Nasazení a vyhodnocení bezpečnostních hrozeb v ATA

Daniel Hejda

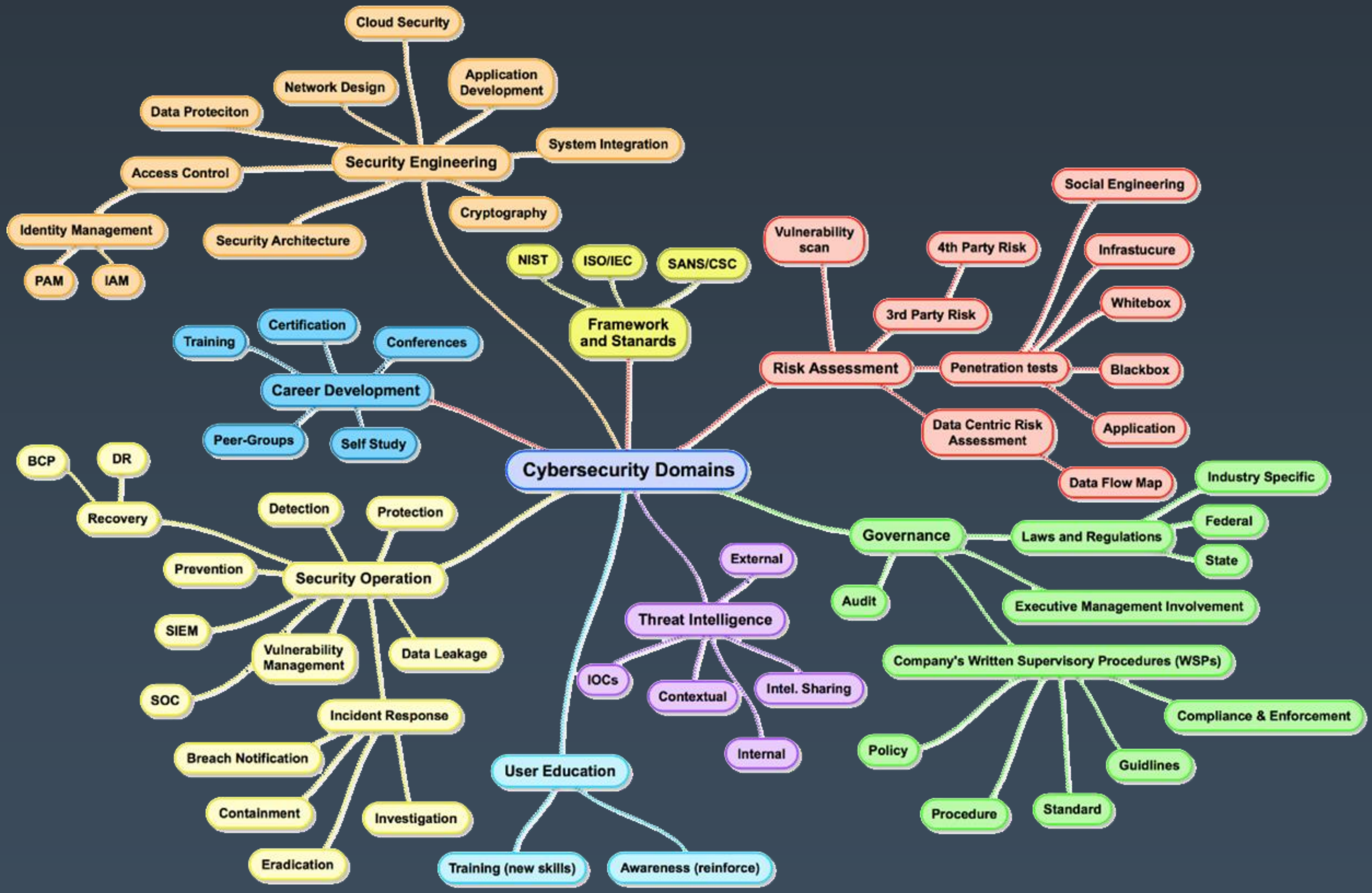
MCSD: Azure Solutions Architect

MCSE: Cloud Platform and Infrastructure

MCSE: Productivity

hejda@kpcs.cz | daniel.hejda@defense-ops.com | www.defense-ops.com

Bezpečnost musí být komplexní



Microsoft Security Products

Microsoft

- Advanced Threat Analytics
- Cloud App Security
- Intune
- Windows Server 2016
- SQL Server 2016

Windows

- Windows Trust Boot
- Privileged Identity Management
- Credential Guard
- Microsoft Passport
- Windows Hello
- Windows Defender ATP
- Windows Update for Business
- Windows Information Protection

Microsoft Azure

- Azure Active Directory
- Azure Security Center
- Azure Storage Service Encryption
- Azure Key Vault
- Azure Information Protection
- Operation Management Suite

Office 365

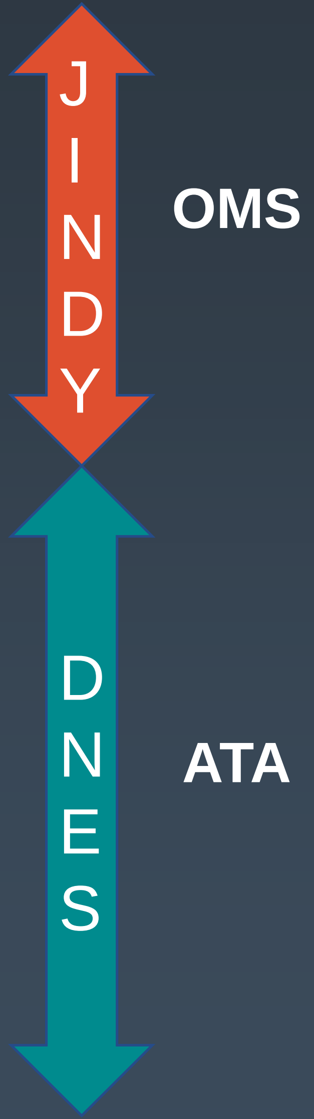
- Advanced Threat Protection
- Anti-Spam / Anti-Malware
- Message Encryption
- Data Loss Prevention
- Threat Intelligence
- Advanced Security Management

Co nás čeká nebo bude čekat

- Brute Force na HTTPS a jeho detekce
- Brute Force na RDP a jeho detekce
- Vytěžení dat ze Skype klienta
- Další obecné detekce (new user, add member to group, atd..)
- Detekce vytvoření „Hide Enterprise administrator“
- Detekce průzkumu DNS
- Brute Force na LDAP Simple Bind
- Detekce autorizovaného LDAP dotazu
- Honey Token - návnada
- Detekce Pass-the-hash
- Detekce Pass-the-ticket
- Detekce útoku na Golden ticket (Encryption downgrade aktivity a Malicious replication)

Co nás čeká nebo bude čekat

- Brute Force na HTTPS a jeho detekce
- Brute Force na RDP a jeho detekce
- Vytěžení dat ze Skype klienta
- Další obecné detekce (new user, add member to group, atd..)
- Detekce vytvoření „Hide Enterprise administrator“
- Detekce průzkumu DNS
- Brute Force na LDAP Simple Bind
- Detekce autorizovaného LDAP dotazu
- Honey Token - návnada
- Detekce Pass-the-hash
- Detekce Pass-the-ticket
- Detekce útoku na Golden ticket (Encryption downgrade aktivity a Malicious replication)



Co je ATA

- Detekuje vytěžování informací z vnitřní infrastruktury
- Detekuje podezřelé chování v síti/doméně
- Detekuje využití nebezpečných nástrojů a vykrádání hesel

- ATA vyhledává
  - Škodlivé kódy
  - Nestandardní chování
  - Bezpečnostní problémy a rizika

