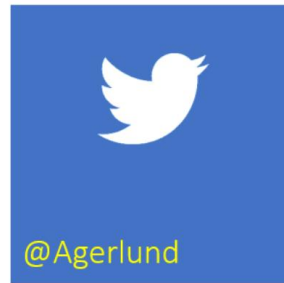




What can possibly go wrong in an Enterprise Client Environment, and how you mitigate that

KENT AGERLUND



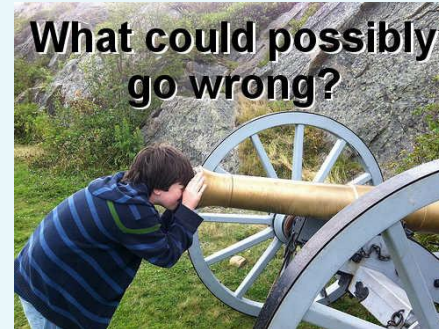
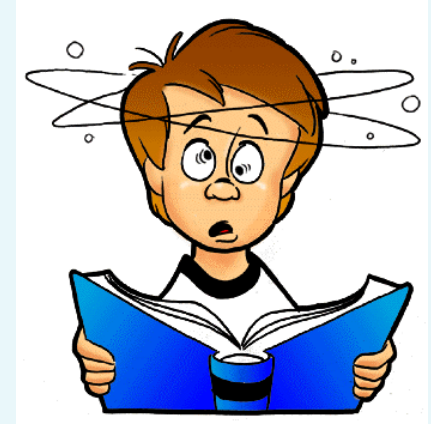
NIC

AGENDA

What can possible go wrong

Why is it so difficult

How can Configuration Manager be used to mitigate the risk



NIC



THE STORM IS NOW

WannaCry, Adylkuzz and Petya are a great examples how neglecting security patches can have a catastrophic impact on businesses.



It took 7 minutes from first incident until all devices were down

Our estimated loss is \$278 million

We thought it was just another evening with no e-mail

We realized no one owned the incident. We have plans for earthquakes, terror attacks, flooding – but not cyberattacks

Software Vulnerabilities and Patching

At the center of security incidents

Top External Intrusion
Method:

Software
Vulnerabilities

42%

- *Forrester*

Clients report:
“Remediation is a
perennial point of
failure in vulnerability
management
programs.”

- *Gartner*

NIC

It takes organizations much longer to
apply security patches than it takes
hackers to ramp up the exploitation of
unpatched vulnerabilities...

