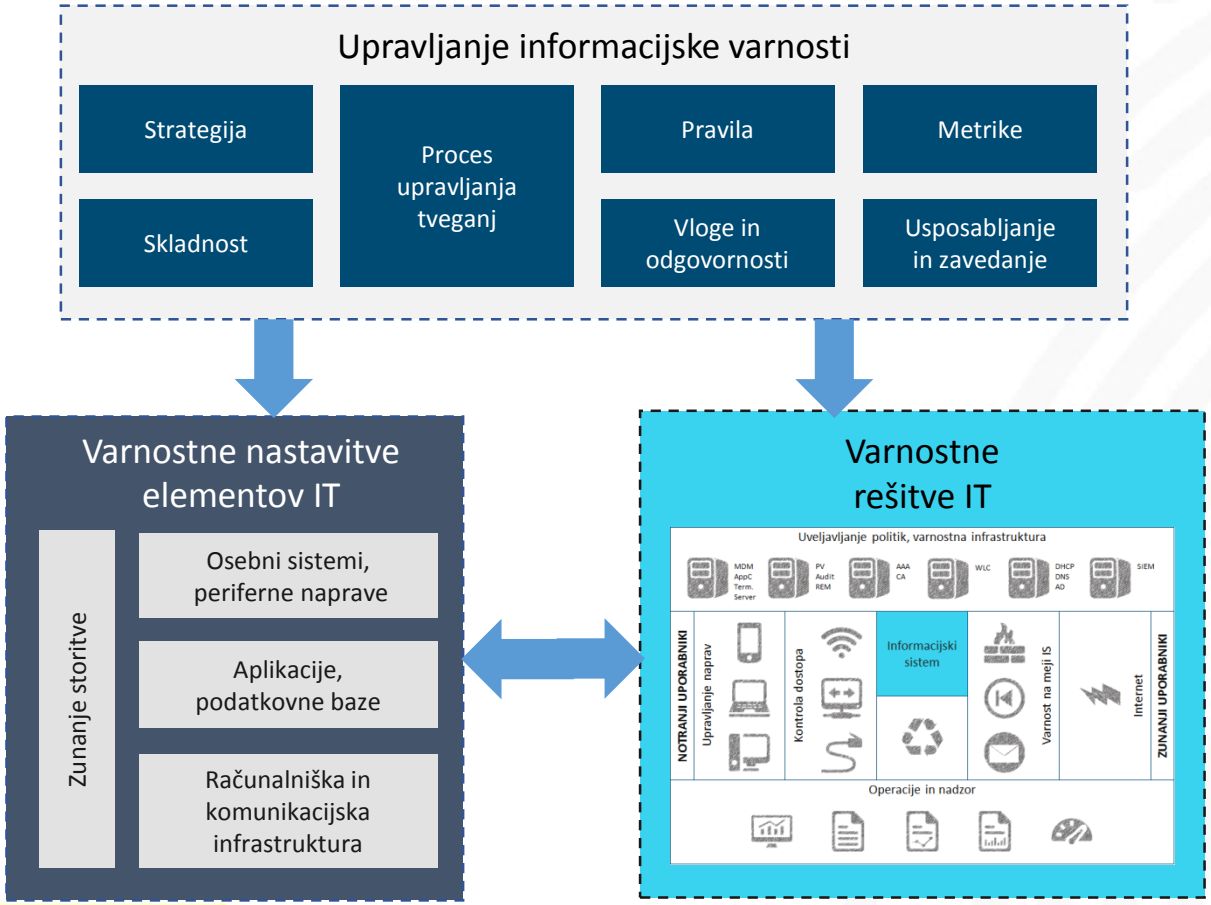
Kako nadzorujemo poskuse dostopov v omrežje?

Samo Gaberšček & Gašper Črnugelj
SRC

Dostopi – ali jih razumemo?

