“The One About Microsoft Advanced Threat Analytics”

Russell Butturini (@tcstoolhax0r)

Skydogcon 2017

WHOIS Record

-Security architect at a Top 20 CPA firm (Who I’m not representing here today in any way, shape or form)

-15 years in IT and 10 full time doing enterprise security (pen testing, infrastructure, cloud stuff)

-**Not** a Microsoft fanboy

-Original creator of NoSQLMap (@codingo_ maintains it now, he’s awesome, go help him out!)

Why give this talk?

-There aren’t enough “Car and Driver road test” talks at security cons.

-IMO not enough people know about ATA; it’s a great tool, but there’s a lot of ways to screw it up, and the documentation provided by Microsoft is cluttered.

-All the non-vendor talks and blogs out there on ATA were either about bypassing it, or running it in a lab, but not on running it in production.

DISCLAIMER: I don’t work for Microsoft. These are my experiences. I probably got stuff wrong. Your mileage may vary.

Agenda

-What is Advanced Threat Analytics? (And more importantly, what ATA isn’t!)

-Architecture, setup, and security considerations

-”Find all the things”

-Maintenance and troubleshooting

-Questions/comments/profanity

What is Advanced Threat Analytics?

-Monitoring solution based on Aorato acquisition.

-Included with Enterprise CAL suite, Enterprise Mobility Suite + Security, and Enterprise Cloud Suite licenses.

-Uses behavioral analytics, network traffic, and event logs to detect advanced threats in the network (e.g. pass-the-hash, Kerberos golden ticket abuse, AD recon attacks, password spraying)

-Also can find authentication configuration issues (cleartext LDAP, broken trusts, remote process starts ,etc.)

-Designed with “alert fatigue” in mind

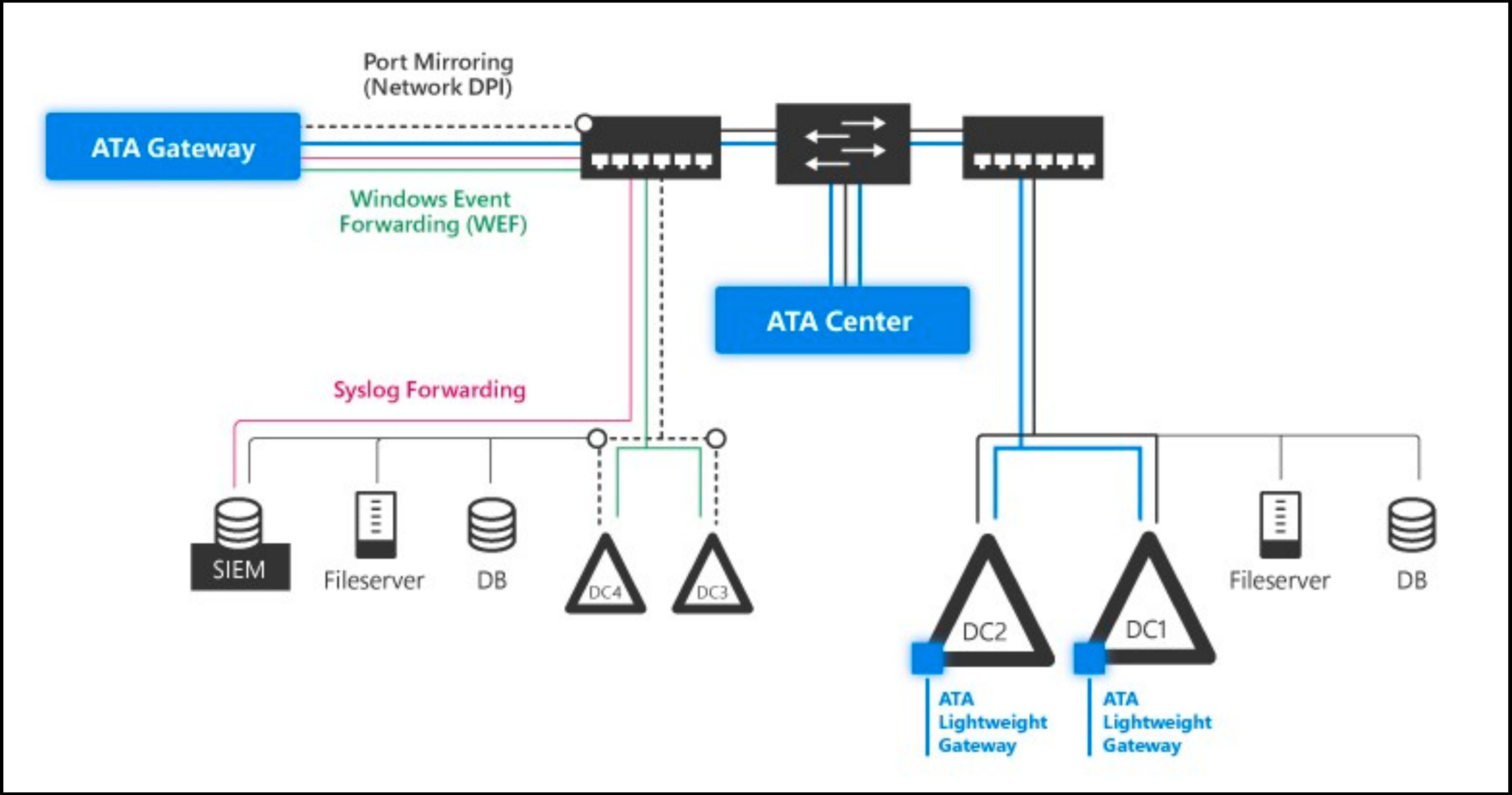
What ATA is **NOT**

-A replacement for your SIEM

-A solution that will check many compliance requirement boxes

- A robust reporting tool

ATA Eye Chart



ATA Architecture

-Two components: Centers and Gateways

-Centers do all the alerting, configuration, management, data aggregation.

