huld

Beyond tomorrow

Speaker

Name:
Mr. Tarmo Kellomäki

Occupation:
Director, Digital Security & Functional Safety, Huld Oy

Education:
MSc., Cyber Security (JYU)
MSc., Economics (JYU)

Background:
Background in military system development & operation, Cyber Defence, recent focus in industrial security

Other:
Board member in Suomen Automaatioseura Turvallisuus –section

Member of IEC TC65 WG10

Huld in Numbers

Huldians

500+

40+ Revenue (2021) M€

16 Offices

10 000+

Projects Done

Bold Ideas with Humane Touch

Digital Services & Software

Product Design & Development

Embedded Solutions

Safety & Security

Safety & Security

"Unique approach for protecting digitalized cyber-physical systems"

DIGITAL SECURITY

- Security Management
- Technical Security & Testing
- Industrial & Software Security
- Space Security
- Cloud & Digitalization Security
- Medical Device Security

CYBERSAFETY

- CyberSafety management
- CyberSafety assessment
- CyberSafety reporting

FUNCTIONAL SAFETY

- Safety Concepts
- Safety Development and V&V
- Safety Management
- Independent Safety Assessments (ISA)
- System Assessments
- Medical Safety

SERVICE MODELS

- Projects & Assignments
- Partnership

TEAM

- +30 experts
- 5 competence teams

C&A

Personnel:
CISSP, OSCP, OSWP, CySA+, ISO 27001 Lead Auditor, Azure & AWS security, IEC 61508

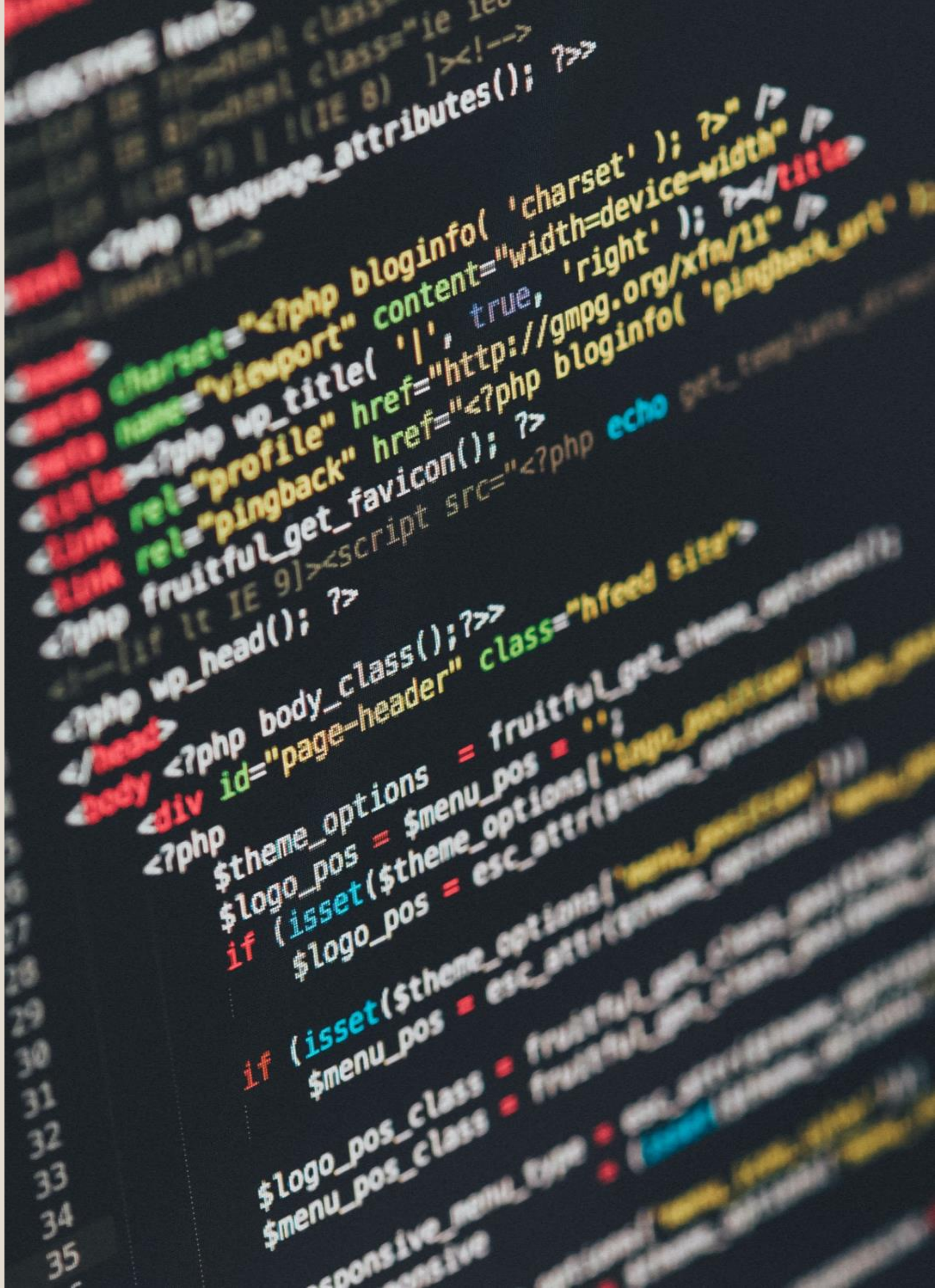
Company:

