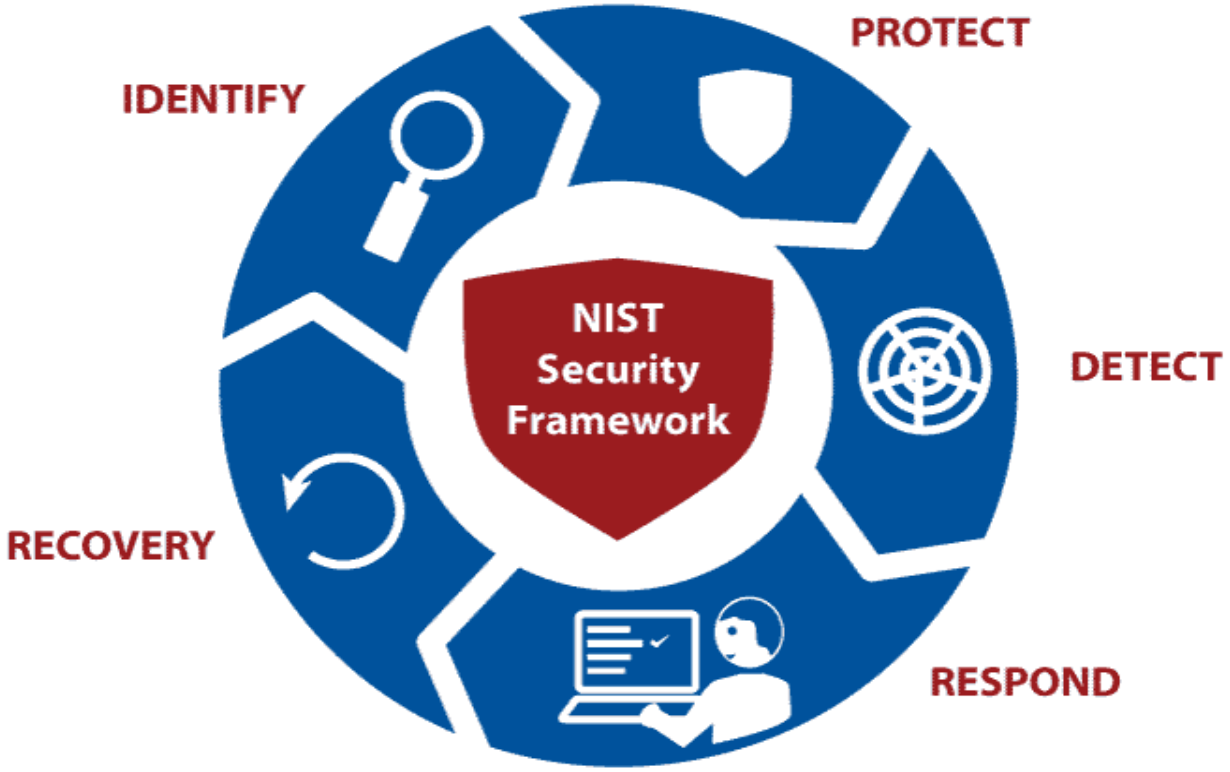
How to Perform IT Risk Assessment

Sergey Akhrameev
Pre-Sales Engineer

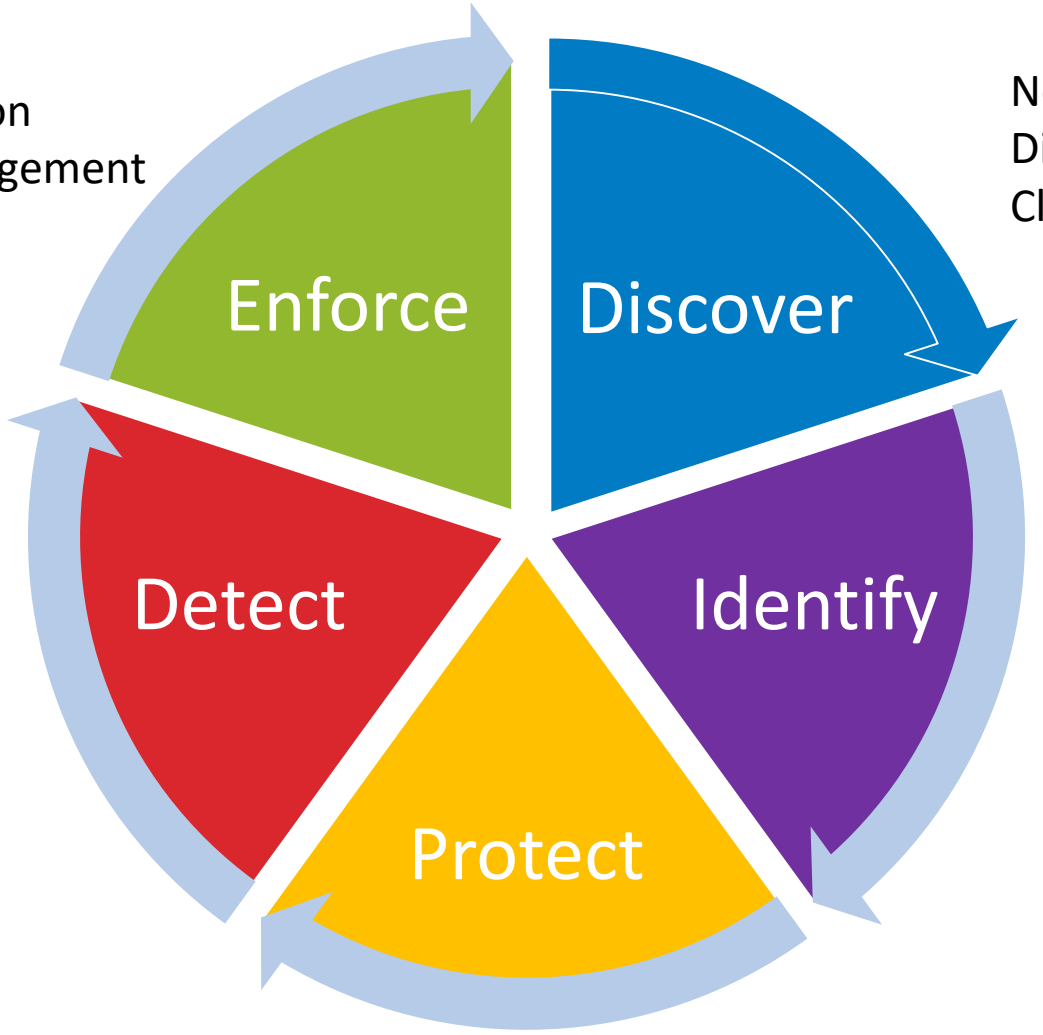
Evgenia Izotova
Account Executive

Risk management

