32ND ANNUAL | NOVEMBER 16-18, 2020

FIRST CONFERENCE

VIRTUAL EDITION WHERE DEFENDERS SHARE

WWW.FIRST.ORG

FIRST™

The Intelligent Process Lifecycle of Active Cyber Defenders

Desiree Sacher-Boldewin and Eireann Leverett

About us

Desiree Sacher

- Principal Security Architect of Operational IT @ Finanz Informatik
- 10 years finance industry experience as IT Security Engineer & Security Analyst

Finanz Informatik

- German IT service provider for the German Savings Banks Finance Group
- 32k servers / 324k devices, incl. ATMs

Eireann Leverett

- Senior Scientist in Cyber Innovation
- 3 Years in ICS Red Team/ 7 Years in Risk

Airbus Operations Limited

- 140 Nationalities and 4 generations
- 10 Types of aircraft
- 4 Externally Facing SOCs

Disclaimer
The opinions and views expressed here are our own and do not represent the opinions of our employers

Quick recap of FIRST 2019 presentation

- Detailed paper on https://github.com/d3sre/Use_Case_Applicability/
- FIRST sponsored peer reviewed ACM DTRAP paper https://dl.acm.org/doi/10.1145/3370084

Categories Summary

FIRST 2019

Categories	Solution Type	Alert Cause
a) Announced administrative/user action		
b) Unnannounced administrative/user action		
c) Log management rule configuration error		
d) Detection device/rule configuration error		
e) Bad IOC/rule pattern value		
f) Test alert		
g) Confirmed Attack with IR actions		
h) Confirmed Attack attempt without IR actions		

BENEFITS

Hack.lu 2019

- Statistics for effectiveness of internal security measures & architecture → new KPI possibility

KPI	Explanation	Target Value
Number of Log Management Rule Configuration Error events per month	This value reflects the rules configured in the SIEM by the SOC Analysts. A high number suspects bad quality of rules, more training or experience needed.	< 10 %
Number of Announced Administrative/User Action events per month	This value reflects suppressions that should be improved.	< 10 %
Number of Bad IOC/rule pattern value events per month	If too many events were created by bad IOCs or rule pattern values, the source or the trust in it should be questioned.	< 5 %
Number of Confirmed Attack attempt without IR actions (best matched with Log Source Category)	Number of events detected but prevented by measures in place or where the alert isn't viewed as a high risk.	> 50 %
Number of Confirmed Attack attempt with IR actions (best matched with Log Source Category)	Very high numbers → Security Architecture should be updated Very low numbers → The rules aren't detecting or you are safe	☺

Benefits - Reports

CyberCrimeCon2019

CYBER CRIME CONFERENCE

External Threat Heatmap

	MITRE ATT&CK Tacticts	Target Enviroment	Jan	Feb	Mar	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec	Sample Use Cases:
Low	Initial Access	Client Systems													Exploit Public-Facing Application, Spearphishing Link, Spearphishing Attachment
		Company Infrastructure													
		Customer Service Infrastructure													
		Development systems													
Medium	Persistance Defense Evasion Command and Control	Client Systems													Scheduled Task, New Service, File Deletion, Registry Run Keys / Startup Folder, Remote Access Tools, Remote File Copy, Standard Application Layer Protocol
		Company Infrastructure													
		Customer Service Infrastructure													
		Development systems													
High	Discovery Privilege Escalation Execution Credential Access	Client Systems													Network Service Scanning, Security Software Discovery, Bypass User Account Control, Signed Binary Proxy Execution, Powershell, Scheduled Task, Brute Force, Credential Dumping
		Company Infrastructure													
		Customer Service Infrastructure													
		Development systems													
Critical	Lateral Movement Collection Exfiltration Impact	Client Systems													Windows Remote Management, Logon Scripts, Data from Local System, Exfiltration over C2 Channel, Data Encrypted, Remote File Copy, Remote Access Tools, Standard Application Layer Protocol, Data Destruction, Defacement,
		Company Infrastructure													
		Customer Service Infrastructure													
		Development systems													

