semperis

SEMPERIS VORSTELLUNG

Verteidigung gegen Ransomware beginnt mit dem Schutz von Active Directory und Azure AD

Ein umfassendes Paket für den gesamten Lebenszyklus vor, während und nach einem Angriff auf Identitätsverzeichnisse wie AD und Azure AD

Oliver Keizers
Area Vice President Central Europe, Semperis


oliverk@semperis.com


www.semperis.com/contact

semperis

KEYS TO THE KINGDOM

Identity ist der neue Perimeter

Für mehr als 90% der Unternehmen beginnt **Identity jedoch mit Active Directory** als zentralem Anmelde- und Verzeichnisdienst.

Legacy AD Infrastrukturen stellen die Basis für **hybride Cloud Identitäten** dar.

semperis

KEYS TO THE KINGDOM

Und wenn AD nicht sicher ist, ist es nichts mehr

Cloud Identity ist die Erweiterung des Active Directory. Veränderungen und Schäden hier haben einen Folgeeffekt in der gesamten Identity-Infrastruktur.

Auch das Zero Trust Modell basiert darauf, dass die einzig vertrauenswürdige Komponente Identity ist.

semperis

BEKANNTE ANGRIFFE

Im Fadenkreuz der Angreifer

Active Directory wurde in vergangenen Jahren einem wichtigen Einfallstor und Schwerpunkt für Angriffe.

Und das On-Premise-AD wird zunehmend als Sprungbrett für den Zugriff auf Cloud-Umgebungen genutzt.

SOLARWINDS
2020

BEIERSDORF
2017

MONDELĒZ
2017

BUNDESTAG
2015

TARGET
2013

NTT COMMUNICATIONS
2020

NORSK HYDRO
2019

MAERSK
2017

RUAG
2016

SONY
2014

Und bitte denken Sie an Kaseya, Hafnium, ZeroLogon, PrintNightmare und all die anderen kürzlich aktiven Lücken

semperis

PHASEN EINES RANSOMWARE-ANGRIFFS

Initialer Zugang

- Phishing E-Mails
- Kompromittierte Web-Seiten
- Gezielter Angriff mit **gestohlenen Zugangs-Kennungen**

Nach dem Exploit

- Download von Malware für die **Recon-Phase**
- Verbindungen zu den C2* Systemen herstellen
- Fern-Verbindungen zur Kontrolle des weiteren Angriffs sind vorhanden

Suchen & Erkennen

- Reconnaissance
- Prüfen der **AD Schwachstellen** mit dem Ziel zur **Kontroll-Übernahme der AD Domäne**
- Laterale Verbreitung auf anderen Systeme
- Sammeln von Anmelde-Kennungen und Elevation der Berechtigungen

Kernangriff

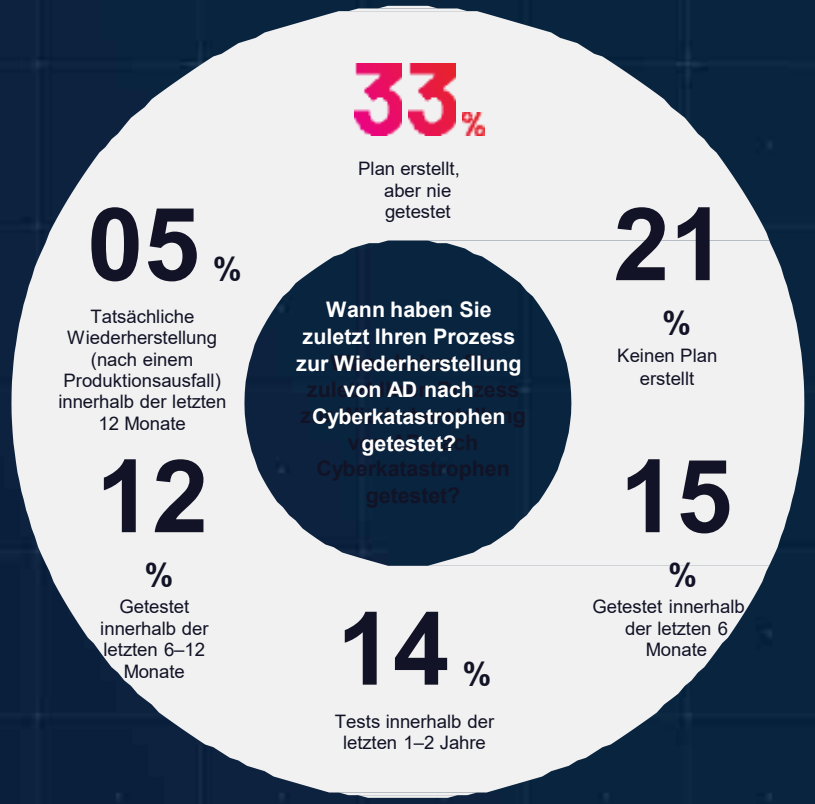
- Zugriff auf und Extraktion von Kerngeschäftsdaten
- Verschlüsselung von allen Systemen, inklusive der Backups und häufig einschließlich **AD-Domänencontrollern**

* C2 = Command-and-Control

WIE SCHNELL KÖNNEN SIE AD WIEDERHERSTELLEN?