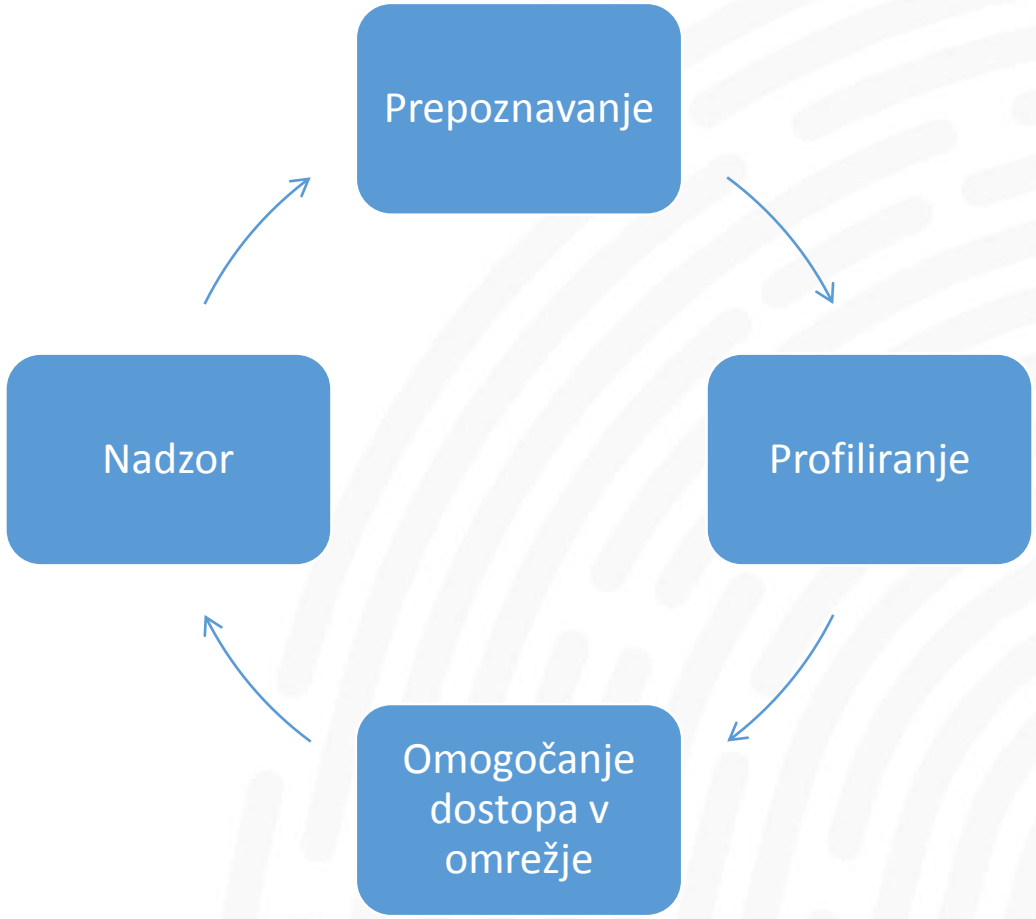
- Kdo so uporabniki?
- Katere naprave?
- Kam dostopajo/poskušajo?

Integrirana varnost



Identity Services Engine

- Cisco ISE je platforma za nadzor in upravljanje dostopov.
- Avtomatizira in poenostavlja upravljanje dostopov.