- ISA body accreditation
- ISO 13485 certification

Security by and for developers

Agenda

1. Security landscape
2. Basic security concepts
3. Secure software development?

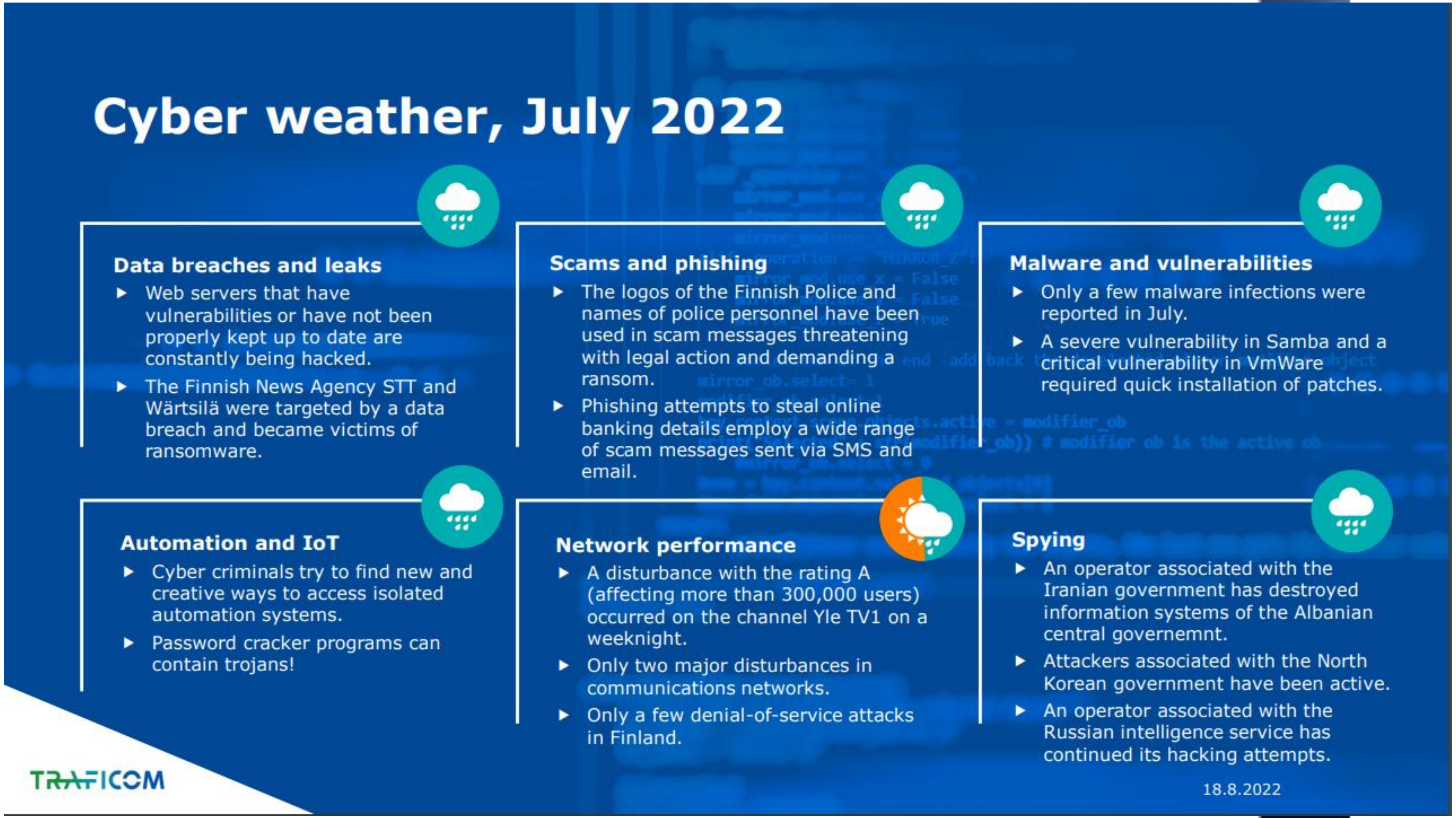


Security landscape

huld

Cyber Weather by Traficom

- Ransomware
- Phishing
- Data breaches & leaks
- Exploitation of system & technology vulnerabilities (Internet exposure)
- Attacks against industrial IoT systems



Cyber weather, July 2022

Data breaches and leaks

- Web servers that have vulnerabilities or have not been properly kept up to date are constantly being hacked.
- The Finnish News Agency STT and Wärtsilä were targeted by a data breach and became victims of ransomware.

Scams and phishing

- The logos of the Finnish Police and names of police personnel have been used in scam messages threatening with legal action and demanding a ransom.
- Phishing attempts to steal online banking details employ a wide range of scam messages sent via SMS and email.

Malware and vulnerabilities

- Only a few malware infections were reported in July.
- A severe vulnerability in Samba and a critical vulnerability in VmWare required quick installation of patches.

Automation and IoT

- Cyber criminals try to find new and creative ways to access isolated automation systems.
- Password cracker programs can contain trojans!

Network performance

- A disturbance with the rating A (affecting more than 300,000 users) occurred on the channel Yle TV1 on a weeknight.
- Only two major disturbances in communications networks.
- Only a few denial-of-service attacks in Finland.

Spying

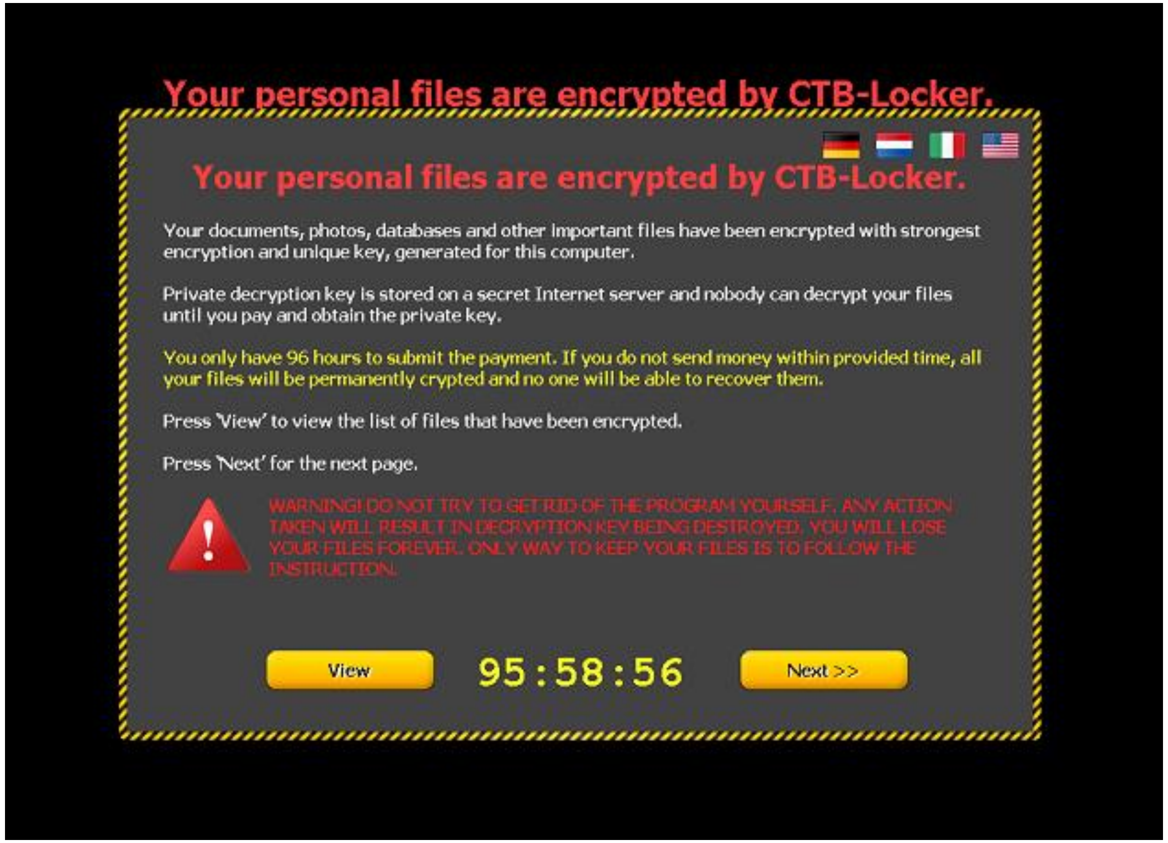
- An operator associated with the Iranian government has destroyed information systems of the Albanian central governemnt.
- Attackers associated with the North Korean government have been active.
- An operator associated with the Russian intelligence service has continued its hacking attempts.

TRAFICOM

18.8.2022

Ransomware

- Usually a **worm** (self-replicating malware)
- Encrypts machines it can spread to
- Modern ransomware can infect cloud services like Sharepoint Online
- Deletes shadow copies from the operating system
- Presents users with ransom note (usually asking for BTC)
- Promises decrypting the data if ransom is paid
- No guarantee you will get your data back



Your personal files are encrypted by CTB-Locker.

Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

How it usually start?