	>2 Confirmed Attack with IR actions
	1 Confirmed Attack with IR actions
	20+ Confirmed Attack attempt without IR actions
	10-20 Confirmed Attack attempt without IR actions
	5-10 Confirmed Attack attempt without IR actions
	1-5 Confirmed Attack attempt without IR actions
	0 Confirmed Attack attempt without IR actions
	No coverage

Sample External Threat Heatmap

Benefits - Reports

CyberCrimeCon2019

CYBER CRIME CONFERENCE

Internal Security Heatmap

	MITRE ATT&CK Tacticts	Target Enviroment	Jan	Feb	Mar	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec	Sample Use Cases:
Low	Initial Access	Client Systems													Exploit Public-Facing Application, Spearphishing Link, Spearphishing Attachment
		Company Infrastructure													
		Customer Service Infrastructure													
		Development systems													
Medium	Persistance Defense Evasion Command and Control	Client Systems													Scheduled Task, New Service, File Deletion, Registry Run Keys / Startup Folder, Remote Access Tools, Remote File Copy, Standard Application Layer Protocol
		Company Infrastructure													
		Customer Service Infrastructure													
		Development systems													
High	Discovery Privilege Escalation Execution Credential Access	Client Systems													Network Service Scanning, Security Software Discovery, Bypass User Account Control, Signed Binary Proxy Execution, Powershell, Scheduled Task, Brute Force, Credential Dumping
		Company Infrastructure													
		Customer Service Infrastructure													
		Development systems													
Critical	Lateral Movement Collection Exfiltration Impact	Client Systems													Windows Remote Management, Logon Scripts, Data from Local System, Exfiltration over C2 Channel, Data Encrypted, Remote File Copy, Remote Access Tools, Standard Application Layer Protocol, Data Destruction, Defacement,
		Company Infrastructure													
		Customer Service Infrastructure													
		Development systems													

Internal Events consists of: Unannounced administrative/user action, Detection device/rule configuration error, Bad IOCs/rule pattern values

	20+ Events
	15-20 Events
	10-15 Events
	5-10 Events
	1-5 Events
	0 Events
	No coverage