Identity Services Engine

- Podpira celoten proces upravljanja varnostnega dogodka

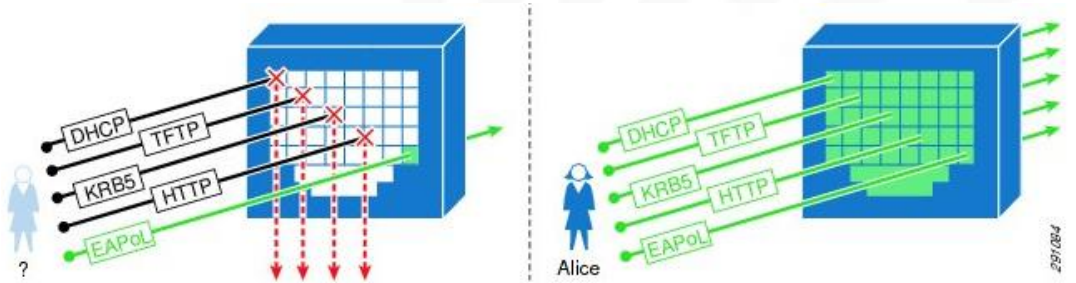
Agenda

- Proces uvedbe, izkušnje iz prakse
- ISE

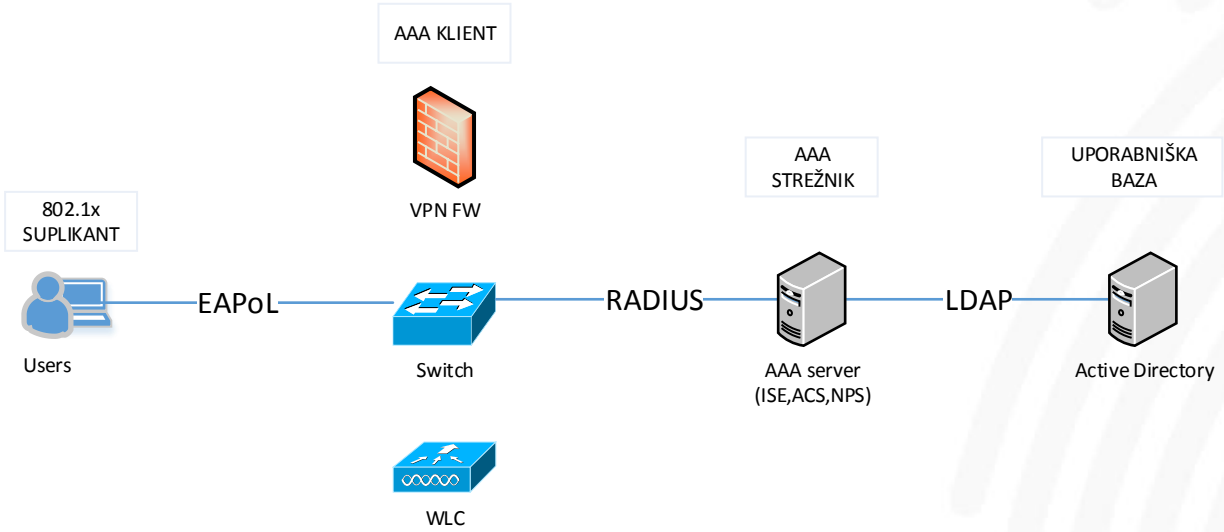
Proces uvedbe

- Analiza in načrtovanje
- Pilotska postavitev
- Implementacija

NAC koncept



NAC Gradniki



Analiza in načrtovanje

- Splošni podatki
- AAA strežnik
- AAA klient
- Končne naprave

Analiza in načrtovanje – obseg vpeljave

REMOTE ACCESS

WIRELESS ACCESS

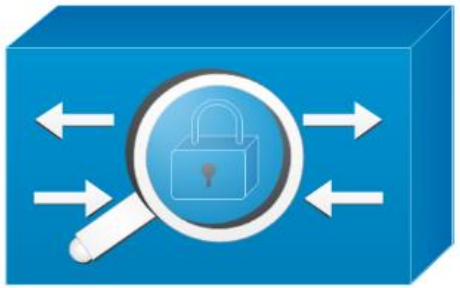
WIRED ACCESS

TERMINAL ACCESS

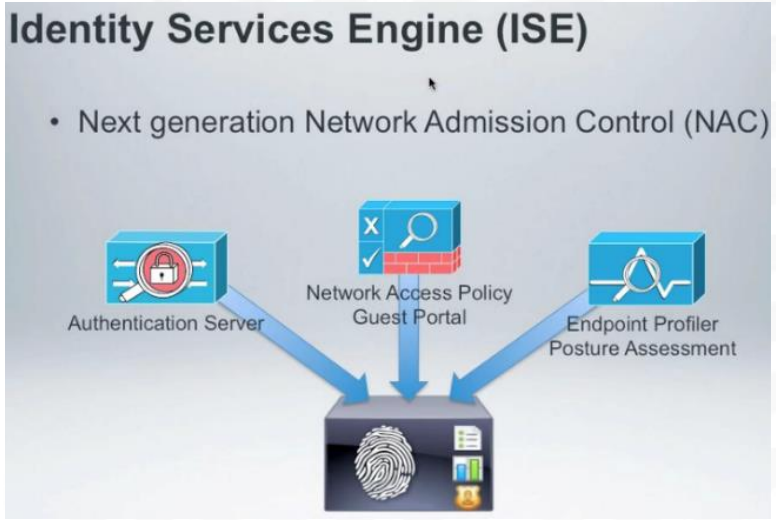
Analiza in načrtovanje

Microsoft

Network Policy Server



ACS



Analiza in načrtovanje – AAA klienti

- Omejevanje dostopa

RADIUS

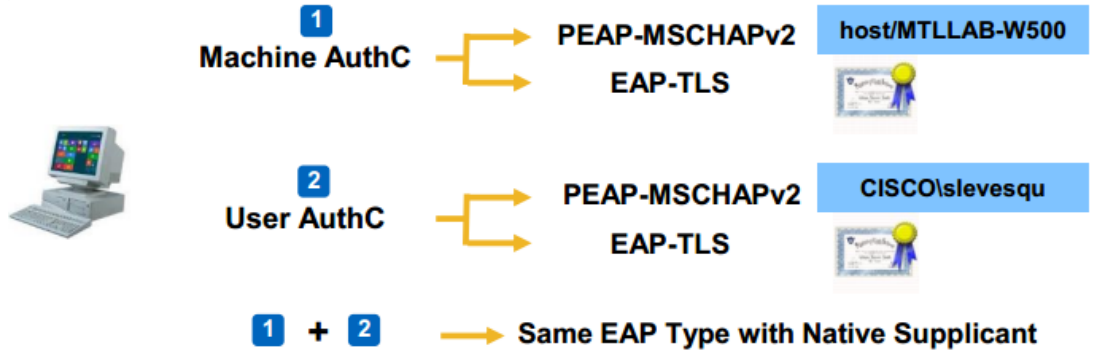
TACACS

Analiza in načrtovanje – AAA klienti

Poenotena konfiguracija?

