WAYRAY

How to measure your SOC efficiency: the Devil is in details

SOC Forum 2017

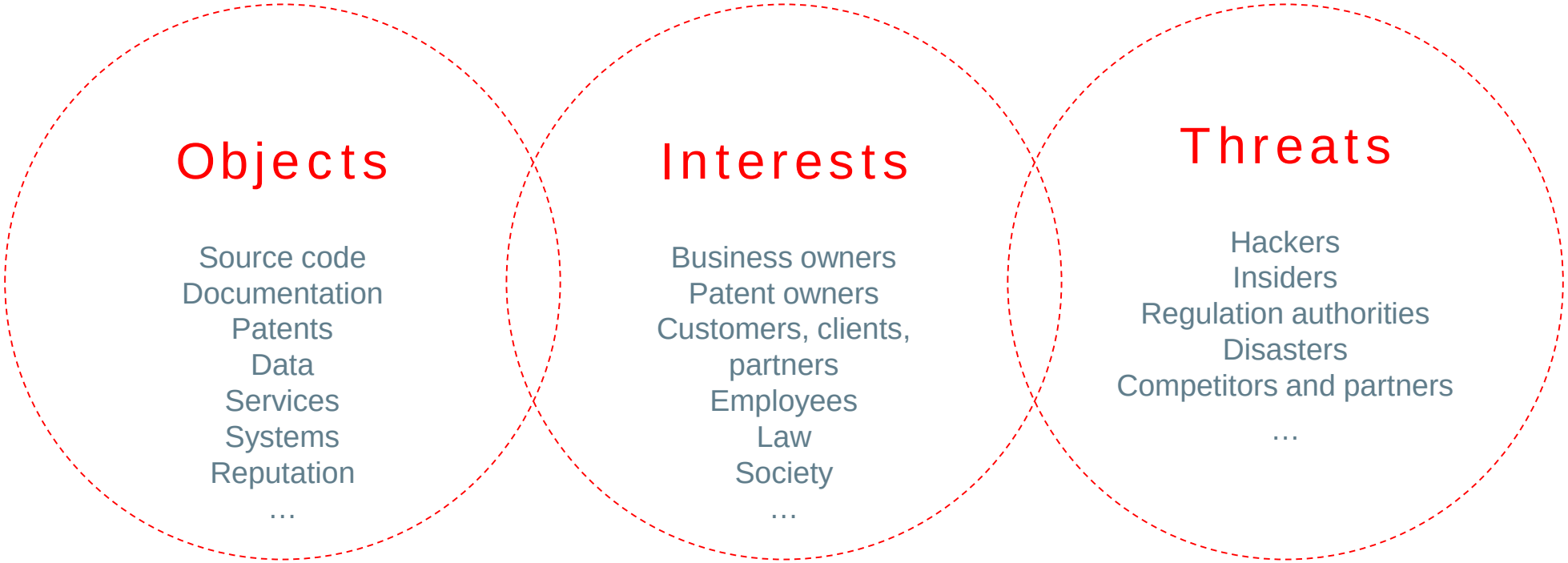
22.11.2017

Mona Arkhipova

CSO/CIO at WayRay

Past:

- Unit manager of infrastructure security and monitoring at Arconis, Lead information security expert and United monitoring team manager at QIWI group, Security Analyst at General Electric, independent security consultant for fintech startups.
- *nix and network administrator as a background
- 11+ years experience in IT and 7+ of that in IT security



”Silver Bullet” solutions

- Gather references, mostly from hands-on specialists
- Try to pilot on large amount of various data
- Performance testing under overload
- There’s no silver bullet

Small/Mid

- Good point to start
- …if your production would stay the same size
- May be supported by IT
- (most) processes may be easily changed

Mid/Large

- Also good point to start
- …if you don't have compliance requirements on retention
- And if you have enough resources for internal development
- Calculate solution cost on different lifecycle stages

- Support response speed (please tell me about issues with critical severity)
- Patching speed (scan your “hypersecure” vendor’s appliance)
- Amount of experts on solution at market
- Professional services costs

Does the solution needed or may be applied only for security team tasks?

Hardware/Software

- Server requirements
- Network requirements
- Workstations requirements
- Deployment and integration
- Licenses cost
- Warranties
- Vulnerability risks
- Lifecycle risks (upgrades, patches, licensing)

Operations cost

- Infrastructure (may include electricity)
- Personnel (IT, Security) and trainings
- Performance issues cost
- Outage/downtime and other failures cost
- Backup/Recovery (DRP)
- Change management
- Security issues risk cost
- Audit costs

A long time ago in a galaxy far, far away: Replacement, Scalability and Decommissioning

- Look for enhancements
- Recheck the covered scopes
- Solution criticality to your daily operations
- Calculate TCO for current solution
- Calculate average TCO for planned solution
- Plan changes or replacement