NIST Cybersecurity Framework



Securing Data with Netwrix Auditor



Data Loss Prevention
Information Rights Management

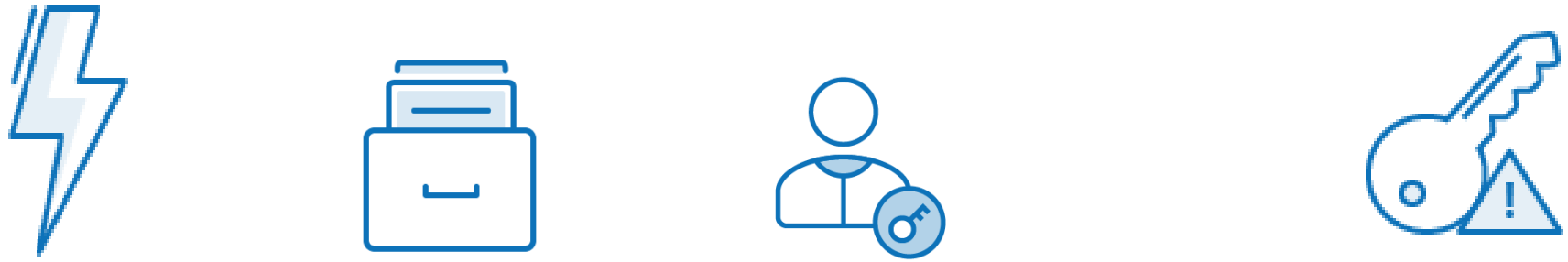
Netwrix Data
Discovery and
Classification

