THE INTELLIGENT PROCESS LIFECYCLE OF ACTIVE CYBER DEFENDERS:

THE EXTENDED VERSION

DESIREE SACHER-BOLDEWIN

ABOUT ME

Desiree Sacher-Boldewin

- Security Architect @ 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

finanz **informatik**

Disclaimer
The opinions and views expressed here are my own and do not represent the opinions of my employer

GOAL & WHY

Sustainable security

by building **intelligent processes**,

and **efficient workflows**

and detection capabilities

Intelligent processes – why?

- **guide junior analysts to think the right way to learn to ask the right questions**

Efficient workflows – why?

- **prevent bore out and blunting of employees**
- **optimal use of internal resources**

  → save time and money

Efficient detection capabilities – why?

- **optimal use of vendor capabilities**

  → save time and money

How?
By resolving the source of false alarms in a structured approach so they won´t occur again

THREAT MANAGEMENT – DO WE HAVE A PROBLEM?

It depends – who is asking?

The scope of the problem

Steve Stone, Mandiant senior director of advanced practices, told SearchSecurity that defining the scale of the "patching problem" is impossible.

"I'm not sure we can give you a perspective on what the world looks like," Stone said. "I actually think part of the challenge is that I don't think anybody can. I don't think any organization anywhere can tell you how large or how small the problem is, because I don't think anyone has that visibility. I actually think that's indicative of how challenging of a problem this is."

There are too many products, too many vulnerabilities, and such a varying level of visibility that the problem cannot be quantified in any reliable way. In fact, even in issues where there is some visibility -- like in the case of RiskIQ and ProxyLogon-vulnerable servers -- getting a complete picture of what any known statistic means is far from easy.

Source: https://www.techtarget.com/searchsecurity/news/252503950/Why-patching-vulnerabilities-is-still-a-problem-and-how-to-fix-it

Vulnerability fatigue – why you need to get on top of patch management

More and more vulnerabilities are being discovered every day, leaving in-house teams struggling to provide corrective patches quickly. Hackers are taking advantage of this lead time to analyse information systems, find vulnerabilities and launch successful attacks.

Last year alone, 22,000 new vulnerabilities were published. At the same time, 80% of attacks are being carried out on known vulnerabilities, which indicates that enterprises are generally slow to patch. Approximately 25% of new vulnerabilities are patched in a month. Move along eight months, and only 75% of new vulnerabilities are normally patched. This means some vulnerabilities are never patched at all.

Source: https://www.orangecyberdefense.com/global/blog/threat/vulnerability-fatigue-why-you-need-to-get-on-top-of-patch-management

THREAT MANAGEMENT – DO WE HAVE A PROBLEM?

It depends – who is ask

The scope of the problem

Steve Stone, Mandiant senior director of advanced practices, told SearchSecurity that defining

ıe world looks like," Stone said. "I actually
can. I don't think any organization
ɔlem is, because I don't think anyone has
allenging of a problem this is."

, and such a varying level of visibility that
n fact, even in issues where there is some
ɣulnerable servers -- getting a complete
easy.

get.com/searchsecurity/news/252503950/Why-
ll-a-problem-and-how-to-fix-it

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Alerts and Tips Resources

National Cyber Awareness System > Alerts > Weak Security Controls and Practices Routinely Exploited for Initial Access

Alert (AA22-137A)

Weak Security Controls and Practices Routinely Exploited for Initial Access

Original release date: May 17, 2022

Print Tweet Send Share

Source: https://www.cisa.gov/uscert/ncas/alerts/aa22-137a

Vulnerability fatigue – why you r
to get on top of patch managen

More and more vulnerabilities are being discovered every day
house teams struggling to provide corrective patches quickly
are taking advantage of this lead time to analyse information
find vulnerabilities and launch successful attacks.