Sample Internal Security Heatmap

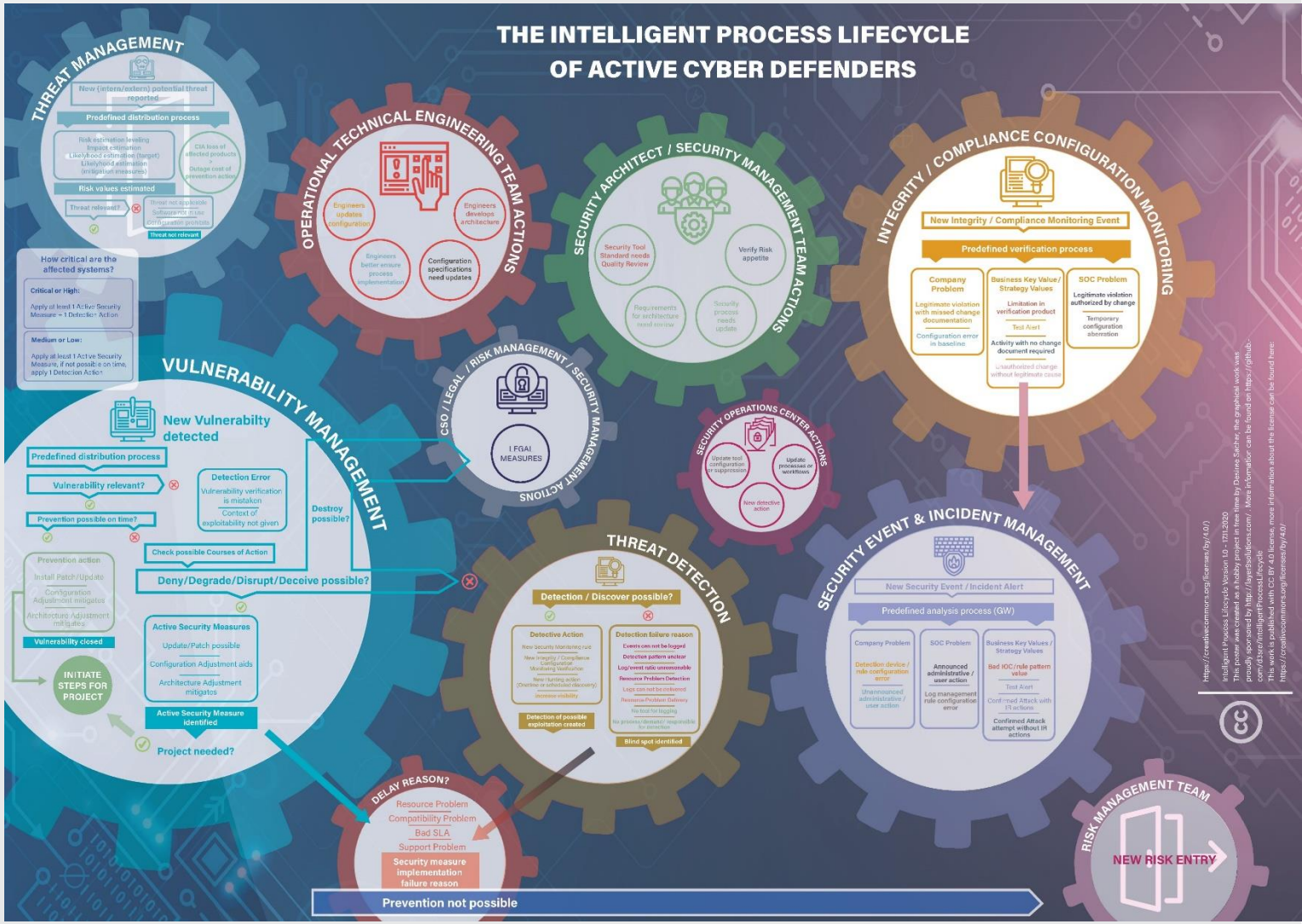
Motivation for Update

- Cloud infrastructure more relies on secure configuration of systems
- Detection of configuration changes is of key importance
- SOC services quality reflect overall security quality state of infrastructure
- Number of vulnerabilities seem to be rising....