Netwrix Auditor

Netwrix Data Discovery and
Classification Plus/
Metadata

Netwrix Auditor /
Netwrix Data Discovery and Classification

Risk Determination



RISK = ASSET x THREAT x VULNERABILITY

ASSETS

- Data
- Servers
- Websites
- Cash
- Real estate
- Time

THREATS

- Accidental human interference
- Malicious humans
- System failure
- Natural disasters

VULNERABILITIES

- Excessive access permissions
- Wrong security settings
- Old equipment
- Unpatched workstations

How valuable are your assets?

DATA is the main ASSET

- What kind of data are you **responsible** of?
- Do you have **sensitive data** on storages?
- **How much** would it cost if data was **stolen**?
- **How much** would it cost if data was **lost**?
- **How much** would it cost if data was **changed/corrupted**?

Who is accessing your data and why?

A HUMAN is the main THREAT

- Do you know what users are doing in your IT environment?
- Are there failed access attempts?
- Are there behavior anomalies?
- Who owns potentially harmful files on file shares?

What are the weak points in your infrastructure?

Internal policies and actual settings must fulfil security requirements

- What is your password policy? Actual passwords settings?
- What is your permissions policy? Actual permissions?
- What is your administrative groups policy? What is actual status?
- Who has access to sensitive data?

Main vulnerabilities 1

Password security

X accounts with non-expiring passwords (X% of total)

X accounts that do not require passwords (X% of total)

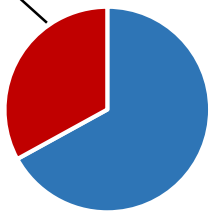
Potentially harmful files on file shares

X potential harmful files

(X% of total)

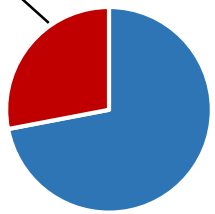
Users with administrative permissions

X users (X% of total)
have administrative permissions



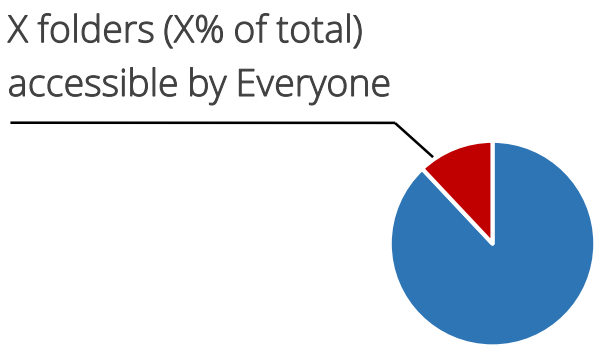
Administrative groups

X groups (X% of total)
are administrative



Main vulnerabilities 2

Shared folders accessible by Everyone



Sensitive files by source

X files (total)

- X Sensitive files
- X GDPR files
- X GLBA files
- X PCI DSS files
- Etc.

Overexposed Files and Folders

- X folders
- X files

Excessive permissions to sensitive data

- X users

Contractors have Read permissions to:

- X folders
- X files

Next Steps

- Low, Medium or High
- Low, Medium or High
- Determine the level of risk for each threat/vulnerability pair. Low, Medium or High

Our Upcoming Workshops

Continuous Risk Assessment with Netwrix Auditor

Red Hall

March 20

10:10

Reducing IT Risks with Netwrix Auditor

Orange Hall

March 20

10:10