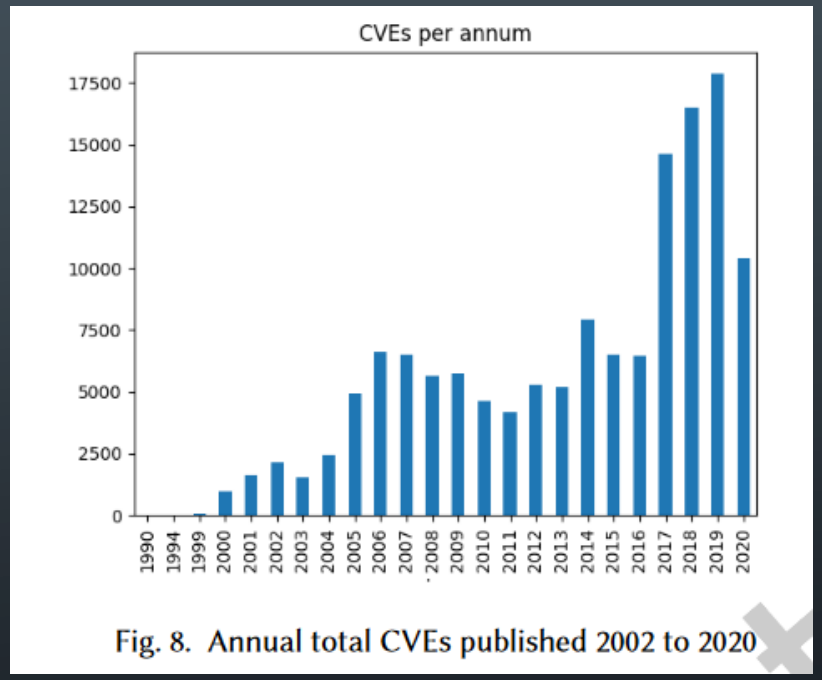
Last year alone, 22,000 new vulnerabilities were published. At the
80% of attacks are being carried out on known vulnerabilities, wh
that enterprises are generally slow to patch. Approximately 25% of new
vulnerabilities are patched in a month. Move along eight months, and only
75% of new vulnerabilities are normally patched. This means some
vulnerabilities are never patched at all.

Source: https://www.orangecyberdefense.com/global/blog/threat/vulnerability-fatigue-why-you-need-to-get-on-top-of-patch-management

VULNERABILITIES ARE ON THE RISE

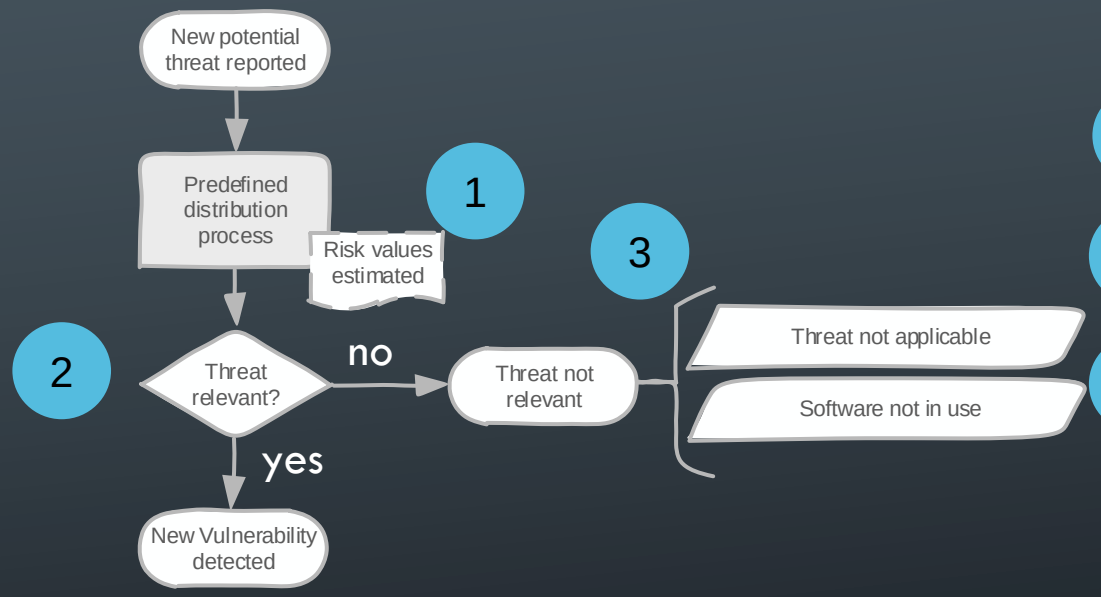
Interesting reads

- https://epub.uni-regensburg.de/38099/1/Forecasting%20IT%20Security%20Vulnerabilities.pdf
- https://arxiv.org/pdf/2012.03814.pdf
- https://www.danielwoods.info/assets/pdf/DW2021_blessed_NSPW.pdf
- https://www.cisa.gov/uscert/ncas/alerts/aa22-137a