-Gateways receive traffic and event log events for analysis and forwarding to centers.

ATA Center

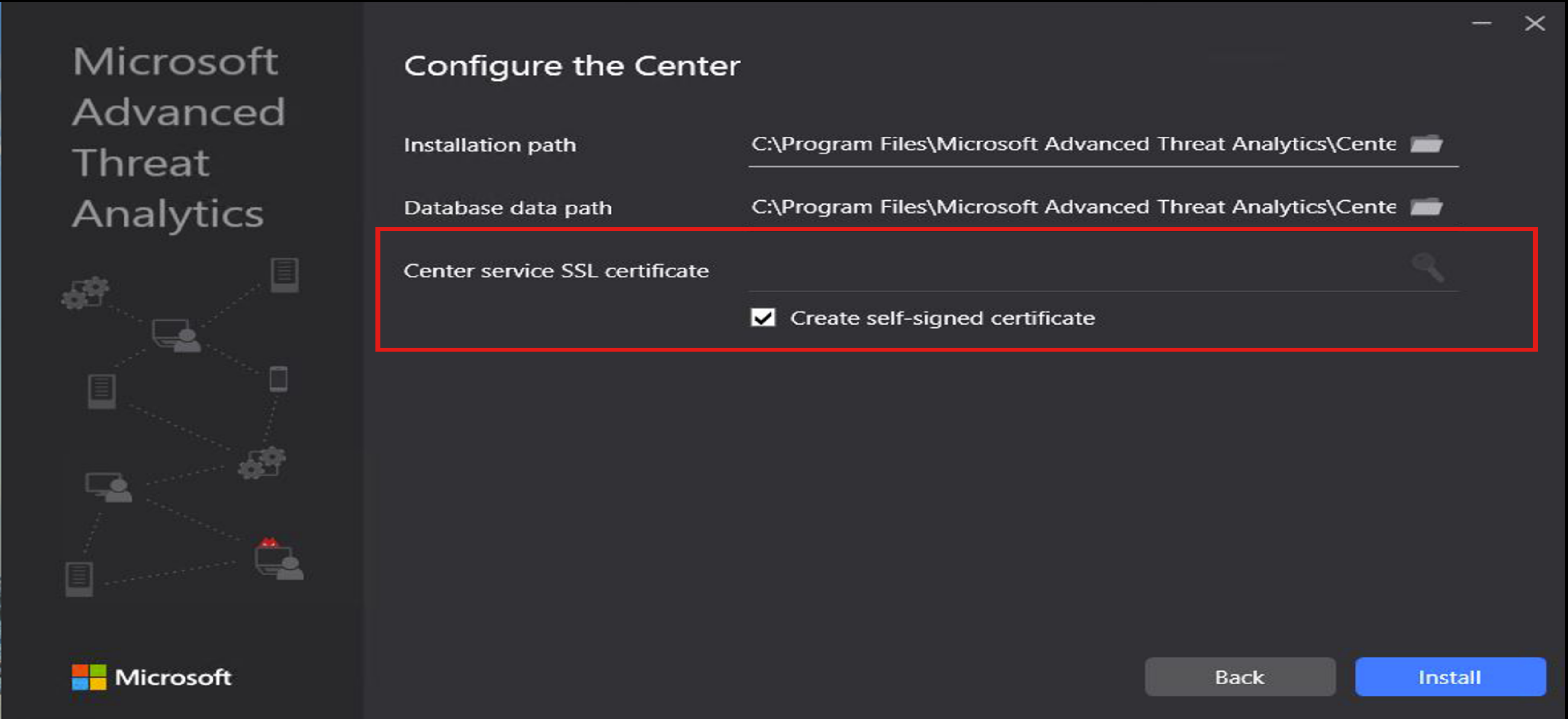
-The “brains” and user interface of ATA

-Uses MongoDB to store traffic data and event logs forwarded from domain controllers (more on this later)

-Needs lots of resources! (2 procs, 32 GB RAM minimum-More is better)

-Can forward generated alerts to SIEM, email, or other external sources.

