CENTRALEYEZER

SANDLINE
IT CORE SECURITY

Security Team – Reporting Problems

- Security teams use various static and dynamic tests
- Red Team also produce results from **manual tests**
- **Different report formats** depending on each source
- Tests might describe same flaw **differently**
- **Duplicated Vulnerabilities - common issue**

Security Team – Reporting Problems

All these end up in hard to follow Excel files

- → Hard to manage
- → Hard to keep track
- → Hard to keep it updated
- → Demand time and additional resources

Vulnerabilities – Facts & Statistics

"Critical and high-risk vulnerabilities have an average age of 300 and 500 days respectively."

*"The average time-to-fix varies by industry from 100 days to 245 days."**

*https://info.whitehatsec.com/rs/675-YBI-674/images/WH-2016-Stats-Report-final.pdf

CENTRALEYEZER

Centraleyezer – Reporting Solution

- ✓ One Single View Security State Dashboard
- ✓ Easy Vulnerability Tracking
- ✓ Consolidated Results
- ✓ Automatic Vulnerability Follow-up
- ✓ Automatic Vulnerability Escalation
- ✓ Vulnerability Duplicate Merge
- ✓ Customizable Report
- ✓ Customizable Email Notification
- ✓ Enterprise Ready

CENTRALEYEZER

- ✓One Single View for Overall Security State
- ✓Customizable Dashboard
- ✓Auto-adjusted based on Assets Permissions
- ✓One Step Search
- ✓Active Directory Integration

https://centraleyezer.io

CENTRALEYEZER

Import Vulnerabilities from 3rd Party Vulnerability Scanners or from Manual Penetration Tests

Automatically assigned of each vulnerability to Asset Owner based on Asset types:

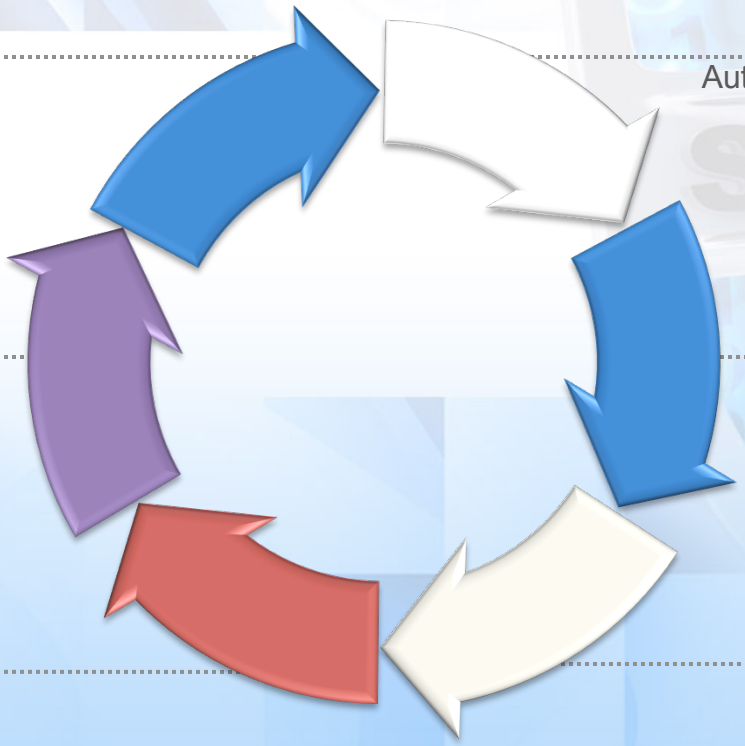
- IP Addresses
- Web Applications
- Mobile Applications

Asset Owner gets notified and can start working on solving the issue based on the recommendation. In case of no reaction form Asset Owner vulnerability get automatically escalate to superior hierarchy.

Vulnerability is closed by Asset Owner after being fixed or workaround in place.

Security Team is notified by email and in-app notifications about new status change in current assigned vulnerabilities and check closed ones.

Fixed vulnerabilities are closed. The ones which are not correctly fixed are re-opened for further investigation.