- Phishing
- Unknown USB drives
- **Third party components**
- Pirated software

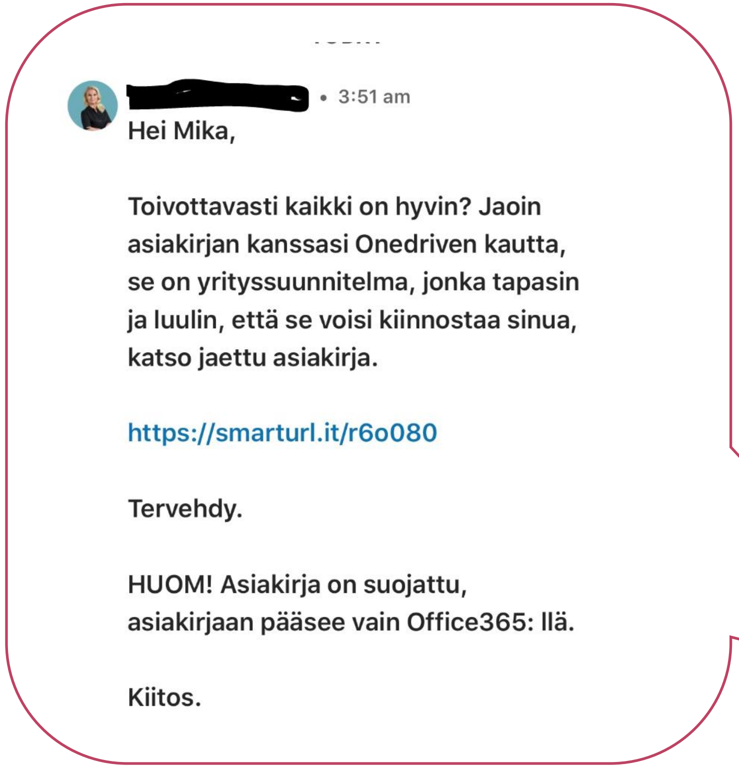
huld

Phishing

- A message meant to coerce the user to do something malicious
- “Hello, send me money, I am Nigerian prince”
- “Here is a free voucher, click this link!”
- “Hello, this is [ADMIN], please send me your password”

Phishing can take many different forms, not only e-mail!

Case Huld CEO



[redacted] • 3:51 am

Hei Mika,

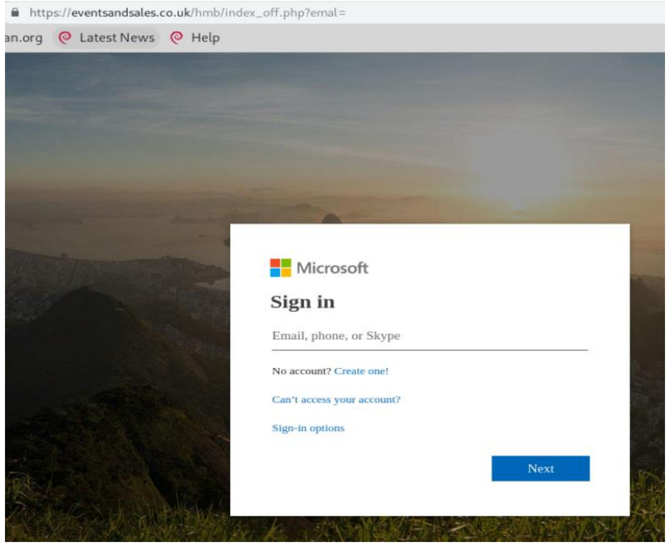
Toivottavasti kaikki on hyvin? Jaoin asiakirjan kanssasi Onedriven kautta, se on yrityssuunnitelma, jonka tapasin ja luulin, että se voisi kiinnostaa sinua, katso jaettu asiakirja.

https://smarturl.it/r6o080

Tervehdy.

HUOM! Asiakirja on suojattu, asiakirjaan pääsee vain Office365: llä.

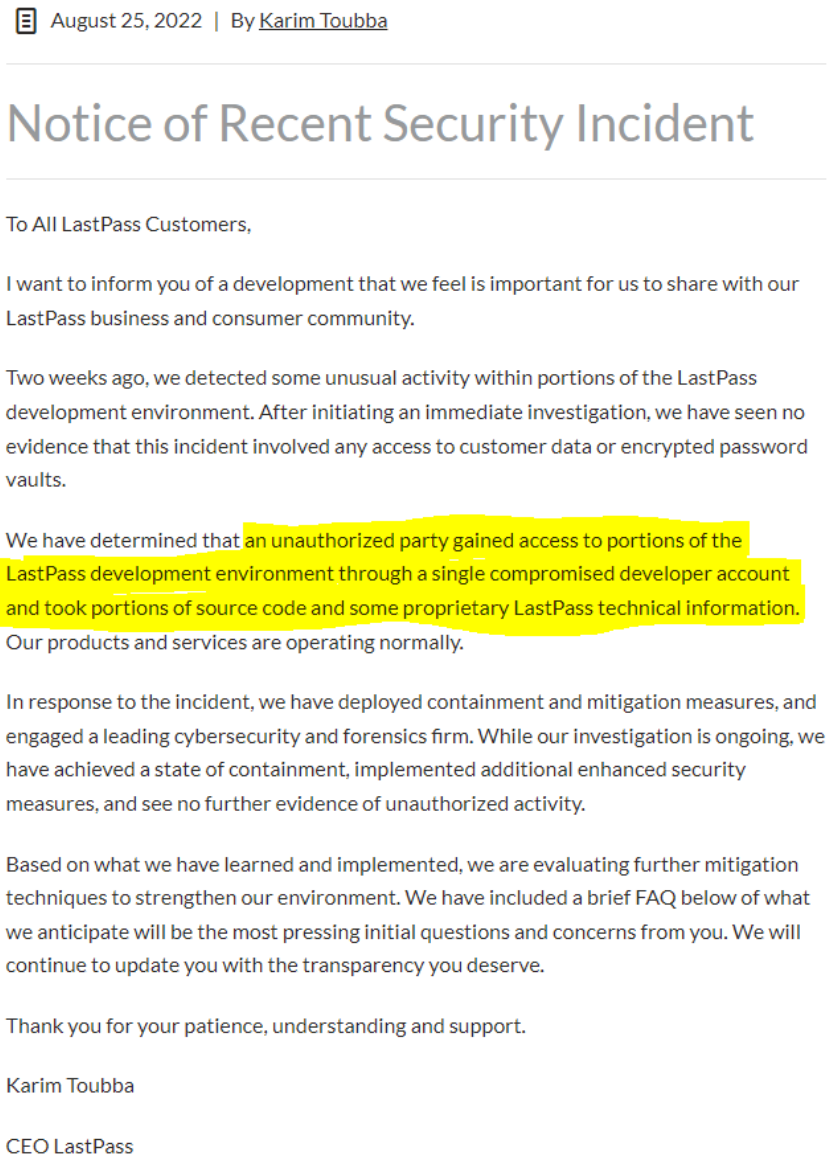
Kiitos.



https://eventsandsales.co.uk/hmb/index_off.php?emal=

Data breach - LastPass

- Unauthorized access to development environment from developer account.
  - Brute-force attack? MFA not in use? Phishing?
- Portions of source code stolen
- Security of development environment?



