semperis

Defusing an In-Progress Identity System Attack

Guido Grillenmeier
Semperis Chief Technologist

July 14, 2021, as part of the

NIST

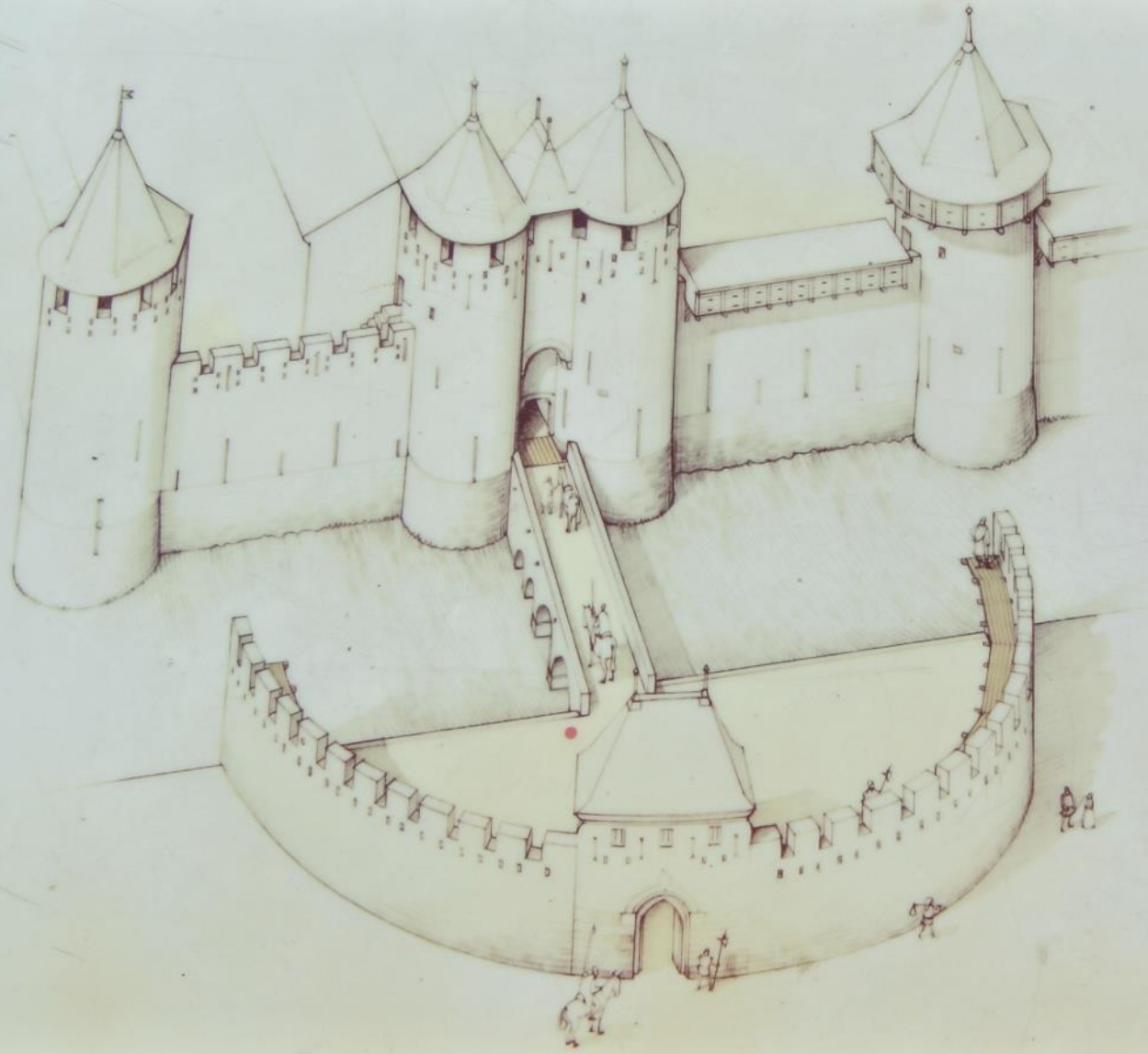
Virtual Workshop on Preventing and Recovering from Ransomware and Other Destructive Cyber Events

CARCASSONNE, France

Various defense layers protected the core of this city – THEIR BUSINESS!

