



#TARABICA

IT CONFERENCE

Belgrade May 12th, 2018

#tarabica¹⁸



**KEEP
CALM
AND
SECURE WINDOWS SERVER**

Who am I


- Vladimir Stefanović
- System Engineer @Superadmins
- Technical Trainer @ATC
- MCSA, MCSE, MCT, IAMCT Regional Lead, Speaker
- stefanovic.vladimir@hotmail.com
- www.tech-trainer.info
- <https://github.com/Wladinho/Presentations>



Agenda

- Security stats and approach
- Can we harden Windows and how
- Other techniques and solutions
- Q & A

(Un)fortunately, session based
on true story



Kaže da su hakovani.

Šta kaže,
šta kaže?

Eeeee, pa tu onda ni
mi ne možemo da im
pomognemo . . .

Security stats and approach

Traditional vs. Modern defense approach

Traditional

- *I'm not a target*
- *Attack can come only from outside*

Modern

- *Protect*
- *Detect*
- *Respond*

Attack Vectors

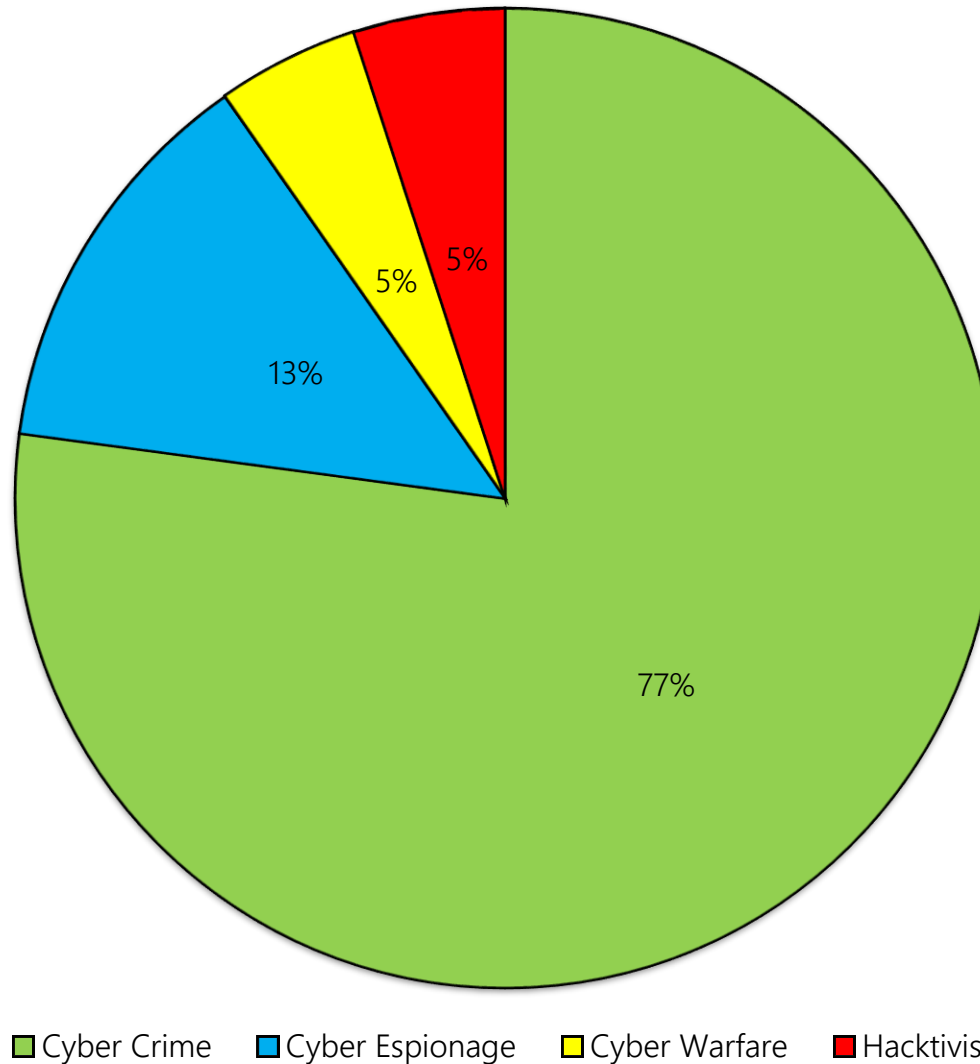
Threats

- *Compromise privileged accounts*
- *Exploit unpatched vulnerabilities*
- *Phishing attacks*
- *Malware infections
(ransomware, trojans, logic bombs...)*