August 25, 2022 | By Karim Toubba

Notice of Recent Security Incident

To All LastPass Customers,

I want to inform you of a development that we feel is important for us to share with our LastPass business and consumer community.

Two weeks ago, we detected some unusual activity within portions of the LastPass development environment. After initiating an immediate investigation, we have seen no evidence that this incident involved any access to customer data or encrypted password vaults.

We have determined that an unauthorized party gained access to portions of the LastPass development environment through a single compromised developer account and took portions of source code and some proprietary LastPass technical information. Our products and services are operating normally.

In response to the incident, we have deployed containment and mitigation measures, and engaged a leading cybersecurity and forensics firm. While our investigation is ongoing, we have achieved a state of containment, implemented additional enhanced security measures, and see no further evidence of unauthorized activity.

Based on what we have learned and implemented, we are evaluating further mitigation techniques to strengthen our environment. We have included a brief FAQ below of what we anticipate will be the most pressing initial questions and concerns from you. We will continue to update you with the transparency you deserve.

Thank you for your patience, understanding and support.

Karim Toubba

CEO LastPass

Internet exposure - Open source intelligence

Information gathering is all the time easier using services and tools like Shodan.io, Amass or Maltego.

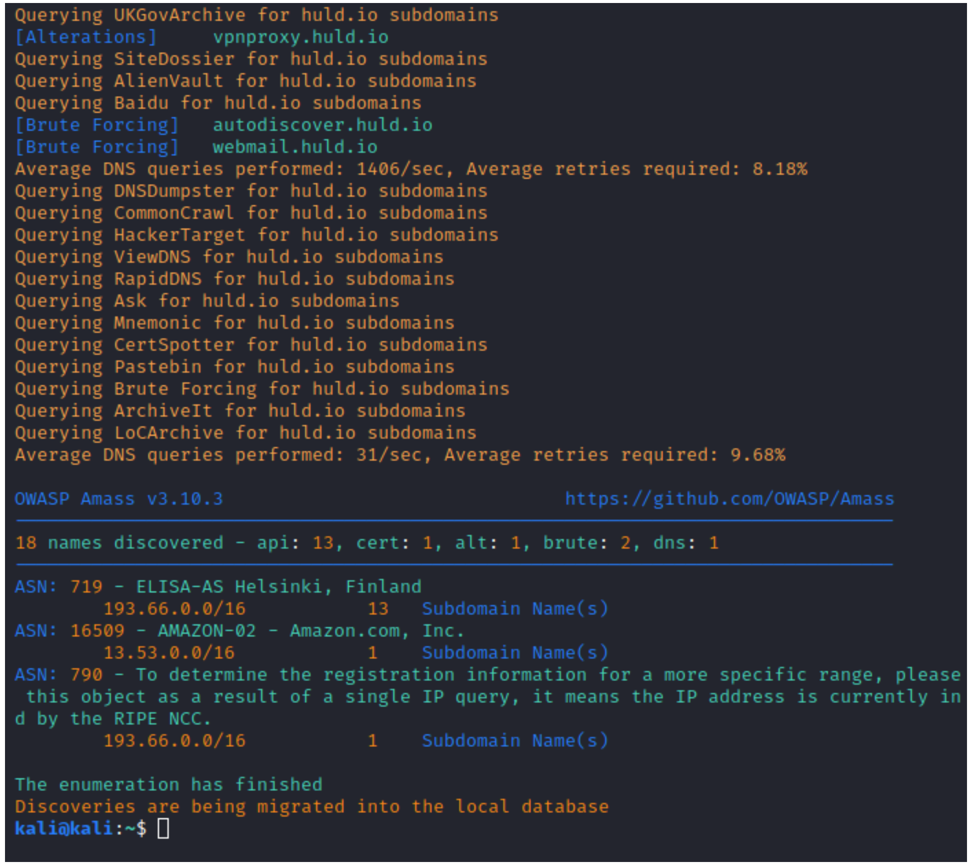
Public information (websites, email addresses, phone numbers, IP addresses, DNS entries etc) get indexed by search engines.

Company domain:

- *company.com*

Dev environment:

- *dev.company.com*

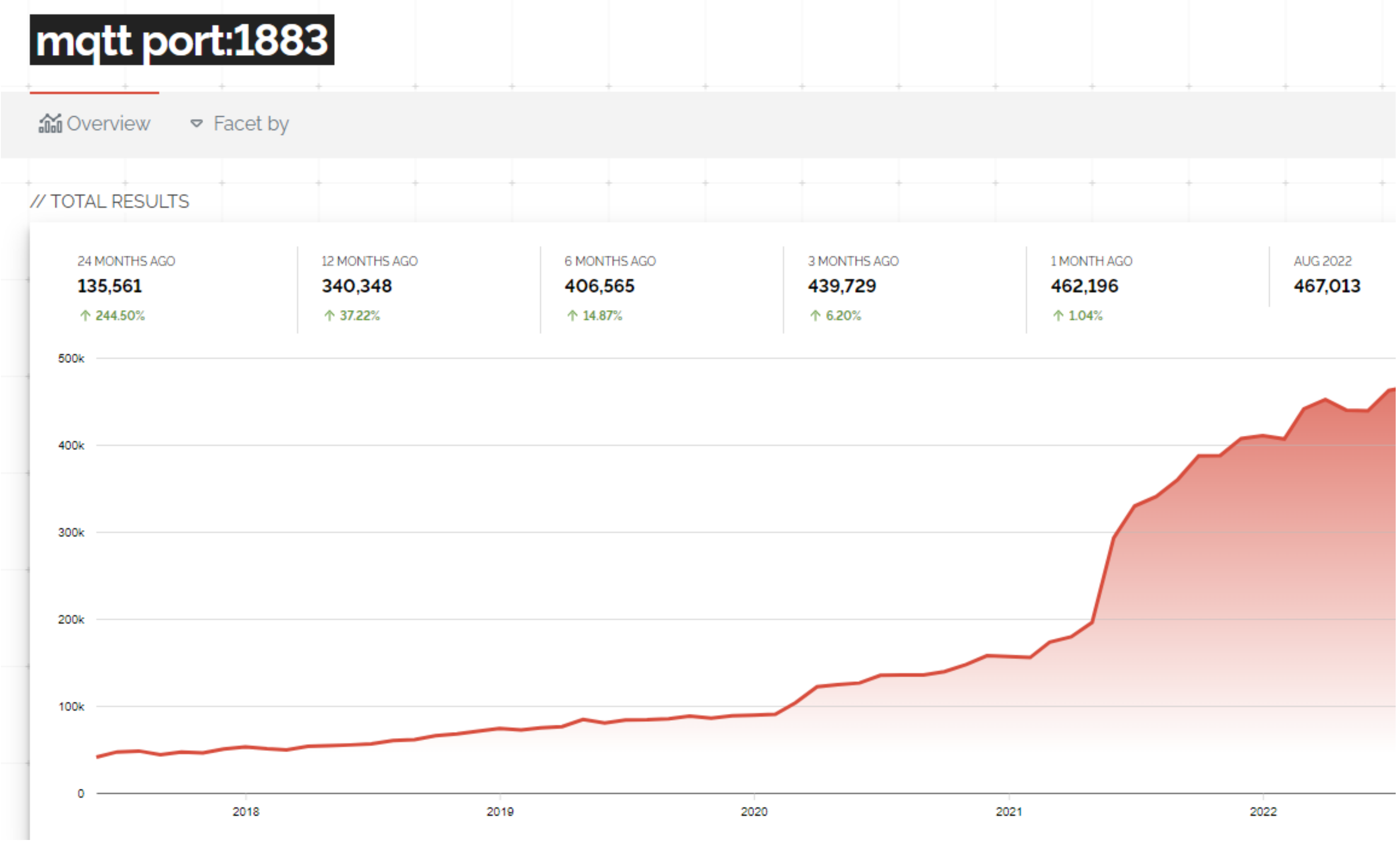


```
Querying UKGovArchive for huld.io subdomains
[Alterations]     vpnproxy.huld.io
Querying SiteDossier for huld.io subdomains
Querying AlienVault for huld.io subdomains
Querying Baidu for huld.io subdomains
[Brute Forcing]   autodiscover.huld.io
[Brute Forcing]   webmail.huld.io
Average DNS queries performed: 1406/sec, Average retries required: 8.18%
Querying DNSDumpster for huld.io subdomains
Querying CommonCrawl for huld.io subdomains
Querying HackerTarget for huld.io subdomains
Querying ViewDNS for huld.io subdomains
Querying RapidDNS for huld.io subdomains
Querying Ask for huld.io subdomains
Querying Mnemonic for huld.io subdomains
Querying CertSpotter for huld.io subdomains
Querying Pastebin for huld.io subdomains
Querying Brute Forcing for huld.io subdomains
Querying ArchiveIt for huld.io subdomains
Querying LoCArchive for huld.io subdomains
Average DNS queries performed: 31/sec, Average retries required: 9.68%

OWASP Amass v3.10.3                                  https://github.com/OWASP/Amass
--------------------------------------------------------------------------------
18 names discovered - api: 13, cert: 1, alt: 1, brute: 2, dns: 1
--------------------------------------------------------------------------------
ASN: 719 - ELISA-AS Helsinki, Finland
        193.66.0.0/16           13    Subdomain Name(s)
ASN: 16509 - AMAZON-02 - Amazon.com, Inc.
        13.53.0.0/16            1     Subdomain Name(s)
ASN: 790 - To determine the registration information for a more specific range, please
 this object as a result of a single IP query, it means the IP address is currently in
d by the RIPE NCC.
        193.66.0.0/16           1     Subdomain Name(s)

The enumeration has finished
Discoveries are being migrated into the local database
kali@kali:~$ ▯
```