CARCASSONNE, France

"Thanks to these defenses, it was never taken by force!"



Vous êtes ici
You are here
Estás aquí

le château fortifié

La barbacane, avec ses murs courbes crénelés, constitue un premier obstacle à franchir pour l'assaillant. S'il y parvient, il doit ensuite parcourir l'espace découvert, à la portée des arbalétriers du château. Le pont qui enjambe le fossé, était doté à l'origine d'une partie mobile, dont le retrait constituait le deuxième obstacle. Enfin la porte étroite est encadrée par les tours jumelles dotées de nombreuses embrasures de tirs (archères). Herses, assommoir et porte en fer renforcent encore le château du côté de la cité. Grâce à ces défenses, il ne fut jamais pris par la force.

The barbican, with its curved crenellated walls, was the first obstacle for an attacker to overcome. If he managed it, he then had to cross an open space, within range of the castle crossbowmen. The bridge across the moat was originally part drawbridge, which when lifted formed the second line of defence. Lastly, the narrow entrance is flanked by twin towers with numerous firing apertures (loopholes). Portcullises, murder holes and an iron door further strengthened the castle on the town side. Thanks to these defences, it was never taken by force.

La barbacana, con sus muros curvados almenados, constituye el primer obstáculo que debe salvar el asaltante. Si llega a ella, tiene que recorrer a continuación el espacio descubierto, al alcance de los ballesteros del castillo. El puente que cruza el foso, era en parte levadizo y constituia el segundo obstáculo. Finalmente, la puerta estrecha está rodeada por las torres gemelas dotadas de numerosos huecos para el disparo (saeteras). Además, rastrillos, matacán y puerta de hierro refuerzan el castillo por el lado de la ciudad. Gracias a estas defensas, nunca pudo tomarse por la fuerza.