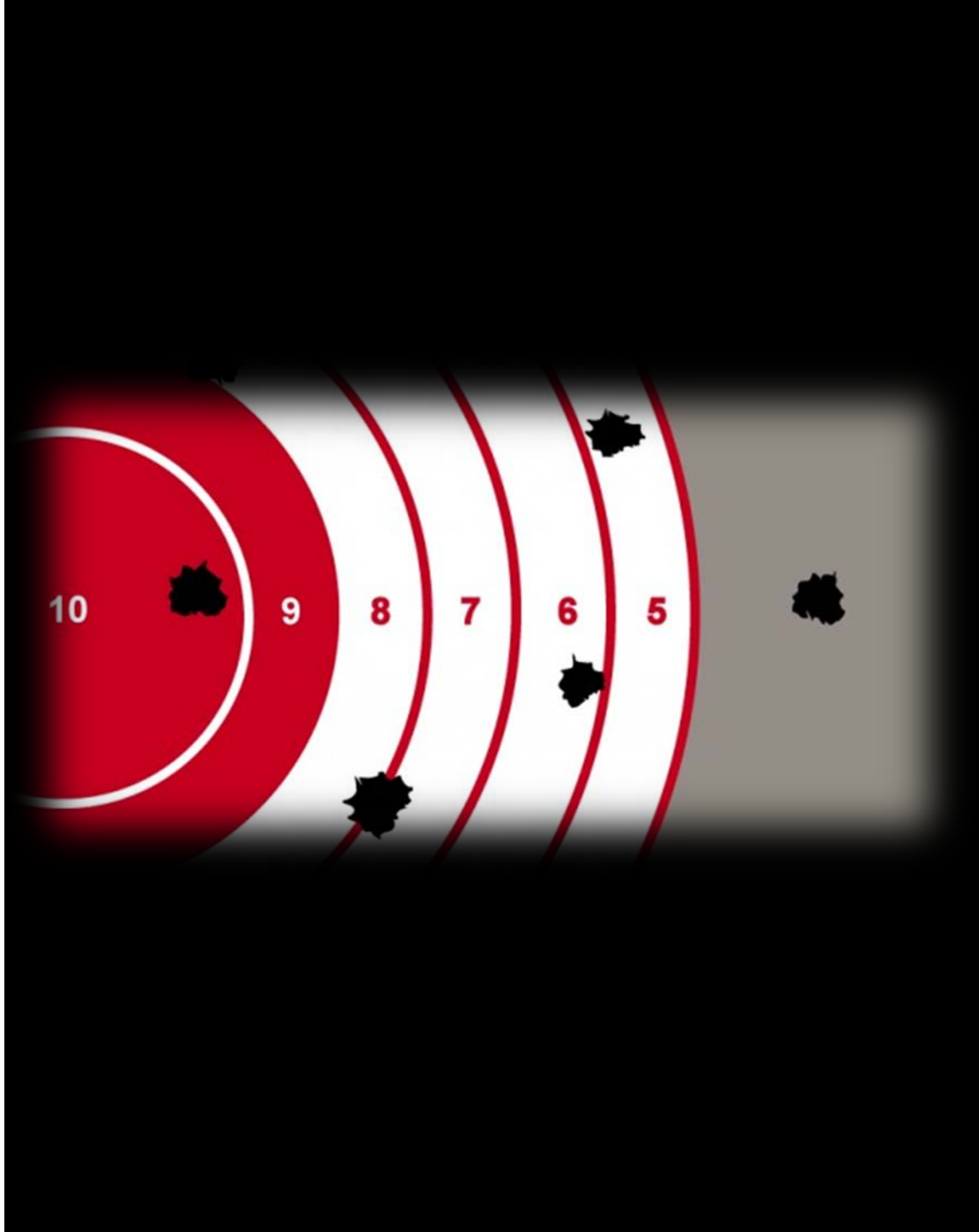
Personnel

- Inventory
- Initial setup
- Hardening/post-install
- Monitoring/incidents handling
- Access management
- In-depth knowledge of services/networks
- Awareness and user help
- Win-win deployments (share your tools!)

Many security things may be a part of IT processes

 Security-related KPIs – “best practices” vs real-life

- Processes check results
- ISO 27001/002 controls
- Penetration test results
- Incidents cost
- Major incidents count
- Security-related downtimes
- Implementation/upgrade duration
- Patching speed
- Incidents per some time



- Clear processes on load/tasks
- Clear ways to change position (management/technical)
- Rotation or internship programs
- Do not divide operations and architecture
- “Step-down” practice for all levels
- Skip-level or any other ways to gather feedback on key players
- Mentorship!

Testing

- Most popular
- Limited systems scope and attack vectors
- Single vendor (team, specialist, etc.)
- Well-known scenarios (oh, that scanners again!)
- Approved ‘testing windows’
- Whitelisting as a requirement
- “This is for compliance”
- Lack of coverage

Ok, you may show real attackers your compliance certificate and penetration testing issue remediation

- Good for large systems
- Full coverage of internals
- Scope is related to all security and awareness processes (not only IT systems)
- Greatest way to test your team and tools
- Safe way to get a ’real’ incident and apply appropriate mitigations

Cons

- Price
- DoS and urgent changes
- Urgent reinstall
- All employees are the target too
- IT security team overload
- 24x7 attacks

- Same team/vendor/etc every year
- Scenarios recheck
- ”Blind spots” staying uncovered
- Continuous measurements of tools performance
- Deep root cause analysis not performed in many cases
- We’ve got disappointed in tools but we would stay on them for ’some reasons’ (hello, legacy?)
- What’s about internal tests for non-tech employees?

Mona Arkhipova
Chief Security Officer/Chief Information Officer

mona@wayray.com

wayray.com