IoT vulnerabilities

Mqtt port: 1883

No encryption mechanism (TLS)



mqtt port:1883

// TOTAL RESULTS

24 MONTHS AGO	12 MONTHS AGO	6 MONTHS AGO	3 MONTHS AGO	1 MONTH AGO	AUG 2022
135,561	340,348	406,565	439,729	462,196	467,013
↑ 244.50%	↑ 37.22%	↑ 14.87%	↑ 6.20%	↑ 1.04%	

Introduction to information and cyber security

Information Security?

Digital Security?

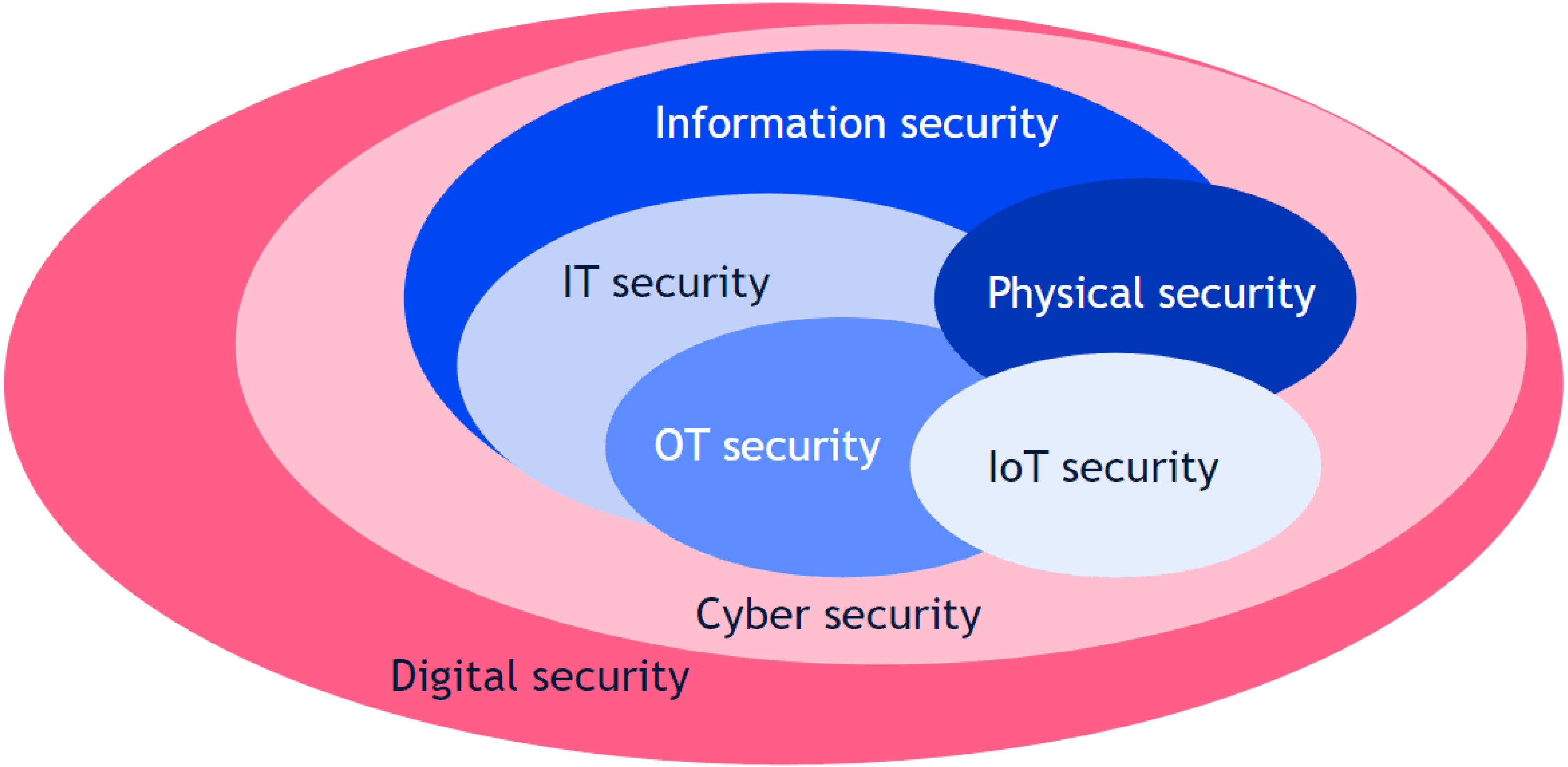
Cyber Security?

Physical Security?

IoT Security?

IT Security?

