A1

A1 ICT kaVARNA

Kako z upravljanjem privilegiranih dostopov do večje kibernetske varnosti?

11. marec | Maribor
13. marec | Ljubljana

wallix

| A1 ICT Distribucija

Kdo je privilegiran uporabnik?

Kdo je privilegiran uporabnik?

— vim — 80×24

```
[core]
        repositoryformatversion = 0
        filemode = true
        bare = false
        logallrefupdates = true
        ignorecase = true
        precomposeunicode = true
[remote "origin"]
        url = https://
        fetch = +refs/heads/*:refs/remotes/origin/*
[branch "master"]
        remote = origin
        merge = refs/heads/master
[remote "
        url = https://                @          .scm.azurewebsites.net:443/          .git
        fetch = +refs/heads/*:refs/remotes,          /*
~
~
~
                                                    /.git/config" 16L, 475C
```

1

2

Select Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.16251.0]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>net user pcunlocker
User name                    pcunlocker
Full Name
Comment
User's comment
Country/region code          [redacted]
Account active               Yes
Account expires              Never

Password last set            8/7/2017 7:50:07 AM
Password expires             Never
Password changeable          8/7/2017 7:50:07 AM
Password required            Yes
User may change password     Yes
```

K2.pub | id_rsa.pub | controller.php | index.html | config.inc.php

```php
<?php

/* Servers configuration */
$i = 0;

/* Server: localhost [1] */
$i++;
$cfg['Servers'][$i]['verbose'] = 'localhost';
$cfg['Servers'][$i]['host'] = 'localhost';
$cfg['Servers'][$i]['port'] = '';
$cfg['Servers'][$i]['socket'] = '';
$cfg['Servers'][$i]['connect_type'] = 'tcp';
$cfg['Servers'][$i]['extension'] = 'mysqli';
$cfg['Servers'][$i]['auth_type'] = 'config';
$cfg['Servers'][$i]['user'] = 'root';
$cfg['Servers'][$i]['password'] = 'root';
$cfg['Servers'][$i]['AllowNoPassword'] = true;

/* End of servers configuration */

$cfg['DefaultLang'] = 'en-utf-8';
$cfg['ServerDefault'] = 1;
$cfg['UploadDir'] = '';
$cfg['SaveDir'] = '';


/* rajk - for blobstreaming */
$cfg['Servers'][$i]['bs_garbage_threshold'] = 50;
$cfg['Servers'][$i]['bs_repository_threshold'] = '32M';
$cfg['Servers'][$i]['bs_temp_blob_timeout'] = 600;
$cfg['Servers'][$i]['bs_temp_log_threshold'] = '32M';