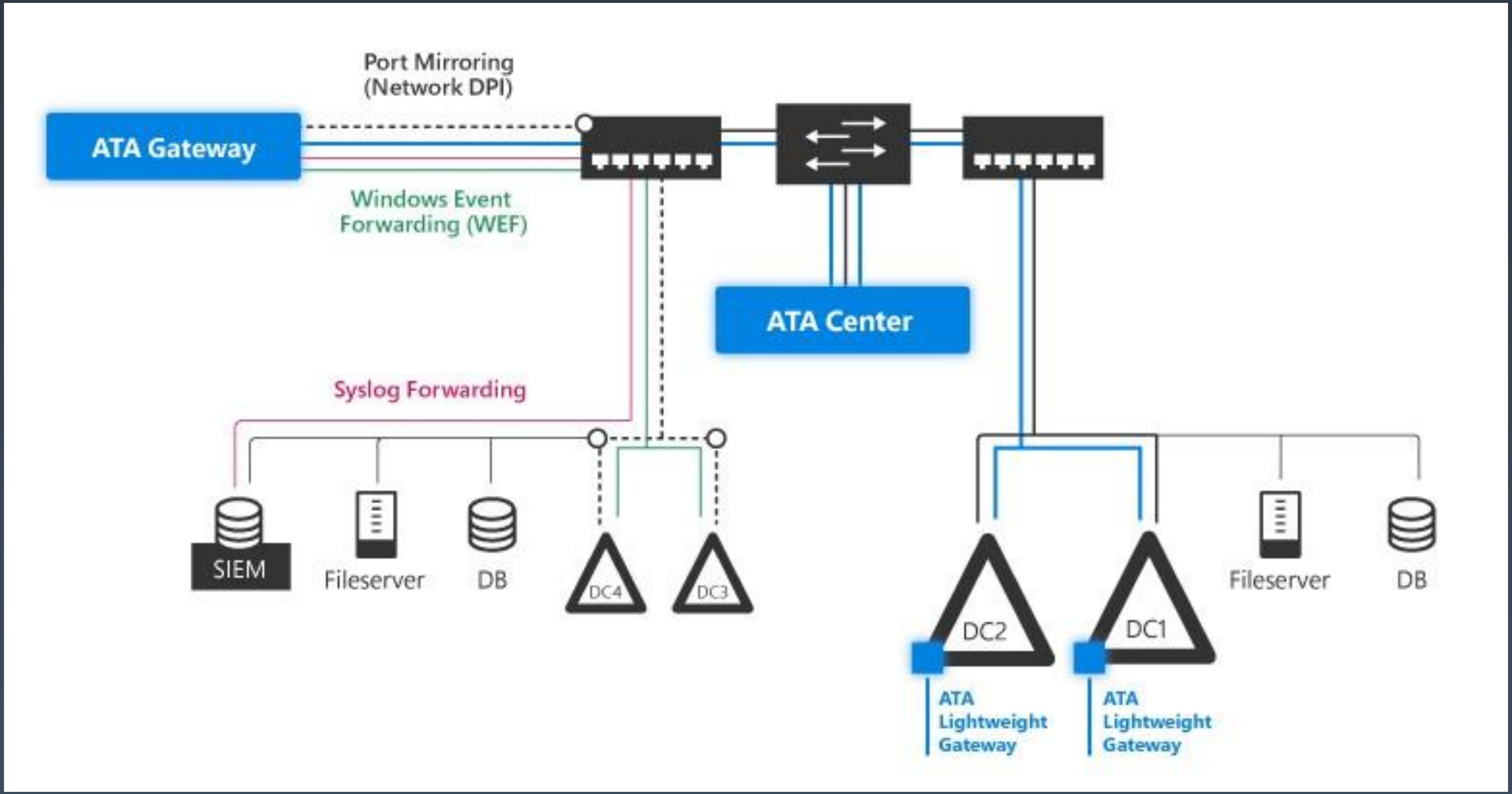
Co ATA umí detekovat

- Pass-the-Ticket (PtT)
- Pass-the-Hash (PtH)
- Overpass-the-Hash
- Podvržení certifikátu v krbgt tiketu
- Golden ticket
- Škodlivé replikace
- Rekognoskace
- Hrubá síla
- Vzdálené spuštění
- A spoustu dalších…

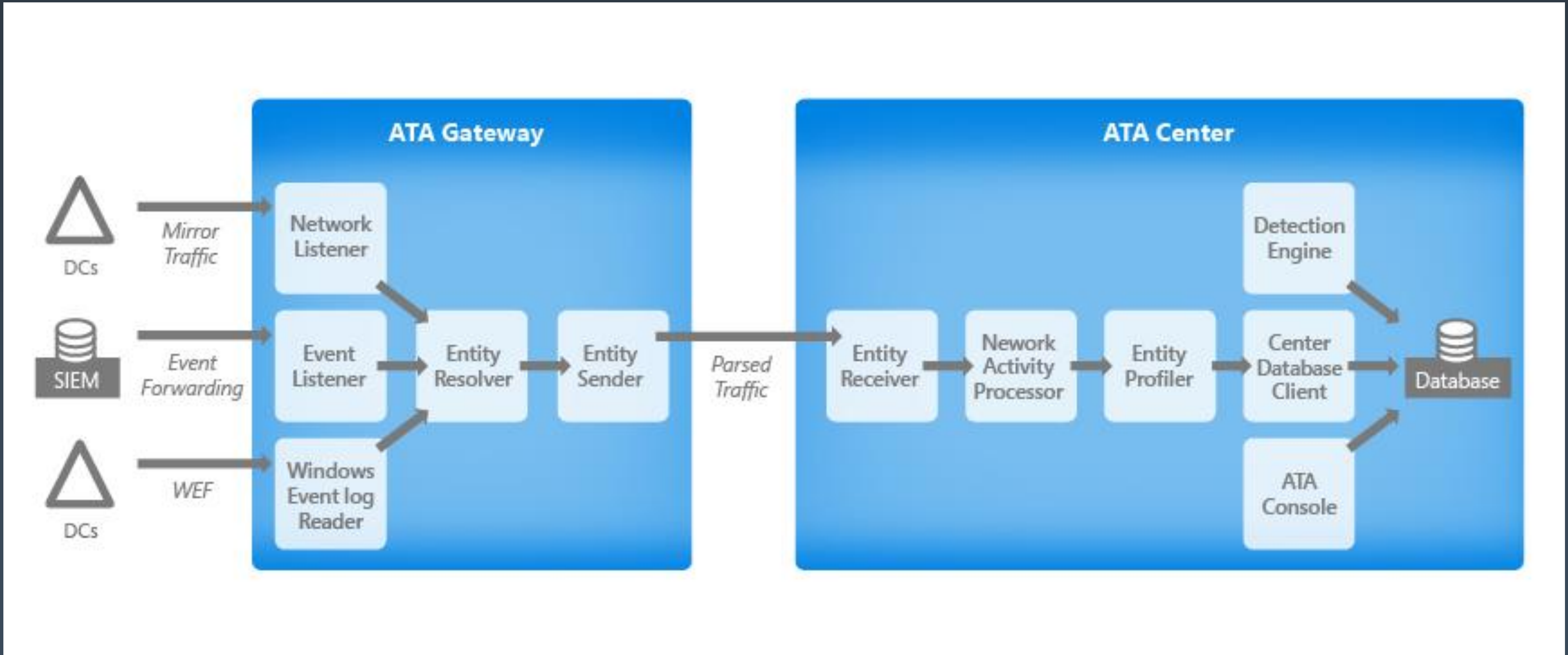
Novinky ve verzi 1.7

- Rekognoskace pomocí výčtu adresářových služeb
- Vylepšení proti útoku typu Pass-the-Hash
- Vylepšení proti útoku typu Pass-the-Ticket
- Vylepšení proti nestandardnímu chování
- Vylepšení proti neobvyklé implementaci protokolu
- Management
  - Řízení přístupu na základě role
  - Podpora Windows Serveru 2016 a Windows Server Core

Architektura



Sběry dat a informací



Pozor na výkon

- ATA Center

Paketů za sekundu ze všech řadičů domény	Procesor (jádra*)	Paměť (GB)	Úložiště databáze za den (GB)	Úložiště databáze za měsíc (GB)	IOPS**
1 000	2	32	0.3	9	30 (100)
10 000	4	48	3	90	200 (300)
40 000	8	64	12	360	500 (1 000)
100 000	12	96	30	900	1 000 (1 500)
400 000	40	128	120	3&600;	4&000; (5&000;)

*To zahrnuje fyzická jádra, ne jádra typu Hyper.

**Průměrné počty (počty ve špičce)

Pozor na výkon

ATA Lightweight Gateway

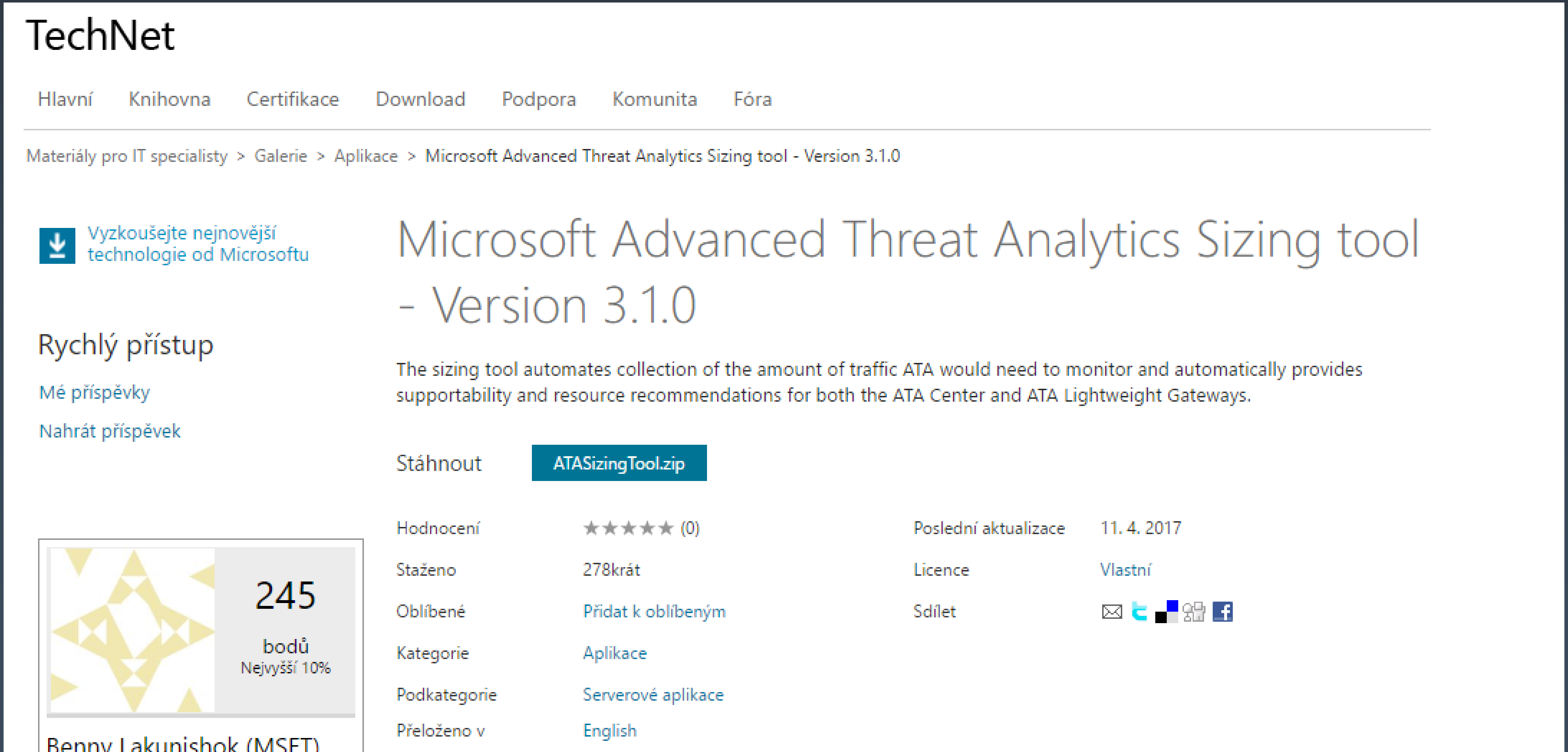
Pakety za sekundu*	Procesor (jádra**)	Paměť (GB)***
1 000	2	6
5,000	6	16
10 000	10	24

ATA Gateway

Pakety za sekundu*	Procesor (jádra**)	Paměť (GB)
1 000	1	6
5,000	2	10
10 000	3	12
20 000	6	24
50 000	16	48