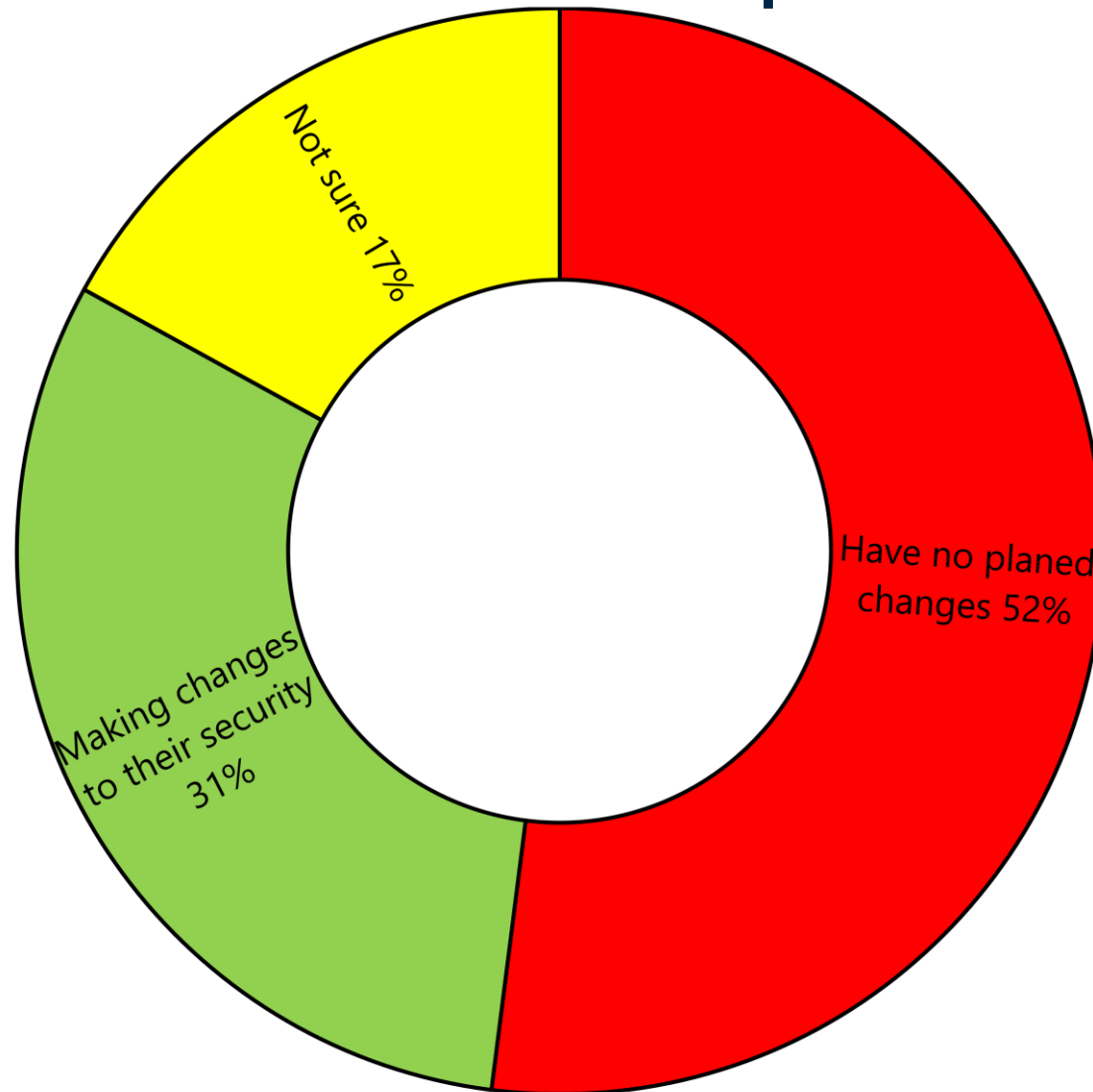
Motives for attack

- *Profit*
 - *By selling data*
 - *By ransoming data*
- *Destroying infrastructure*