?>
```

Kdo je privilegiran uporabnik?

Trendi, ki vzpodbujajo potrebno kibernetske varnosti

- UPRAVLJANJE TVEGANJ

✓ Vdori
✓ Renome
✓ Intelektualna lastnina
✓ Strateška sredstva

- SKLADNOST

✓ Regulacije in standardi industrij, držav,…
  - GDPR,
  - NIS
  - PCI-DSS
  - HIPPA / HDS
  - ISO-27001
  - …

- MIGRACIJA V OBLAK

✓ Tehnična kompleksnost
✓ Migracija v javni oblak / Hibridna okolja

- DIGITALNA TRANSFORMACIJA

✓ Dev Ops širitev
✓ Iz IT v OT in IoT omrežja
✓ Mobilnost
✓ Interoperabilnost
✓ Hitro širjenje števila naprav


wallix
80%
vdorov izkorišča
privilegirane račune

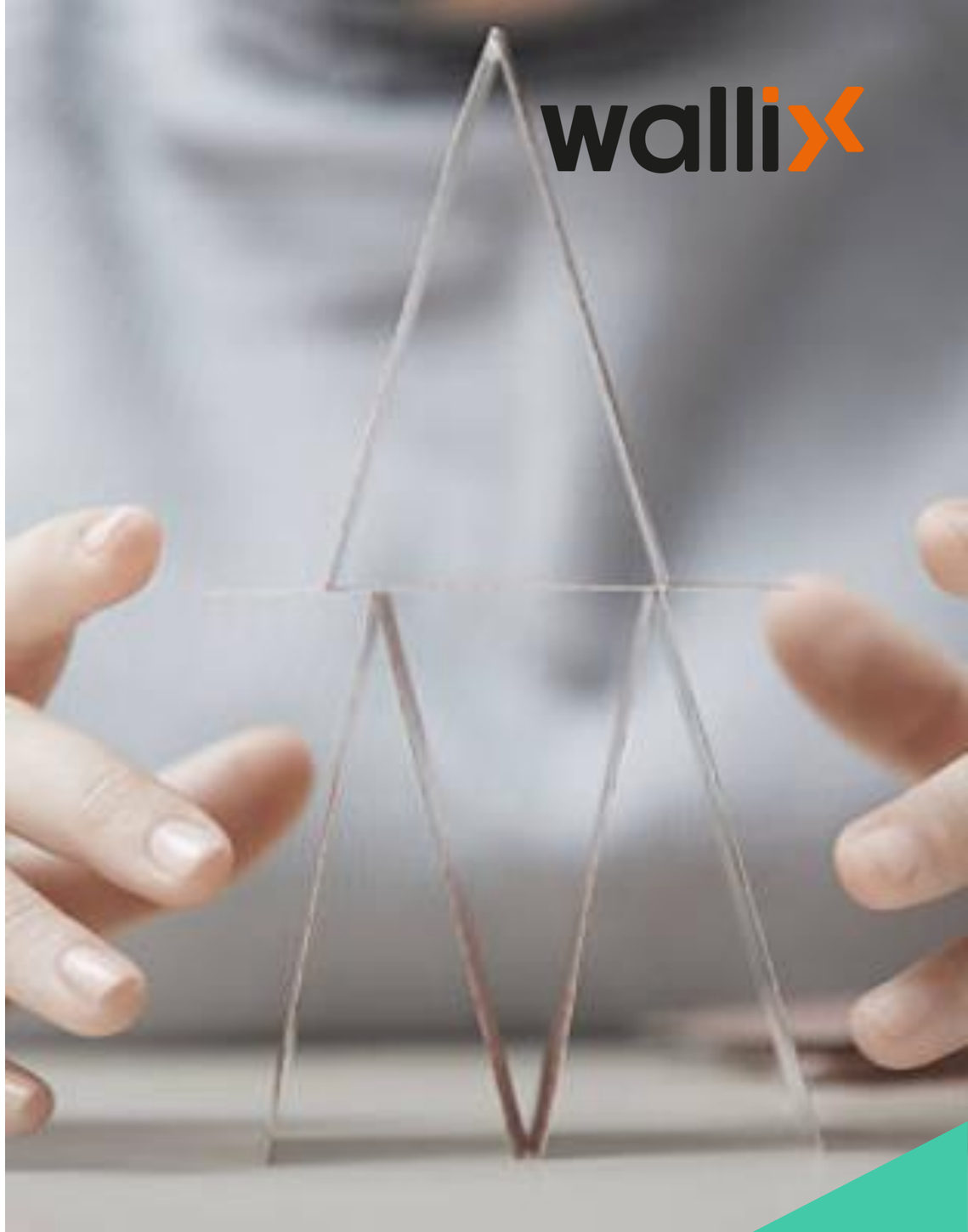
EKSPLOZIJA PRIVILEGIJEV

Uporabniki
Aplikacije
Naprave
DevOps

Kaj se zgodi ob kompromisu privilegiranih računov?