ATA Sizing Tool

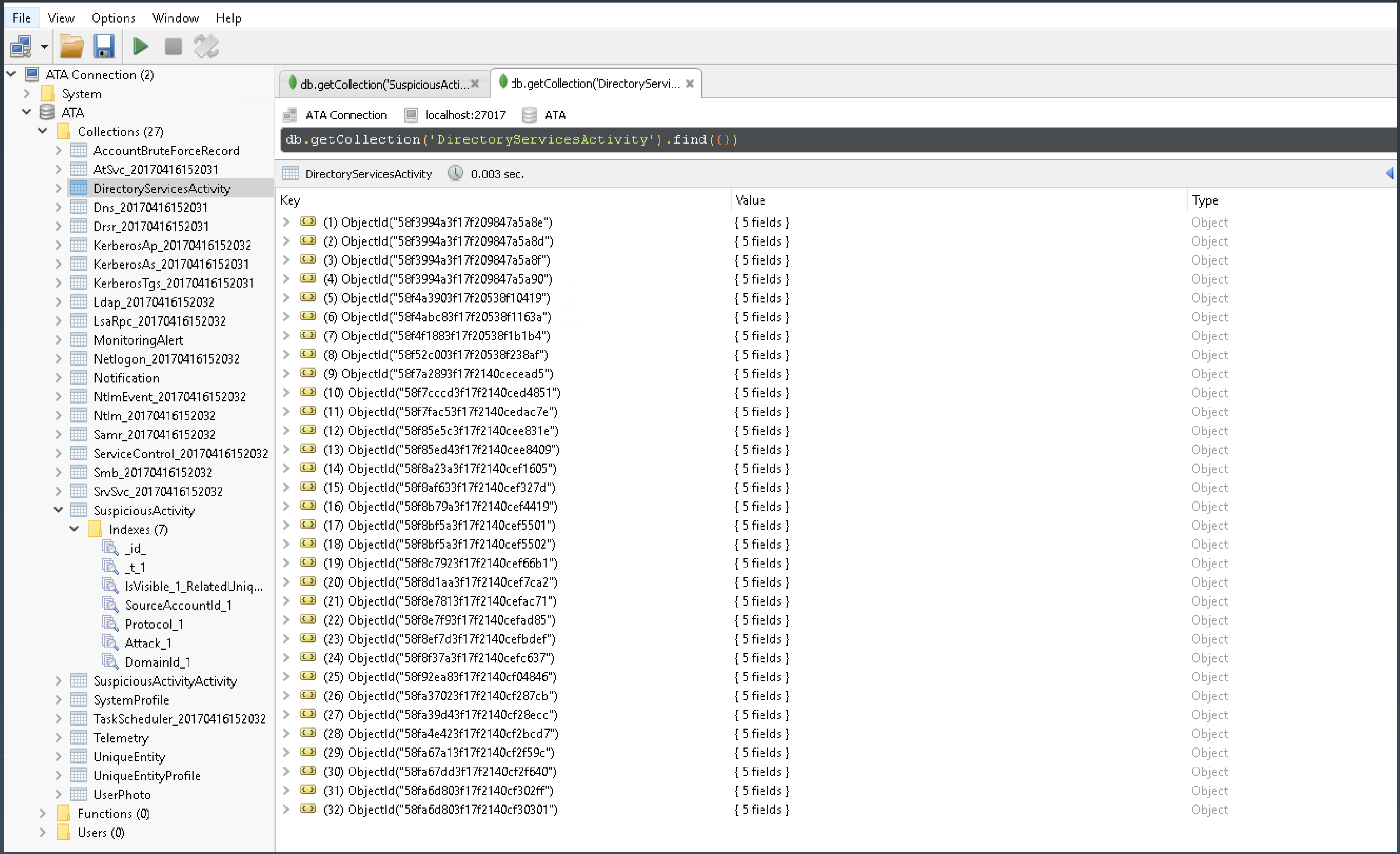
- ATA Sizing Tool - http://aka.ms/atasizingtool



Kritéria provozu služby

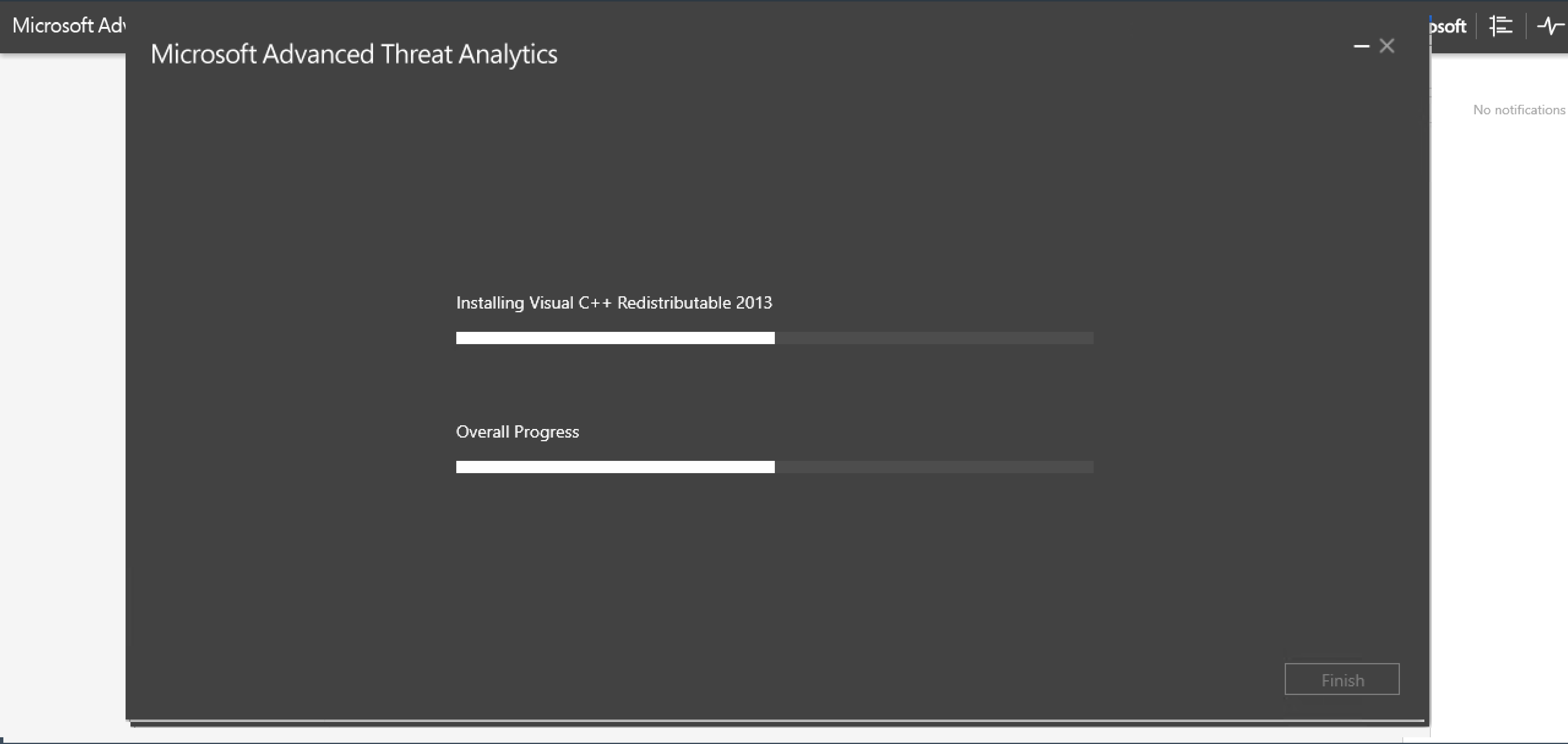
- Agregované maximum 400 000 snímků za sekundu
- 20% volného místa – vždy
- Pokud 20% nebo 100GB začnou se staré kolekce odmazávat až do 5% nebo 50GB volného místa – pak se služba zastaví
- Latence na disku Read/Write < 10ms
- Power Management – High Performance
- Zakázat NUMA, pokud běží server na fyzickém HW