Načrtovanje – avtentikacijska metoda

- EAP-TLS
- PEAP
- PEAP-TLS
- EAP-FAST
- MAB



Končne naprave

- Domenske uporabniške
- Nedomenske uporabniške
- IP telefoni
- Virtualne končne uporabniške
- Tiskalniki
- Kontrola pristopa
- Video kamere

Načrtovanje - avtorizacija

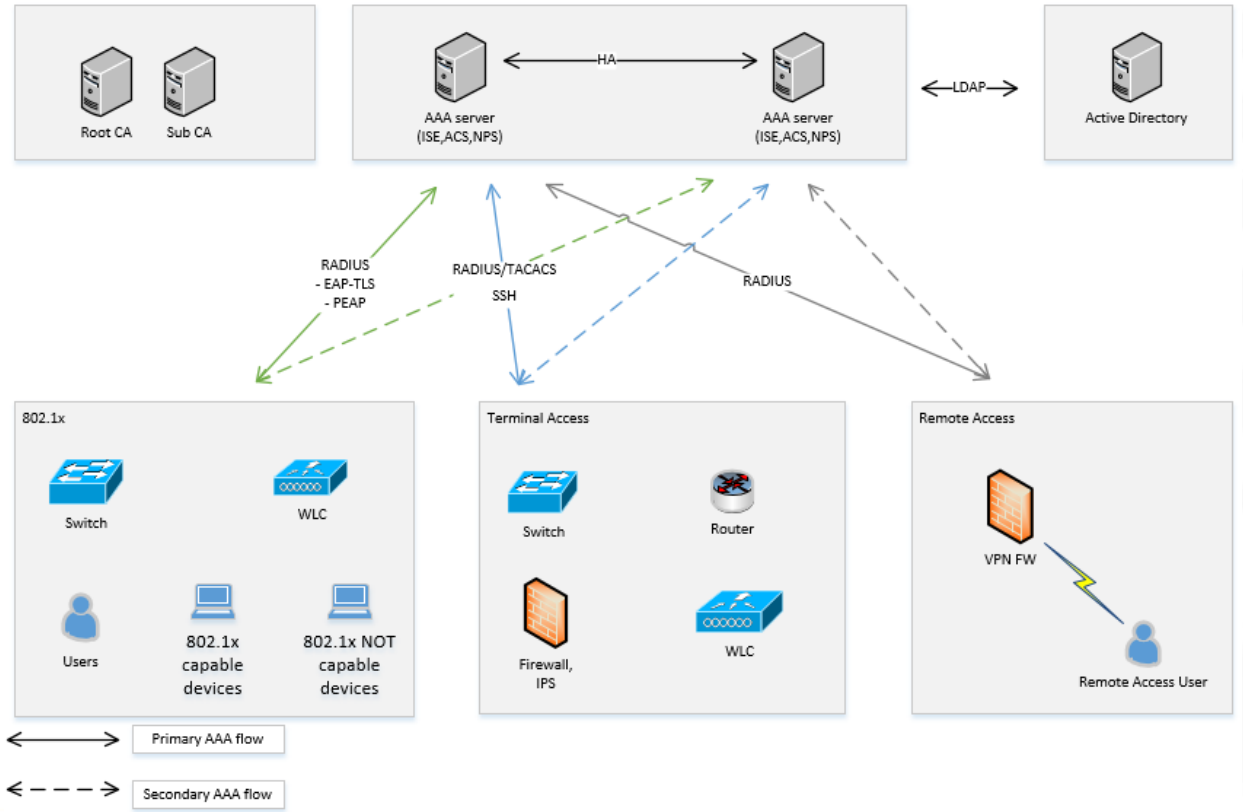
NAC – žični del:

- dACL
- Dynamic VID
- Redirect URL
- NEAT

Terminalski dostop:

- Privilege level
- Command Authorization

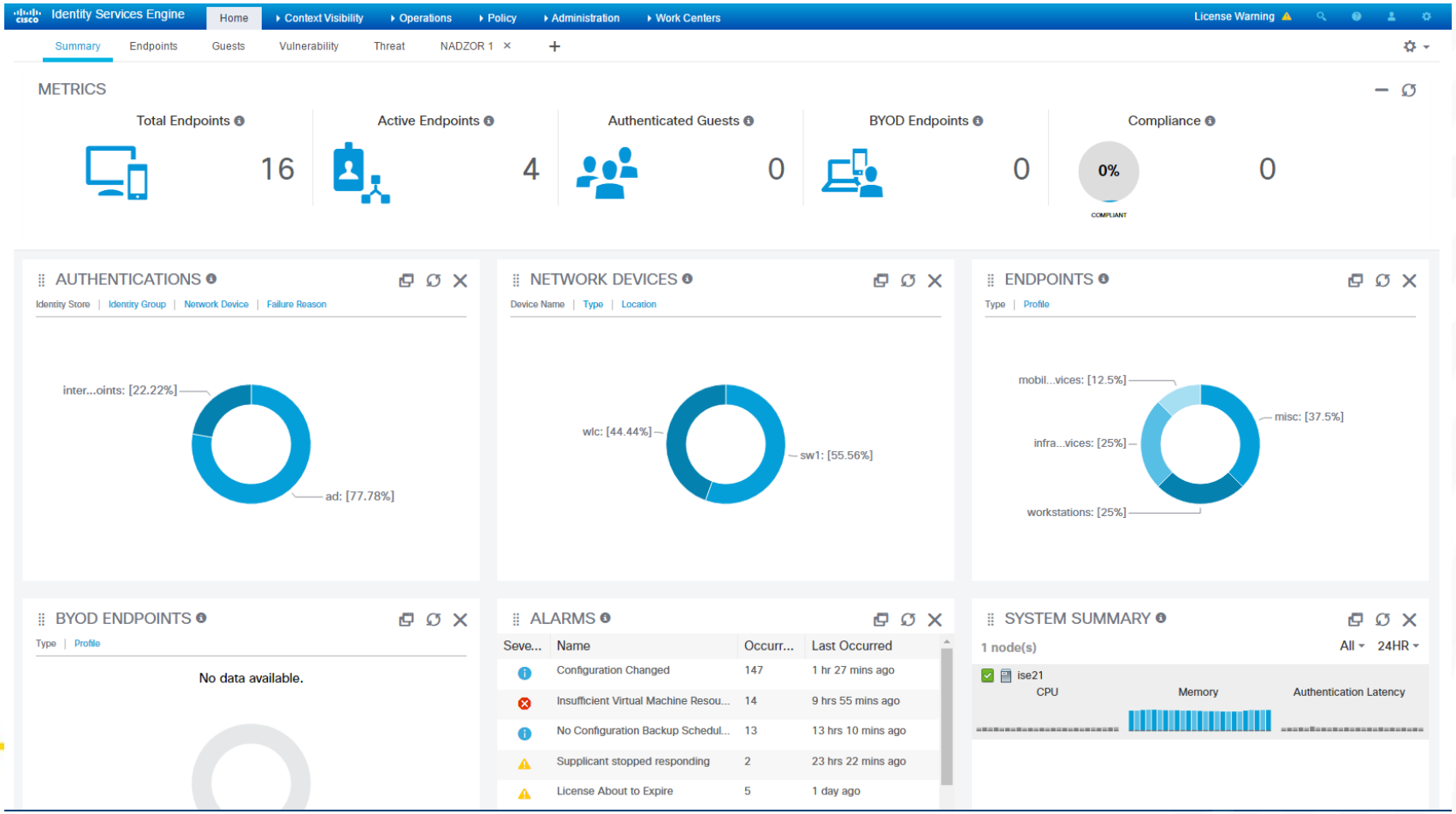
Arhitektura



Implementacija

- Naprave
- Politika – AAA strežnik
- Mrežni vmesniki

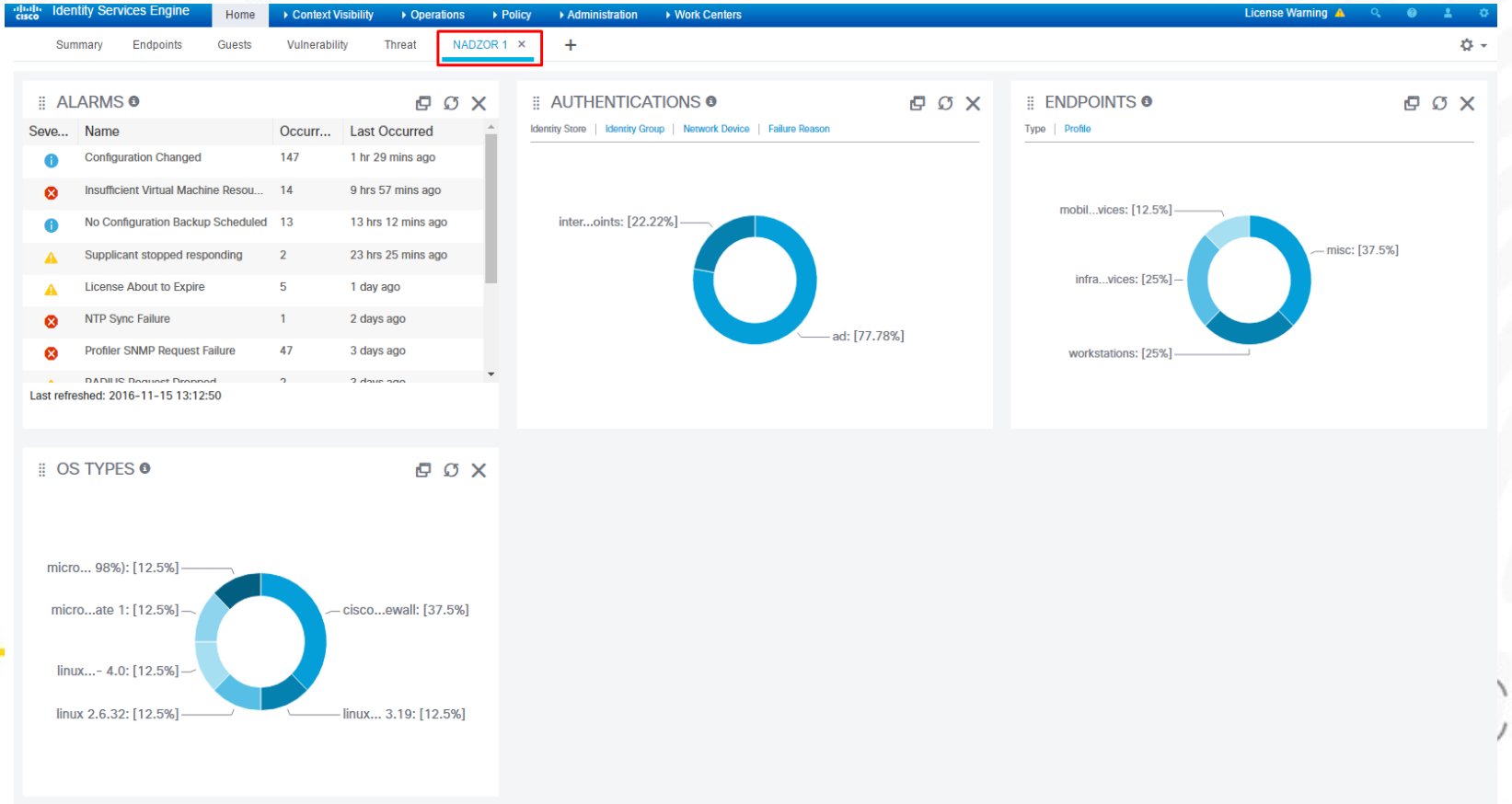
ISE

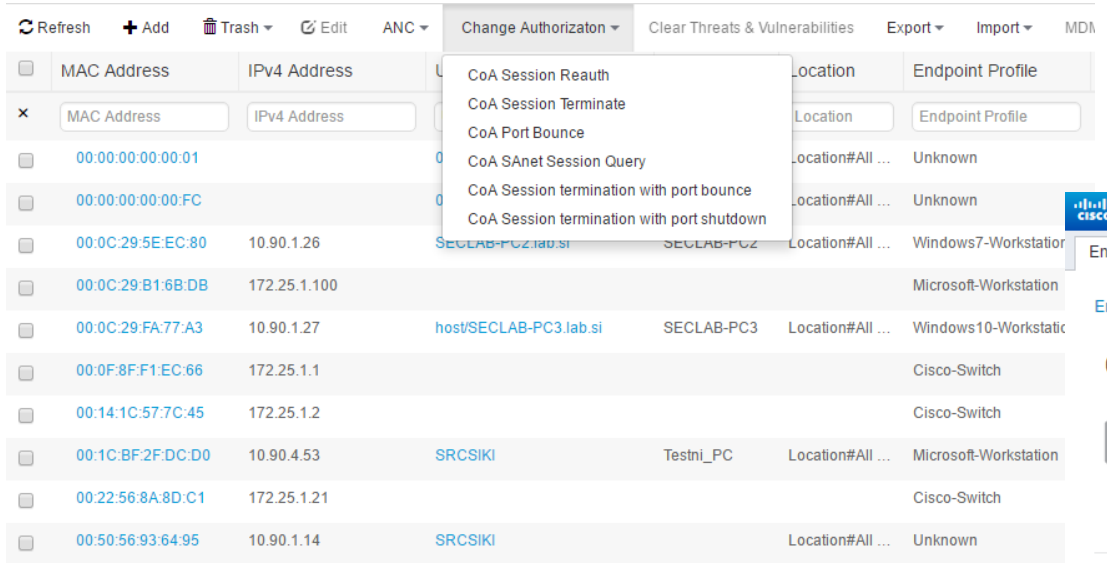

Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
License Warning
Summary
Endpoints
Guests
Vulnerability
Threat
NADZOR 1
METRICS
Total Endpoints
16
Active Endpoints