“ Tega ne boste vedeli… dokler ne bo prišlo do vdora. ”

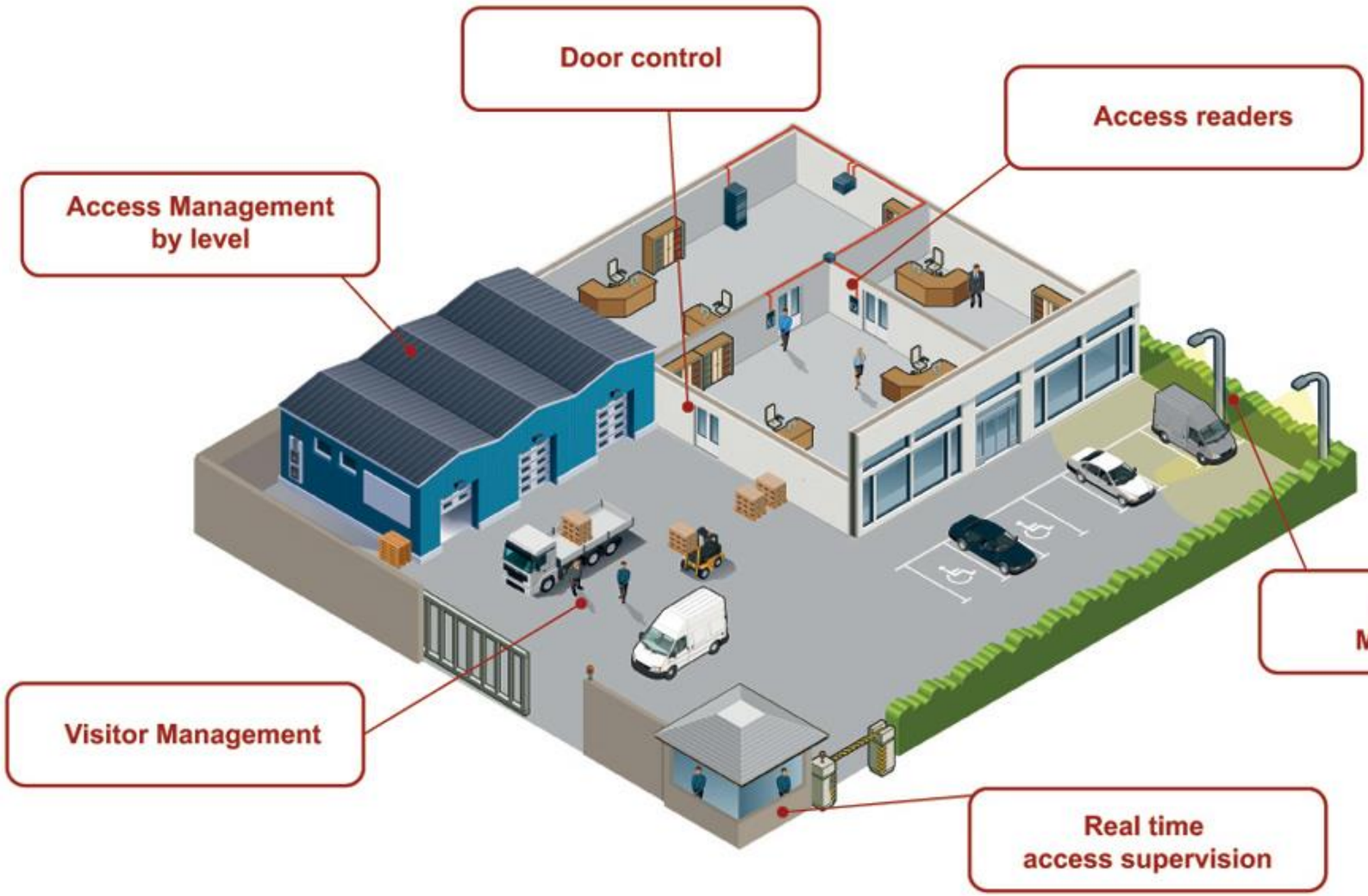
- Zunanji napadalci imajo veliko potencialnih tarč, preko katerih lahko tiho izvajajo akcije
- Zlonamerni notranji uporabniki lahko prevzamejo nadzor infrastrukture
- Težava z notranjimi vdori… le-ti niso videti kot vdori, saj delujejo kot redni zaposleni z odobrenimi privilegiji



Kdo ima ključe kraljestva?

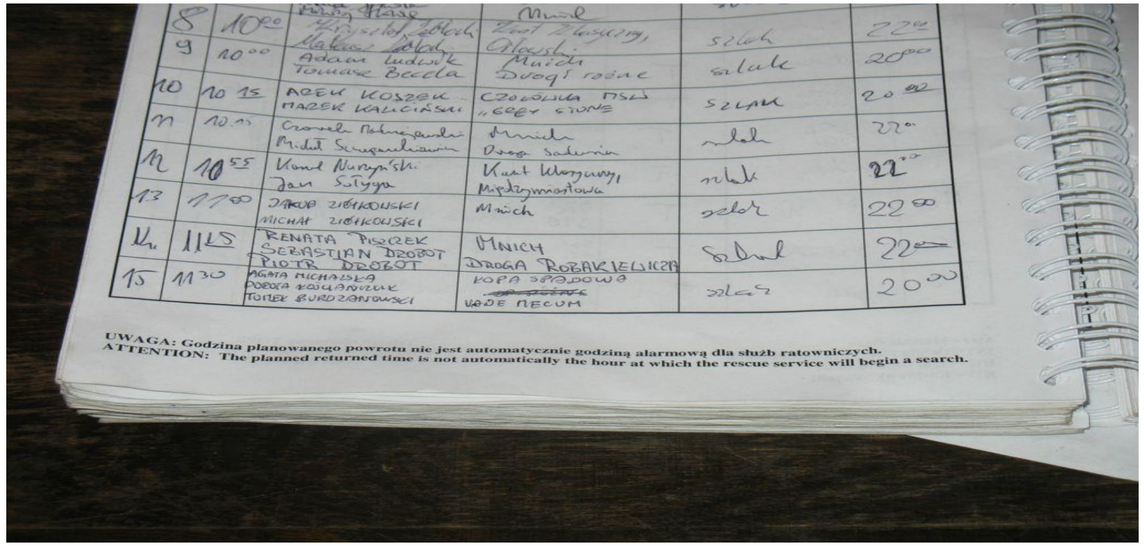
DOSTOP JE PRIVILEGIJ,
NE PRAVICA!

Fizična varnost



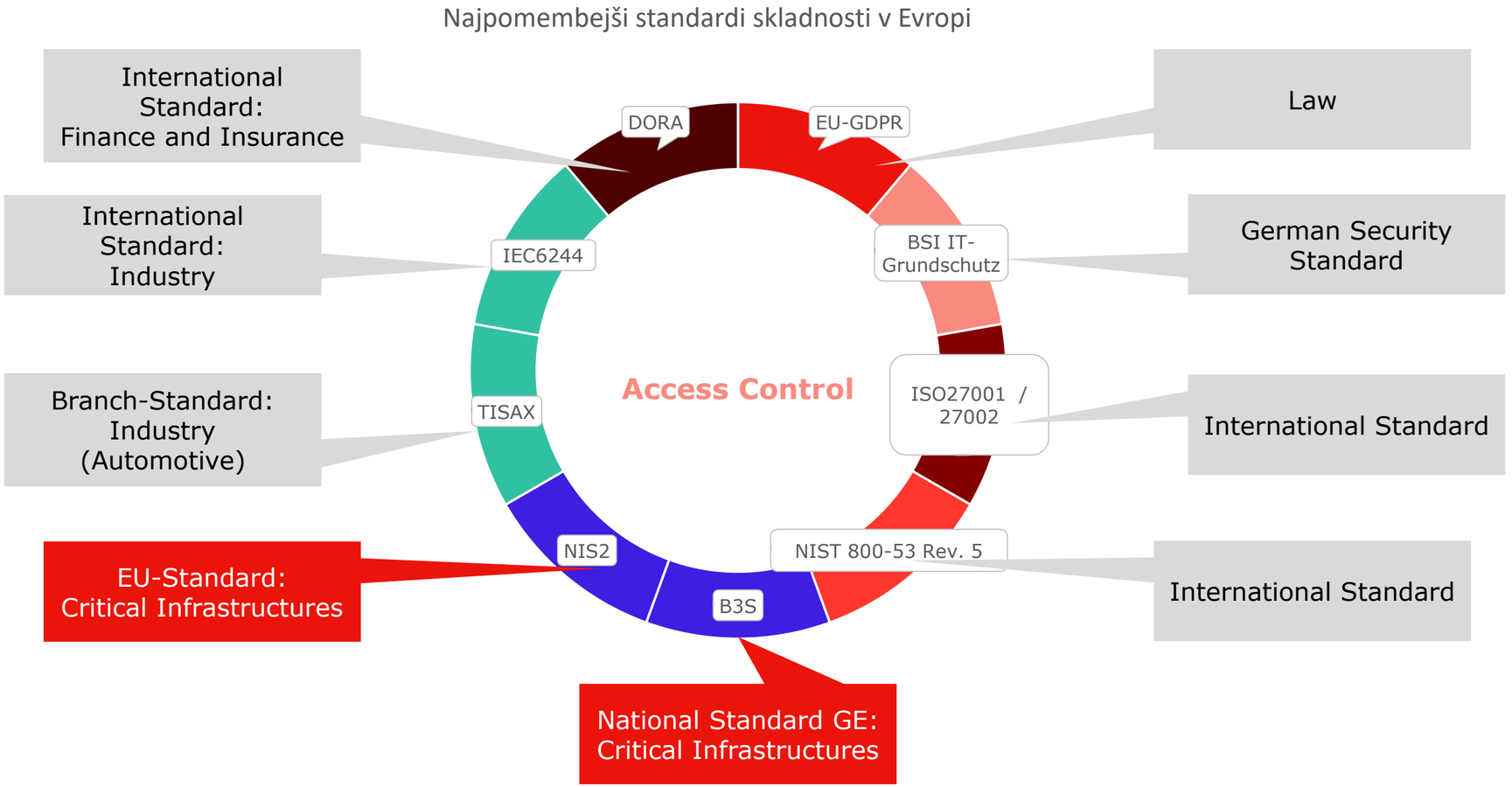
Kako z upravljanjem privilegiranih dostopov do večje kibernetske varnosti?

Fizična varnost



A1 ICT Distribucija

Skladnost in standardi