MongoDB


File
View
Options
Window
Help
ATA Connection (2)
System
ATA
Collections (27)
AccountBruteForceRecord
AtSvc_20170416152031
DirectoryServicesActivity
Dns_20170416152031
Drsr_20170416152031
KerberosAp_20170416152032
KerberosAs_20170416152031
KerberosTgs_20170416152031
Ldap_20170416152032
LsaRpc_20170416152032
MonitoringAlert
Netlogon_20170416152032
Notification
NtlmEvent_20170416152032
Ntlm_20170416152032
Samr_20170416152032
ServiceControl_20170416152032
Smb_20170416152032
SrvSvc_20170416152032
SuspiciousActivity
Indexes (7)
_id_
_t_1
IsVisible_1_RelatedUniq...
SourceAccountId_1
Protocol_1
Attack_1
DomainId_1
SuspiciousActivityActivity
SystemProfile
TaskScheduler_20170416152032
Telemetry
UniqueEntity
UniqueEntityProfile
UserPhoto
Functions (0)
Users (0)
db.getCollection('SuspiciousActi...
db.getCollection('DirectoryServi...
ATA Connection
localhost:27017
ATA
db.getCollection('DirectoryServicesActivity').find({})
DirectoryServicesActivity
0.003 sec.
Key
Value
Type
(1) ObjectId("58f3994a3f17f209847a5a8e") { 5 fields } Object
(2) ObjectId("58f3994a3f17f209847a5a8d") { 5 fields } Object
(3) ObjectId("58f3994a3f17f209847a5a8f") { 5 fields } Object
(4) ObjectId("58f3994a3f17f209847a5a90") { 5 fields } Object
(5) ObjectId("58f4a3903f17f20538f10419") { 5 fields } Object
(6) ObjectId("58f4abc83f17f20538f1163a") { 5 fields } Object
(7) ObjectId("58f4f1883f17f20538f1b1b4") { 5 fields } Object
(8) ObjectId("58f52c003f17f20538f238af") { 5 fields } Object
(9) ObjectId("58f7a2893f17f2140ceceead5") { 5 fields } Object
(10) ObjectId("58f7cccd3f17f2140ced4851") { 5 fields } Object
(11) ObjectId("58f7fac53f17f2140cedac7e") { 5 fields } Object
(12) ObjectId("58f85e5c3f17f2140cee831e") { 5 fields } Object
(13) ObjectId("58f85ed43f17f2140cee8409") { 5 fields } Object
(14) ObjectId("58f8a23a3f17f2140cef1605") { 5 fields } Object
(15) ObjectId("58f8af633f17f2140cef327d") { 5 fields } Object
(16) ObjectId("58f8b79a3f17f2140cef4419") { 5 fields } Object
(17) ObjectId("58f8bf5a3f17f2140cef5501") { 5 fields } Object
(18) ObjectId("58f8bf5a3f17f2140cef5502") { 5 fields } Object
(19) ObjectId("58f8c7923f17f2140cef66b1") { 5 fields } Object
(20) ObjectId("58f8d1aa3f17f2140cef7ca2") { 5 fields } Object
(21) ObjectId("58f8e7813f17f2140cefac71") { 5 fields } Object
(22) ObjectId("58f8e7f93f17f2140cefad85") { 5 fields } Object
(23) ObjectId("58f8ef7d3f17f2140cefbdef") { 5 fields } Object
(24) ObjectId("58f8f37a3f17f2140cefc637") { 5 fields } Object
(25) ObjectId("58f92ea83f17f2140cf04846") { 5 fields } Object
(26) ObjectId("58fa37023f17f2140cf287cb") { 5 fields } Object
(27) ObjectId("58fa39d43f17f2140cf28ecc") { 5 fields } Object
(28) ObjectId("58fa4e423f17f2140cf2bcd7") { 5 fields } Object
(29) ObjectId("58fa67a13f17f2140cf2f59c") { 5 fields } Object
(30) ObjectId("58fa67dd3f17f2140cf2f640") { 5 fields } Object
(31) ObjectId("58fa6d803f17f2140cf302ff") { 5 fields } Object
(32) ObjectId("58fa6d803f17f2140cf30301") { 5 fields } Object

Instalace a nasazení

Instalace


Microsoft Adv
Microsoft Advanced Threat Analytics
Installing Visual C++ Redistributable 2013
Overall Progress
Finish
No notifications

Detekce pomocí ATA

Jak se útočník pohybuje po síti

- V případě proniknutí do sítě provede útočník
  - Mapování sítě
  - Nalezení doménových řadičů
  - Nalezení DNS Serverů
  - Detekování privilegovaných účtů
  - Průzkum global catalogu v AD
- Následně je zahájen útok na vnitřní infrastrukturu

Útok z vnitřní sítě

- Základní předpoklady
  - Máme přístup k počítači v doméně
  - Máme heslo administrátora
  - Máme heslo doménového uživatele

- Doménový řadiče/řadiče je/jsou napojeny na ATA Center

Detekce průzkumu DNS

- **Cíl:** Získat z DNS umístěného na doménovém řadiči informaci o počítačích v síti a jejich IP
- **Popis:**
  - Použít nslookup a dotázat se na jméno serveru
- **Výsledek:** Dotaz do DNS nepovolen – ATA zastavila požadavek jako podezřelé chování
- **Odhadovaný čas detekce: 20 sekund**

Demo

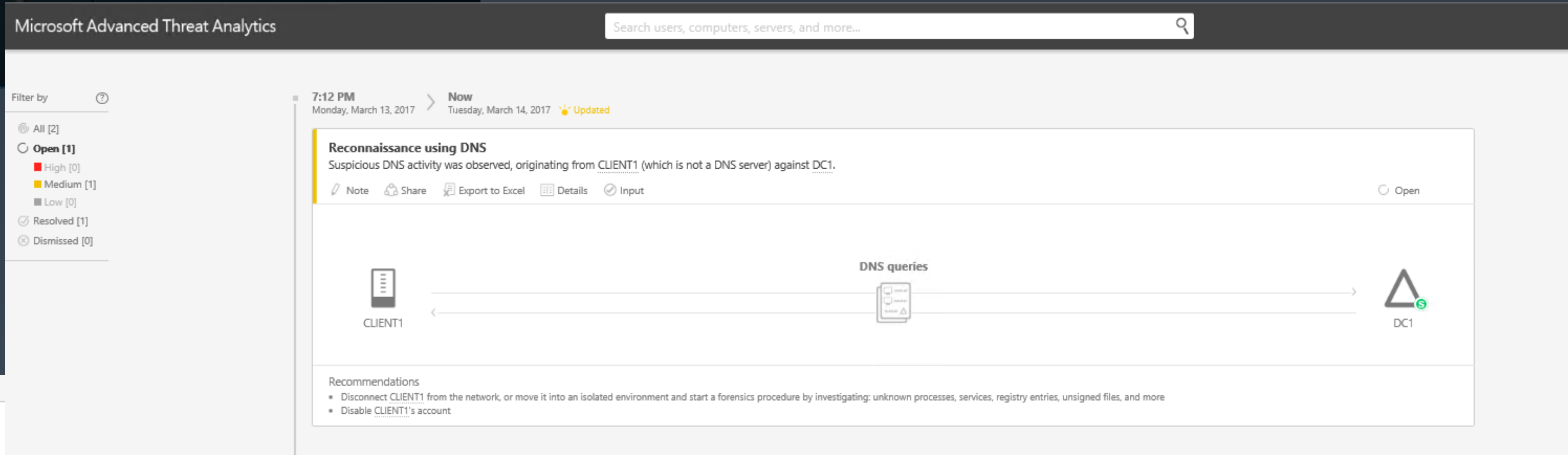
Útok a detekce

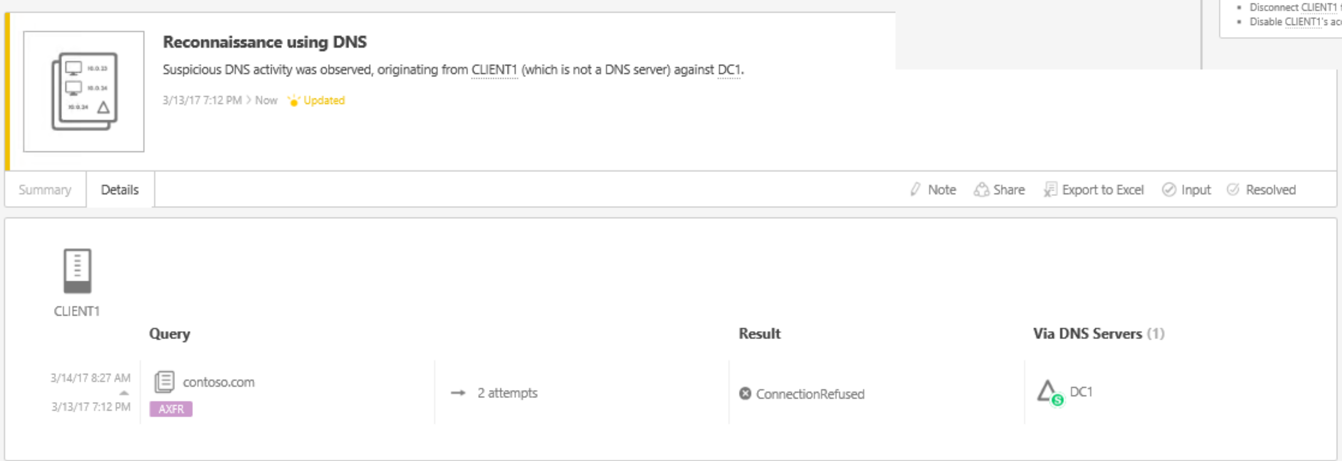
Detekce průzkumu DNS

```
C:\Windows\system32>nslookup
nslookup
Default Server:  UnKnown
Address:  192.168.20.26

> ls contoso.com
*** Can't list domain contoso.com: Query refused
The DNS server refused to transfer the zone contoso.com to your computer. If this
is incorrect, check the zone transfer security settings for contoso.com on the DNS
server at IP address 192.168.20.26.

[UnKnown]
>
```