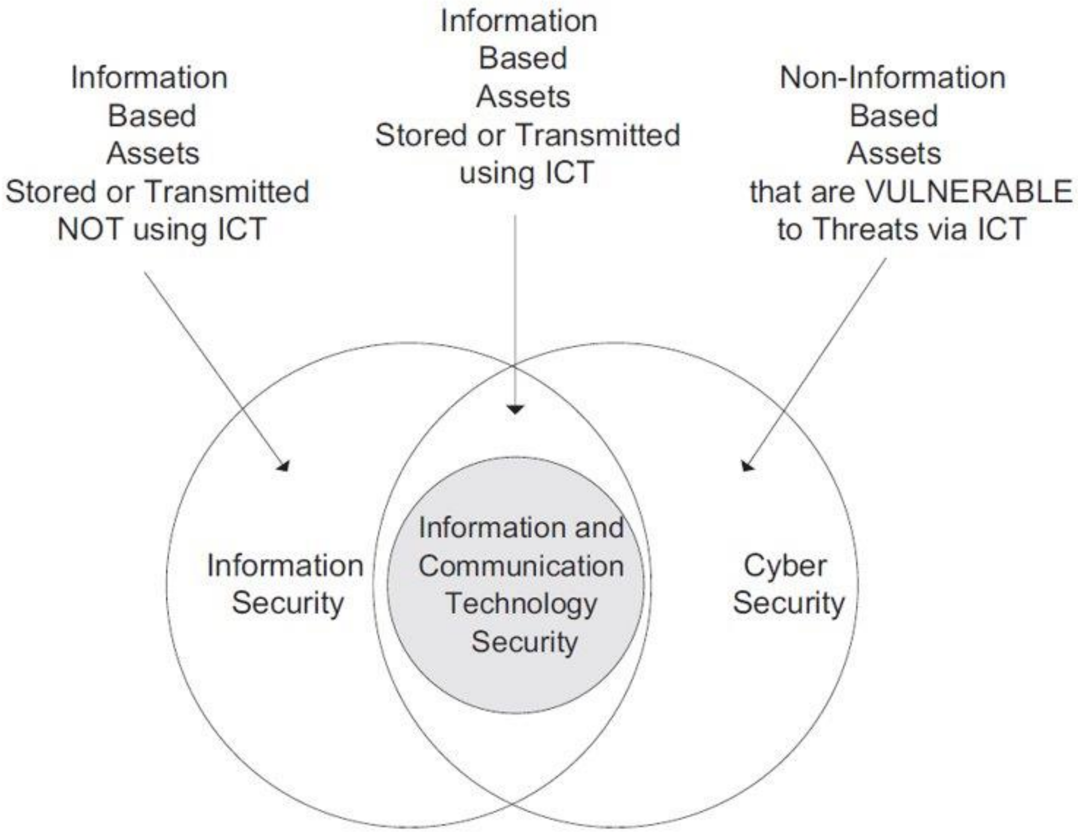
Digital security encompasses all

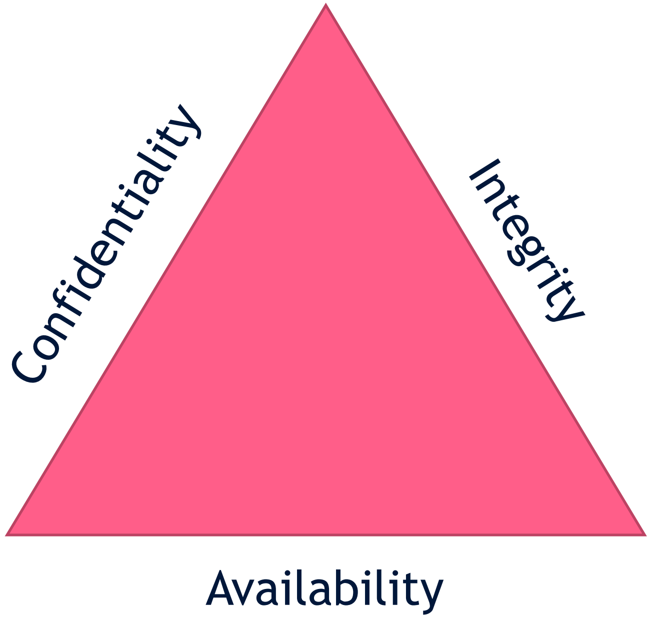


Source: Gartner

What’s the difference?

Information versus cyber security


Information Based Assets Stored or Transmitted NOT using ICT
Information Based Assets Stored or Transmitted using ICT
Non-Information Based Assets that are VULNERABLE to Threats via ICT
Information Security
Information and Communication Technology Security
Cyber Security



Concepts

Risk

- Probability x harmfulness or severity of injury/uncertainty
- Risk is the impact of uncertainty on the achievement of the objectives
- Can be positive or negative

Threat (security threat)

- potentially adverse event or trajectory that is exposed to information security and, if it occurs, jeopardises it

Vulnerability

- vulnerability to security threats
- the vulnerability may be any weakness that allows damage to be realised or can be used to cause damage

Asset (suojattava kohde)

- Anything material or immaterial thing that has value to an organization

Risk treatment

- Risk prevention or elimination
- Change in the likelihood of a risk
- Conscious retention, tolerance or addition of risk
- Sharing a risk with another party

