



Sinergija18
Digital breakthrough

Powered by
Microsoft

A (bad) day in SysAdmin life

Vladimir Stefanović
SuperAdmins

Sinergija18, Beograd 25.10.2018

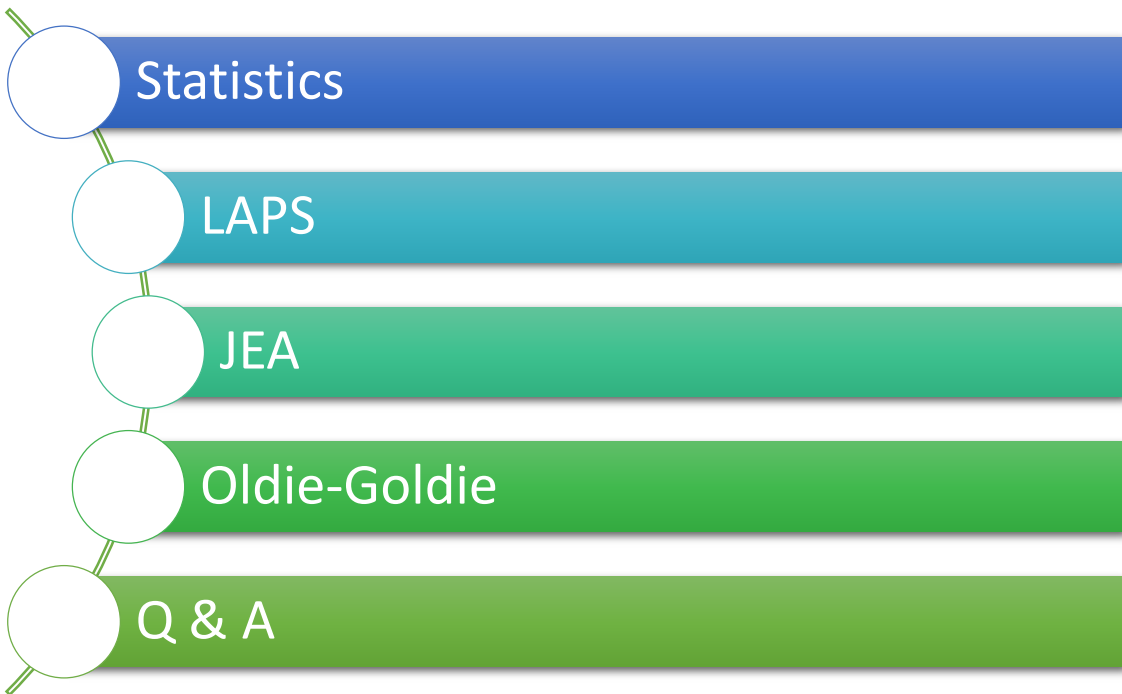



Who am I

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



Agenda





**(Un)fortunately, this session is
based on true story ...**

Approach and attack vector