semperis

NIST Cybersecurity Framework applied to AD

Before an attack | During an attack | After an attack

Forensics & Investigation

Vulnerability Assessments

Identify

Cyber-First Disaster Recovery

IOE & IOC Discovery & Monitoring

Protect

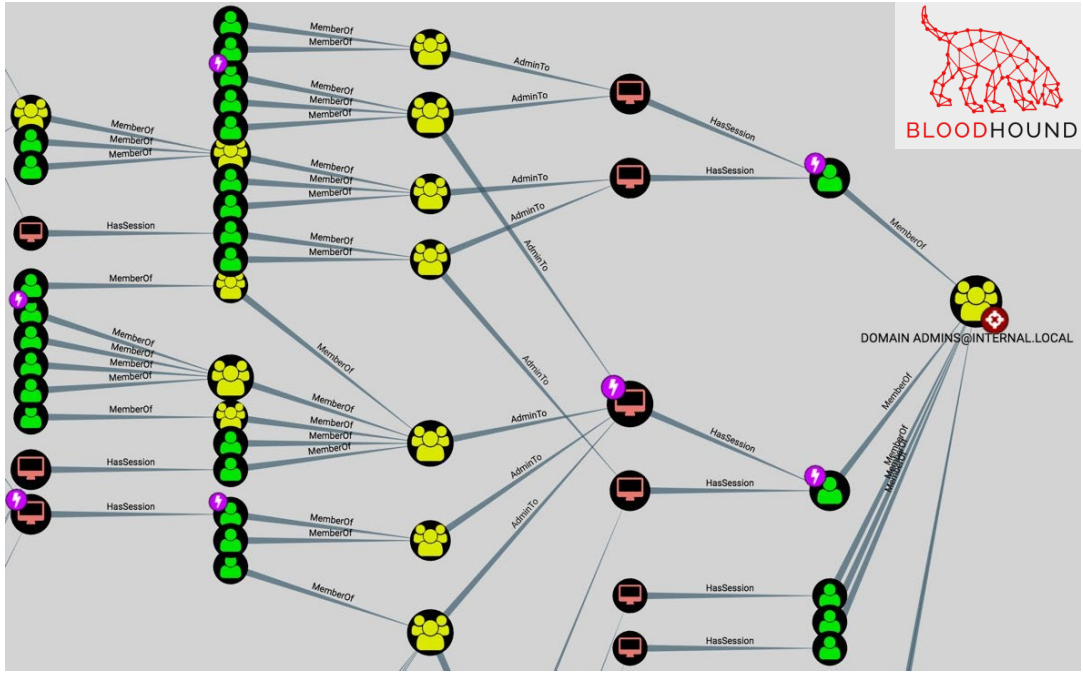
Auto-Remediation & IR

Threat Detection & Visibility

Know the tools available to scan your AD for vulnerabilities

Some examples of powerful and **free tools**:

- **BloodHound**
  - Requires installation of Java and NeoJ4 DB
  - Separate extraction of AD data through additional tool – which is then processed by BloodHound tool for visualization of attack-paths
- **PingCastle**
  - Command-Line tool for evaluation security posture of an AD domain
- **Semperis Purple Knight**
  - Powerful UI-tool for evaluating security posture of a complete AD forest
  - Continuously updated with new vulnerability checks