ATA Center Installation



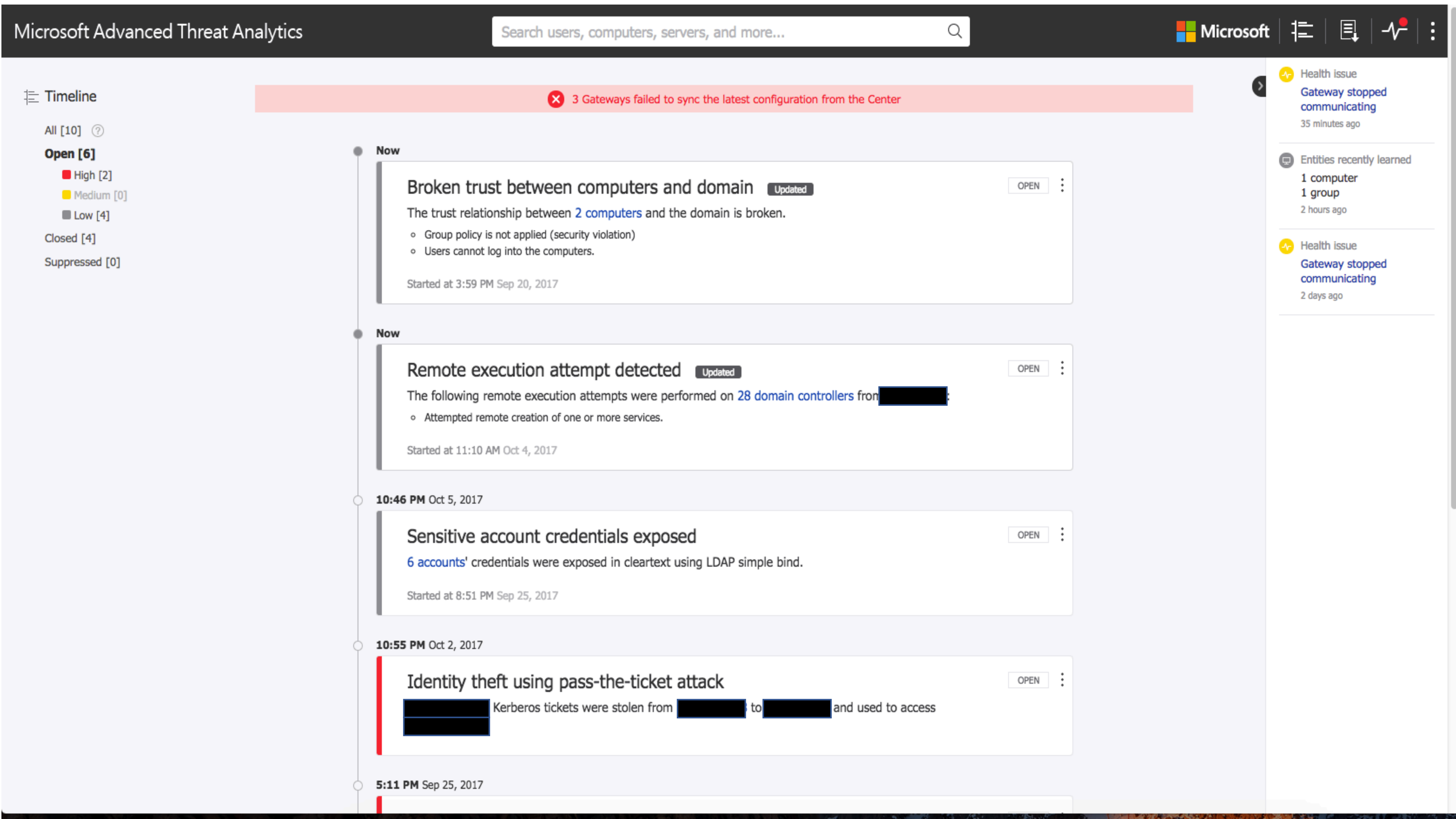
Configure the Center

Installation path: C:\Program Files\Microsoft Advanced Threat Analytics\Cente

Database data path: C:\Program Files\Microsoft Advanced Threat Analytics\Cente

Center service SSL certificate

☑ Create self-signed certificate



Microsoft Advanced Threat Analytics

Search users, computers, servers, and more...

Microsoft

Timeline

All [10]

Open [6]

🟥 High [2]

🟨 Medium [0]

■ Low [4]

Closed [4]

Suppressed [0]

3 Gateways failed to sync the latest configuration from the Center

Now

Broken trust between computers and domain Updated

OPEN

The trust relationship between 2 computers and the domain is broken.

- Group policy is not applied (security violation)
- Users cannot log into the computers.

Started at 3:59 PM Sep 20, 2017

Now

Remote execution attempt detected Updated

OPEN

The following remote execution attempts were performed on 28 domain controllers fro[redacted]:

- Attempted remote creation of one or more services.

Started at 11:10 AM Oct 4, 2017

10:46 PM Oct 5, 2017

Sensitive account credentials exposed

OPEN

6 accounts' credentials were exposed in cleartext using LDAP simple bind.

Started at 8:51 PM Sep 25, 2017

10:55 PM Oct 2, 2017

Identity theft using pass-the-ticket attack

OPEN

[redacted] Kerberos tickets were stolen from [redacted] to [redacted] and used to access [redacted]

