storebrand

# Vulnerability Management

# Main Misunderstandings

Oleksandr Kazymyrov
15.06.22

# Agenda

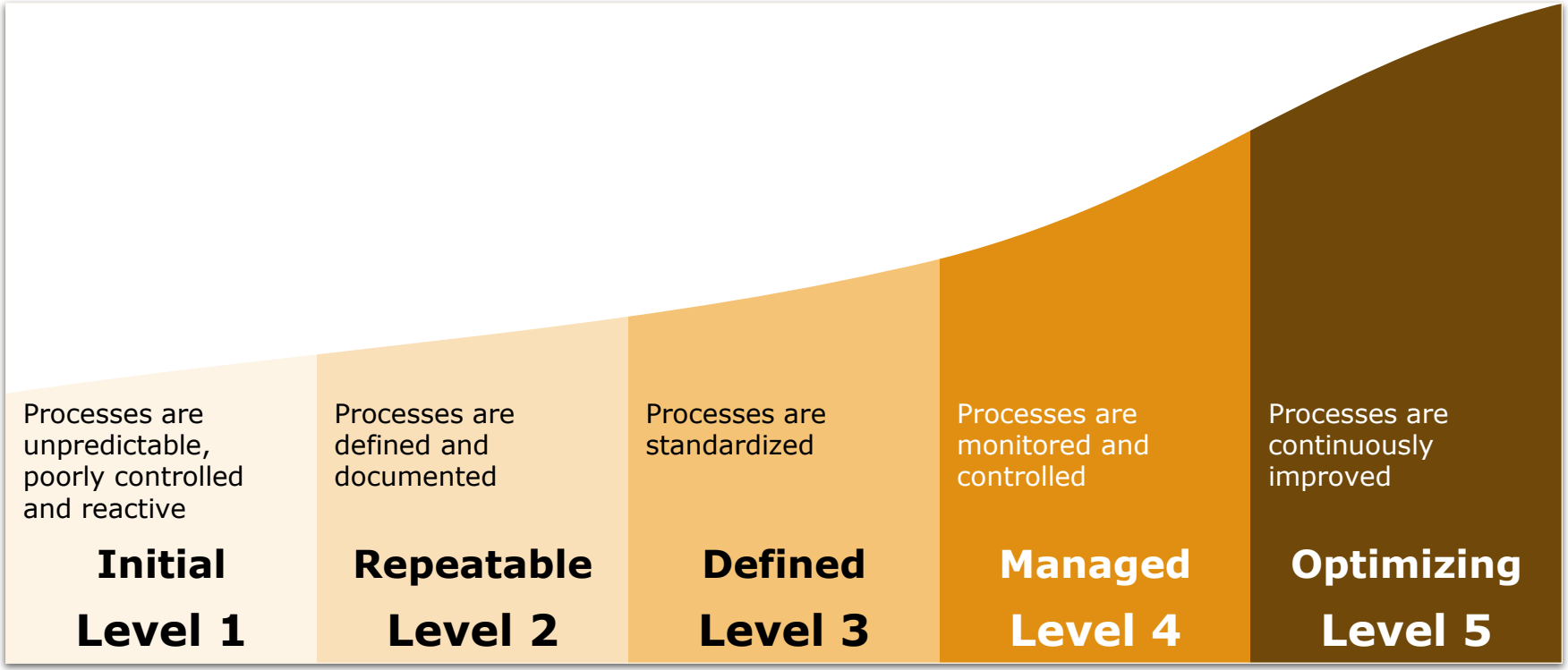
Introduction

Common misunderstandings

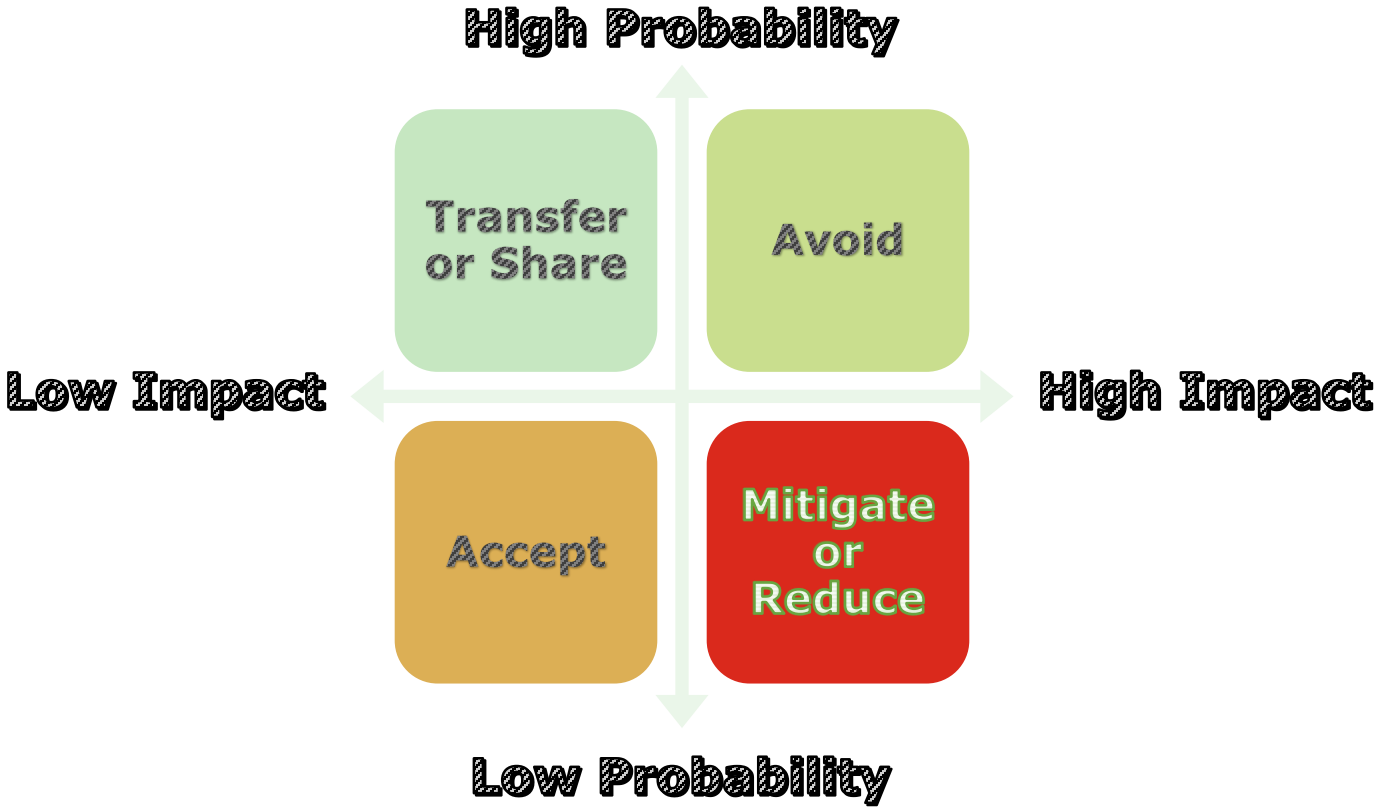
Challenges

Summary

# (Capability) maturity level



# Types of risk treatment



Reports from our patch management solution show that vulnerabilities are patched