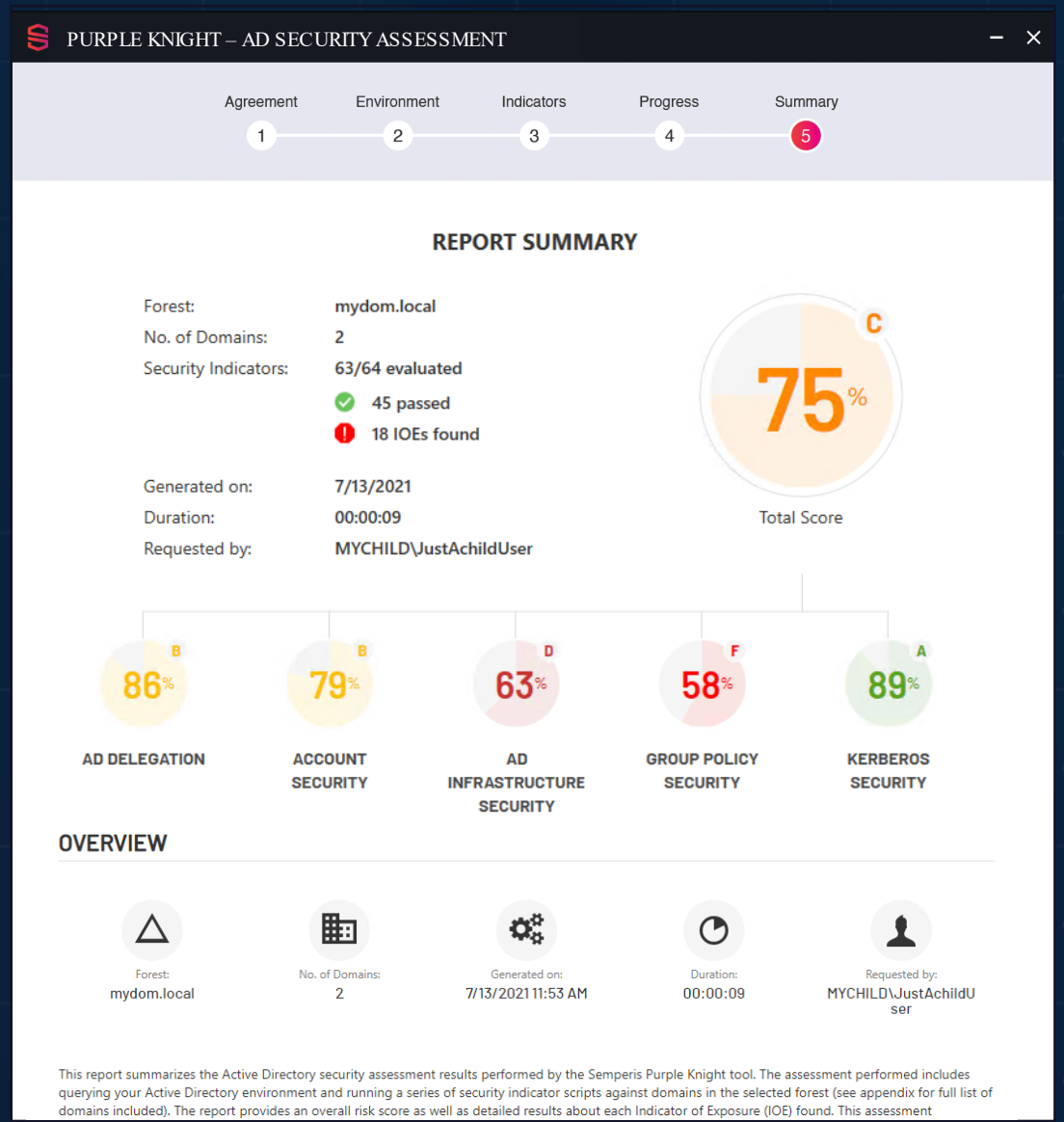


semperis

SECURITY REPORT CARD

Spot weaknesses before attackers do.

- Pre- and post-attack security indicators
- Community-driven threat models
- Prioritized, actionable guidance
- MITRE ATT&CK correlation
- **FREE** → www.purple-knight.com



FIRST ACTIONS you can take immediately to reduce attack surface of your AD in the event of an intrusion

1. **Ensure SID-Filtering is active across all the trusts between the AD forests**
   this would prevent attacks from one forest to the other by adding a privileged group to SID-history of an account in the already compromised domain.

2. **Reset the KRBTGT Account in every domain twice**
   ensuring forced replication between each reset—this would avoid attackers from creating valid Kerberos Ticket Granting Tickets (TGT), aka "Golden Tickets," should they have compromised the KRBTGT account already.

3. **Disable the Printer-Service on all Domain Controllers**
   this will prevent an attacker from coercing a DC to authenticate to some other compromised client via the "printer-bug," which is a trivial task if an attacker gains hold of a computer that is configured to allow unconstrained delegation.

4. **Add all privileged users to the Protected Users group in their respective domains**
   this will minimize credential exposure of these accounts by no longer allowing to authenticate via NTLM (Kerberos only) or using DES or RC4 for Kerberos pre-authentication. Users in this group can also not be delegated with constrained or unconstrained delegation.

5. **Ensure that a recent backup of every domain of every forest is safely stored**
   use an offline repository, in case it is required for forest recovery, should a crypto-locker still be kicked off in the environment.

LONGER TERM ACTIONS …
… depend on what's found in your AD security scan

- **Follow the guidance of other vulnerabilities found in your AD by the AD scanning tools**
  No two ADs are configured the same – use the intelligence given to you to help to protect your AD
- **Reconfigure your Service-Accounts to be UNPRIVILEGED in your AD**
  Usually only require permissions on the target system hosting the application they are configured for – grant those permissions via delegation, not by adding Service-Accounts to domain-admin group! Passwords of Service Accounts with SPNs (Service-Principal-Names) are easily retrievable via the Kerberoasting attack!
- **Old Admin-Passwords are a real risk – do ensure that they are changed periodically**
  Plenty of ADs are operating with privileged account from decades ago – how security sensitive have you been 10 or 20 years ago? At the same time, reduce the number of your Admin accounts.
- **Reconfigure systems that are allowed to use unconstrained Kerberos delegation**
  This will prevent an attacker from coercing a DC to authenticate to some other compromised client via the "printer-bug," which is a trivial task if an attacker gains hold of a computer that is configured to allow unconstrained delegation.
- **Ensure your Domain Admins do NOT logon to any "lower tier" systems**
  Pass the hash attacks are a reality in AD environments – elevation of privileges can be avoided by not using the same systems to manage AD, that you use to manage other servers or clients. Think about PAWs (Privileged Access Workstations)