- Nur 37 % der Unternehmen sind sich der Komplexität der Wiederherstellung von Forests bewusst
- Mehr als 50 % der Befragten haben ihren AD-Wiederherstellungsprozess noch nie getestet –

  oder haben nicht einmal einen ausgearbeitet



semperis

Gartner empfiehlt AD-spezifische Sicherheit und Wiederherstellung.

*“Unternehmen, die über kein geeignetes AD-Backup-System verfügen, haben kaum eine andere Wahl, als **das Lösegeld zu zahlen**.”*

Nik Simpson, Gartner
Gartner: How to Protect Backup Systems from Ransomware

"Tools von Anbietern wie ... Semperis ... bieten eine umfangreichere **Sicherungs- und Wiederherstellungsplattform** für Active Directory als die AD-Sicherungsmodule, die in den meisten Enterprise Backup Produkten enthalten sind."
Gartner: How to Protect Backup Systems from Ransomware

“Wenn Active Directory nicht **bereinigt und abgesichert** wird, bevor Anwendungen wieder online gestellt werden, besteht ein hohes Risiko, dass Angreifer schnell die Kontrolle über wiederhergestellte Systeme erlangen.”
Gartner: Restore vs. Rebuild — Strategies for Recovering Applications After a Ransomware Attack

“Regelmäßige Backups von Active Directory an einem sicheren Ort, z. B. in einem Datentresor aufbewahren und den Wiederherstellungsprozess üben. Wenn möglich, **Active Directory-spezifische Backup-Tools** einsetzen, um den Prozess zu erleichtern und zu beschleunigen.”
Gartner: Restore vs. Rebuild — Strategies for Recovering Applications After a Ransomware Attack

semperis

SEMPERIS IN DER REGION

Semper Paratus: Ständig bereit

2013 gegründet

2015 US Inc.

2020 Europa

2021 D-A-CH

320+ im Team

+28 Länder

<300 AD Konten

>240 Kunden

>3 Mio. AD Konten

Stark in deutschsprachigen Mittelstand über sämtliche Industriezweige hinweg:

- Lebensmittelproduktion
- Maschinenbau
- Chemie
- Logistik
- Consulting
- Textil
- Pharma
- Medien
- Etc.

Von 300 Mitarbeitern bis zu vielen Tausenden. Egal, ob IT in-house oder draußen, ob IT-intensiv oder nicht.

semperis

Wenn AD nicht sicher ist, ist nichts sicher.

“Obwohl Unternehmen die Bedeutung von AD erkannt haben, wird die Sicherheit von AD oft nicht bedacht. Wenn AD geknackt wird, erhält ein Angreifer **praktisch uneingeschränkten Zugriff** auf das gesamte Netzwerk und die Ressourcen des Unternehmens. Dies macht AD zu einem **besonders wertvollen Ziel** für Angreifer.”

— Gartner

Source: Gartner, Emerging Technologies and Trends Impact Radar: Security Published 12 October 2021