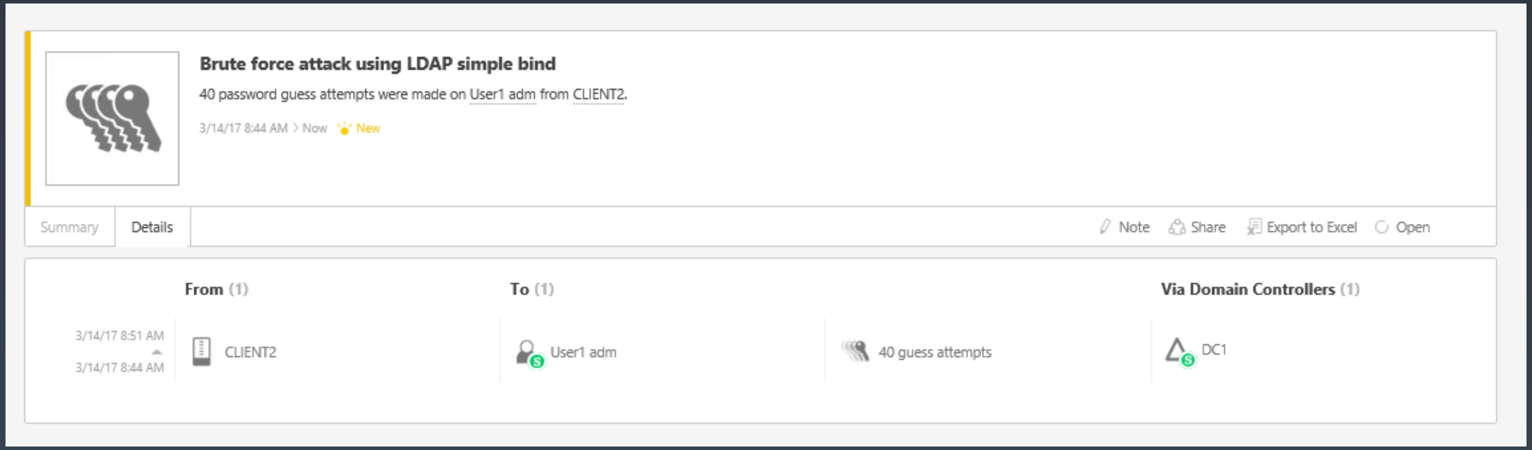
Brute Force na LDAP Simple Bind

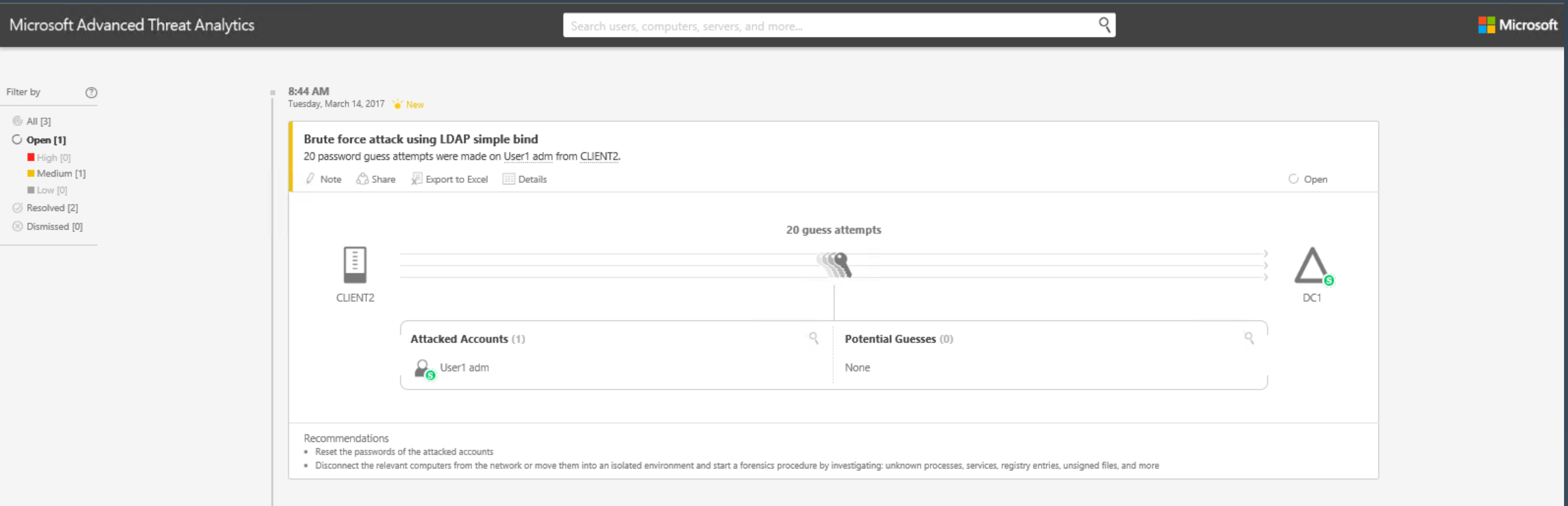
- **Cíl:** Cílem je na kompromitovaném PC zahájit Brute Force útok na LDAP
- **Popis:**
  - Získat jména z Global Catalogu (veřejná informace)
  - Získat slovník hesel
  - Spustit script
  - Čekat na výsledek
- **Výsledek:** Zjištění hesla se po nějaké době povede a heslo bude prolomeno, nicméně délka zjištění hesla bude v řádu hodin – dní, pokud budou použita slabá hesla
- **Odhadovaný čas detekce:**

Demo

Útok a detekce

Brute Force na LDAP Simple Bind





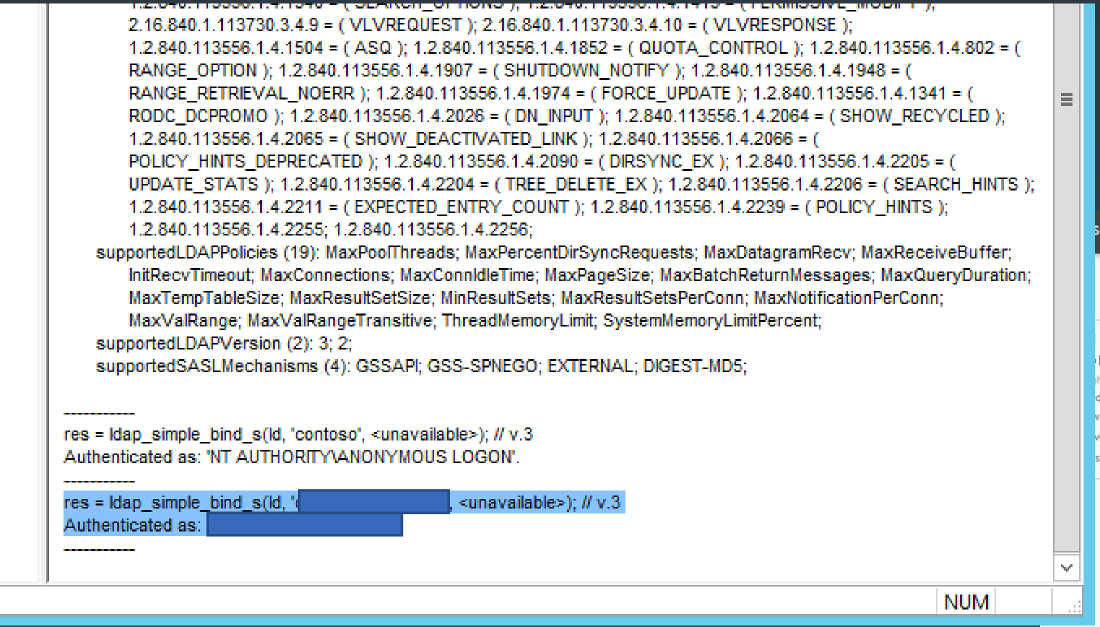
Detekce autorizovaného LDAP dotazu

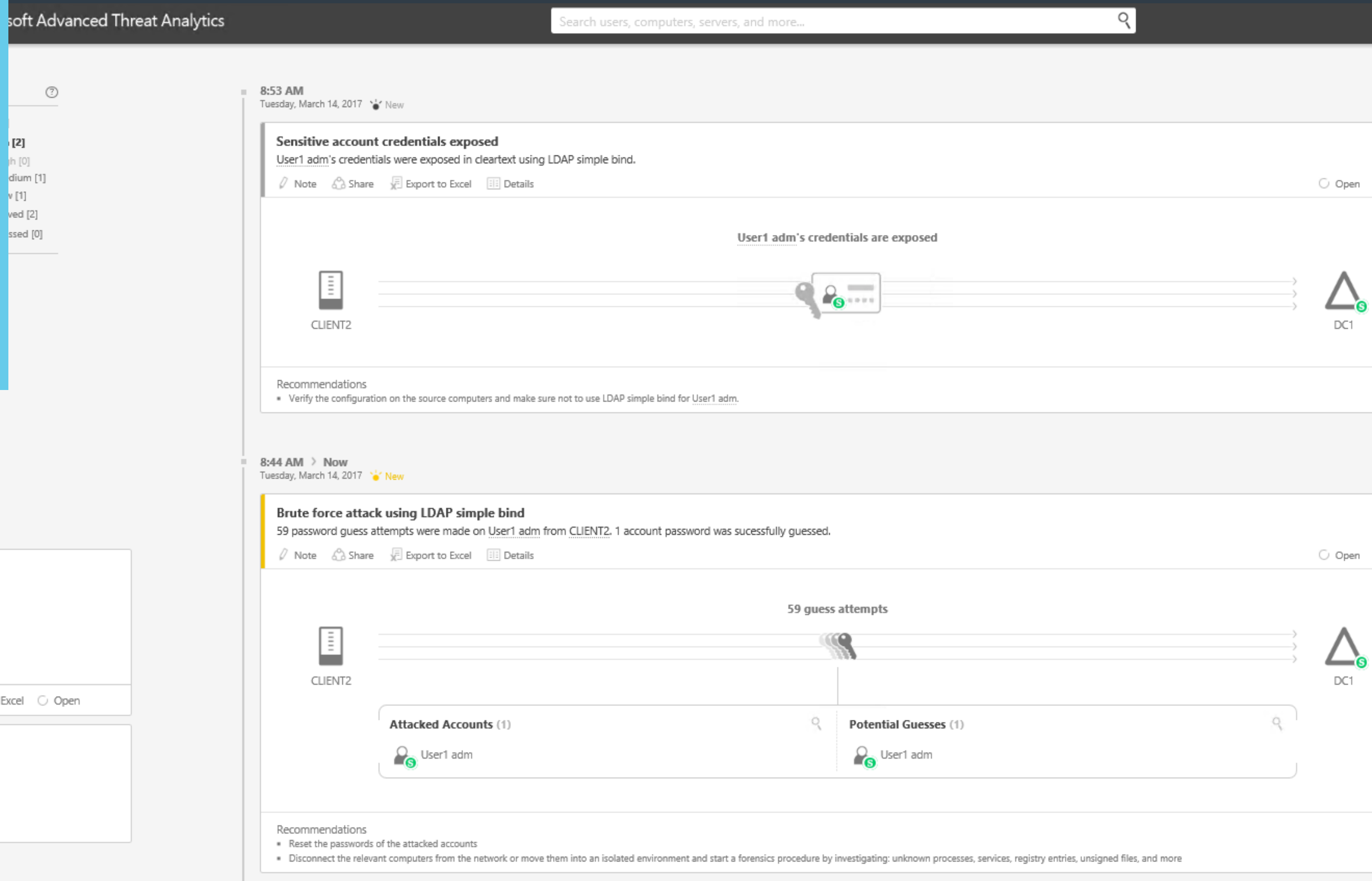
- **Cíl:** Prolomení hesla se povedlo, ale účet dělá dotaz do DNS, který je nestandartním chováním uživatele
- **Popis:**
  - Na kompromitovaném PC spustit ldp.exe
  - **Connection-Connect (Port: 389)**
  - **Connection – Bind (Type: Simple Bind, User: DEFENSE-OPS:User1**
  - **Password: ********************
- **Výsledek:** Přístup do systému je povolen, nicméně vše je zaznamenáno do systému. V systému se objeví Sensitive Account credentials exposed
- **Odhadovaný čas detekce: 20 sekund**