SOC becomes **operational data verification** and **technical security quality assurance center** with **cyber incident investigation & analysis capabilities**

Poster

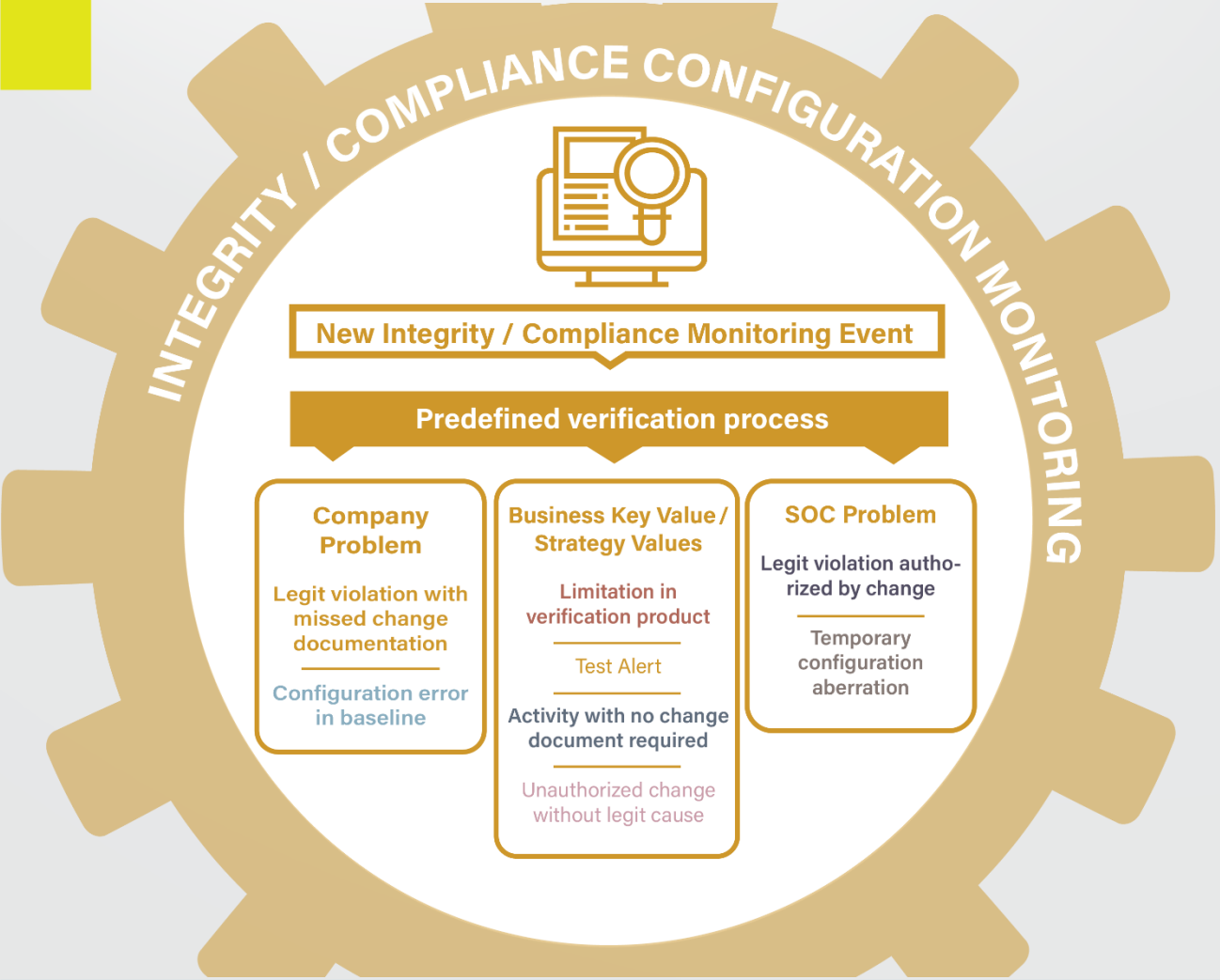
- Display of categorised «false positives» states, error types and problems
- Visibility of «continuous improvement» action to correct state of problem
- Based on «Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains” paper by Lockheed Martin