Source: https://dl.acm.org/doi/pdf/10.1145/3492328

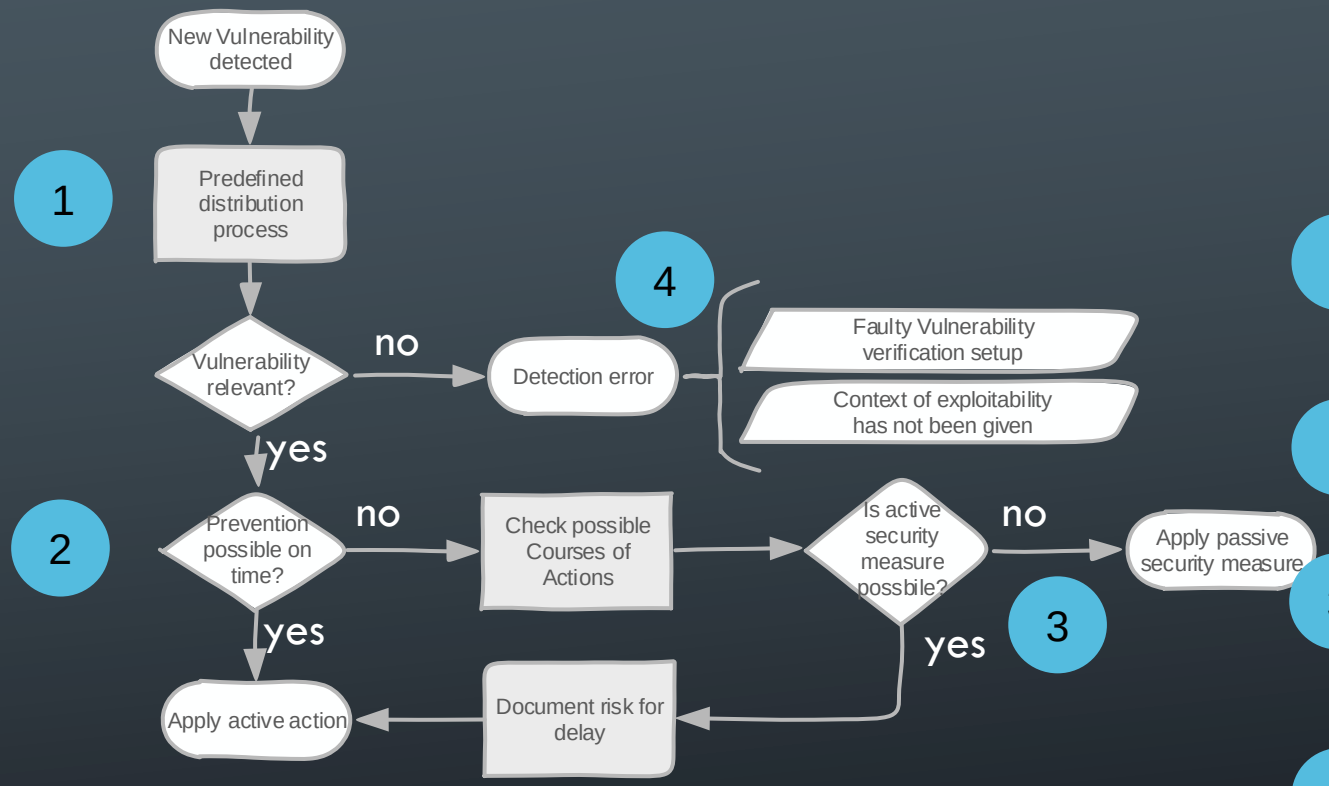
RECAP:
SIMPLIFIED PROCESS FOR THREAT ASSESSMENT



Requirements

1. Defined risk acceptance values
2. Inventory of all software/products
3. Inventory of protection applied per target system

RECAP:
SIMPLIFIED PROCESS FOR VULNERABILITY ASSESSMENT



Requirements

1. Correct responsible needs to be identified
2. The defined specifications need to be actionable
3. Possible next steps need to be clear
4. Working Vul. detection setup

COURSES OF ACTIONS

Active Courses of Actions

Deny

Example:
- Blocking Connection
- ACL

Degrade

Example:
- Queuing
- Quality of Service (QoS)