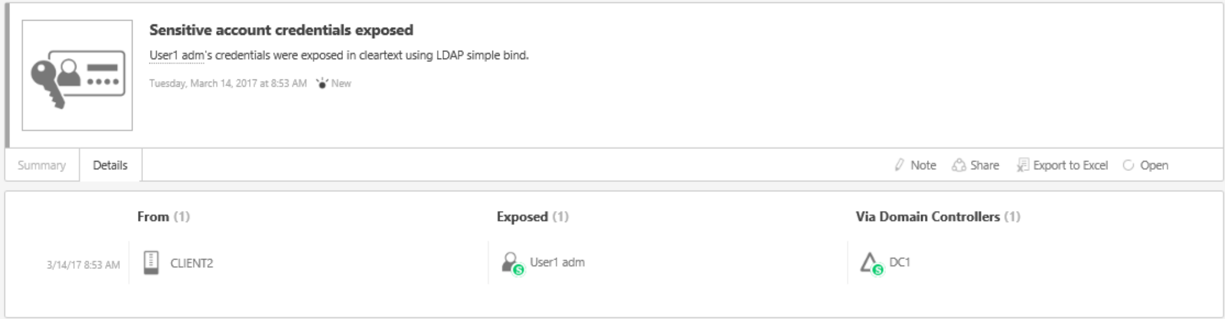
Demo

Útok a detekce

Detekce autorizovaného LDAP dotazu







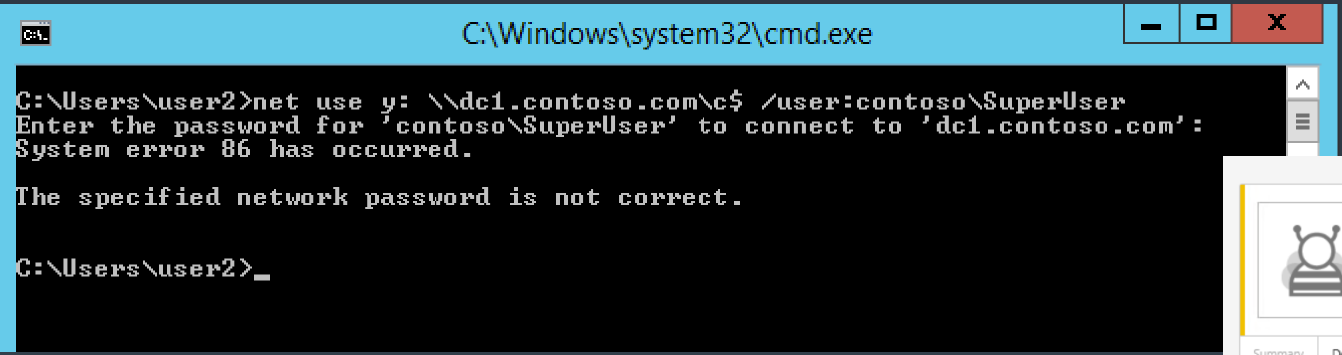
Honey Token - návnada

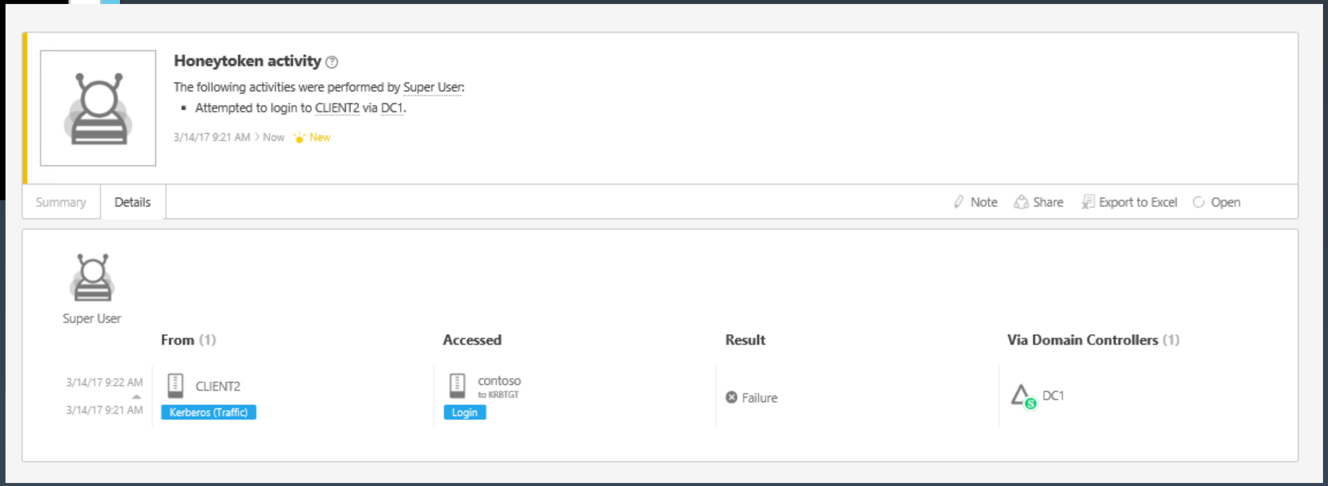
- **Cíl:** Útočník se snaží získat heslo k nějakému zajímavému účtu (CxO nebo Spravce, Admin, atd..)
- Popis:
  - Administrátor označil účty, které slouží jako návnada, účty jsou zakázány a nesmí přistupovat do sítě.
  - Útočník našel zajímavý účet (SuperUser, atd..)
  - Útočník nemá heslo k danému účtu, ale pokusí se s ním přistoupit do sítě
- **Výsledek:** Systém detekoval, že se někdo snaží přistupovat do sítě pomocí Honey Tokenu, účtu který byl nastražen pro útočníka
- **Odhadovaný čas detekce: 20 sekund**

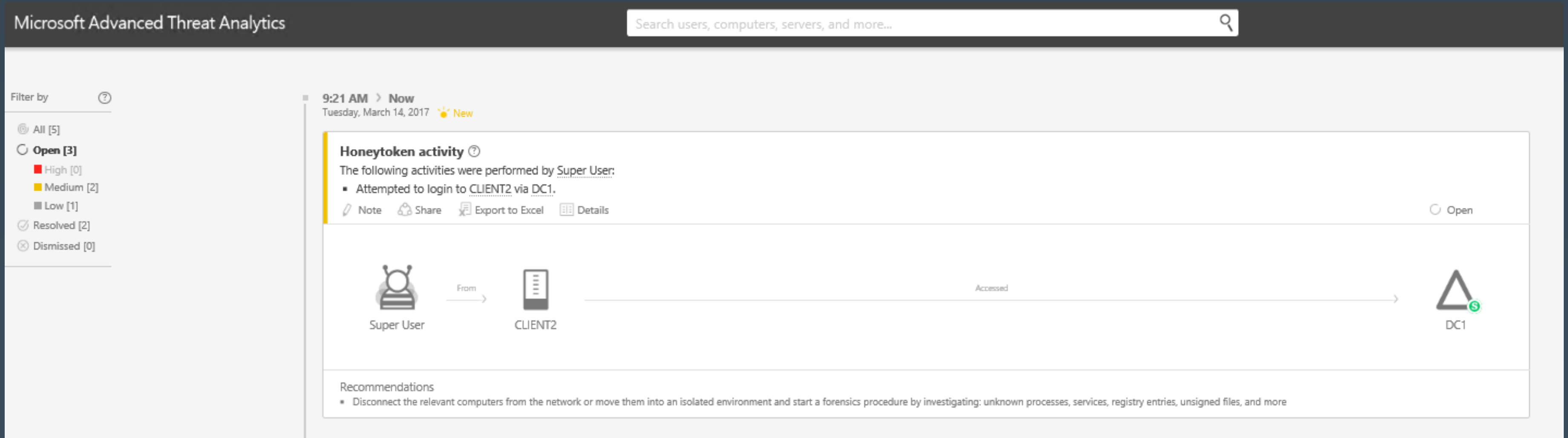
Demo

Útok a detekce

Honey Token - návnada







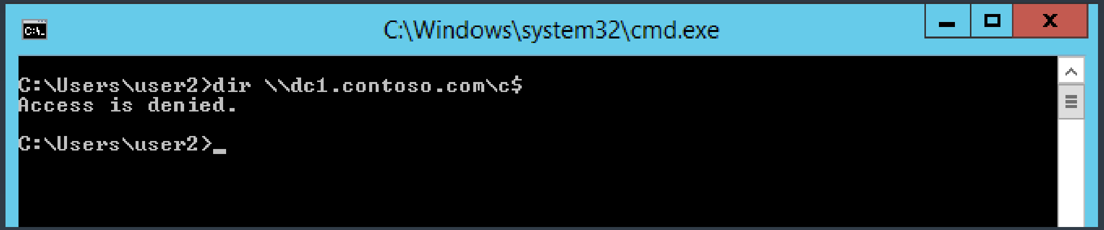
Detekce Pass-the-hash

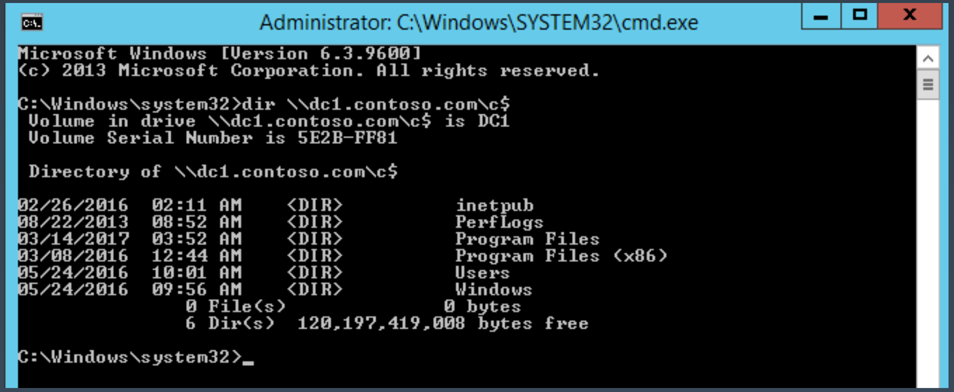
- **Cíl:** Útočník se pokusí přistoupit s uživatelským oprávněním na doménový řadič, poté co získá NTLM Hash uživatele v doméně
- **Popis:**
  - Pokus o otevření a přístup na doménový řadič
  - Zajištění NTLM Hashe z počítače
  - Otevření sdílení s NTLM Hashem
- **Výsledek:** Útočníkovi se přístup povede, získá přístup do sdílení na doménovém řadiči, ale jeho počin je detekován
- **Odhadovaný čas detekce: 2,5 minuty**