Frequency: Often

# Vulnerability scanning is vulnerability management

Frequency: Often

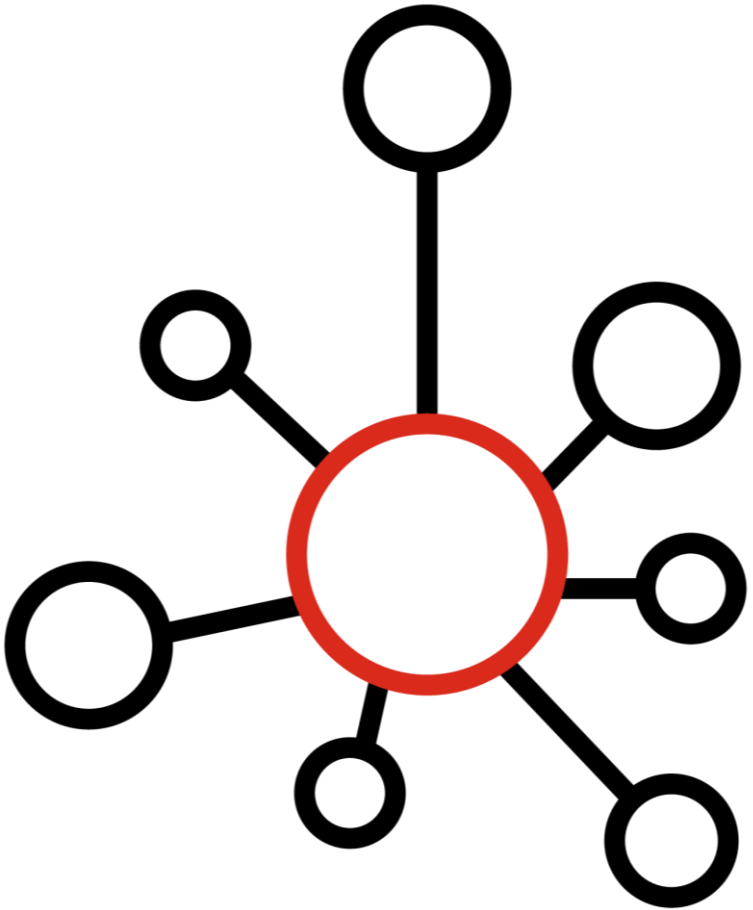
Technology

Process

People

# Servers are not infrastructure

- Clients/workstations
- Network devices
- Databases
- Containers
- IoT
- Hypervisors
- Web Applications
- …