4
Authenticated Guests
0
BYOD Endpoints
0
Compliance
0%
0
COMPLIANT
AUTHENTICATIONS
Identity Store | Identity Group | Network Device | Failure Reason
inter...oints: [22.22%]
ad: [77.78%]
NETWORK DEVICES
Device Name | Type | Location
wlc: [44.44%]
sw1: [55.56%]
ENDPOINTS
Type | Profile
mobil...vices: [12.5%]
misc: [37.5%]
infra...vices: [25%]
workstations: [25%]
BYOD ENDPOINTS
Type | Profile
No data available.
ALARMS
Seve...
Name
Occurr...
Last Occurred
Configuration Changed
147
1 hr 27 mins ago
Insufficient Virtual Machine Resou...
14
9 hrs 55 mins ago
No Configuration Backup Schedul...
13
13 hrs 10 mins ago
Supplicant stopped responding
2
23 hrs 22 mins ago
License About to Expire
5
1 day ago
SYSTEM SUMMARY
1 node(s)
All
24HR
ise21
CPU
Memory
Authentication Latency

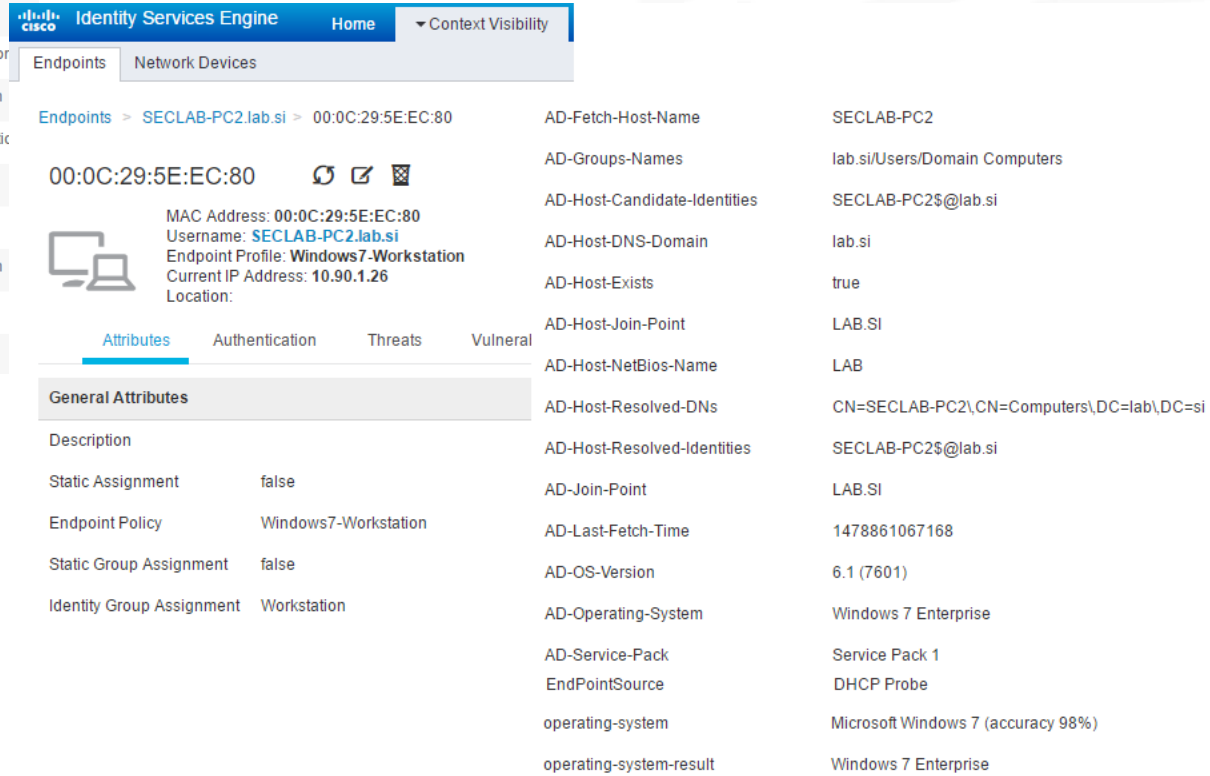
Add Dashlet(s)