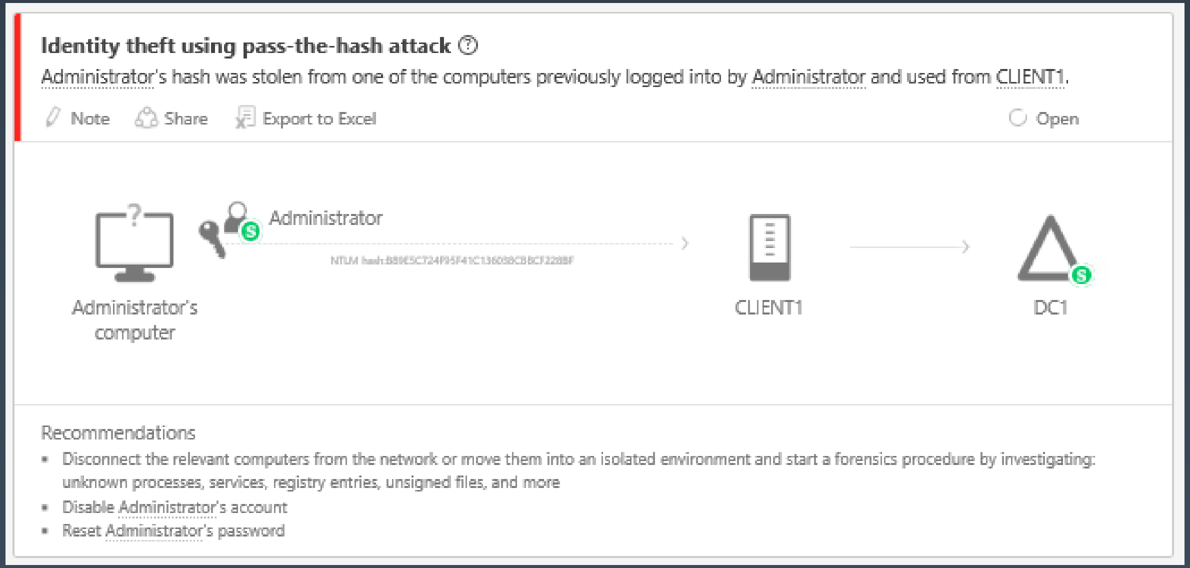
Demo

Útok a detekce

Detekce Pass-the-hash



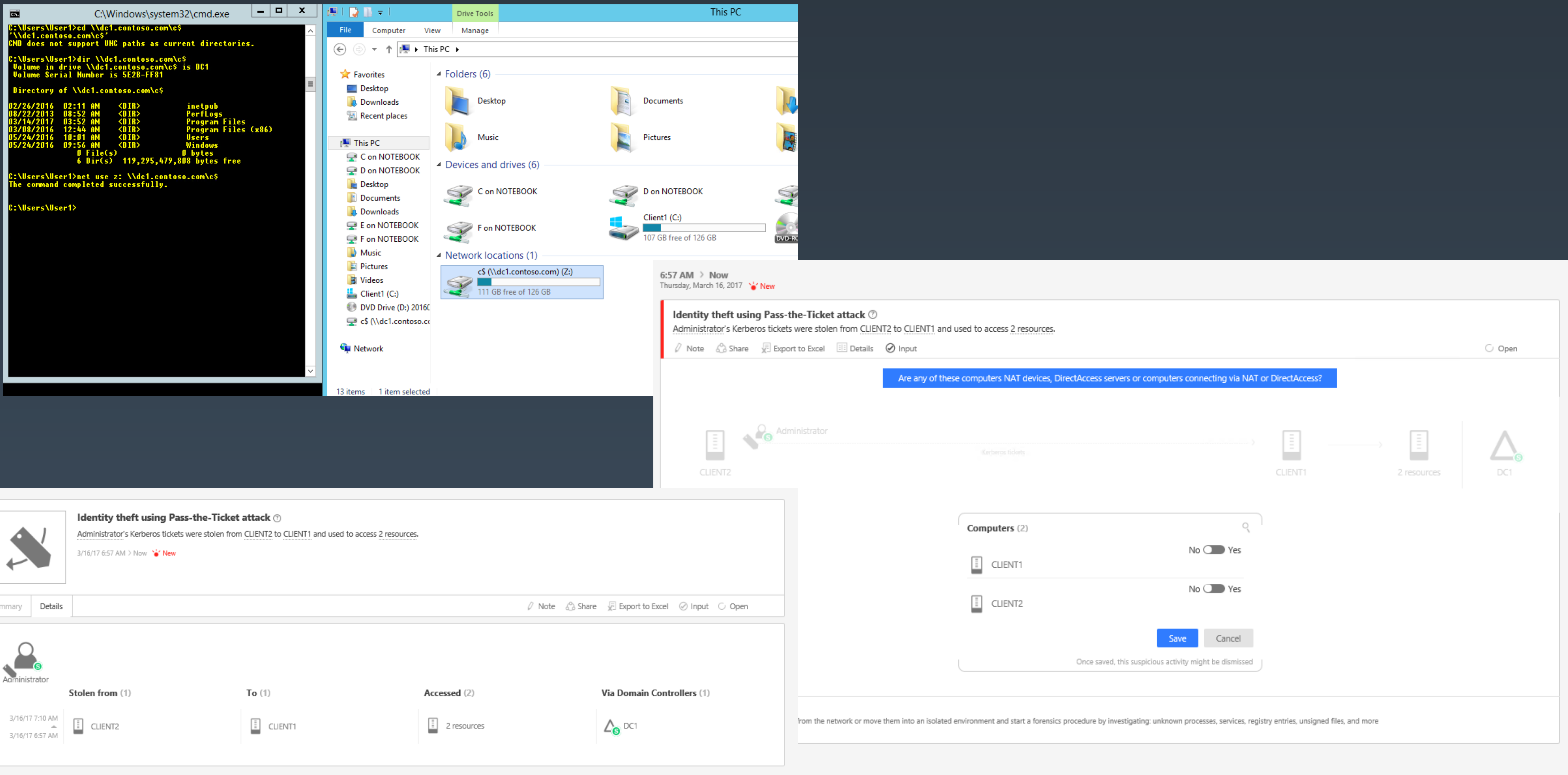




Detekce Pass-the-Ticket

- **Cíl:** Útočník se chce maskovat a přistupit k požadovaném zdroji jiným účtem a z počítače než, na kterém je skutečně přihlášen. Tudíž využije administrátorský tiket z jednoho PC a využije jej na počítači jiném
- **Popis:**
  - Útočník přistoupí na jeden z doménových počítačů
  - Spustí připravený script
  - Přejde na počítač jiný a injektuje získaný tiket
  - Otevře network share na doménovém řadiči
- **Výsledek:** Přístup je detekován, ale administrátor získal přístup
- **Odhadovaný čas detekce:** 35 sekund