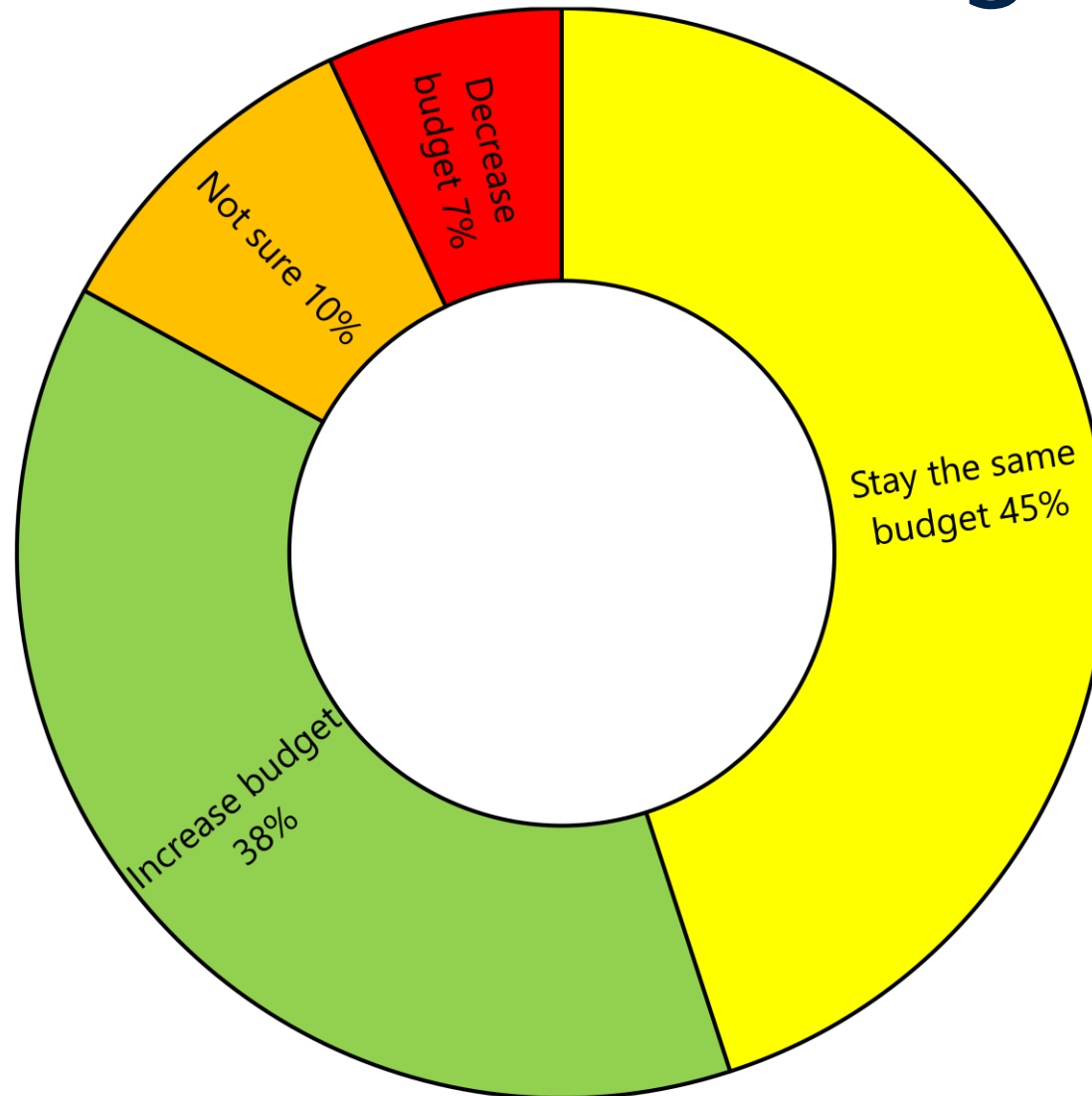
Statistics 2017 - Attack motives



Statistics 2017 - After attack plans



Statistics 2017 - After attack budget



Can we harden Windows infrastructure, and how?

LAPS - Overview

- Local administrator passwords are unique on each computer
- LAPS randomizes and changes local administrator passwords
- LAPS stores local administrator passwords and secrets securely inside active directory
- Access to passwords is configurable

LAPS - Requirements

- Any domain member computer (*server or client*)
- Domain Functional level 2003 or higher
- AD Schema must be extended to use LAPS
- LAPS client on managed computers
- .NET Framework 4.0
- Windows PowerShell 2.0 or later

LAPS - Configuring and managing

- Install LAPS on management server
- Extend schema by PowerShell command
 - *msMcsAdmPwd* and *msMcsAdmPwdExpirationTime*
- Configure permissions for LAPS client computers
- Install LAPS client on desired computers (*manually or GPO*)
- Configure LAPS with GPO
 - *Enabling LAPS*
 - *Password complexity, length, expiration*

LAPS – Demo

tweet [#tarabica18](#)

[#tarabica](#)¹⁸

JEA - Just Enough Administration

- JEA provides RBAC on Windows PowerShell remoting
- The endpoint limits the user to use predefined PowerShell cmdlets, parameters, and parameter values
- Actions are performed by using a special machine local virtual account
- Native support in Windows Server 2016 and Windows 10
- Supported on other operating systems with installed WMF 5.0

JEA - Disadvantages

- Not suitable for troubleshooting tasks
- Setup requires understanding precisely which cmdlets, parameters, aliases, and values are needed to perform specific tasks
- JEA works only with Windows PowerShell sessions
- User must be familiar with PowerShell

JEA - Configuring

- Create role-capability file(s)
 - *Configure visible cmdlets*
 - *Configure visible functions*
 - *Configure visible external commands*
- Create session-configuration file(s)
 - *Configure role definitions*
- Creating JEA endpoint / Register session-configuration file(s)
- Connect to JEA endpoint
 - *Enter-PSSession -ComputerName \$ -ConfigurationName \$*

