagę

Zapraszamy do kontaktu:

Paweł Żuchowski
p.zuchowski@qdp.com.pl
601 445 882

Robert Głowacki
r.glowacki@qdp.com.pl
666 891 311