Disrupt

Example:
- AntiVirus
- Data Execution Prevention
- Intrusion Prevention

Deceivce

Example:
- DNS redirect
- Honeypot

Destroy

Example:
Legal Measures

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

Passive Courses of Actions

Detection

Example:
- EDR
- Intrusion Detection
- AV
- Sysmon
- *

Discover

Example:
- Hunting with YARA rules
- Discovery searches with SIEM/EDR
- *

COURSES OF ACTIONS

Active Courses of Actions				Passive Courses of Actions	
Deny	Degrade	Disrupt	Deceivce	Detection	Discover
• Blocking Connection	• Queuing • Quality of	• Antivirus • Data • Intrusion Prevention	• DNS redirect	• EDR • Intrusion • Sysmon • *	• Hunting with YARA searches with SIEM/EDR • *
Destroy	Example: Legal Measures				

Critical or High:
At least 1 Active Security Measure + 1 Passive Action

Medium or Low:
At least 1 Active Security Measure, if not possible to resolve on time: apply 1 Passive Action

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

THE CHALLENGE

- So, why can't those patches be installed on time?

DELAY REASONS - 1

Resource Problem

- Low staffing, too many projects or different priorities communicated to the team can lead to too few engineers being able to properly test and roll out the needed updates on time

Possible Actionable Steps

- Document resource assignment over period of time
- Document what patches were not installed on what systems
- File a risk entry for the relevant systems and patches not installed OR for resources not being permitted

Suggested KPIs

- Number of delays due to resource problems
- Average number of days delays due to resource problems

DELAY REASONS - 2

Compatibility problem

- Business products or solutions can rely on fixed dependencies or tight setups which break when installing an update. This can for example happen when a company relies on a product that has long stopped being supported by the vendor or skills to advance your product have left the company.

Possible Actionable Steps

- Initiate project to update/redesign affected solution
- File a risk entry for the relevant systems and patches not installed OR for deprecated system still not being switched off
- Connect risk entry with the delayed patch (if only comments)

Suggested KPIs

- Number of delays due to compatibility problems
- Number of filed risk entries for deprecated systems

DELAY REASONS - 3

Bad SLA

- High SLA KPIs for products, bad service design, bad service management monitoring or combinations of these elements can lead to teams not being allowed to install patches on time. This can appear with a team only receiving change windows once a month or less but having patching times of 21 days or less.

Possible Actionable Steps

- Create “high impact security” flag for urgent changes
- Document the number of patches/systems needed to be installed per change window
- Influence change team when change windows are planned
- Escalate/file risk entry for bad service design in regard to SLA commitments

Suggested KPIs

- Number of delays due to unreasonable SLA

SLA = service level agreement

DELAY REASONS – 4

Support Problem

- The specific product version installed relies on a software component of another product (for example open source) that has been fixed in the original version, but not yet been updated by vendor you use your product version from.

Possible Actionable Steps

- Document the number of patches/systems affected
- Update process for partner evaluation to include “bad experiences with supplier” in decision management (correlated to possible risk they created)
- Escalate/file risk entry for slow supply of security fixes

Suggested KPIs

- Number of delays due to missing patch by partner
- Average number of days delays due to missing patch

THE PARTIES INVOLVED – 1ST DIMENSION

CSO/Legal
Risk Management

Operational
Technical Teams

Security Operation
Center

Supply Chain
Management

Security
Management

Focus: Create transparency for your management
Role: Take the lead in communication
Highlight: what systems are affected

Focus: Report patch delay
Role: Advice for patching priorisation
Highlight: what risk is created if patch is not installed

IT Service
Management

THE PARTIES INVOLVED – 1ST DIMENSION

CSO/Legal Risk Management

Focus:
- Do we get a contractual problem because of this?
- Is risk management already covering this?
- Do we need to report this to customers/top management?

Role:
- Last point of escalation

Language needed:
- „these customers/customer services are affected“
- „this reputation problem can occur“

Security Management

Focus:
- Is this affecting our compliance reporting?
- Are there controls that define responsibilites to handle this problem & are they being followed?

Role:
- Ensure all occuring security & compliance challenges are treated in an effective manner

Language needed:
- „this customer services can not be uphold if state A occurs“

THE PARTIES INVOLVED – 1ST DIMENSION

IT Service Management

Focus:
- Can we provide the services to our customers that we need to?