Kontrola pristopa ima ključno vlogo v vseh standardih, s čimer se zagotavlja integriteta podatkov in omejuje dostop do kritičnih podatkov in sistemov.

Skladnost in standardi

NIS2

- **(44)** | Skupine CSIRT bi morale imeti možnost, da na zahtevo bistvenega ali pomembnega subjekta spremljajo njegova sredstva, povezana z internetom, tako v njegovih prostorih kot drugje, da bi prepoznale, razumele in obvladale splošna organizacijska tveganja za subjekt, kar zadeva na novo odkrite grožnje v dobavni verigi ali kritične ranljivosti. Subjekt bi bilo treba spodbujati, naj skupini CSIRT sporoči, ali uporablja **privilegirani upravljalni vmesnik**, saj bi to lahko vplivalo na hitrost sprejemanja ublažitvenih ukrepov.

- **(49)** | Politike kibernetske higiene predstavljajo temelje za zaščito varnosti infrastruktur omrežnih in informacijskih sistemov, strojne opreme, programske opreme in spletnih aplikacij ter poslovnih podatkov ali podatkov končnih uporabnikov, ki jih subjekti uporabljajo. Politike kibernetske higiene zajemajo skupni izhodiščni nabor praks, vključno s posodobitvijo programske in strojne opreme, **menjavanjem gesel**, upravljanjem novih namestitev, **omejevanjem računov s skrbniško ravnjo dostopa** in varnostnim kopiranjem podatkov, omogočanjem proaktivnega okvira pripravljenosti ter splošno varnostjo in zaščito v primeru incidentov ali kibernetskih groženj. ENISA bi morala spremljati in analizirati politike kibernetske higiene držav članic.