- Traditional

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

- Modern

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

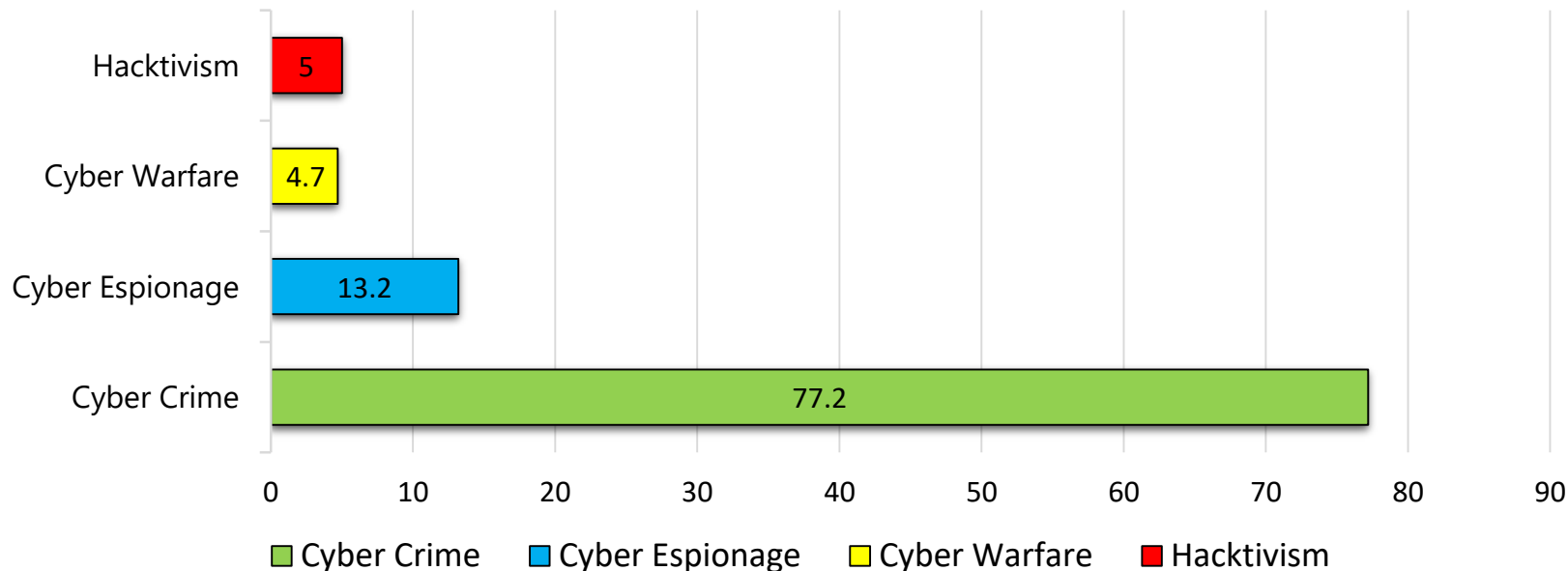
- Threats

- *Compromise accounts*
- *Exploit vulnerabilities*
- *Phishing attacks*
- *Malware*

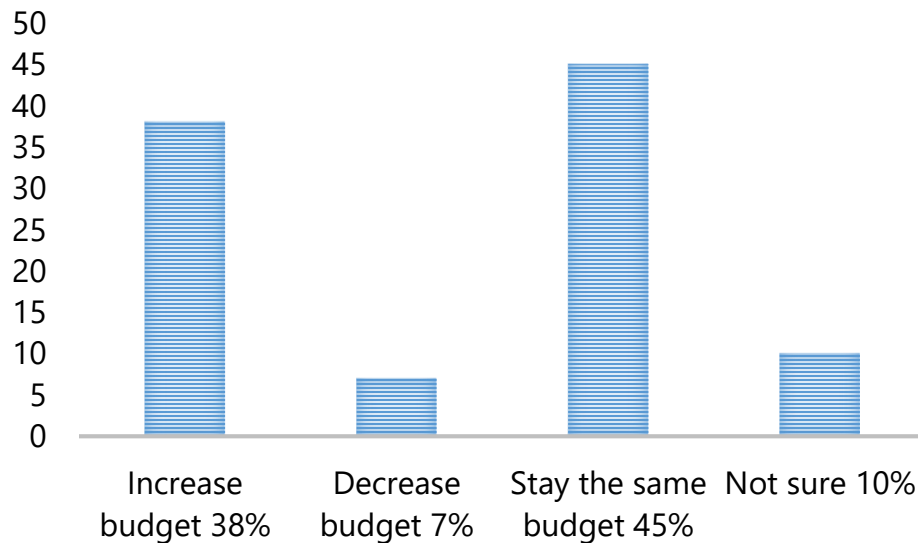
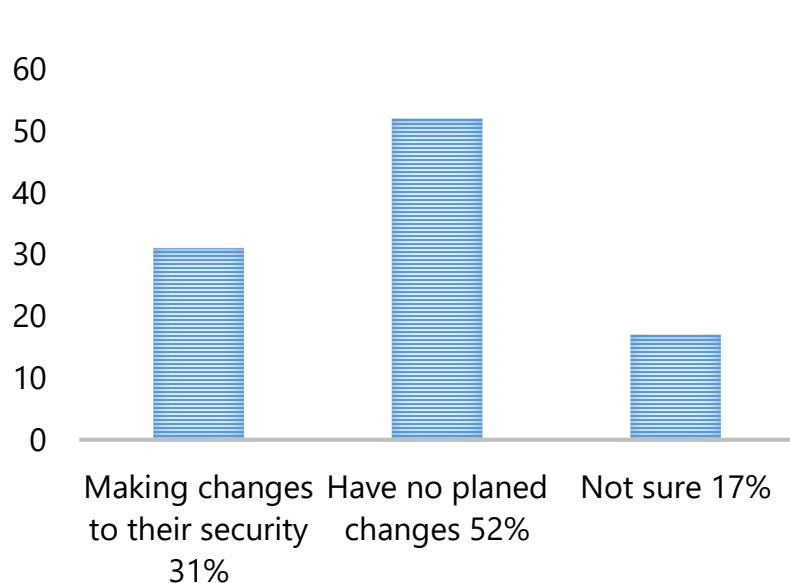
- Motives for attack