JEA - Demo

tweet #tarabica18

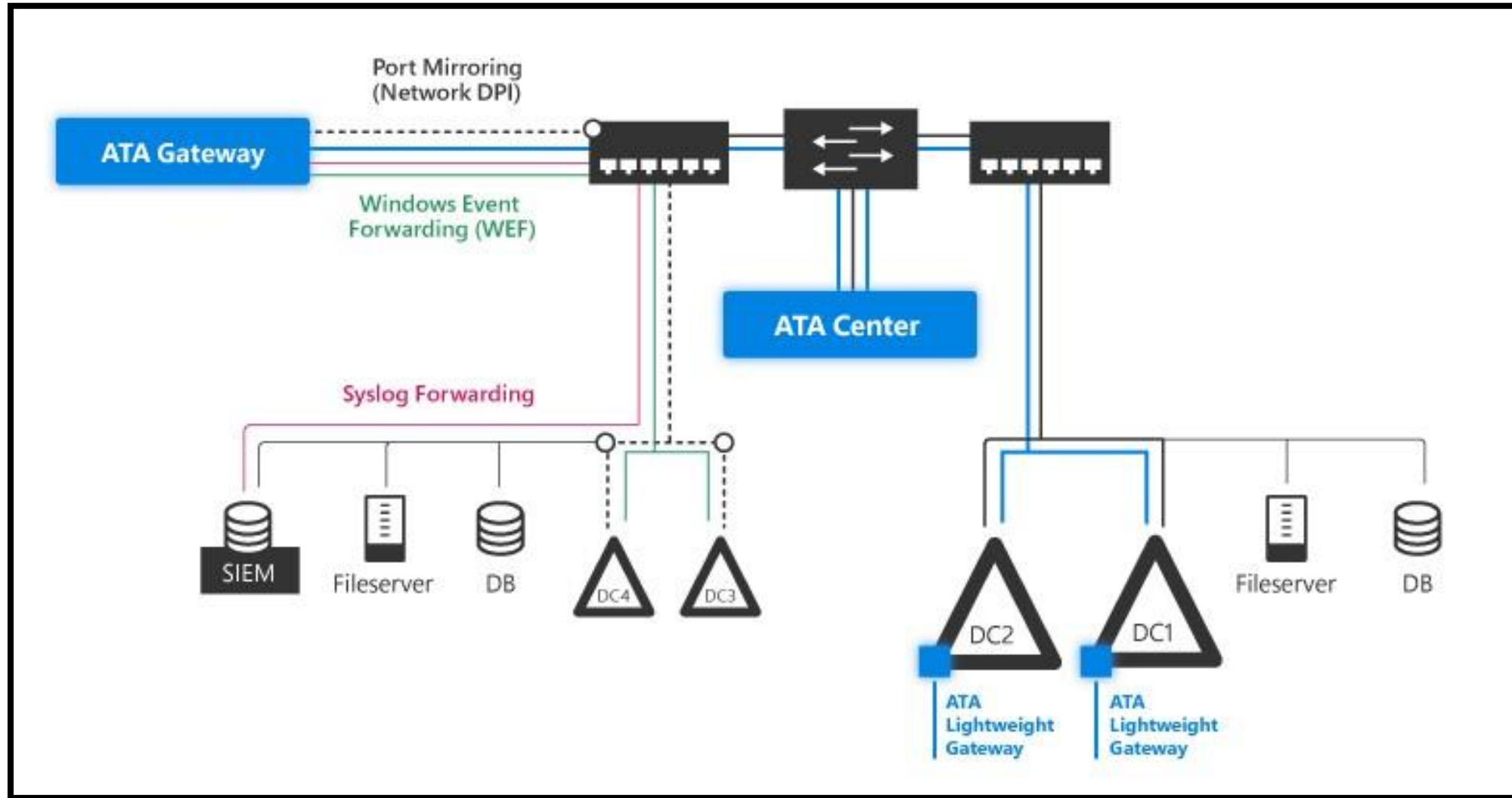
#tarabica¹⁸

Other techniques and solutions

ATA - Advanced Threat Analytics

- Analyze → Learns → Detect → Alert
- ATA is an **N**etwork **I**ntrusion **D**etection **S**ystem
- Prevents all known signature-based attacks
- Perform behavior-based detection and learn user behavior
- Provides recommendations for investigation for each identified suspicious activity or known attack