Search

Alarms	Remove	Guest Type	Add	Top Vulnerability	Add
Authentications	Remove	Identity Group	Add	Total Compromised Endpoints	Add
BYOD Endpoints	Add	Location	Add	Total Vulnerable Endpoints	Add
Compliance	Add	Network Devices	Add	Vulnerability Watchlist	Add
Compromised Endpoints Over Time	Add	OS Types	Remove	Vulnerable Endpoints Over Time	Add
Device Type	Add	Policy Service Node	Add		
Endpoint Categories	Add	Status	Add		
Endpoints	Remove	System Summary	Remove		
Failure Reason	Add	Threats Watchlist	Add		
Guest Status	Add	Top Threats	Add		




Refresh
Add
Trash
Edit
ANC
Change Authorizaton
Clear Threats & Vulnerabilities
Export
Import
CoA Session Reauth
CoA Session Terminate
CoA Port Bounce
CoA SAnet Session Query
CoA Session termination with port bounce
CoA Session termination with port shutdown
MAC Address
IPv4 Address
Location
Endpoint Profile
00:00:00:00:00:01 Unknown
00:00:00:00:00:FC Unknown
00:0C:29:5E:EC:80 10.90.1.26 Windows7-Workstation
00:0C:29:B1:6B:DB 172.25.1.100 Microsoft-Workstation
00:0C:29:FA:77:A3 10.90.1.27 host/SECLAB-PC3.lab.si SECLAB-PC3 Windows10-Workstation
00:0F:8F:F1:EC:66 172.25.1.1 Cisco-Switch
00:14:1C:57:7C:45 172.25.1.2 Cisco-Switch
00:1C:BF:2F:DC:D0 10.90.4.53 SRCSIKI Testni_PC Microsoft-Workstation
00:22:56:8A:8D:C1 172.25.1.21 Cisco-Switch
00:50:56:93:64:95 10.90.1.14 SRCSIKI Unknown


Identity Services Engine
Home
Context Visibility
Endpoints
Network Devices
Endpoints > SECLAB-PC2.lab.si > 00:0C:29:5E:EC:80
00:0C:29:5E:EC:80
MAC Address: 00:0C:29:5E:EC:80
Username: SECLAB-PC2.lab.si
Endpoint Profile: Windows7-Workstation
Current IP Address: 10.90.1.26
Location:
Attributes
Authentication
Threats
Vulneral
General Attributes
Description
Static Assignment false
Endpoint Policy Windows7-Workstation
Static Group Assignment false
Identity Group Assignment Workstation
AD-Fetch-Host-Name SECLAB-PC2
AD-Groups-Names lab.si/Users/Domain Computers
AD-Host-Candidate-Identities SECLAB-PC2$@lab.si
AD-Host-DNS-Domain lab.si
AD-Host-Exists true
AD-Host-Join-Point LAB.SI
AD-Host-NetBios-Name LAB
AD-Host-Resolved-DNs CN=SECLAB-PC2\,CN=Computers\,DC=lab\,DC=si
AD-Host-Resolved-Identities SECLAB-PC2$@lab.si
AD-Join-Point LAB.SI
AD-Last-Fetch-Time 1478861067168
AD-OS-Version 6.1 (7601)
AD-Operating-System Windows 7 Enterprise
AD-Service-Pack Service Pack 1
EndPointSource DHCP Probe
operating-system Microsoft Windows 7 (accuracy 98%)
operating-system-result Windows 7 Enterprise

Kaj dosežemo z uvedbo kontrole

- Višji nivo zaščite in posledično zanesljivost informacijskega sistema
- Popolni nadzor nad uporabniškimi dostopi in napravami, ki so priključene v naš IS
- Poenostavitev upravljanja in vršenja definirane varnostne politike, ki se nanaša na dostop uporabnikov do IS, njegovih servisov in virov
- Centralizacija nadzora in upravljanja dostopa
- Doseganje skladnosti s standardi

Thank you

SRC
info@src.si