- *Profit - Ransoming data*
- *Destroying infrastructure*

Statistics 2018 - Attack motives



Statistics 2018 - After attack plans & budget





Can we harden Windows
infrastructure, and how?

How we can do that?

Configuring user rights

Configuring access

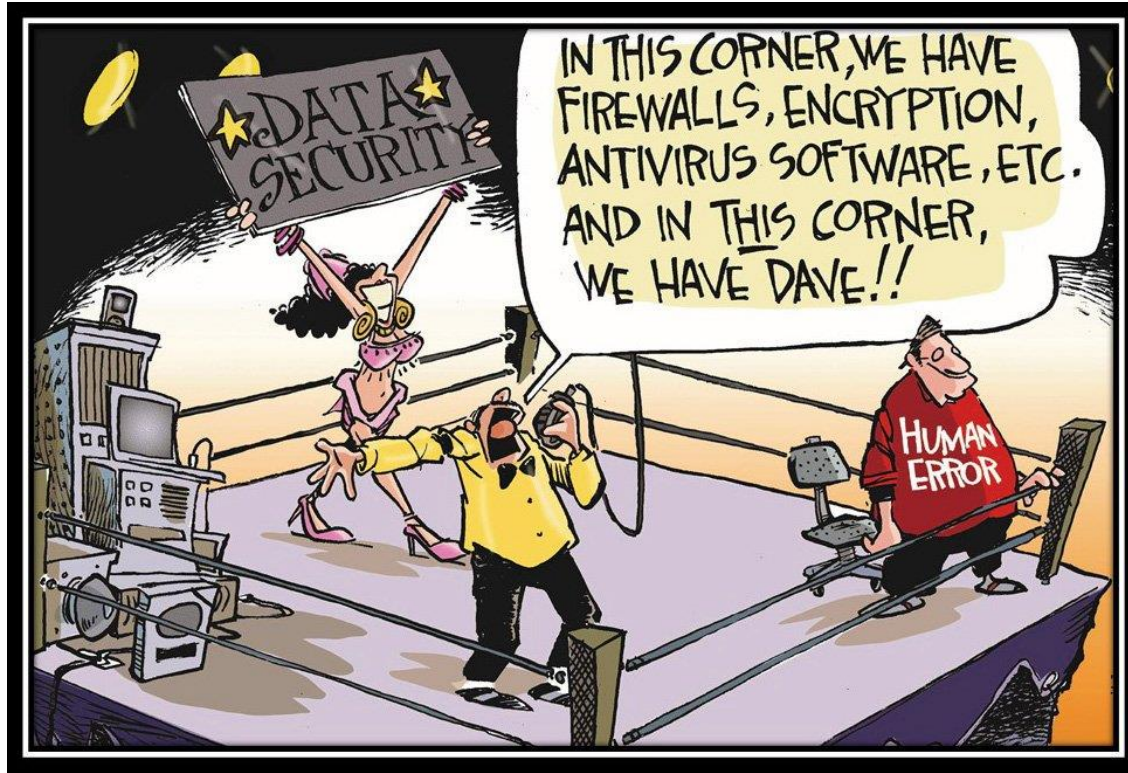
Policy implementation

Logs collecting and analysis

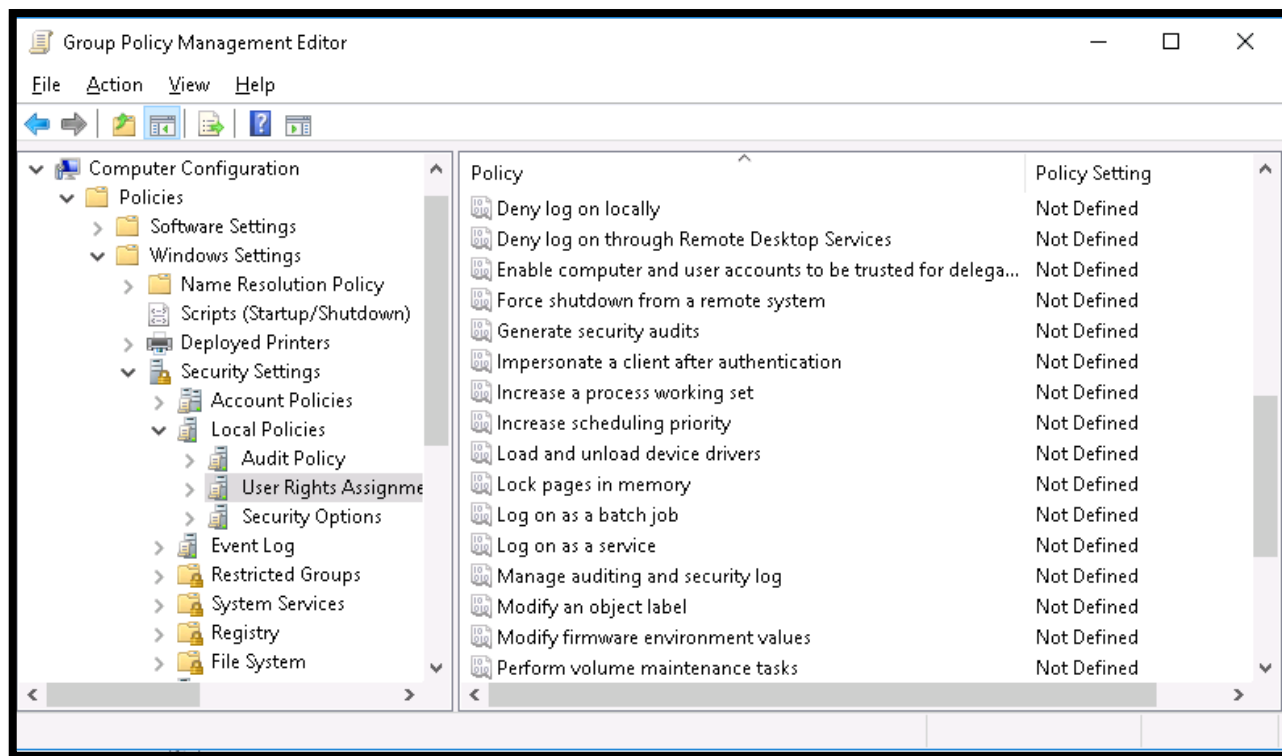
NIDS / NIPS

Oldie-Goldie

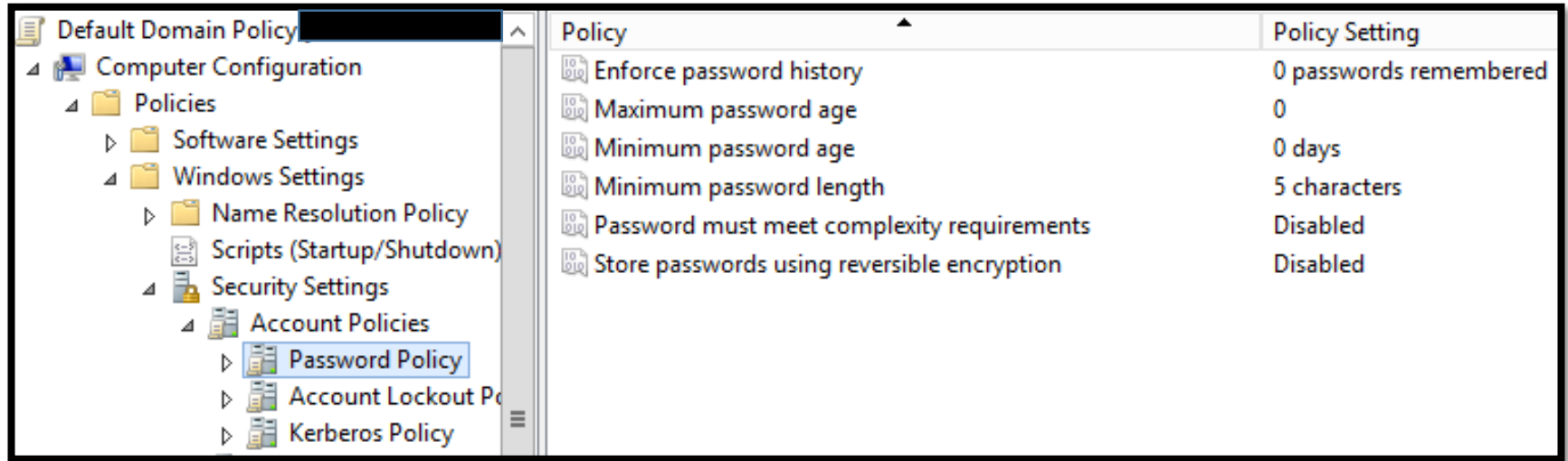
The biggest enemy of IT Security



User rights configuring



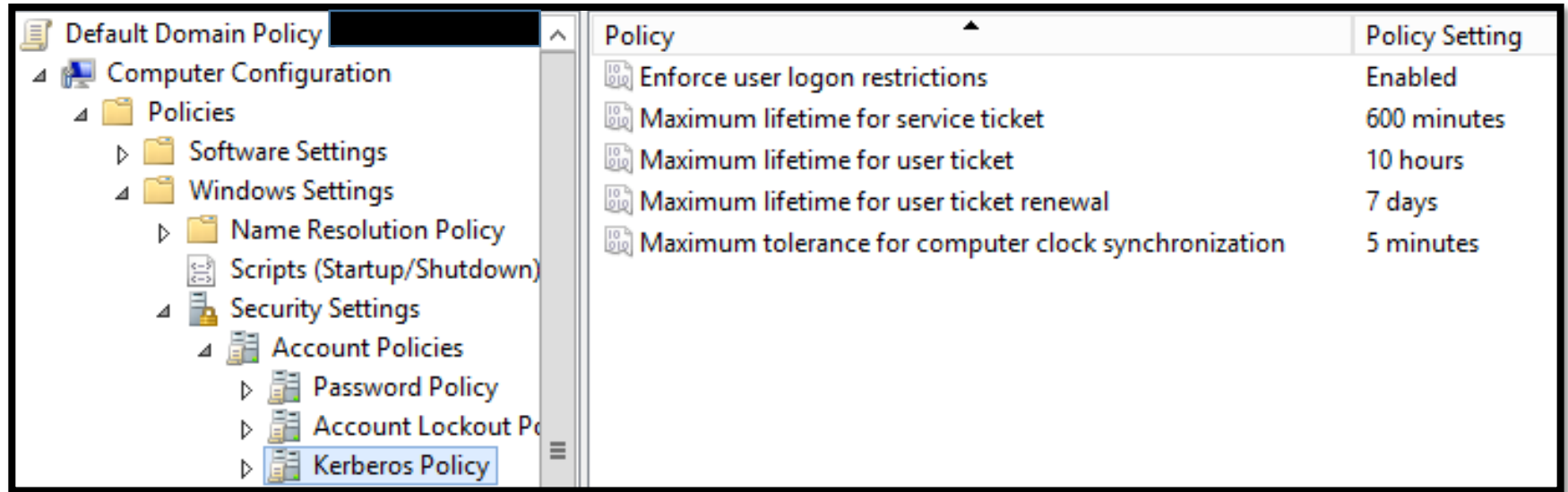
Password policy