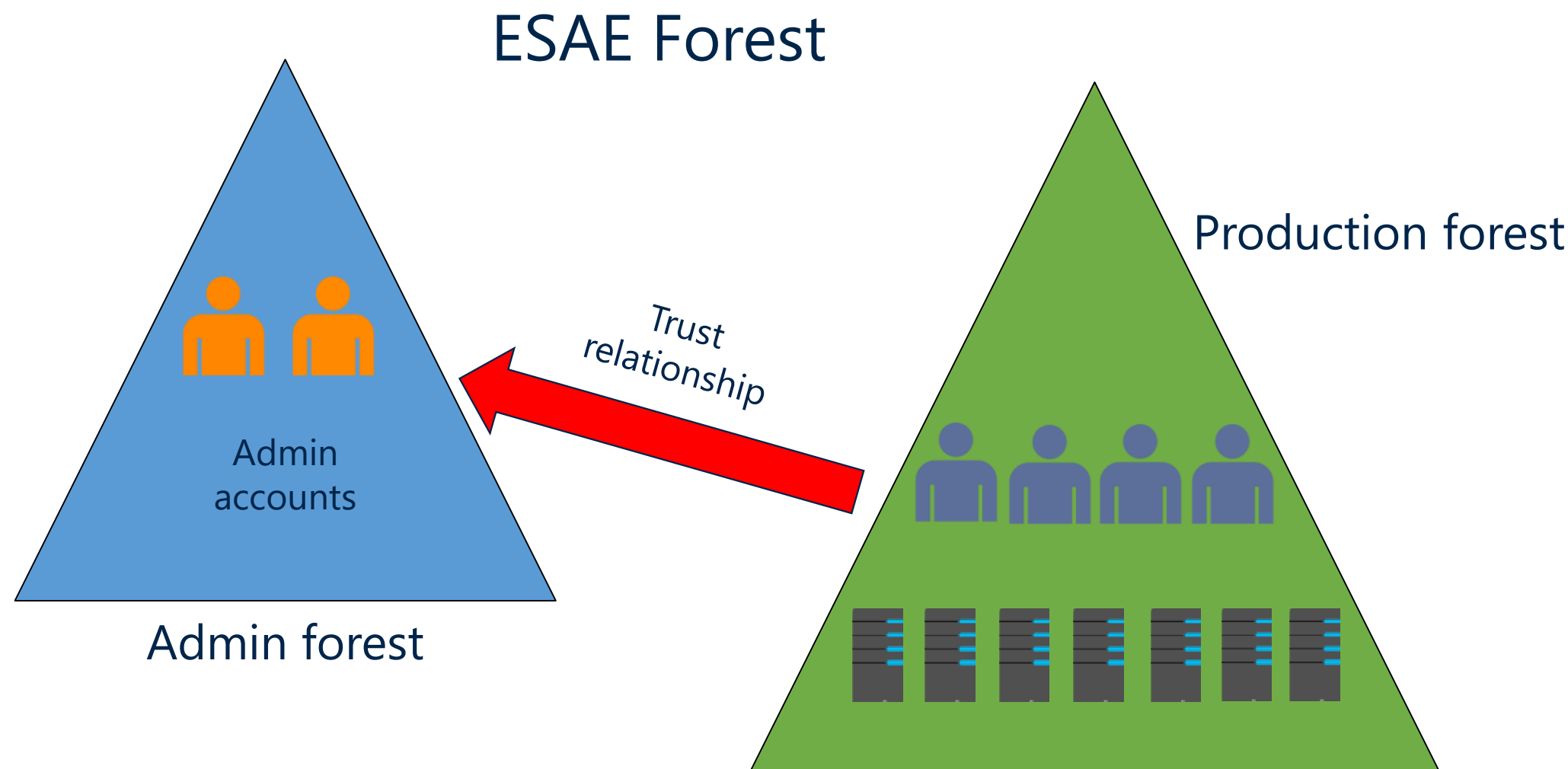
ATA - Advanced Threat Analytics



Enhanced Security Admin Environment

- The ESAE forest should be a single-domain AD forest
- ESAE forest **should** contain only admin accounts for the production forest
- Applications or additional resources **shouldn't** be deployed in the ESAE forest
- One way forest trust **must** exist - Production forest trusts the ESAE forest

Enhanced Security Admin Environment



Other techniques and solutions

- EMET
- App Locker
- Software Restriction Policies
- FSRM
- Dynamic Access Control
- MIM / PAW / JIT
- . . .

We must not forget
a.k.a. Oldie Goldie principles

Oldie goldie

- System patching (manually, WSUS, SCCM)
- Backup (online, onsite, offline)
- Backup testing
- Least privilege
- Separated administrator account
- Password & Kerberos policy
- Disable SMBv1 (*be careful, sensitive task*)
- Disable NTLM (*be careful*)

Sponzori

Partneri konferencije



Zlatni sponzori



Srebrni sponzori



Tehnički sponzor



Q & A

tweet #tarabica18

#tarabica¹⁸

Thank you for your attention