5:11 PM Sep 25, 2017

Health issue

Gateway stopped communicating

35 minutes ago

Entities recently learned

1 computer

1 group

2 hours ago

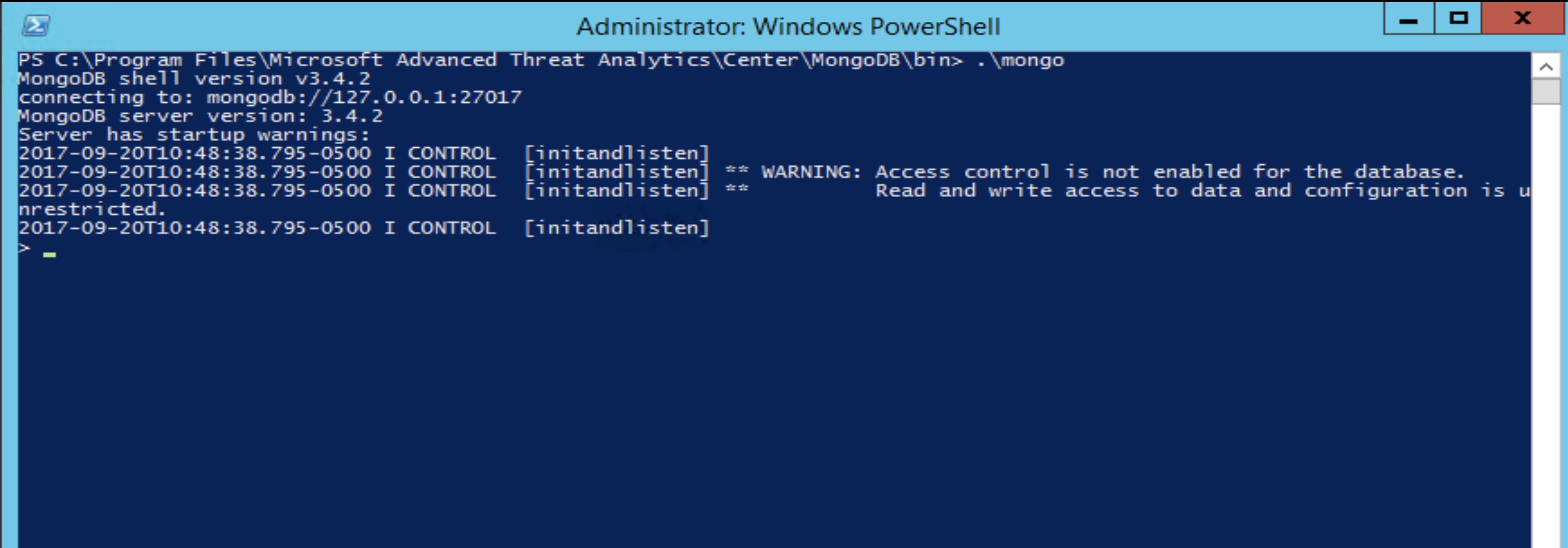
Health issue

Gateway stopped communicating

2 days ago

ATA Center

NIST 800-53 AU-9 – Protection of Audit Information The information system protects audit information and audit tools from unauthorized access, modification, and deletion.



```
PS C:\Program Files\Microsoft Advanced Threat Analytics\Center\MongoDB\bin> .\mongo
MongoDB shell version v3.4.2
connecting to: mongodb://127.0.0.1:27017
MongoDB server version: 3.4.2
Server has startup warnings:
2017-09-20T10:48:38.795-0500 I CONTROL  [initandlisten]
2017-09-20T10:48:38.795-0500 I CONTROL  [initandlisten] ** WARNING: Access control is not enabled for the database.
2017-09-20T10:48:38.795-0500 I CONTROL  [initandlisten] **          Read and write access to data and configuration is u
nrestricted.
2017-09-20T10:48:38.795-0500 I CONTROL  [initandlisten]
> _
```

Managing Access

-ATA Administrators: Full Access to everything

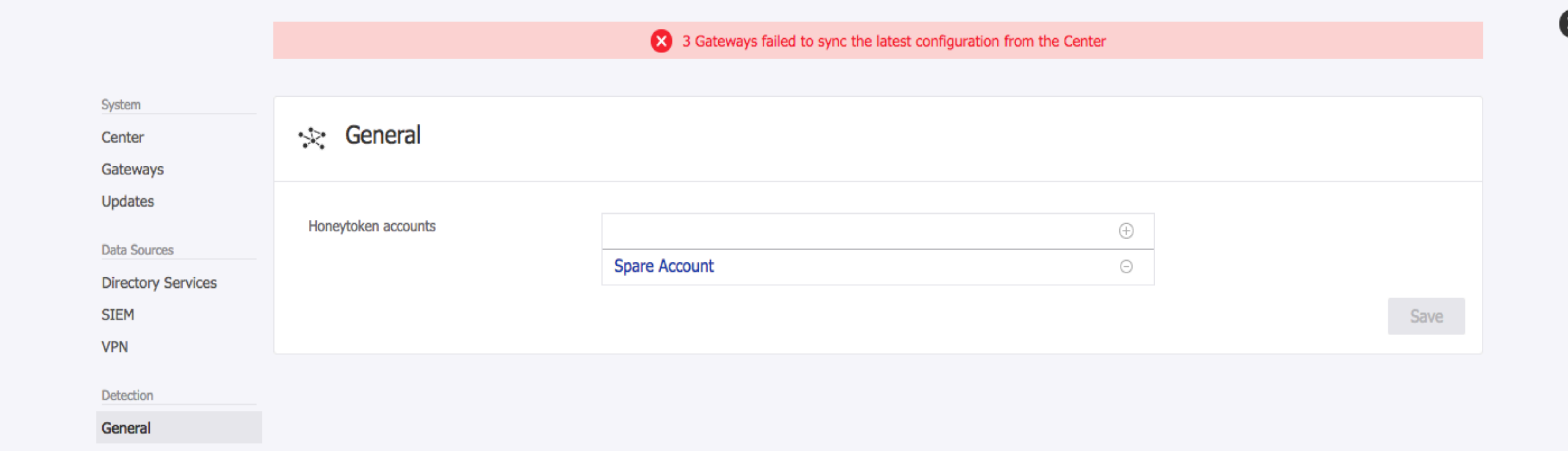
-ATA Users: View/update suspect activity, close incidents, export data

-ATA Viewers: View incidents

Honeytoken Accounts

-Allows specification of bogus AD accounts that should never be used.

-Any activity with this account triggers a high severity alert.



3 Gateways failed to sync the latest configuration from the Center

General

Honeytoken accounts: Spare Account

ATA Gateways

-Come in two flavors: Gateways and lightweight gateways

-Lightweight gateways run directly on DCs and monitor resource usage to prevent performance issues.

-Gateways run on dedicated servers and need port spans/mirroring + Windows Event Forwarding.

-Ingest domain controller network traffic and event logs for analysis and forwarding to the ATA center.

Lightweight Gateway Notes

-MS says lightweight gateways won’t work right on VMWare. Mine work fine.

-As of v1.8, lightweight gateways can read event logs directly from the domain controller, no WEF required.

-Throughput for lightweight gateways is much lower than dedicated gateways. Good for branch offices, use dedicated gateways in data center.