semperis

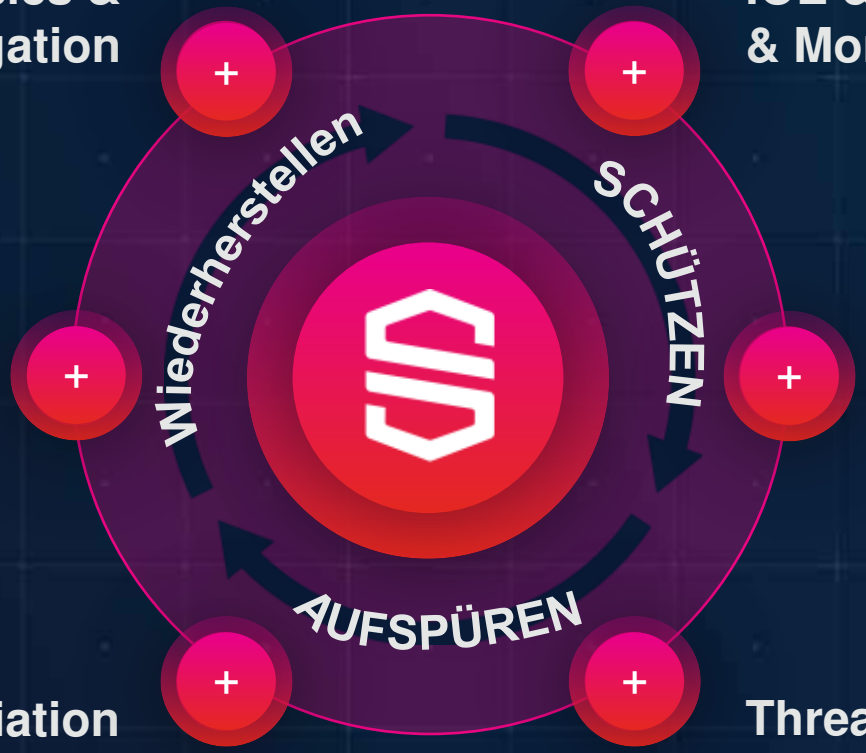
Was also braucht es, um Ihr AD zu schützen, zu sichern und wiederherzustellen?

semperis

Vor dem Angriff | Während des Angriffs | Nach dem Angriff

Forensics & Investigation

IOE & IOC Discovery & Monitoring



Cyber-First Disaster Recovery

Vulnerability Assessments

Auto-Remediation & Incident Response

Threat Detection & Visibility

semperis

PRODUKTANGEBOT

Semperis Purple Knight™

(PK) **Bewertung der Sicherheit eines Kunden AD** mithilfe eines Active Directory-Sicherheitsscanners, der von der Elite der Microsoft-Identitätsexperten entwickelt und gepflegt wird.

Semperis Directory Services Protector™

(DSP) **Echtzeit-Tracking und AD-Auditing** mit granularer Suche, Abgleich und Wiederherstellung von Objekten und Attributen mit höchster Datenintegrität durch Quellkorrelation.

On-Premise Active Directory und Azure Active Directory

Semperis Active Directory Forest Recovery™

(ADFR) **Vollständig automatisierte AD Forest Disaster-Recovery** mittels eines einfachen Restore-Wizards, erstmalig mit Hardware-agnostischer & Malware-freier AD-Wiederherstellung.

semperis

EXPERTENWISSEN

75+ Jahre MSFT MVP Erfahrungen

Microsoft Ventures Alumni | Azure Co-sell Partner | Cloud Alliance

James (Jim) Dogget | CISO
- Former Chief Technology Risk Officer at AIG

Guy Teverovsky | CTO
- Former Senior Premier Field Engineer at Microsoft

Darren Mar-Elia (MVP) | VP of Products
- Former CTO Windows Division at Quest Software
- “GPO Guy”

Guido Grillenmeier (MVP) | Chief Technologist
- Former Chief Technologist at HP | DXC Technology

Jorge de Almeida Pinto (MVP) | Senior Solutions Architect
- +16 years MVP for "Identity and Access - Directory Services"

Gil Kirkpatrick (MVP) | Chief Architect
- Former Chief Architect at Quest Software
- DEC Conference Founder

Igor Baikalov | Chief Scientist
- Former Global Information Security at Bank of America

Sean Deuby (MVP) | Director of Services
- Former Lead Active Directory Architect at Intel
- Former Technical Director at Windows IT Pro

Chris Roberts | Hacker in Residence
- World-Renowned Hacker

semperis

BREACH PREPAREDNESS & RESPONSE SERVICES

Vorbereitung & Härtung | **Reaktion**

- **AD Security Assessment**
- **AD Threat Mitigation**
- **AD DR Planning & Exercise**
- **Cyber-First AD Recovery**
- **AD Incident Investigation & Attack Forensics**
- **AD Threat Removal**

Threat Research Team (IOE & IOC Discovery)