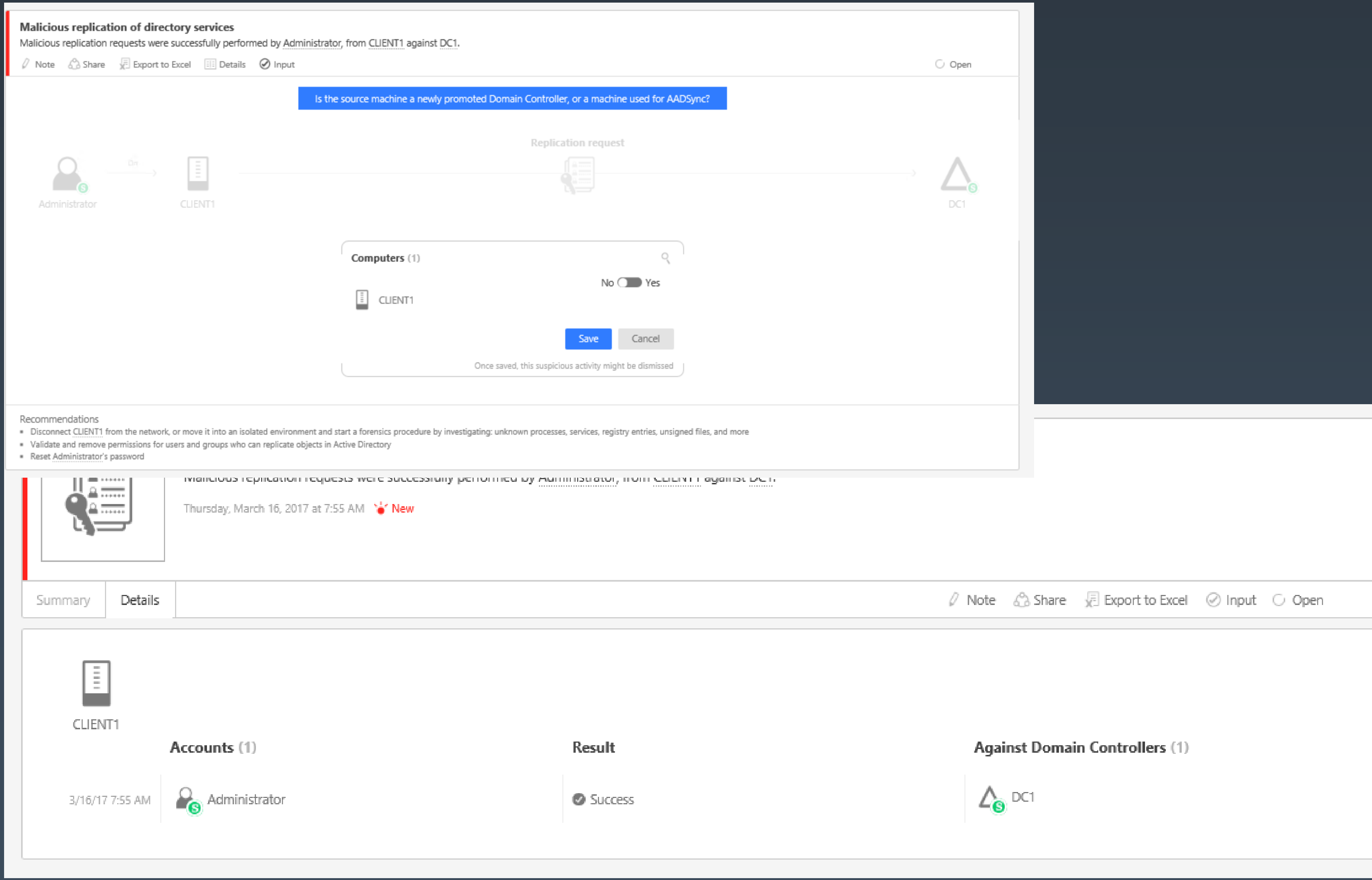
Detekce Pass-the-ticket



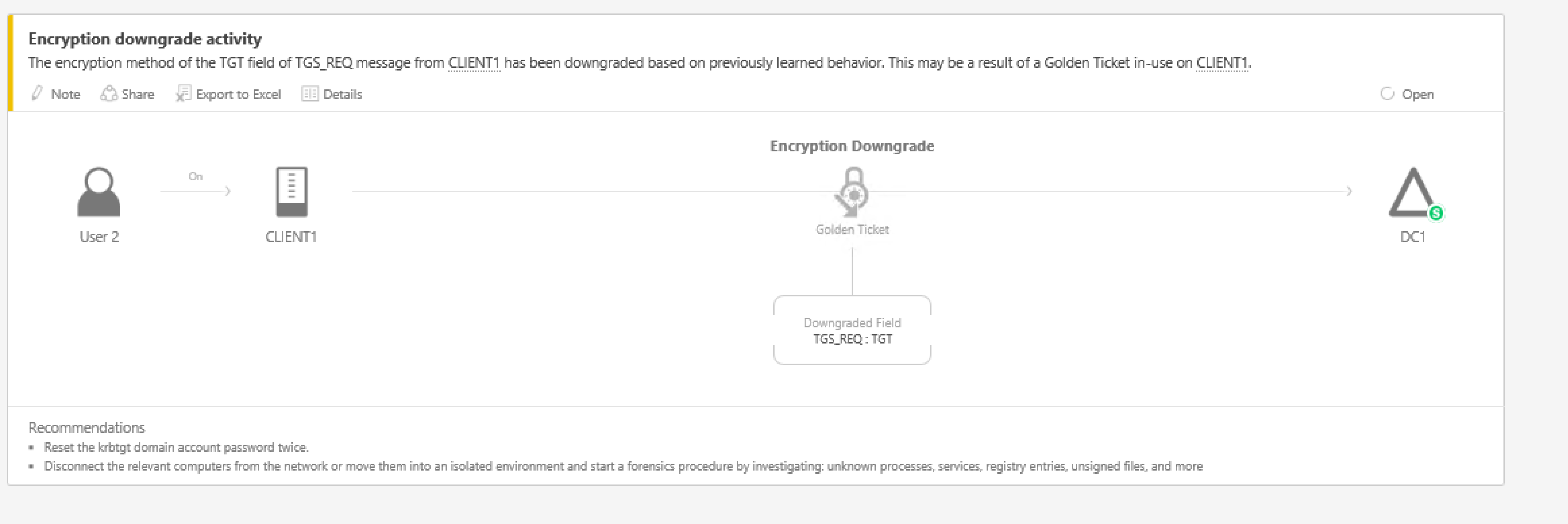
Detekce útoku s Golden ticket

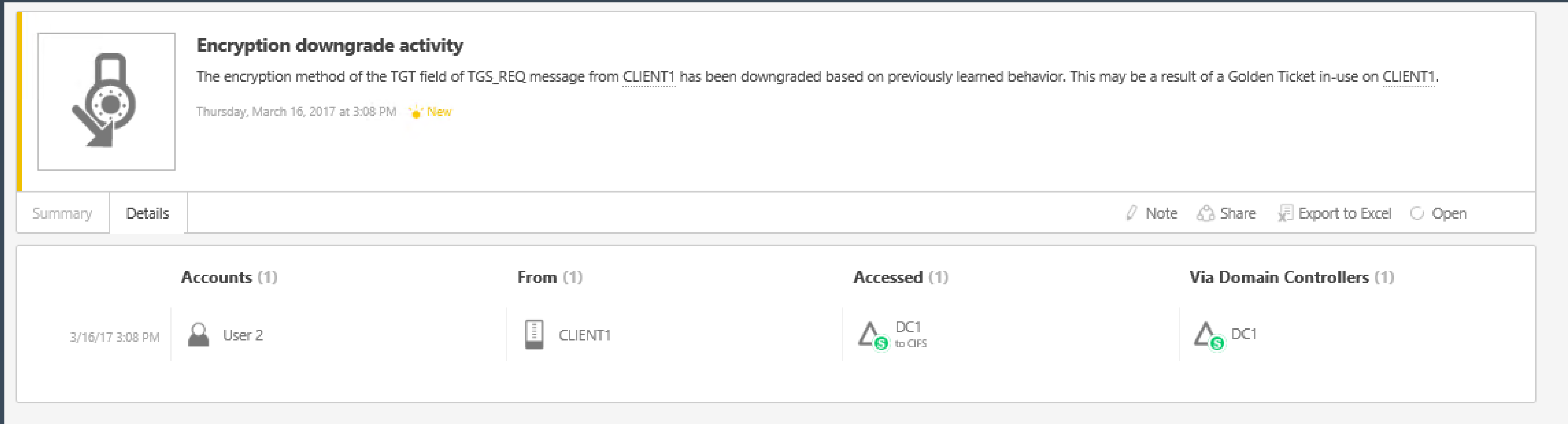
- **Cíl:** Útočník se bude snažit získat ticket služby krbgt, tak aby jej mohl i v budoucnu používat a přistupovat do sítě jako krbgt nebo jako jakýkoliv jiný uživatel.
- **Popis:**
  - Navazujeme na část Pass-The-Ticket
  - Provedeme DCSync pomocí mimikatz – **ATA detekuje za 2,5 minuty**
  - Vytvoření Golden Ticket – ATA detekuje až se naučí jak se uživatelé autentizují (by default 5 dní chování uživatelů v doméně)
  - Vytvoření Golden Ticket s uživatelem User2 a použití v User1 session (délka platnosti 10 let)
  - Přístup do sítě
- Výsledek: Administrátor získal Kerberos ticket účtu krbgt, mohl se tak vydávat za jakéhokoliv uživatele, přičemž provedl modifikaci tiketu a změnil platnost na délku 10 let
- **Odhadovaný čas detekce: 2,5 minuty**

Detekce útoku s Golden ticket



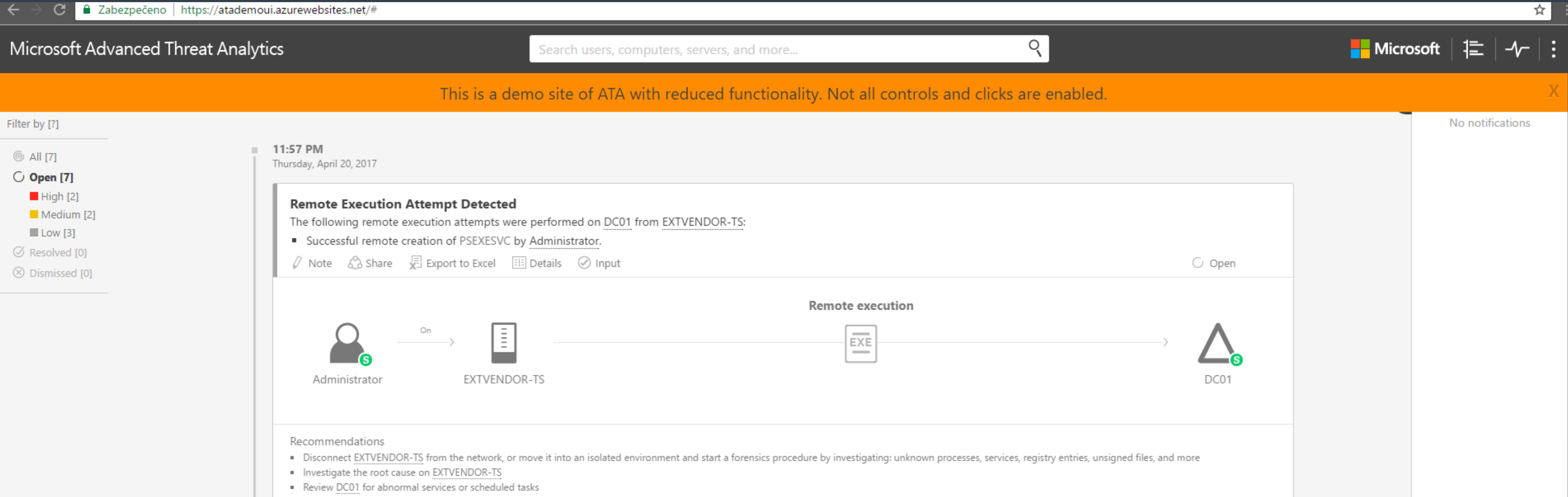
Detekce útoku s Golden ticket





ATA Demo v Microsoftu

- Ukázka základní konzole
- Omezené funkcionality
- DEMO: https://atademoui.azurewebsites.net/#



Závěrečná doporučení

- Věnujte se anomáliím
- Nasazujte bezpečnostní systémy komplexně
- Pamatujte, že útok přijde spíše z vnitřní sítě než z internetu
- Logy, procesy, autorizace
- Při nasazení ATA přemýšlejte nad nutným výkonem DCček
- Myslíte to s bezpečnostní vážně?
  - KPCS ATOM – https://atom.kpcs.cz

KPCS

Office 365

Microsoft Azure

Power BI

Exchange

Skype for Business

Windows

SharePoint

Enterprise Mobility & Security

Microsoft® System Center