Gateway Installation

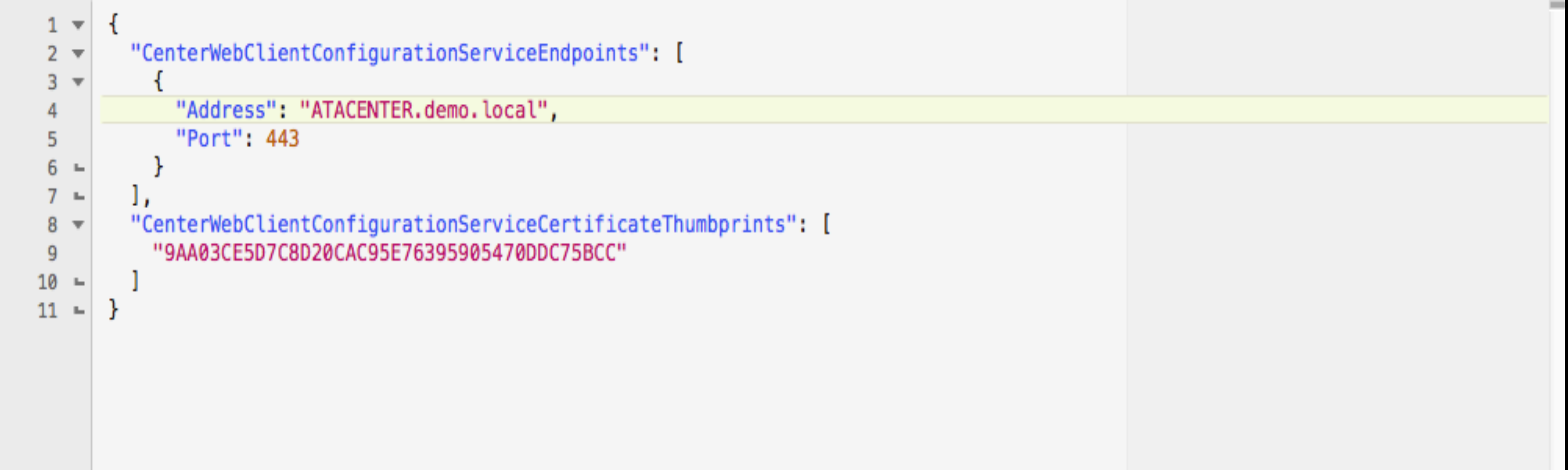
-Uses a customized package in a ZIP file downloaded from the ATA center.

-Contains a JSON file with configuration settings.

-Can be scripted and installed silently; see https://docs.microsoft.com/en-us/advanced-threat-analytics/ata-silent-installation

  -The center can be installed silently too, but I don’t recommend it!

Gateway Installation

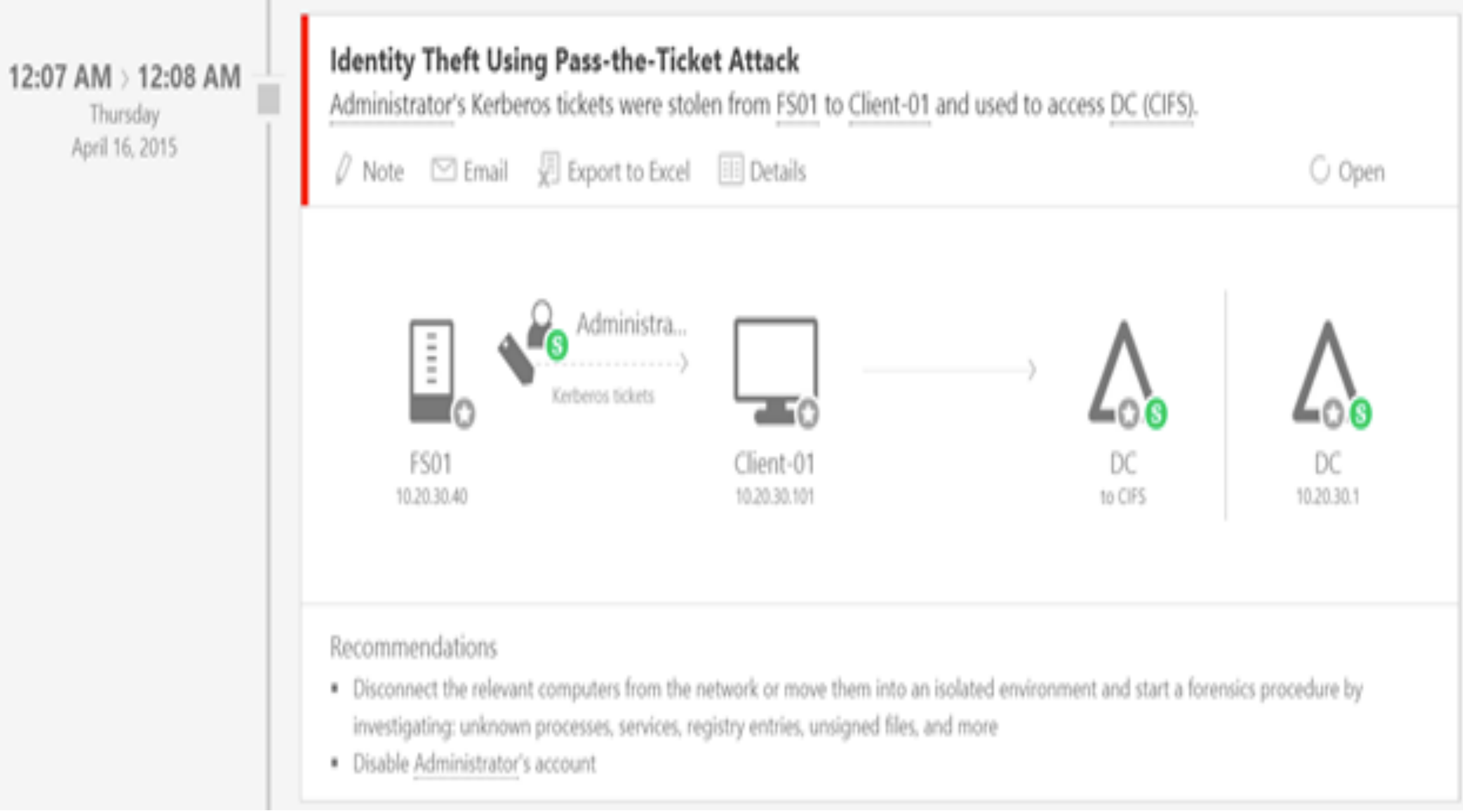


```
{
  "CenterWebClientConfigurationServiceEndpoints": [
    {
      "Address": "ATACENTER.demo.local",
      "Port": 443
    }
  ],
  "CenterWebClientConfigurationServiceCertificateThumbprints": [
    "9AA03CE5D7C8D20CAC95E76395905470DDC75BCC"
  ]
}
```

Gateway Installation

-A backup of the gateway configuration data is made to C:\Program Files\Microsoft Advanced Threat Analytics\Center\Backup once an hour.