Residual risk

- Risk remaining after risk treatment

Security concepts & relationship

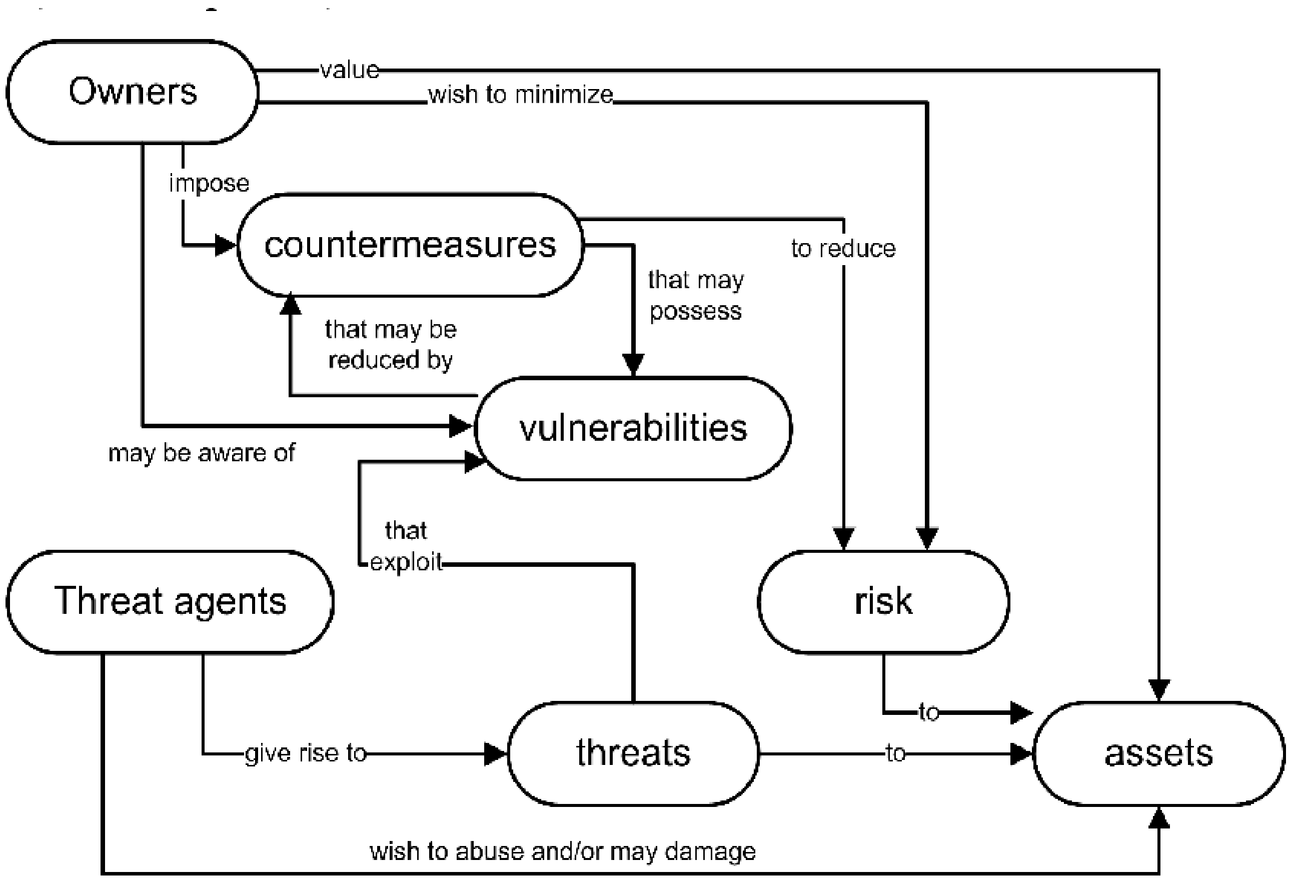


Figure 6. Security concepts and relationships, from ISO/IEC 15408-1:1999(E) (ISO/IEC, 1999).

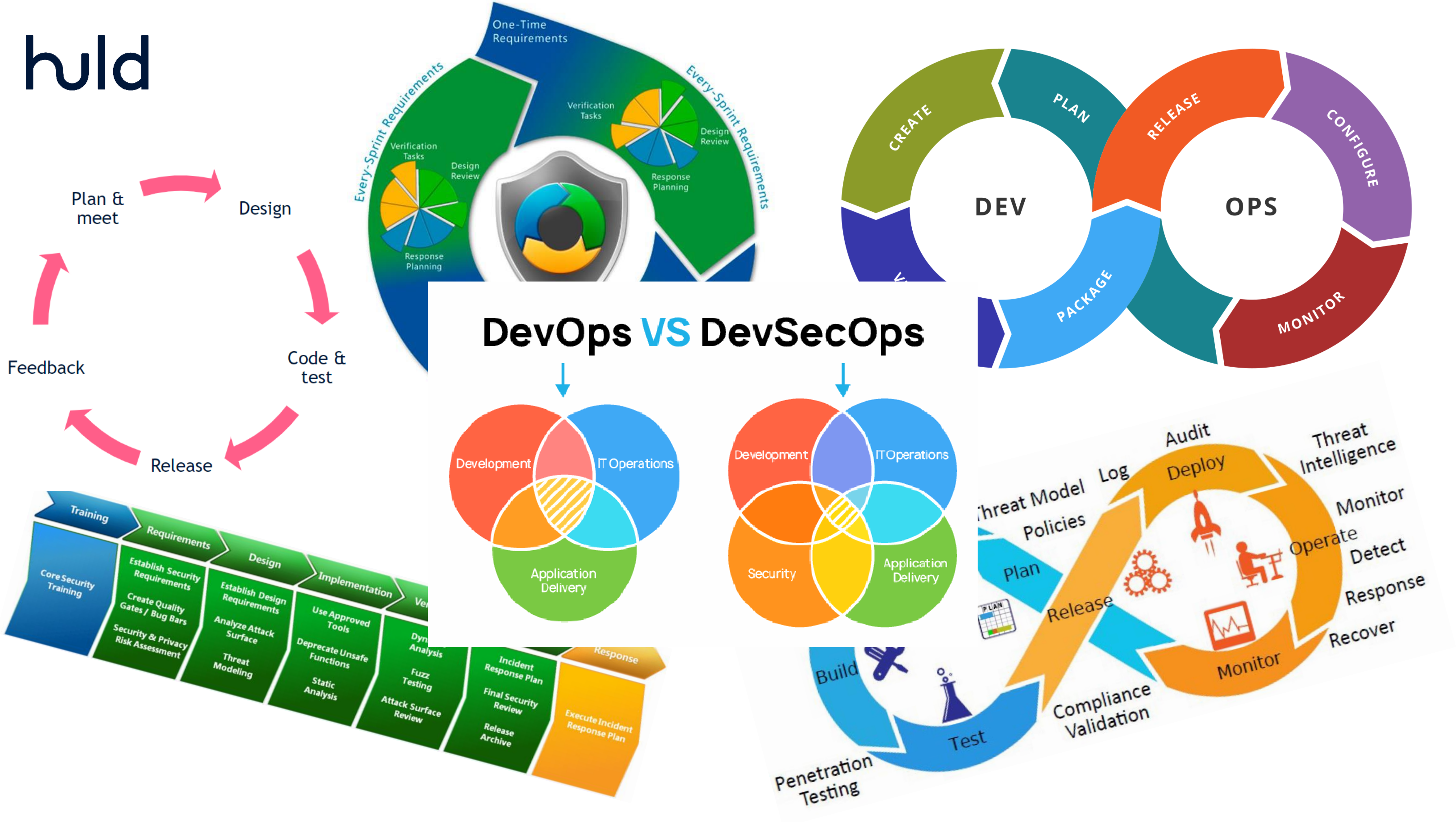
- Asset: Client data
- Owner: Company x
- Threat: Unauthorised access
- Threat agent: Employee, criminal
- Risk: Possibility of unauthorised access
- Countermeasures (security controls): Data encryption, MFA user authentication, logging