# Vulnerability management is a one-time project

Frequency: Common

# Network scanning vs agent-based scanning

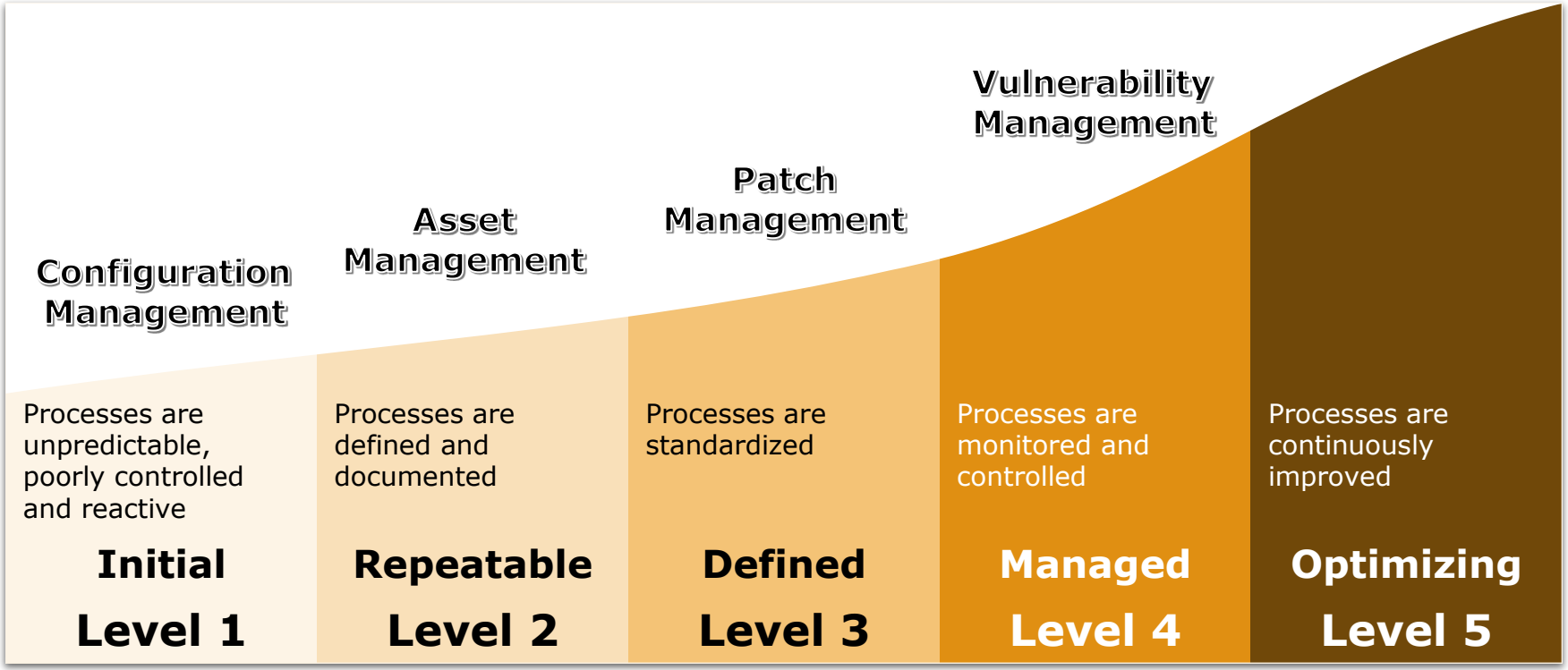
# Vulnerability scanning infrastructure

Support of vulnerability scanning infrastructure is a dedicated process

# Extended vulnerability management

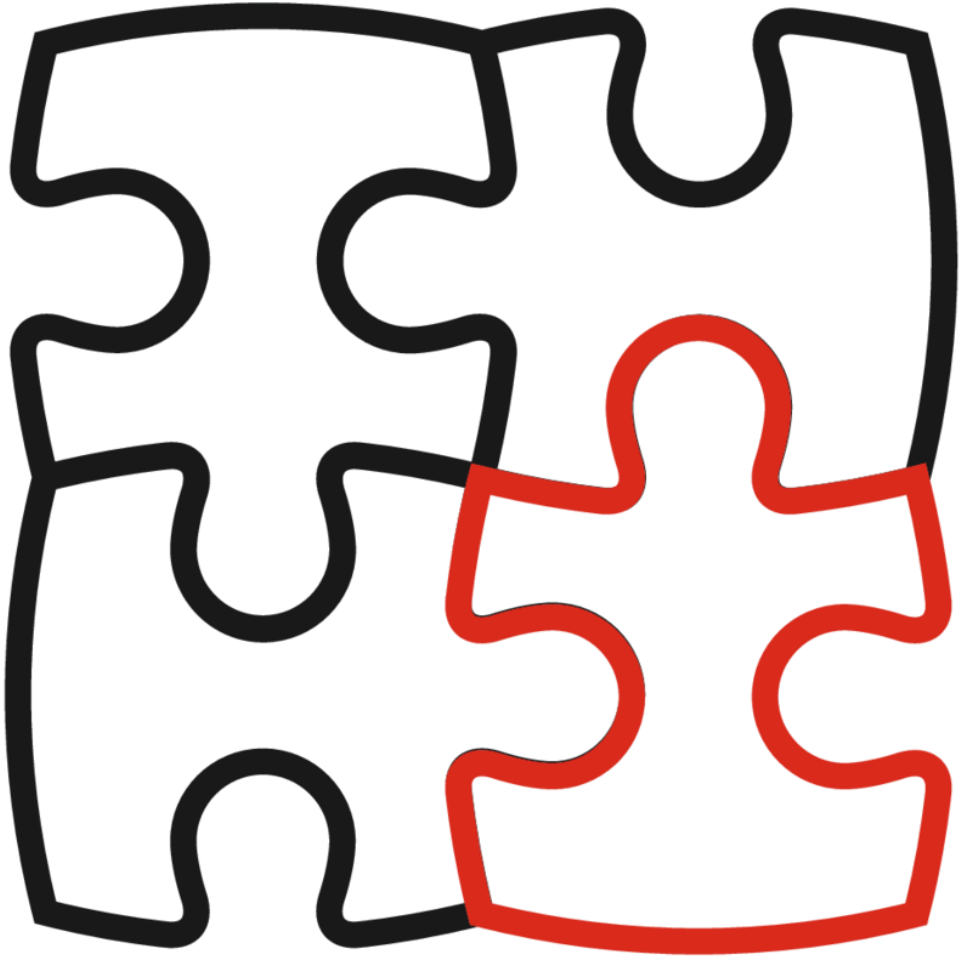
- Integration with patch management system
- Mobile device management
- Cloud infrastructure audit
- SCAP and OVAL Auditing

# (Capability) maturity level

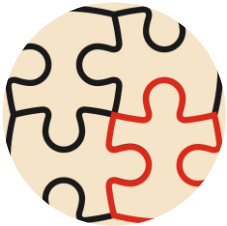


# Vulnerability management relies on other processes

It does not make sense to establish vulnerability management if asset, patch, and configuration management have lower maturity levels



# Takeout



**Dependency**

Improve asset, patch, and configuration management before establishing vulnerability management

**What is not VM?**

Vulnerability management is not a report from a patch management solution

**Maintenance**

Support of vulnerability scanning infrastructure is a dedicated process

**Expansion**

Vulnerability scanners are more than vulnerability collectors

**Resources**

Plan resources far in advance

**Existing tools**

Most EDR has vulnerability overview

# Vulnerability management policy

## External

[untrusted networks (e.g., the Internet or service providers)]

**Motto: zero tolerance**

1. Exploitable vulnerabilities are incidents with P1
2. Vulnerabilities of serenity medium and above must be eliminated (risk is avoided)
3. Active protection controls have informational status
4. Continuous asset reconnaissance
5. Vulnerability scanning from independent environments with minimal period between scans

## Internal

[can impose (security) requirements]

**Motto: zero trust**

1. Exploitable vulnerabilities must be mitigated fist (risk is avoided)
2. Other legacy best practices
3. Active protection controls must be implemented when possible
4. Hybrid vulnerability scanning
5. Accepted risks must have a re-evaluate date