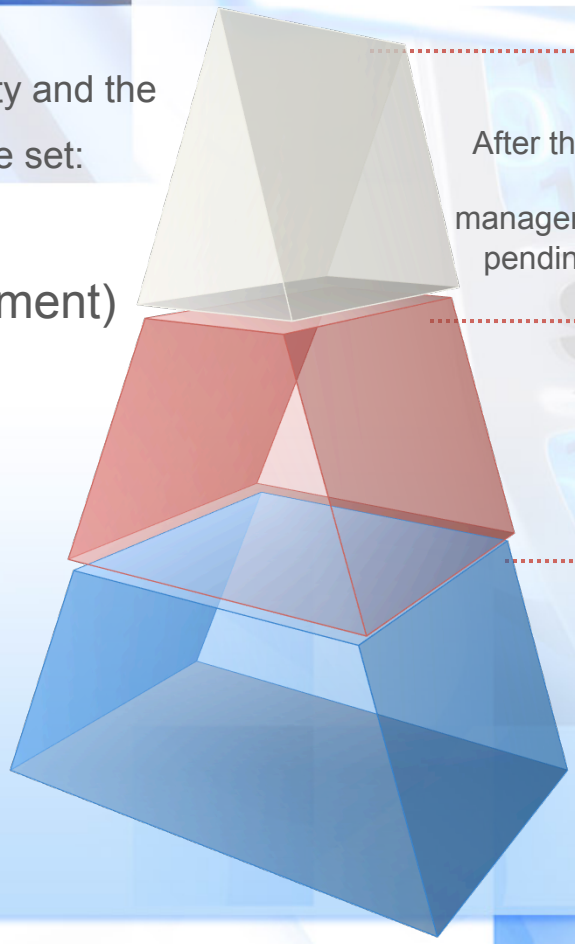


https://centraleyezer.io

CENTRALEYEZER

Based on the Vulnerability Severity and the Asset Risk Value 2 timeframes are set:

- ✓Reaction (Acknowledgement)
- ✓Deadline (Resolution)



After the due date of the vulnerability expired the second level of management will be notified about the pending vulnerabilities still not fixed.

If no reaction has been recorded during the Reaction timeframe, the vulnerability will automatically be escalated next superior level

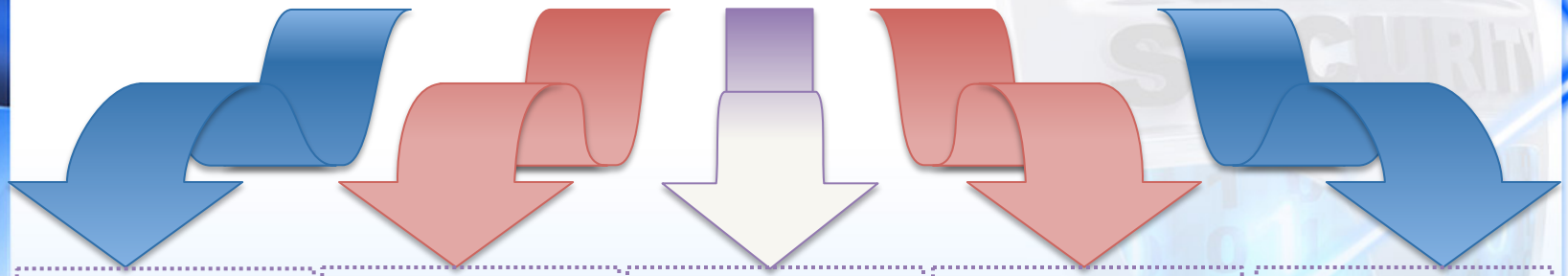
All vulnerabilities of and asset and following notifications are sent to the assigned Asset Owner and to secondary points of contact for the asset

https://centraleyezer.io

CENTRALEYEZER

Prioritize decisions

Real Risk Assessment Methodology - DREAD



Damage	**R**eproducibility	**E**xploitability	**A**ffected Users	**D**iscoverability
How bad would an attack be?	How easy is it to reproduce the attack?	How much work is it to launch the attack?	How many people will be impacted?	How easy is it to discover the threat?

Vulnerability Assessment Scanner Integration

- ✓Nessus
- ✓OpenVAS
- ✓Acunetix
- ✓Qualys
- ✓Tripwire
- ✓Tripwire SIH
- ✓Burp
- ✓Any scanner exporting to CSV format

Contact

contact@centraleyezer.io

Bucharest, RO : +40 722 234 788
Belgium , BE : +32 470 653 911