Skladnost in standardi

NIS2

- **(89)** | Bistveni in pomembni subjekti bi morali sprejeti **širok nabor osnovnih praks računalniške higiene**, kot so načela popolnega nezaupanja, posodobitve programske opreme, konfiguracija naprav, segmentacija omrežja, **upravljanje identitete in dostopa** ter ozaveščenost uporabnikov, organizirati usposabljanje in ozaveščanje svojega osebja v zvezi s kibernetskimi grožnjami podjetjem, lažnim predstavljanjem in tehnikami socialnega inženiringa. Ti subjekti bi morali tudi oceniti lastne zmogljivosti glede kibernetske varnosti in si po potrebi prizadevati za vključevanje tehnologij za povečanje kibernetske varnosti, kot so umetna inteligenca ali sistemi strojnega učenja, da okrepijo svoje zmogljivosti in varnost omrežnih in informacijskih sistemov.

Privileged Access Management (PAM)

A1 ICT Distribucija

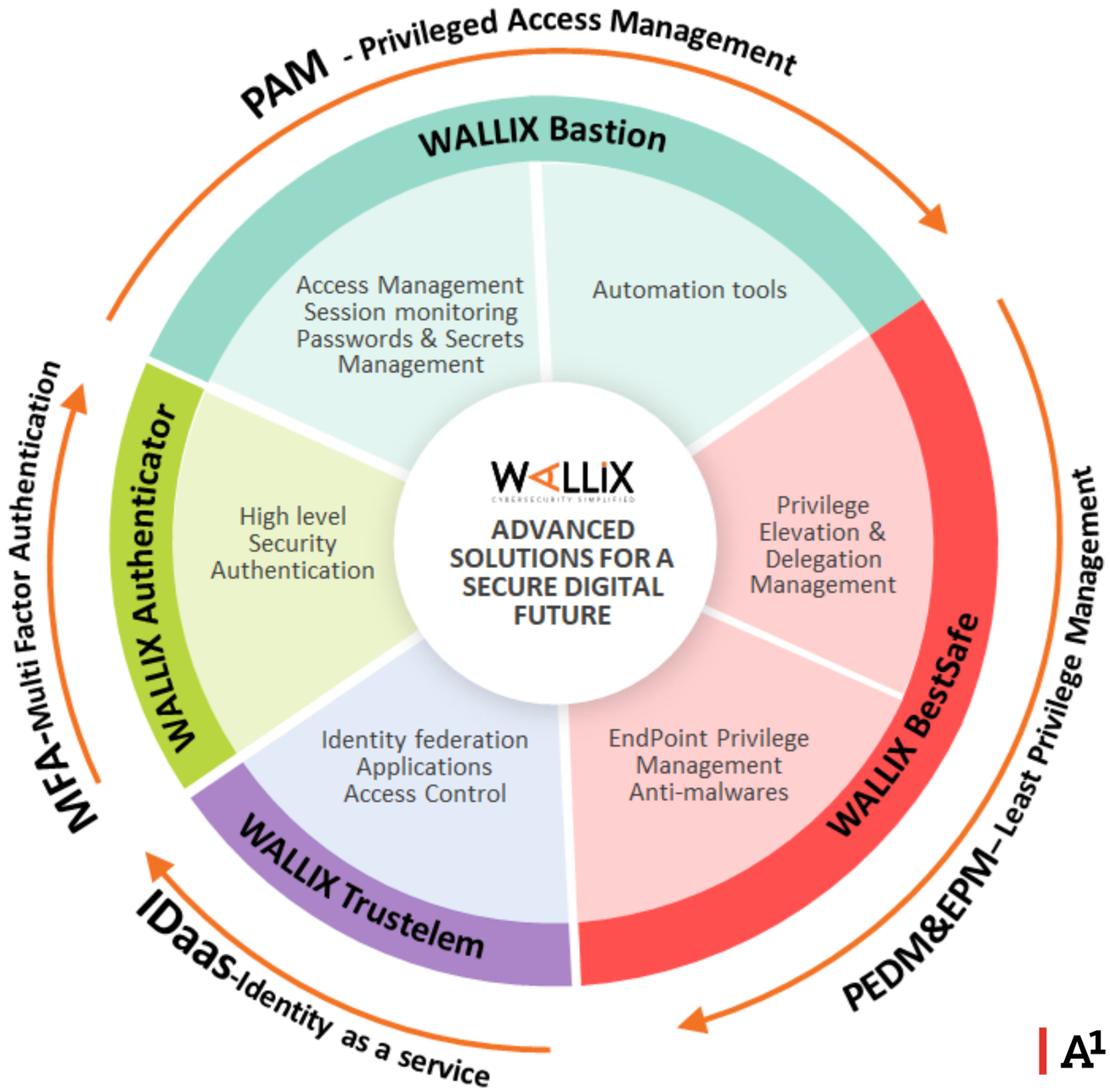
Kako z upravljanjem privilegiranih dostopov do večje kibernetske varnosti?

Kibernetska varnost se začne z upravljanjem identitet in upravljanjem digitalnih dostopov

A1 ICT Distribucija

Kako z upravljanjem privilegiranih dostopov do večje kibernetske varnosti?

WALLIX



WALLIX Bastion

Enostavna rešitev za zaščito privilegiranih dostopov do kritičnih naprav, s čimer se zmanjša varnostno tveganje in uredi skladnost z zahtevanimi regulativami

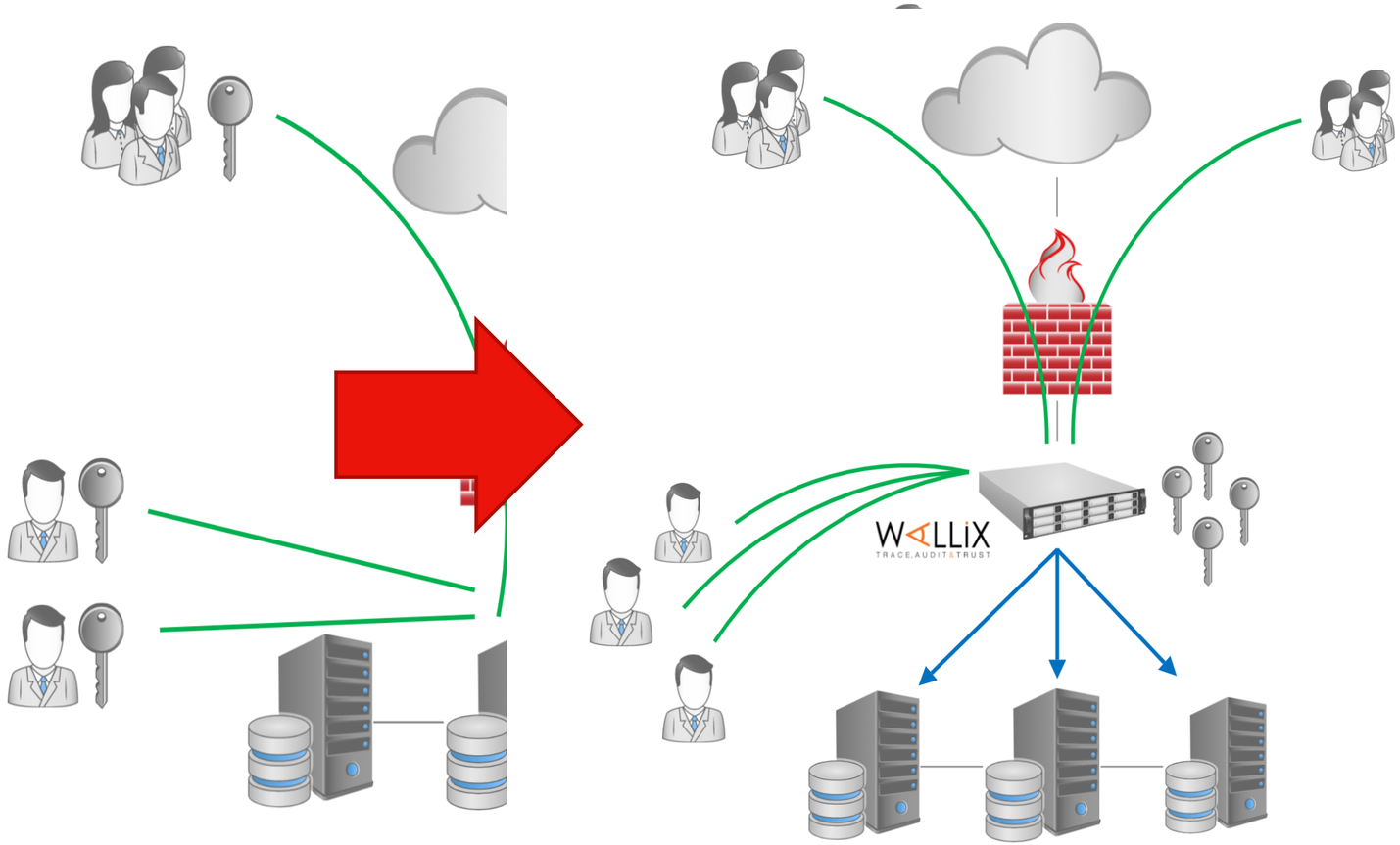
Zaščita oddaljenih dostopov

Zaščita pred notranjimi grožnjami