The screenshot shows the Windows Group Policy Editor interface. On the left, the 'Default Domain Policy' is selected, and the tree view is expanded to 'Computer Configuration' > 'Policies' > 'Windows Settings' > 'Security Settings' > 'Account Policies' > 'Password Policy'. The 'Password Policy' is highlighted. On the right, a table lists the policy settings.

| Policy | Policy Setting |
|---|------------------------|
| Enforce password history | 0 passwords remembered |
| Maximum password age | 0 |
| Minimum password age | 0 days |
| Minimum password length | 5 characters |
| Password must meet complexity requirements | Disabled |
| Store passwords using reversible encryption | Disabled |

Kerberos policy



The screenshot shows the Windows Group Policy Editor interface. On the left, the 'Default Domain Policy' is selected, and the tree view is expanded to 'Computer Configuration' > 'Policies' > 'Windows Settings' > 'Security Settings' > 'Account Policies' > 'Kerberos Policy'. The 'Kerberos Policy' is highlighted. On the right, a table lists the specific policy settings and their current values.

| Policy | Policy Setting |
|--|----------------|
| Enforce user logon restrictions | Enabled |
| Maximum lifetime for service ticket | 600 minutes |
| Maximum lifetime for user ticket | 10 hours |
| Maximum lifetime for user ticket renewal | 7 days |
| Maximum tolerance for computer clock synchronization | 5 minutes |

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

- Install LAPS on management server
- Extend schema by PowerShell command
- Configure permissions for LAPS client computers
- Install LAPS client on desired computers (*manually or GPO*)
- Configure LAPS with GPO



LAPS DEMO

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 OS with installed WMF 5+

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, functions or external commands*
- Create session-configuration file(s)
 - *Configure role definitions*
- Creating JEA endpoint / Register session-configuration file(s)
- Connect to JEA endpoint with ComputerName and Configuration name parameters