Reference: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

Category Summary

Integrity/Technical Security Compliance Monitoring

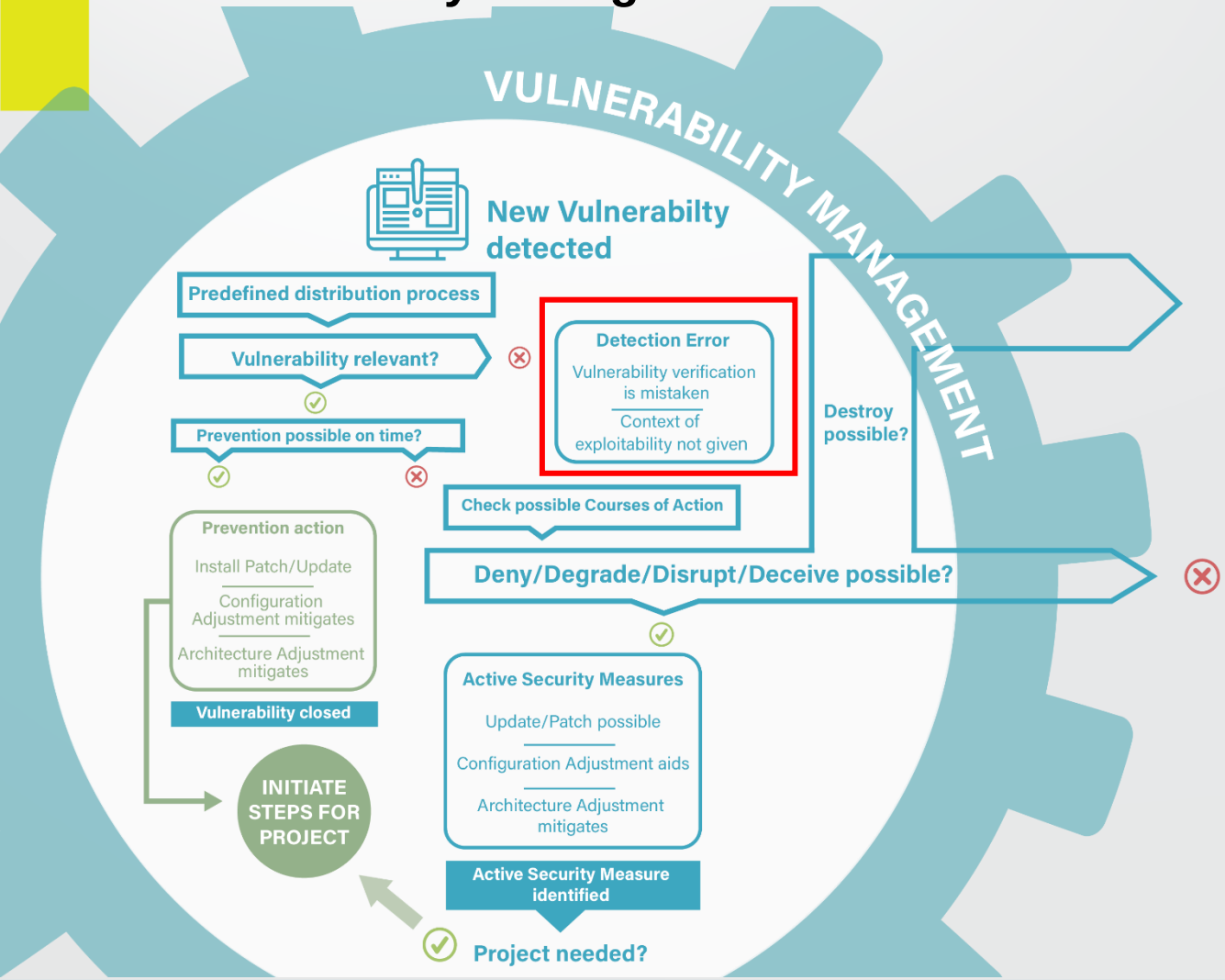


Follow Up Actions

- Adjust baseline configuration, document change
- Security configuration/baseline needs engineer review
- Tool provider should be verified
- Should be excluded from reporting
- Alerts should be forwarded to security management/policy responsible to confirm scope
- Security incident should be opened, and alert followed up on
- Adjust baseline configuration, Update information process to involve SOC
- Save or keep old baseline, possibly add temporary suppression