Role:
- Partner for including needs of technical team in it service processes (change/incident/problem mgmt)

Language needed:
- „we can't provide this availability to this service if…"

Supply Chain Management

Focus:
- Do our partners deliver the needed services in a useful (to us) way?

Role:
- Unify & coordinate dependencies to contracted partners

Language needed:
- „this partner is not acting to the required SLA…"

2ND DIMENSION OF FAILED VUL MANAGEMENT

Organisations & People

- Long term understaffed
- Wrong skills in teams

Information & technology

- No working standard installation & deinstallation routines

Value Streams & Processes

- Missing/bad software governance process

Partners & Suppliers

- Bad supplier management & partner has been out of support

THE PARTIES INVOLVED – 2ND DIMENSION

Human Resources

Operational Technical Teams

Security Operation Center

Architecture Management

Security Management/BCM

Focus: Create transparency for your management
Role: Take the lead in communication
Highlight: what systems are affected

Focus: Report patch delay
Role: Advice for patching priorisation
Highlight: what risk is created if patch is not installed

IT Governance

THE PARTIES INVOLVED – 2ND DIMENSION

Human Resources

Focus:
- Do we have the right skills on board for the direction we want to go as a company?

Role:
- Recruiting & retaining right skills aligned to company strategy

Language needed:
- „our employees need understanding X and training Y to be able to correctly assess Z

Security Management/BCM

Focus:
- Is this affecting our compliance reporting?
- Are there controls that define responsibilites to handle this problem & are they being followed?

Role:
- Ensure continuity of business services in extreme situations

Language needed:
- „this customer services can not be uphold if state A occurs“

THE PARTIES INVOLVED – 2ND DIMENSION

Architecture Management

Focus:
- Are our governing structures clear enough?

Role:
- Create structures & define frameworks to be followed in practice

Language needed:
- „this software/product does not fit in to the current process because…“
- „there is no governing process for X…“

IT Governance

Focus:
- Can we identify a responsible to solve problem X?

Role:
- Assign responsibilities in company & make sure, all topics are covered

Language needed:
- „in this occasion, team A is not responsible for product B, who needs to assist with solving X..“

POSSIBLE SOLUTIONS

None of the products mentioned here are personal endorsements..

- Containers [1]
- Automated patch installation [2]
- Virtual patching [3]
- Streamline your IT processes.. To threat driven vulnerability management

[1] https://www.docker.com/, https://www.ibm.com/de-de/cloud/containers

[2] https://www.dynatrace.com/support/help/setup-and-configuration/dynatrace-managed/operation/apply-operating-system-patches-to-a-node, https://www.tanium.com/products/tanium-patch/

[3] https://www.trenddefense.com/Vulnerability-Protection.asp, https://www.airlock.com/secure-access-hub/features/virtual-patching, https://owasp.org/www-community/Virtual_Patching_Best_Practices

BENFITS: KPI SUGGESTIONS

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	

LESSONS LEARNED

1

Analysing security events is never a binary thing

For every security problem there is never a black or white reason

2

Standardised IT service management processes are the foundation for mature security operations