-10 backups are retained; this file is **CRITICAL** if you have to restore the Center.



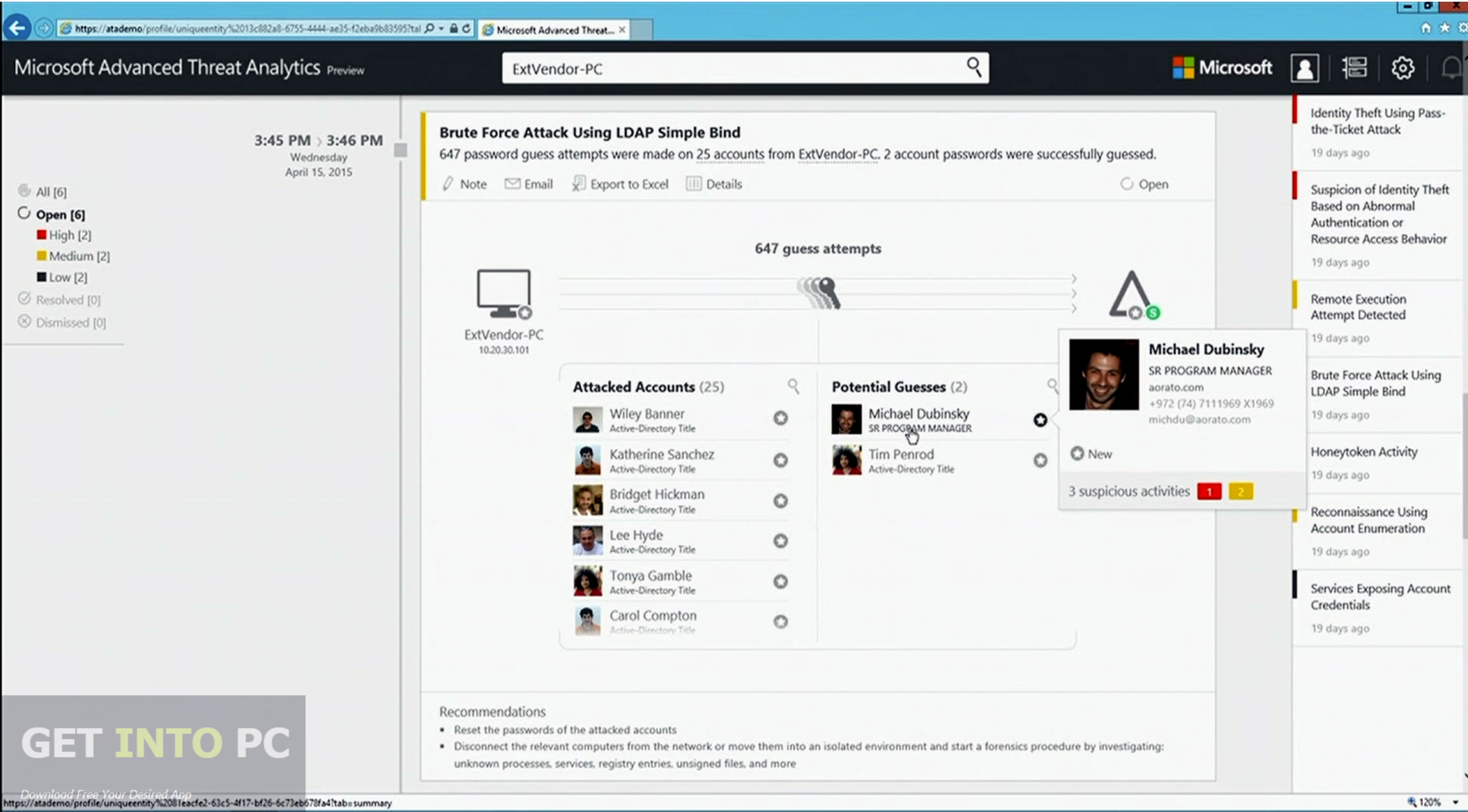
12:07 AM › 12:08 AM
Thursday
April 16, 2015

Identity Theft Using Pass-the-Ticket Attack

Administrator's Kerberos tickets were stolen from FS01 to Client-01 and used to access DC (CIFS).

Recommendations

- Disconnect the relevant computers from the network or move them into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more
- Disable Administrator's account



https://atademo/profile/uniqueentity%2013c882a8-6755-4444-ae35-f2eba9b83595?tal

Microsoft Advanced Threat...

Microsoft Advanced Threat Analytics Preview

ExtVendor-PC

Microsoft

3:45 PM › 3:46 PM
Wednesday
April 15, 2015

All [6]
Open [6]
🟥 High [2]
🟨 Medium [2]
⬛ Low [2]
Resolved [0]
Dismissed [0]

Brute Force Attack Using LDAP Simple Bind

647 password guess attempts were made on 25 accounts from ExtVendor-PC. 2 account passwords were successfully guessed.