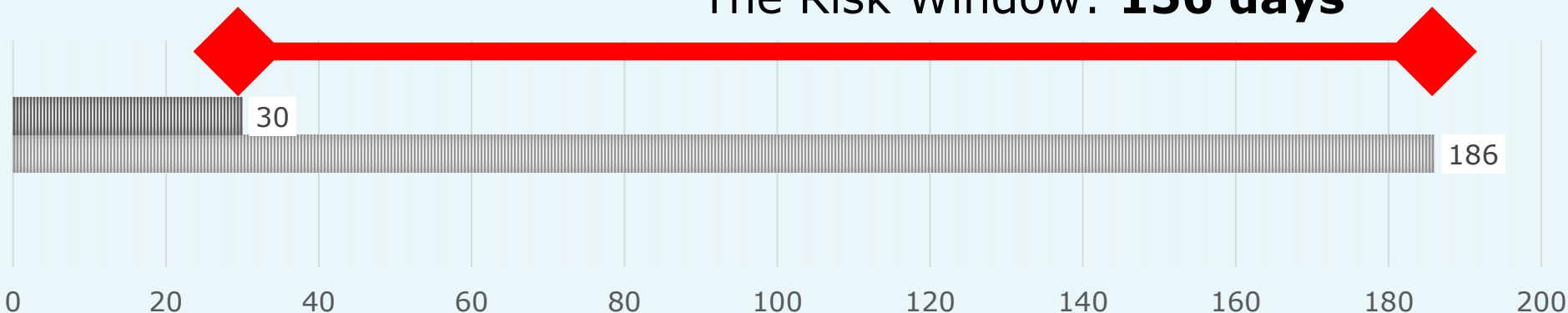


RISK WINDOW: FROM AWARENESS TO MITIGATION

Average time from Disclosure to first Exploitation: 30 days¹

Average time from Identification to Remediation: 186 days²

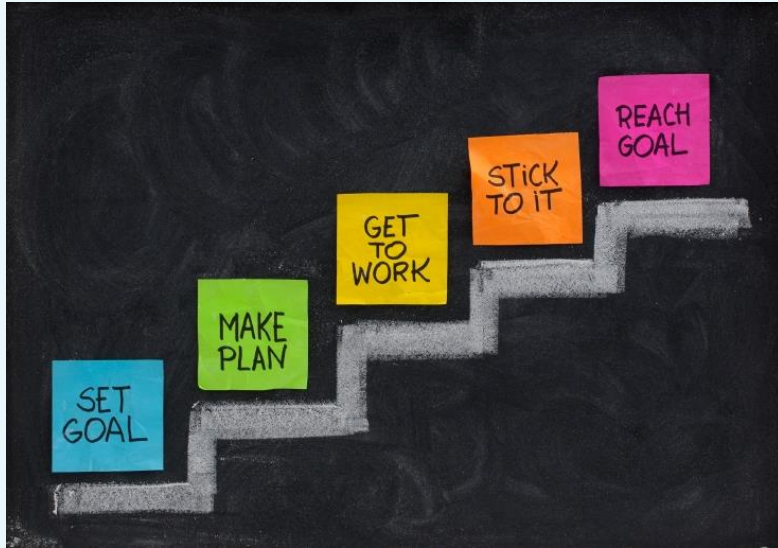
The Risk Window: **156 days**



1 – Source: "2016 Data Breach Investigation Report" Verizon <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/>

2 – Source: "2016 State of Vulnerability Risk Management" NopSec <http://info.nopsec.com/sov>

SOFTWARE UPDATES MAIN BUSINESS CHALLENGES



Infrastructure components

Visual Insight to the entire process

No teamwork

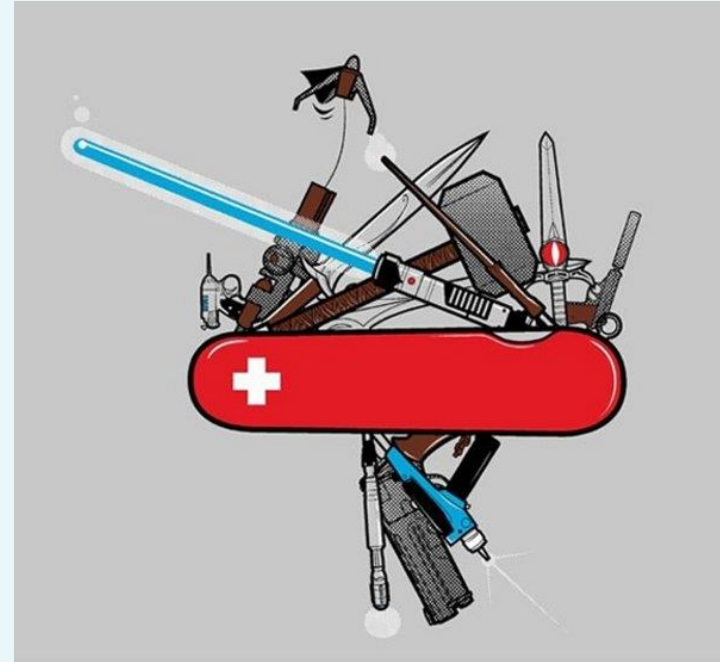
No sponsor

Tools before process

Process before goal

The Toolbelt

- The right tool for the right job
 - 3rd party integration
 - Software update
 - Configuration Items
 - Scripts
- Vulnerabilities
 - Operating System
 - Application
 - Drivers
 - BIOS
 - Network