Zaščita za DevOps

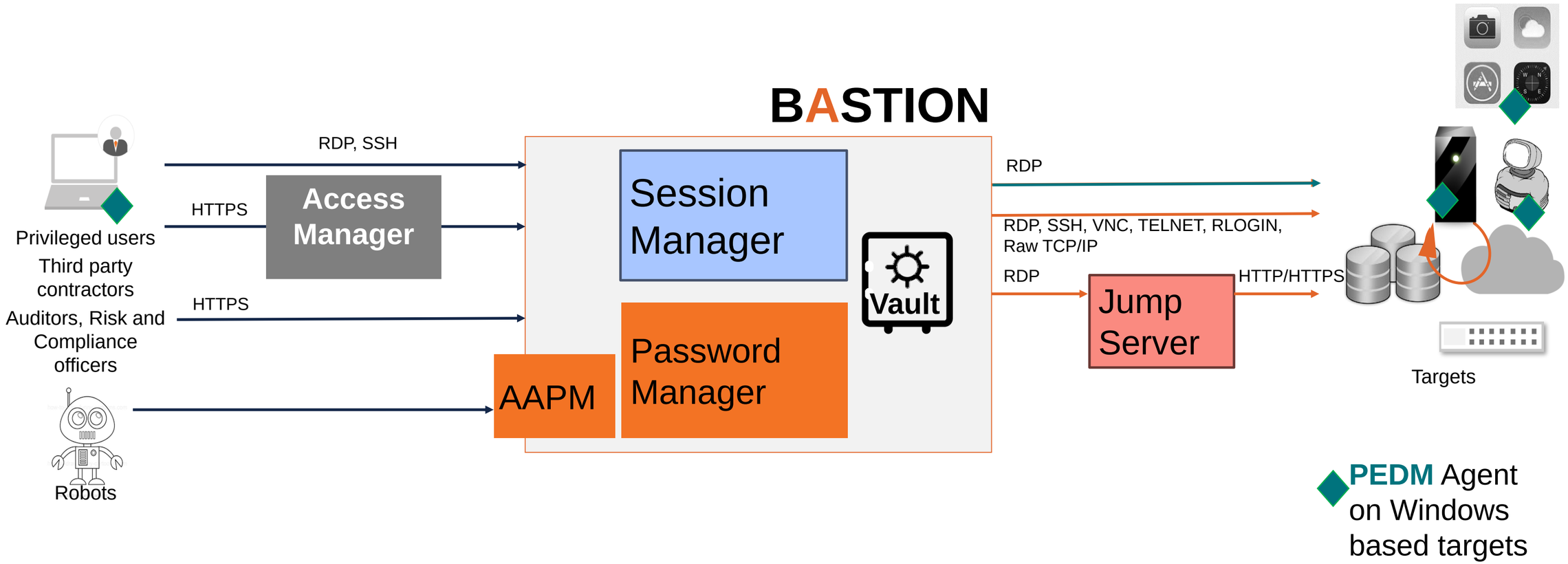
Varnost v OT okolju

Privileged Access Management



Trenutno stanje

Stanje po vpeljavi PAM


BASTION
RDP, SSH
HTTPS
Access Manager
Privileged users
Third party contractors
HTTPS
Auditors, Risk and Compliance officers
Robots
Session Manager
Password Manager
AAPM
Vault
RDP
RDP, SSH, VNC, TELNET, RLOGIN, Raw TCP/IP
RDP
Jump Server
HTTP/HTTPS
Targets
PEDM Agent on Windows based targets

Wallix v Sloveniji

- Stranke v različnih področjih
  - Energetika
  - Finance
  - Zdravstvo
  - …
- Izkušeni, strokovni in certificirani partnerji v Sloveniji
  - Prve postavitve v 2016
- A1 Slovenija distributer leta za regijo CEE 2022 in 2023

Wallix v praksi

A1 ICT Distribucija