Note | Email | Export to Excel | Details | ○ Open

647 guess attempts

ExtVendor-PC
10.20.30.101

Attacked Accounts (25)

Wiley Banner	Active-Directory Title
Katherine Sanchez	Active-Directory Title
Bridget Hickman	Active-Directory Title
Lee Hyde	Active-Directory Title
Tonya Gamble	Active-Directory Title
Carol Compton	Active-Directory Title

Potential Guesses (2)

Michael Dubinsky	SR PROGRAM MANAGER
Tim Penrod	Active-Directory Title

Michael Dubinsky
SR PROGRAM MANAGER
aorato.com
+972 (74) 7111969 X1969
michdu@aorato.com

New

3 suspicious activities 🟥 1 🟨 2

Recommendations

- Reset the passwords of the attacked accounts
- Disconnect the relevant computers from the network or move them into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more

Identity Theft Using Pass-the-Ticket Attack
19 days ago

Suspicion of Identity Theft Based on Abnormal Authentication or Resource Access Behavior
19 days ago

Remote Execution Attempt Detected
19 days ago

Brute Force Attack Using LDAP Simple Bind
19 days ago

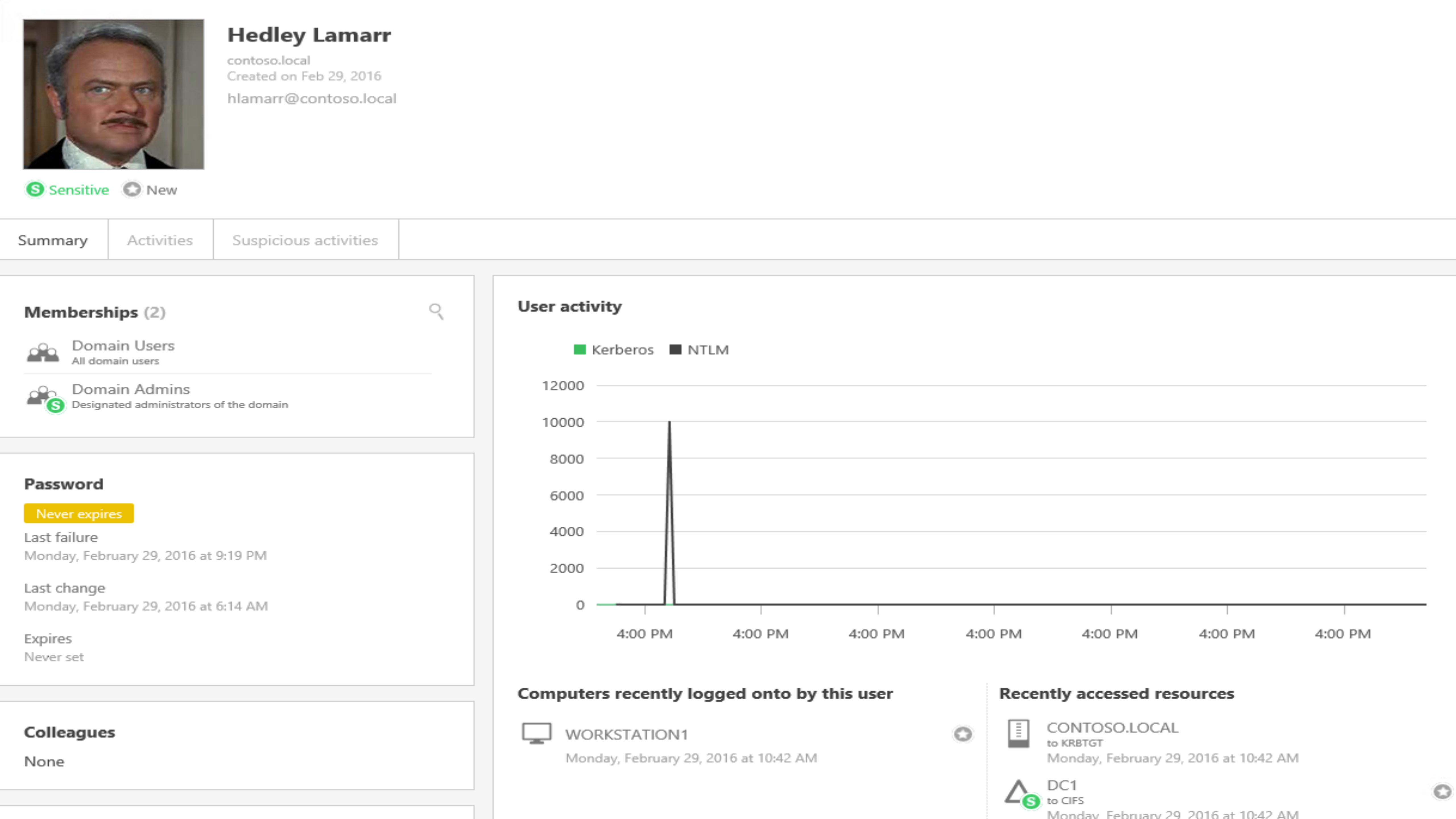
Honeytoken Activity
19 days ago

Reconnaissance Using Account Enumeration
19 days ago

Services Exposing Account Credentials
19 days ago

https://atademo/profile/uniqueentity%2081eacfe2-63c5-4f17-bf26-6c73eb678fa4?tab=summary

120%



Hedley Lamarr

contoso.local
Created on Feb 29, 2016
hlamarr@contoso.local

S Sensitive   New

Memberships (2)