Category Summary

Vulnerability Management

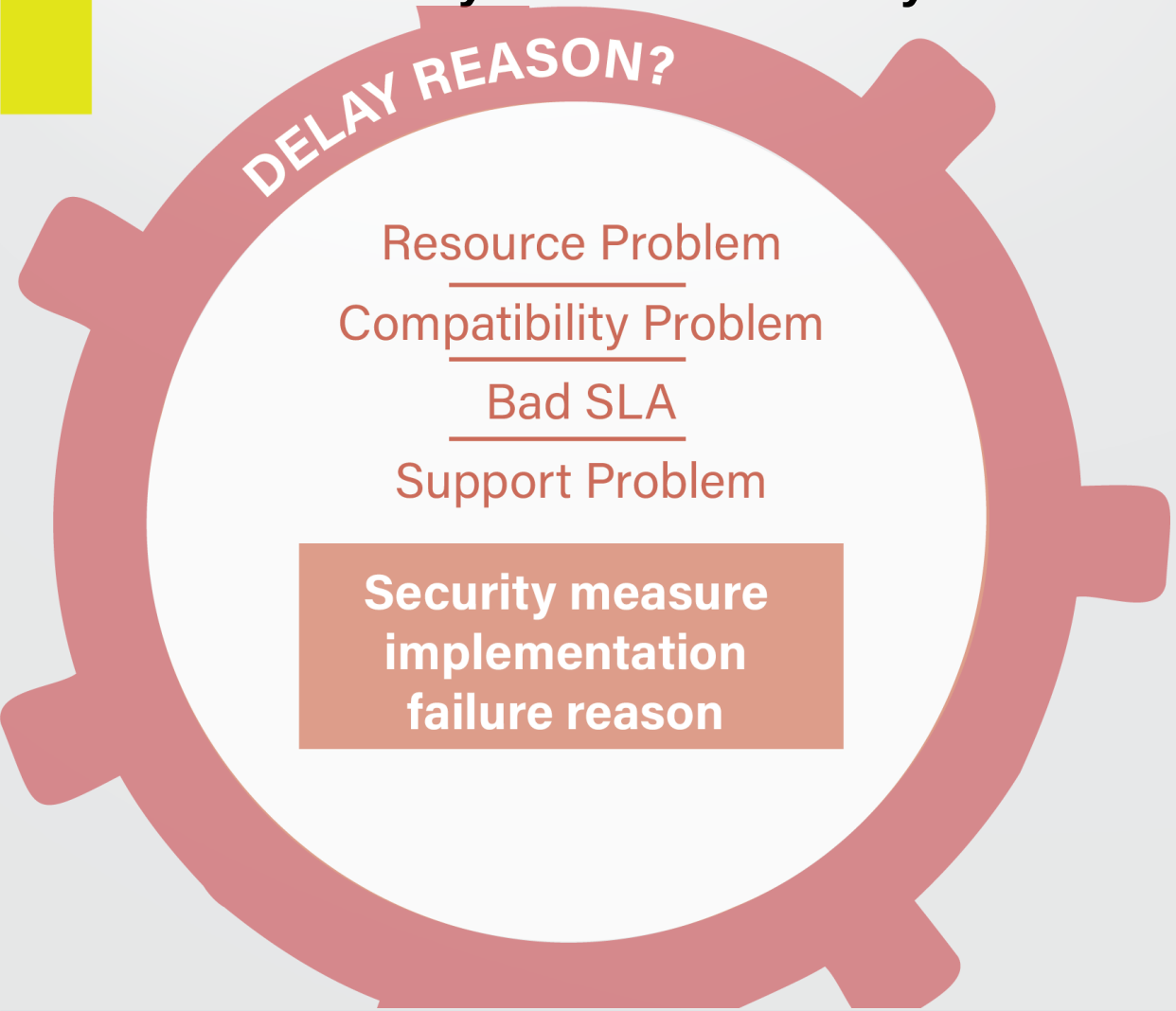


Follow Up Actions

- Verify your tool capabilities
- Verify your security documention of specific context for threat protection measures

Category Summary

Vulnerability remediation delay reason



Follow Up Actions

- Review and if reasonable report risk for staffing/budget priorities
- Review and if reasonable report risk for your product dependencies
- Review and if reasonable update SLA/SLA dependencies or report risk
- Review and if reasonable verify partner dependencies

Category Summary

Detection failure reason

Follow Up Actions

- Report risk, find a close enough approximation
- Report risk, schedule education for SOC engineers
- Report risk, verify economic alternatives
- Report risk, Verify priorities and staffing within SOC
- Report risk, review architecture for possible log transmission
- Report risk, Verify priorities and staffing with security engineers
- Report risk, Security management/IT governance verification
- Report risk, Security management/IT governance verification

Benefits: KPI Suggestions

Integrity/Technical Security Compliance Monitoring

Endogenous Exogenous

KPI	Explanation	Target Value	Owner	Risk Type
Number of legitimate violations authorized by change	This value reflects events which usually are classic false positives, where all official change processes were correctly followed but the SOC was not included in the process and therefore could not prevent the false alarm	< 10 %	Compliance	
Number of configuration errors in baseline (best matched with Log Source Categories	This value reflects what system configurations (or even configuration templates) needs improvement.	< 10 %	Compliance/ Operational	
Number of Limitation in verification products found	If too many of these events were created by configurations, the causing tool should be questioned.	< 5 %	Compliance/ Operational	
Number of activities with no change required	There seems to be a mismatch between the defined security scope and the verified security scope. Gaps should be verified	< 5 %	Policy	
Number of unauthorized changes without legitimate cause	Very high numbers → Security process and IT process integration needs rework Very low numbers → The configurations aren't detecting or you are safe	☺	Policy	

Benefits: KPI Suggestions

Vulnerability Management

Endogenous Exogenous

KPI	Explanation	Target Value	Owner	Risk Type
Number of delays due to unreasonable SLA	If this value is high very often, correlated to the applications you are running you might be able to impact either SLA or policy documents	0	Operational/ Contractual	
Numbers of delays due to resource problems or Average # of days delays due to resource problems	If this happens to often it can illustrate how your staff management is impacting the quality of security services. If occuring too often a risk entry is important	0	Contractual	
Numbers of installed patch on time	This is the goal. If it can't be reached too often policies or failing reasons should be reviewed	>80%	Counter-Party/ Contractual	
Number of blind spots identified	Any time a detection can not be created this should be tracked, possibly by creating risk entries.	< 5 %	Operational/ Contractual	
Number of context of exploitability not given	Very high numbers → You might not be getting honest responses or your threat identification process is faulty	☺	Counter-Party/ Contractual	