NIC

Operating System Security Main Challenges

Local administrator

Group Policies Insight

Insecure Protocols and Windows 10 misconceptions

Windows As A Service

Windows 10 Security Model

Keeping Users happy – BSOD = Not so happy



The right tool for the right job

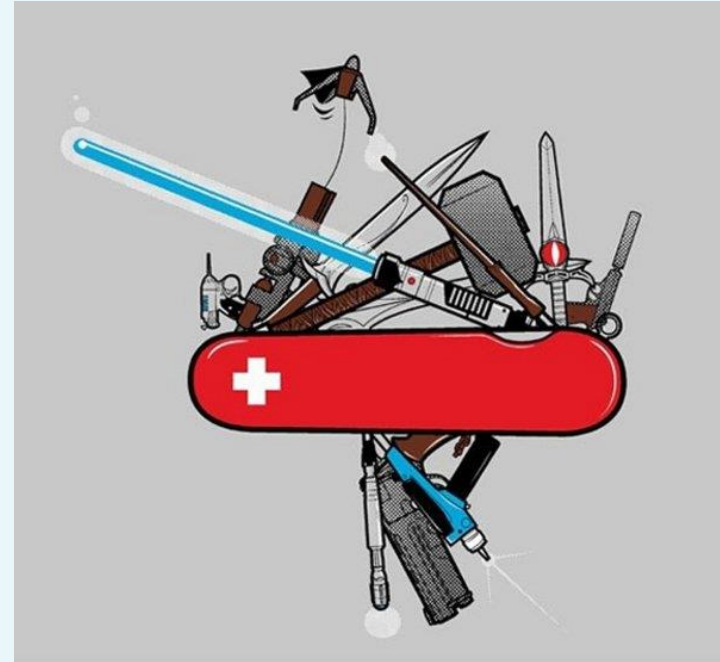
Configuration Items

Scripts

Insights

WAAS Playbook

MDT and Time



NIE



NIC

Trusting The Source Main Challenges

Configuration Manager Client Health

Configuration Manager Client Activity

Understanding the internal process



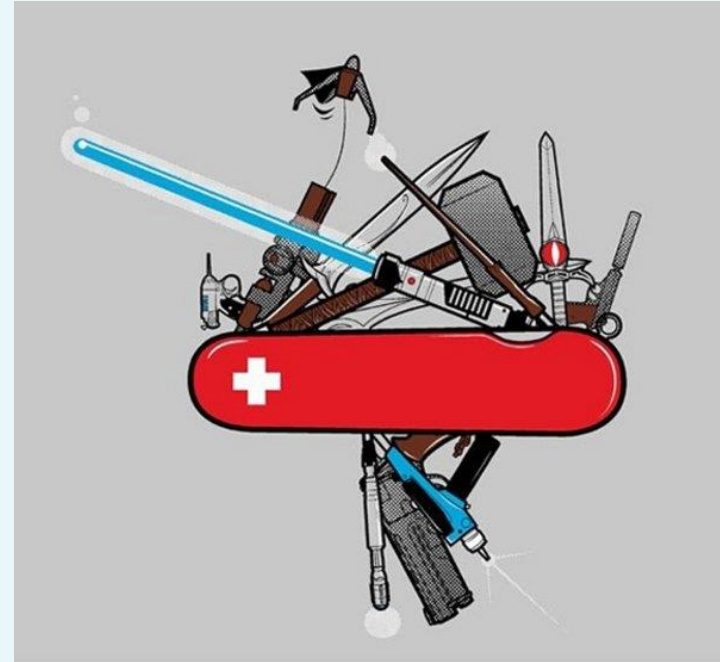
The Toolbelt

The right tool for the right job

Build-In Client Health

Extending Client Health

Extending the Infrastructure



NIC



NIC

WRAP-UP

It's your choice, the Hurricane or the mild storm
Configuration Manager & EM+S are important tools in the belt
If you wait, tomorrow might very well be too late



Resources

Slides and demos from the conference will be available at
github.com/nordicinfrastructureconference/2018 (bit.ly/2y7JhA3)