24/7 Incident Response Team

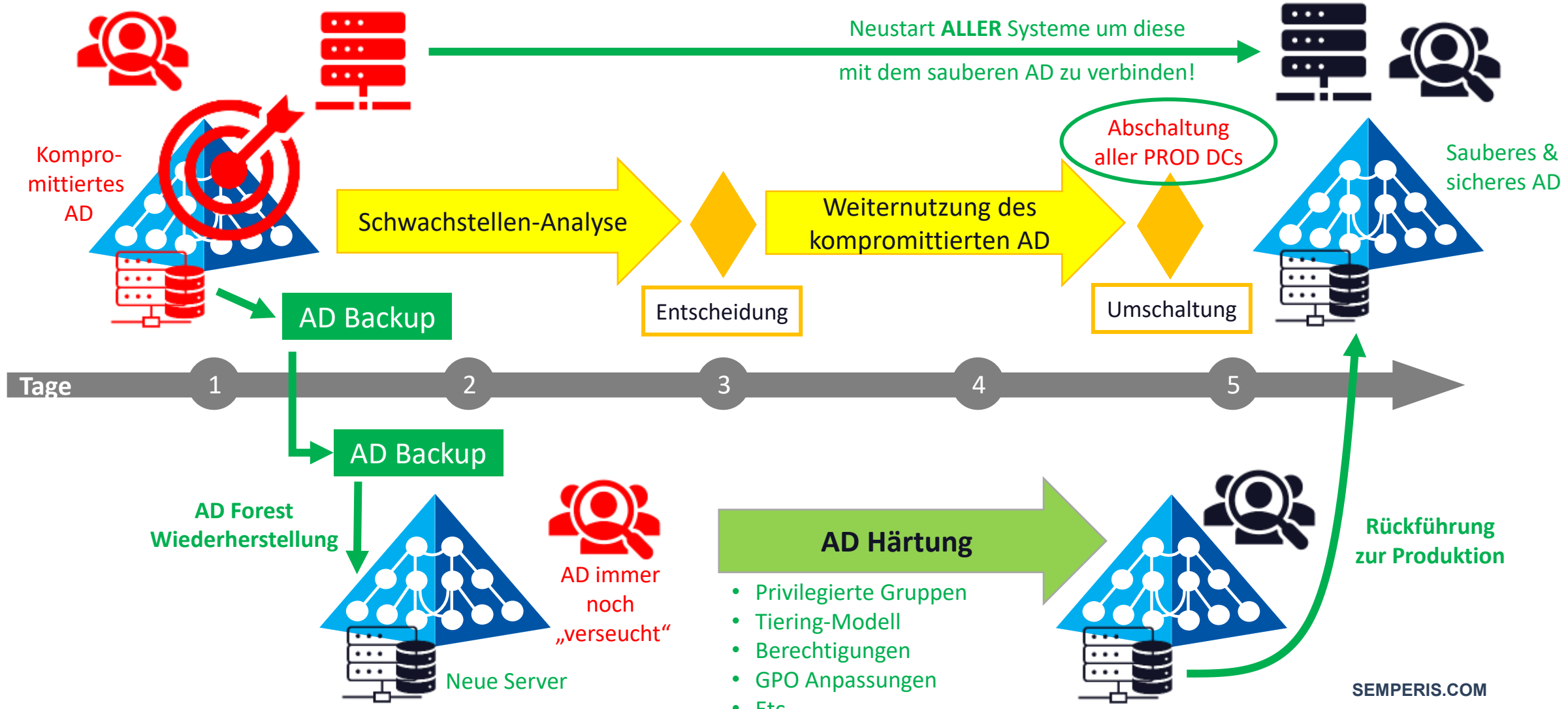
- \+ Einsatzerprobte Experten und leistungsstarke Tools
- \+ Komplexe Dienstleistungen für jede Phase des IR-Zyklus
- \+ Globales 24/7-Supportteam zur Reaktion auf Vorfälle
- \+ Hilfe für Kunden mit oder ohne Semperis-Produkte