Evaluating AD vulnerabilities is an ONGOING task, as NEW THREATS evolve continuously!

semperis

NIST Cybersecurity Framework applied to AD

Before an attack | During an attack | After an attack

Forensics & Investigation

IOE & IOC Discovery & Monitoring

Cyber-First Disaster Recovery

Vulnerability Assessments

Respond

Auto-Remediation & IR

Threat Detection & Visibility

Detect

semperis

Understand attack-vectors that can change settings in your AD without writing any auditing event-log entries

Some examples:

- **Mimikatz DCshadow attack**
  Registers a rogue domain controller (DC) by modifying the Configuration partition of AD – performs any change that then replicates out to other DCs
- **Group Policy changes**
  Eventlogs usually don't contain what was changed in a GPO
- **Zerologon attack**
  Do you check for unexpected password changes on your DCs?
- **Wrongly configured AD Auditing settings**
  Either set by mistake … or by the intruder …

Also see:
https://www.semperis.com/blog/how-to-defend-against-active-directory-attacks-that-leave-no-trace

Ensure to scan your AD for unexpected changes

Must be able to monitor your AD without relying on Audit Events

1. By Metadata: use tools to analyze the AD metadata
   - Free tool example: https://github.com/ANSSI-FR/ADTimeline

2. By Scripting: specific changes can be monitored by scripts comparing deviation of values to a known fixed list
   - e.g. monitoring any changes of memberships in your most privileged groups

3. Using Monitoring Solutions: professional AD monitoring solutions should directly **read the AD replication stream**
   - can track changes that are hidden from security event-logs
   - allows storing AD replication data in a searchable format
   - allows comparison of object and attribute values over time
   - allows forensic analysis of changed AD data
   - stored data can be used to undo AD changes

semperis

NIST Cybersecurity Framework applied to AD

Before an attack | During an attack | After an attack

Forensics & Investigation

IOE & IOC Discovery & Monitoring

Recover

Cyber-First Disaster Recovery

Vulnerability Assessments

Auto-Remediation & IR

Threat Detection & Visibility

semperis

EVALUATING THE RISKS

PROBABILITY

DC failure Networking failure	Other malware	
Admin error (fat fingers)	Malicious insider Failed OS update Admin error (bad script)	Power failure Wiperware attack External comms failure
Unauthorized physical access	Rogue admin Physical attack	Natural disaster Schema failure

IMPACT

Modern Ransome Request

Your documents, photos, databases and other important files **encrypted**

To decrypt your files you need to buy our special software - **General-Decryptor**

Follow the instructions below. But remember that you do not have much time

General-Decryptor price

the price is for all PCs of your infected network

You have 2 days, 23:38:14

* If you do not pay on time, the price will be doubled
* Time ends on **Jul 5, 14:15:38**

Current price 24435.5 XMR ≈ 5,000,000 USD

After time ends 48871 XMR ≈ 10,000,000 USD

Monero address:

* XMR will be recalculated in 5 hours with an actual rate.

Source: Huntress, from their recent KASEYA breach-investigations

semperis

semperis

> ***Nine days for an Active Directory recovery isn't good enough, you should aspire to 24 hours; if you can't, then you can't repair anything else.***

ANDY POWELL, MAERSK CISO

Ensure you can recover your AD forest quickly

1. **Ensure your backups don't contain the malware, when you restore**
   - Ideally done by running a backup of AD without backing up the whole OS

2. **Ensure you can recover your DCs to different target systems**
   - Could be different to hardware / virtual machines / cloud-systems
   - Could be systems in a different IP segment to isolate them from infected systems

3. **Ideally have a fully automated solution in place to recover your AD forest**
   - Microsoft recovery process is complex and prone to human error
   - During time of recovering from disaster, your teams will be under high pressure
   - You can't begin restoration of any of your other systems depending on AD, until your AD is back – every hour counts.

semperis

THANK YOU

Questions? Get in touch …

We even have the proper solutions in place to help you!

Guido Grillenmeier

Semperis Chief Technologist

guidog@semperis.com

www.linkedin.com/in/guidogrillenmeier