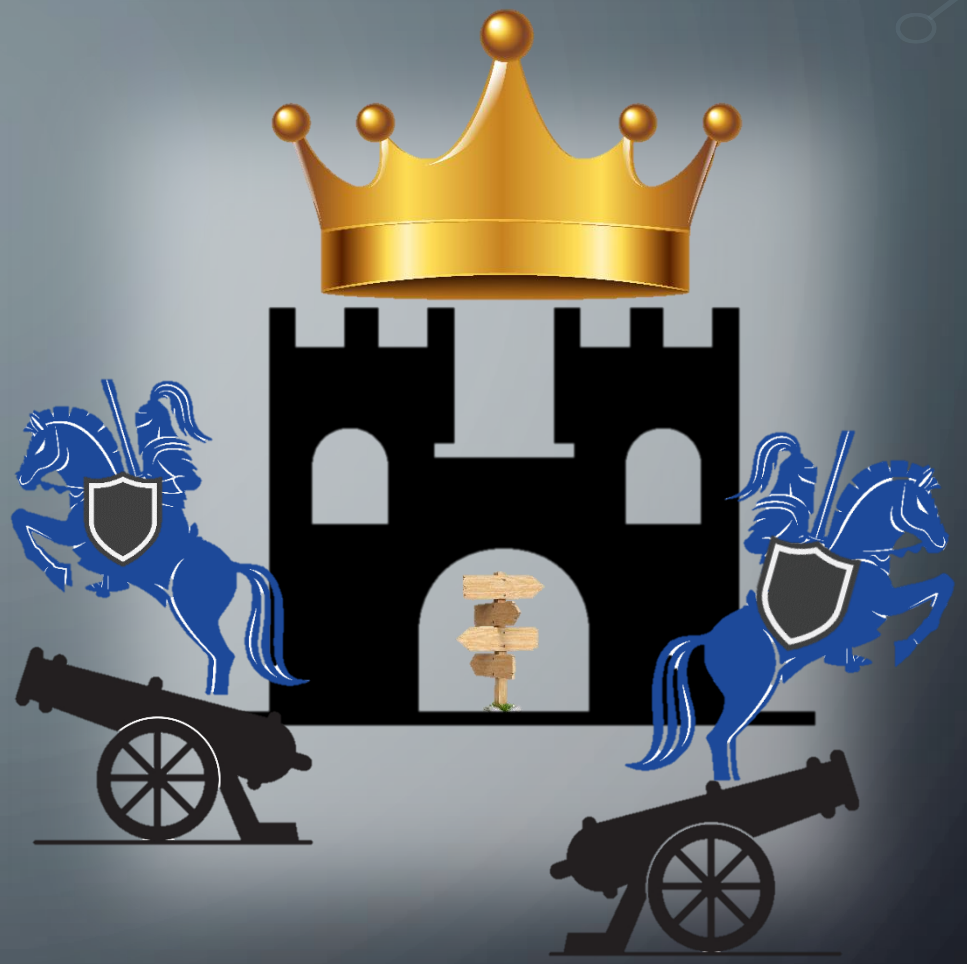
Change management
Incident management
Asset management
Problem management

3

Understanding the problem is fundamental to creating the right solutions

!

CALL TO ACTION



- Request fields to be added to your platform
- Create the data to document your pitfalls

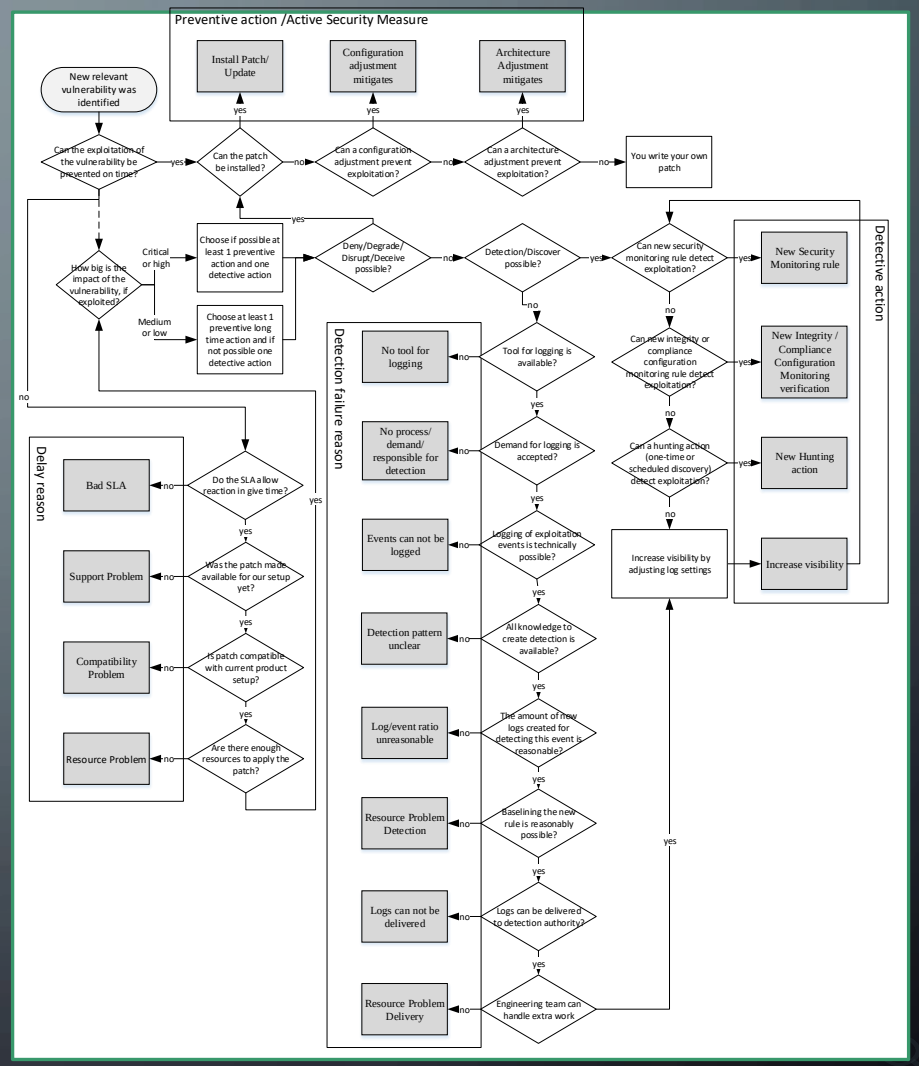
- Twitter: @d3sre
- More information on technical implementation can be found on https://github.com/d3sre/IntelligentProcessLifecycle