Threat/Risk Communication

- Identify where time is actually being spent
- Create statistics for effectiveness of internal security measures & architecture for evidence based discussions
- Integrate possibility for directly initiating continuous improvement into the process

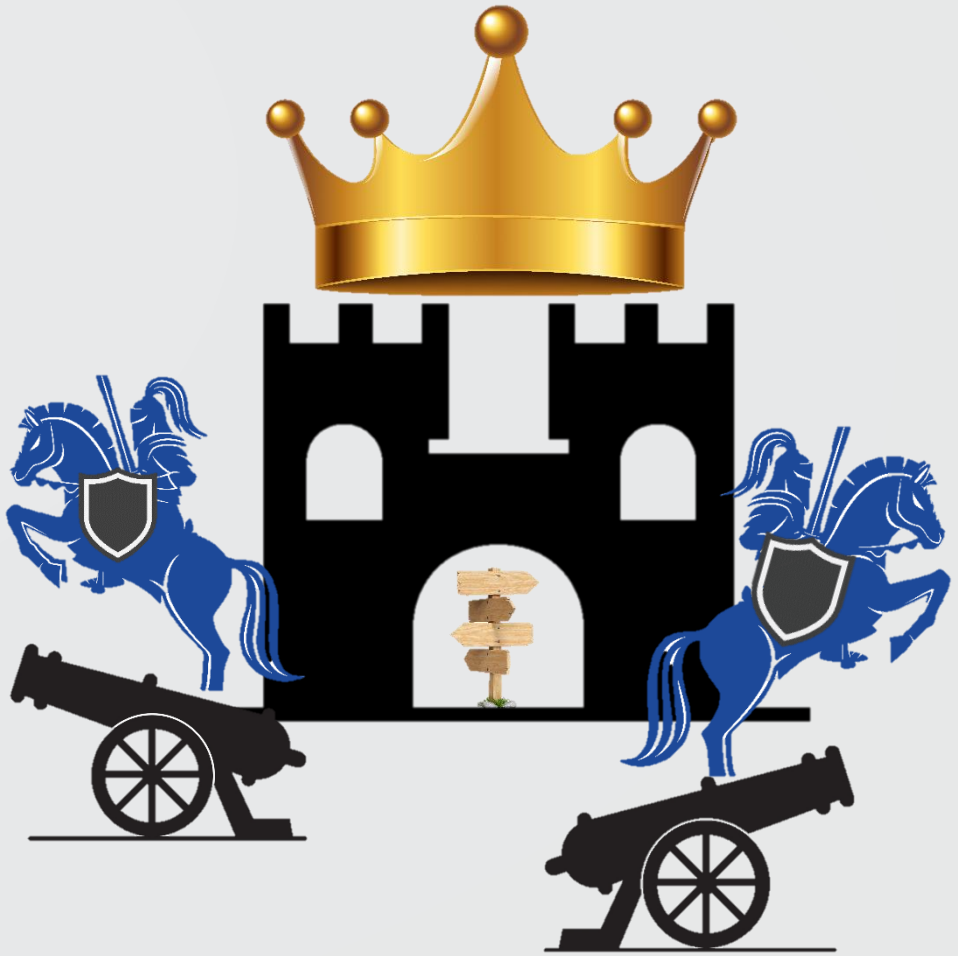
Risk and incentive alignment

- Identify „Value at Risk“ by combining numbers with specifc target environments that are problematic
- Create transparency in your risk treatments (proportinal to severity/proportional to frequency)
- Review VaR by checking contracts

Risk treatments aren‘t booleans!

Call to Action

- Add categories to your security ticketing tool



- Twitter : @d3sre & @blackswanburst
- More information on technical impementation can be found on https://github.com/d3sre/IntelligentProcessLifecycle