Reales Beispiel einer AD-Rettung

semperis

Kompromittiertes Netz

Isoliertes Netz

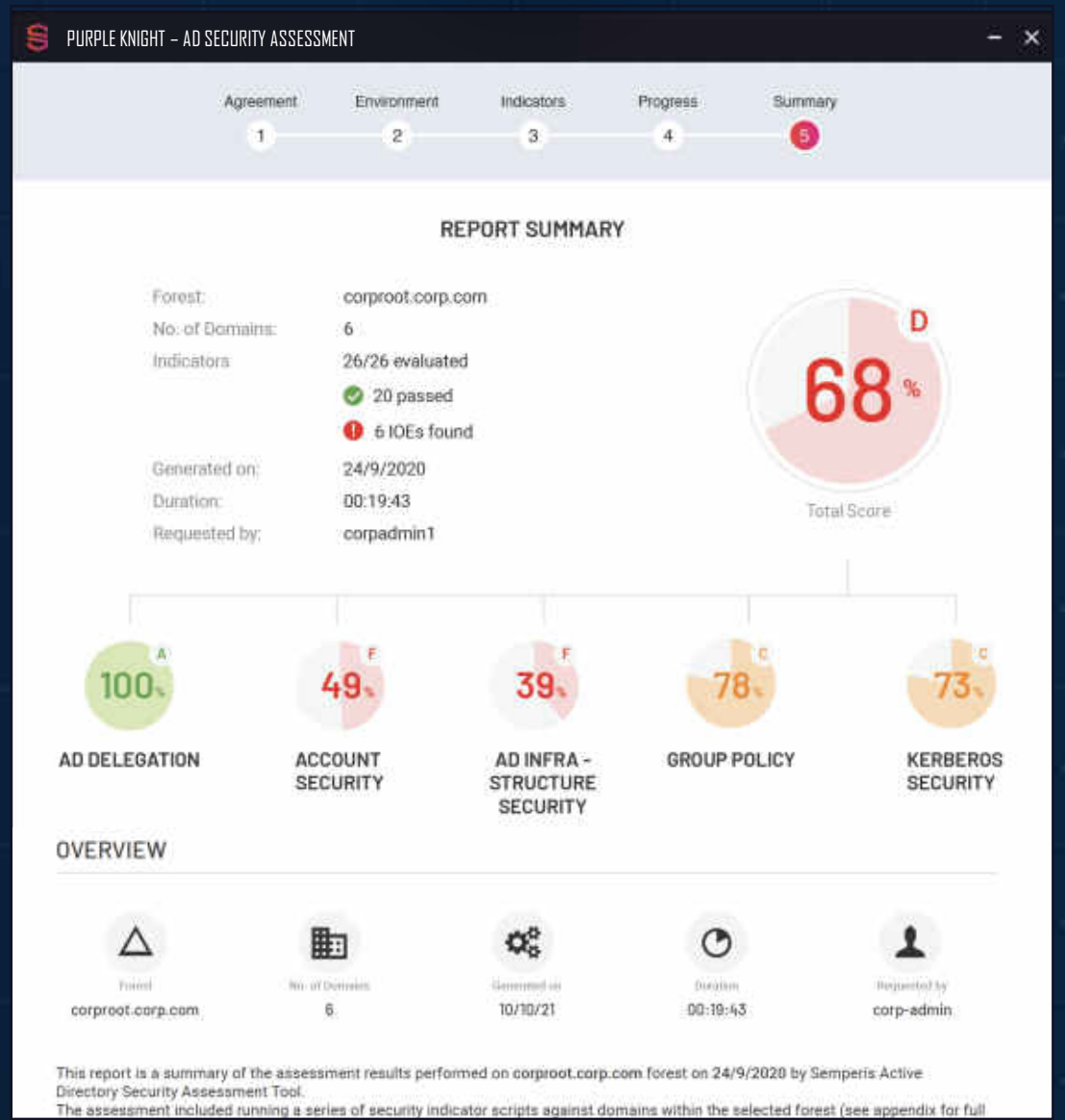


semperis

SECURITY REPORT CARD

Finden Sie Schwachstellen bevor Angreifer es tun.

- Pre- und Post-Attack Sicherheitsindikatoren
- Community-basierte Bedrohungsmuster
- Priorisierte, umsetzbare Anleitungen
- MITRE ATT&CK® Korrelation
- Über unsere Partner zu beziehen



semperis

UMFASSENDE ÜBERWACHUNG

Überwachen, erkennen & reagieren

- Schwachstellenanalyse
- Manipulationssicheres Tracking
- Echtzeit-Alarme
- Auto-Wiederherstellung
- Compliance Reporting

semperis

CYBER-FIRST RECOVERY

Schnellste Wieder-herstellung in Stunden anstatt Tagen

- Sauberer, Malware-freier Restore
- Schnellste Wiederherstellung
- Erweiterte Automation
- “Überall” Wiederherstellung
- Post-Attack Forensik

semperis

Wichtige Schritte

- **Überprüfen Sie Ihre Fähigkeit, Active Directory und Azure AD zu schützen und wiederherzustellen**
  - Indikatoren für Gefährdung und Angriff bewerten
  - Überprüfung von Aktivitäten (z. B. Erstellung von Backdoors)
  - Automatisches Rollback nicht autorisierter Änderungen

- **Bewerten Sie, wie gut Sie auf den Worst Case einer Active Directory Katastrophe vorbereitet sind**
  - Vollständige Forest-Wiederherstellung
  - Risiko einer erneuten Infektion mit Malware
  - Flexibilität der Wiederherstellungsszenarien (z. B. Wiederherstellung auf Cloud-IaaS)

semperis

VIELEN DANK

Mehr gerne in einer persönlichen Demo


oliverk@semperis.com


www.semperis.com/contact