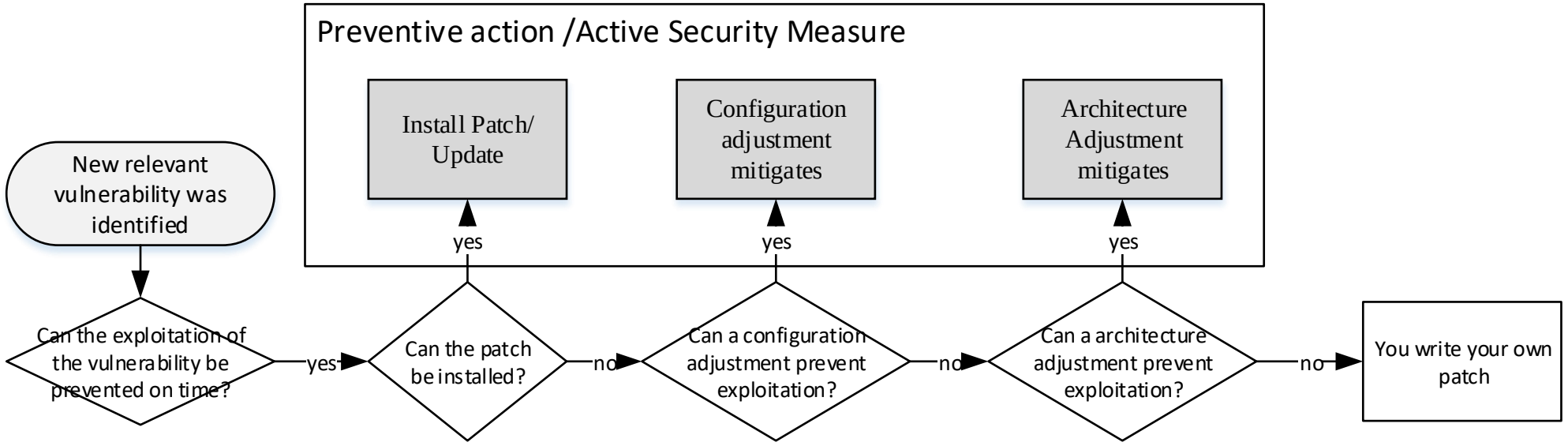
APPENDIX

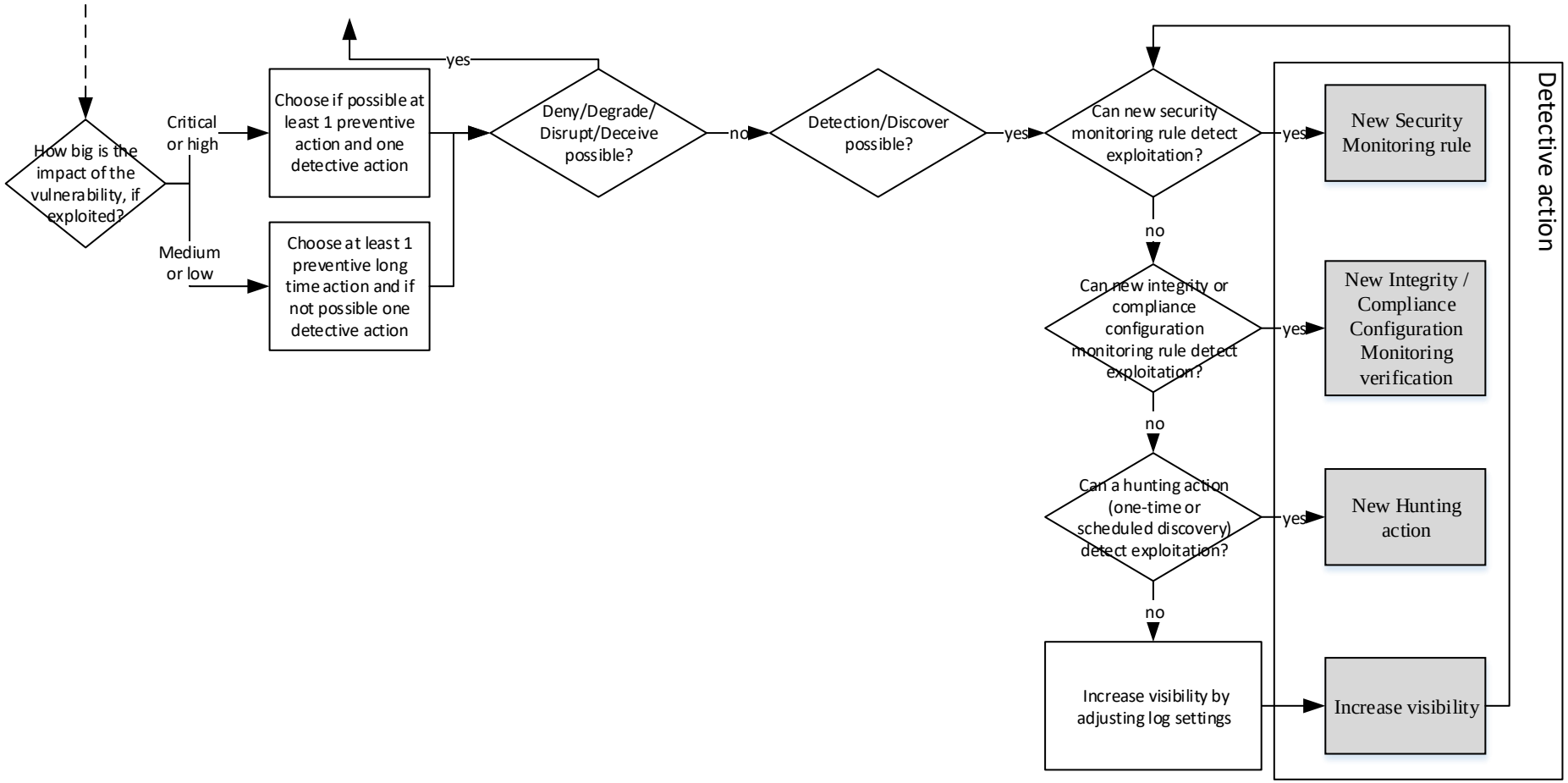
THE INTELLIGENT PROCESS LIFECYCLE OF ACTIVE CYBER DEFENDERS

Full paper:

- https://dl.acm.org/doi/10.1145/3499427




Preventive action /Active Security Measure
Install Patch/ Update
Configuration adjustment mitigates
Architecture Adjustment mitigates
New relevant vulnerability was identified
yes
yes
yes
Can the exploitation of the vulnerability be prevented on time?
yes
Can the patch be installed?
no
Can a configuration adjustment prevent exploitation?
no
Can a architecture adjustment prevent exploitation?
no
You write your own patch


How big is the impact of the vulnerability, if exploited?
Critical or high
Medium or low
Choose if possible at least 1 preventive action and one detective action
Choose at least 1 preventive long time action and if not possible one detective action
yes
Deny/Degrade/ Disrupt/Deceive possible?
no
Detection/Discover possible?
yes
Can new security monitoring rule detect exploitation?
yes
New Security Monitoring rule
no
Can new integrity or compliance configuration monitoring rule detect exploitation?
yes
New Integrity / Compliance Configuration Monitoring verification
no
Can a hunting action (one-time or scheduled discovery) detect exploitation?
yes
New Hunting action
no
Increase visibility by adjusting log settings
Increase visibility
Detective action