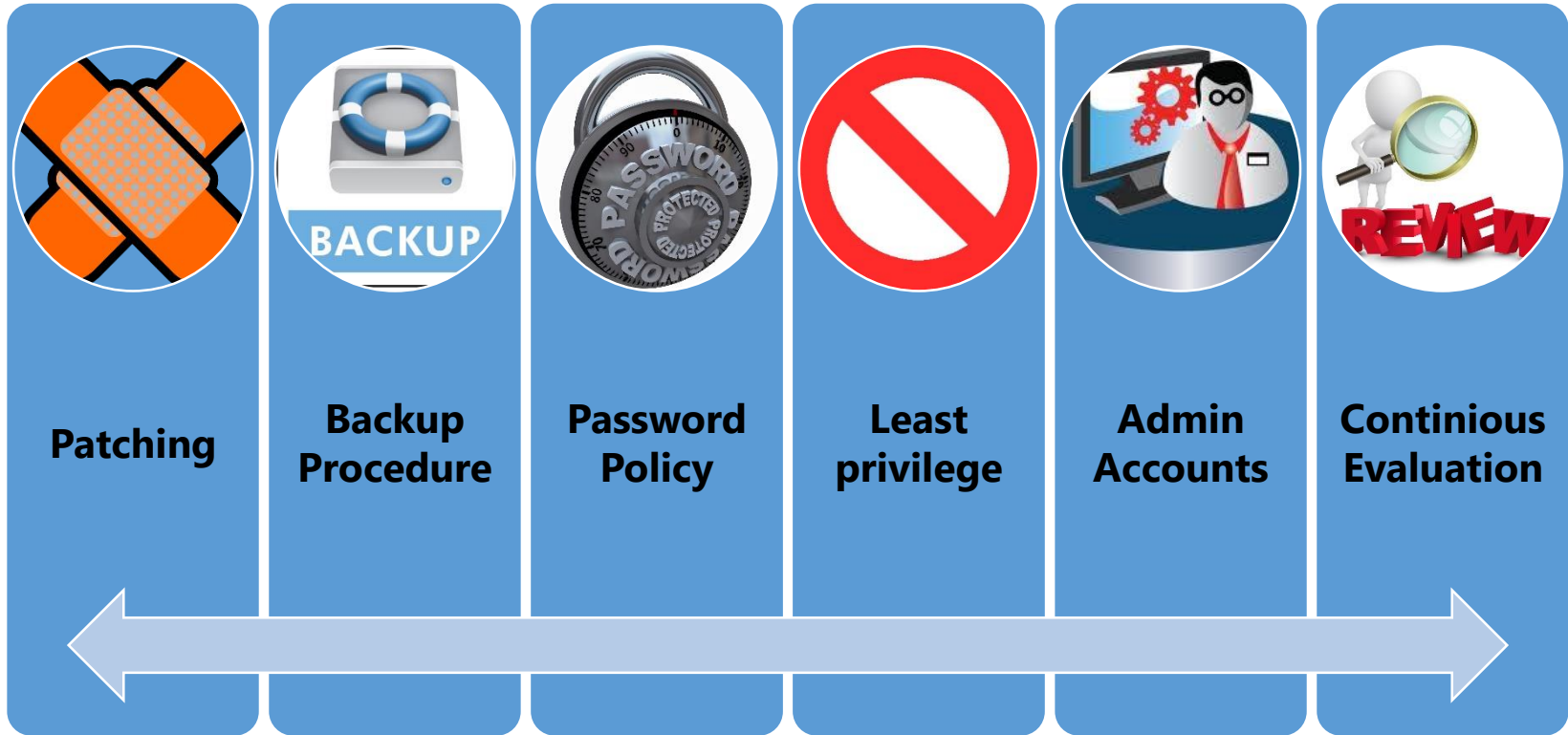


JEA DEMO



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

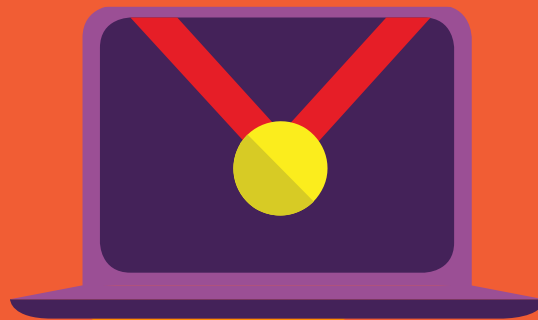
Oldie goldie principles





Ocenite predavanje kako bismo
izabrali najboljeg predavača na
Sinergiji 18!

Popunite konferencijsku anketu i
učestvujte u velikoj nagradnoj igri!





Thank you

Powered by
Microsoft