Domain Users
All domain users

Domain Admins
Designated administrators of the domain

Password

Never expires

Last failure
Monday, February 29, 2016 at 9:19 PM

Last change
Monday, February 29, 2016 at 6:14 AM

Expires
Never set

Colleagues

None

User activity

Computers recently logged onto by this user

WORKSTATION1
Monday, February 29, 2016 at 10:42 AM

Recently accessed resources

CONTOSO.LOCAL
to KRBTGT
Monday, February 29, 2016 at 10:42 AM

DC1
to CIFS
Monday, February 29, 2016 at 10:42 AM

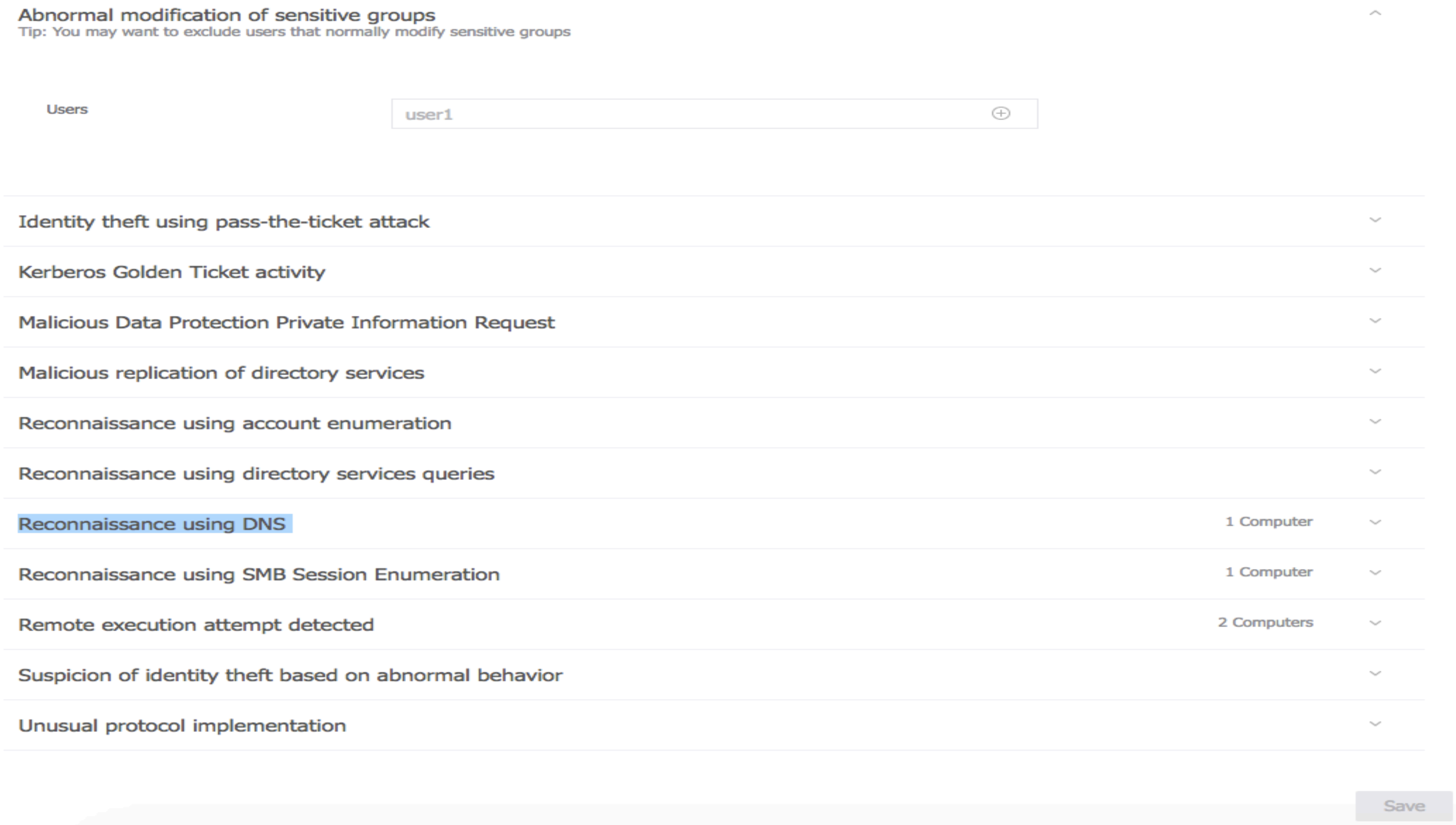
Find all the things!

-ATA alerting is great and well tuned out of the box.

-Behavioral analysis needs about 30 days to work properly.

-IT admin activities (like workstation patching) seem to throw it off; balance between tuning the accounts and ignoring the alert during maintenance windows.

-Users/machines moving in a way DNS can’t be resolved (like VPN) can cause false positives.



Abnormal modification of sensitive groups
Tip: You may want to exclude users that normally modify sensitive groups

Users: user1

Identity theft using pass-the-ticket attack

Kerberos Golden Ticket activity

Malicious Data Protection Private Information Request

Malicious replication of directory services

Reconnaissance using account enumeration

Reconnaissance using directory services queries

Reconnaissance using DNS — 1 Computer

Reconnaissance using SMB Session Enumeration — 1 Computer

Remote execution attempt detected — 2 Computers

Suspicion of identity theft based on abnormal behavior

Unusual protocol implementation

For the truly hardcore threat hunters…

-The ATA MongoDB instance can be queried directly (but remember the security deficiencies we talked about before…)

-Example: You want to know about the NTLM activities John Doe performed on 10/1/2017:

-db.UniqueEntity.find({Name: "John Doe"})

-Note the _id key value pair (123bdd24-b269-h6e1-9c72-7737as875351)

-db.Ntlms_<closest date>.find({SourceAccountId: "123bdd24-b269-h6e1-9c72-7737as875351"})

Reference: https://docs.microsoft.com/en-us/advanced-threat-analytics/troubleshooting-ata-using-ata-database

Getting Help

-ATA support forum: https://social.technet.microsoft.com/Forums/en-US/home?forum=mata

-Constantly monitored by ATA support staff in Israel. Quick support, and will help over email if problems get too complex to resolve on the forum.

What if I don’t own/like this???

-A similar free alternative: https://www.blackhillsinfosec.com/endpoint-monitoring-shoestring-budget-webcast-write/

-Uses Elasticsearch, Logstash, Kibana, and Windows Event Forwarding to gather logs and find anomalous events.

-Not as out of the box ready, but can obtain similar results.

That’s it!

-Slides will be available here: https://github.com/tcstool/ata

-Feel free to send questions to me @tcstoolhax0r

-Also, if you’re interested in an IT manager job building a smart grid from the ground up for a large rural electric cooperative in middle TN, let me know

-Thanks to Skydogcon for letting me speak!