huld

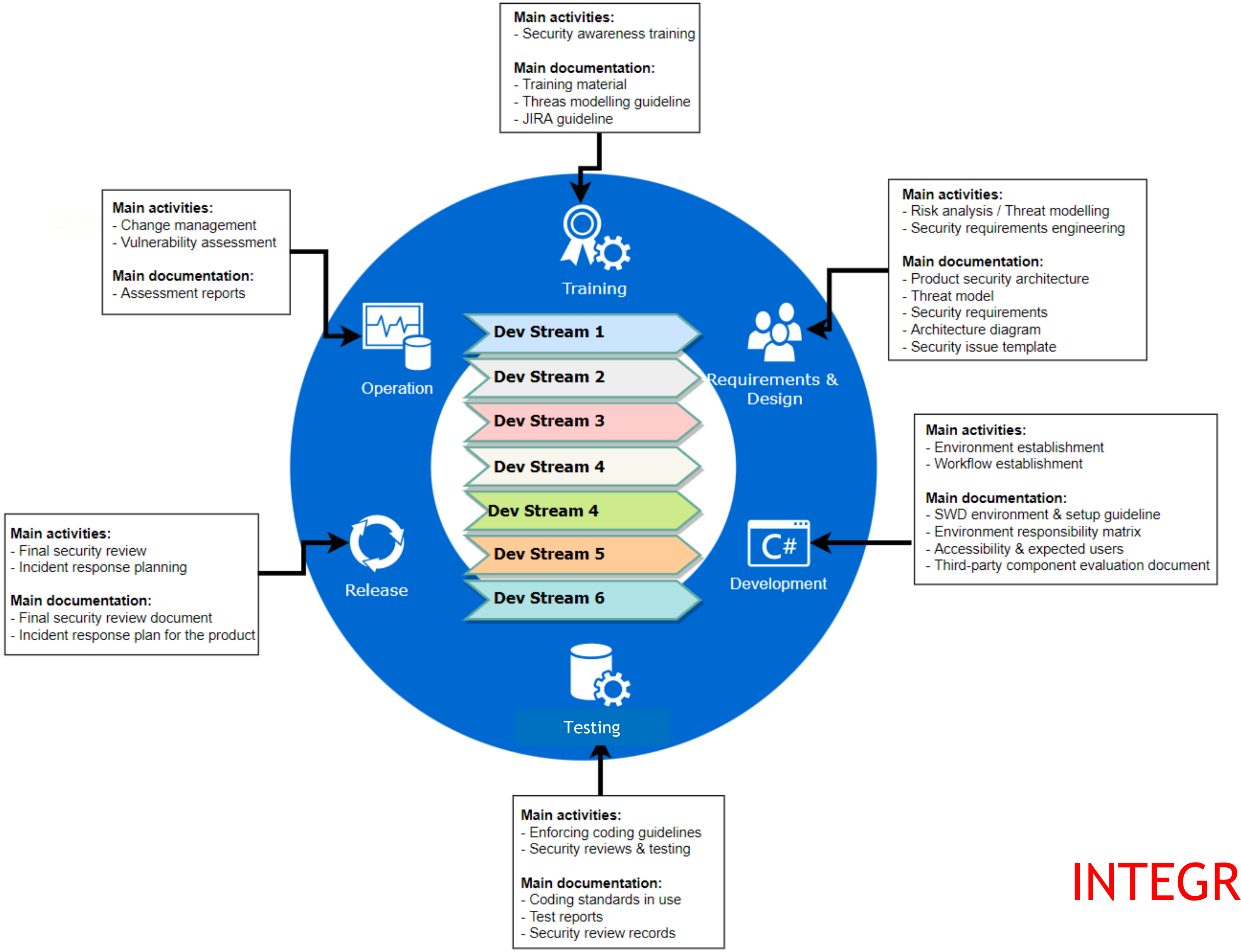
Which ingredients make secure software development?

huld

DevOps VS DevSecOps



From “normal” SDLC to secure SDLC



Main activities:
- Security awareness training

Main documentation:
- Training material
- Threas modelling guideline
- JIRA guideline

Main activities:
- Risk analysis / Threat modelling
- Security requirements engineering

Main documentation:
- Product security architecture
- Threat model
- Security requirements
- Architecture diagram
- Security issue template

Main activities:
- Environment establishment
- Workflow establishment

Main documentation:
- SWD environment & setup guideline
- Environment responsibility matrix
- Accessibility & expected users
- Third-party component evaluation document

Main activities:
- Enforcing coding guidelines
- Security reviews & testing

Main documentation:
- Coding standards in use
- Test reports
- Security review records

Main activities:
- Final security review
- Incident response planning

Main documentation:
- Final security review document
- Incident response plan for the product

Main activities:
- Change management
- Vulnerability assessment

Main documentation:
- Assessment reports

At minimum:

- Security awareness of developers
- Threat modelling
- Definition of security requirements & controls
- Security reviews & testing
- Hardened dev environment and products

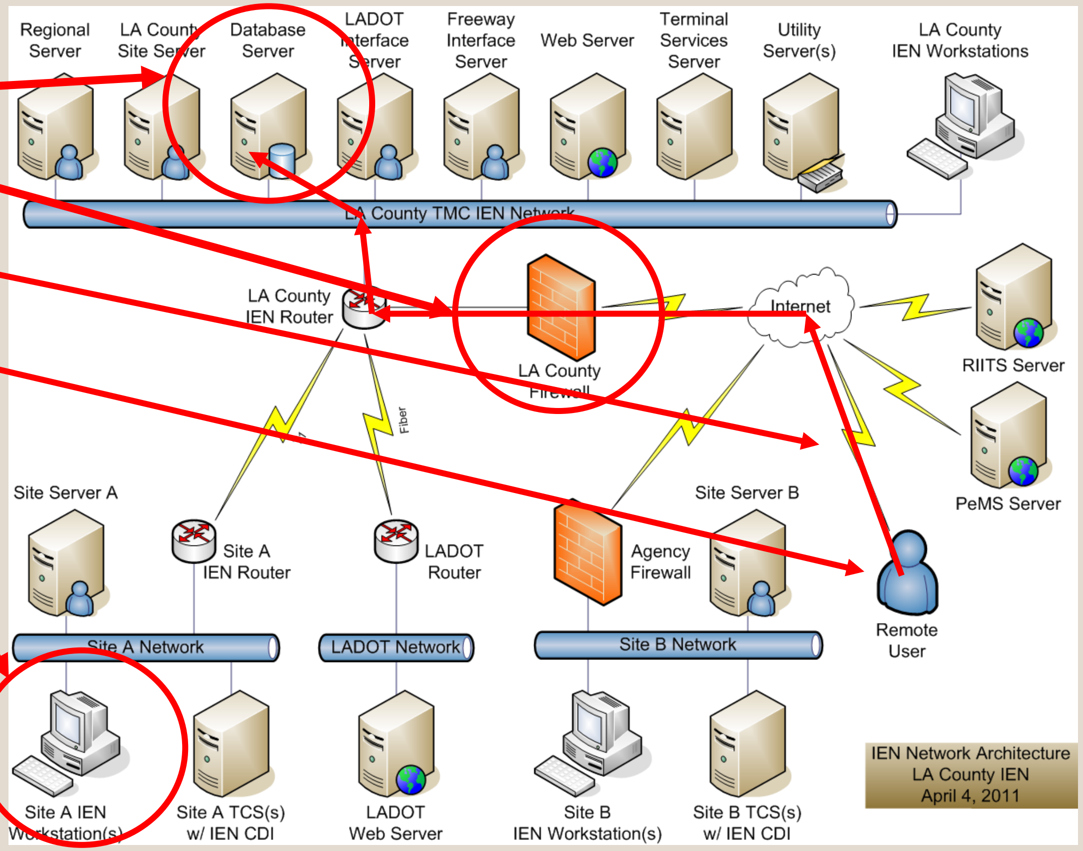
INTEGRATE SECURITY PRACTISES!

Activities

Threat modelling / attack-surface mapping

Process:

1. System architecture walkthrough
2. Identification and listing critical system assets
3. Identification of dataflow (information stream) in system vs. STRIDE
4. Selected use cases vs. threats
   Abuse case identification (threat actors)
   System flaw identification (system owner)
5. Security requirements elicitation (initial ideas / thoughts)



Possible tools & guidelines:

- ✓ ENISA Threat Taxonomy
- ✓ **STRIDE**, DREAD & TRIM -mnemonics
- ✓ BSI IT Grundschutz Catalogues
- ✓ OWASP ASVS
- ✓ CIS Critical Security Controls
- ✓ NIST SP 800

Sources of security requirements

Compliance

- Legal
- Standards
- Business domain

Customers and users

- Business need
- Threat modelling
- Use cases

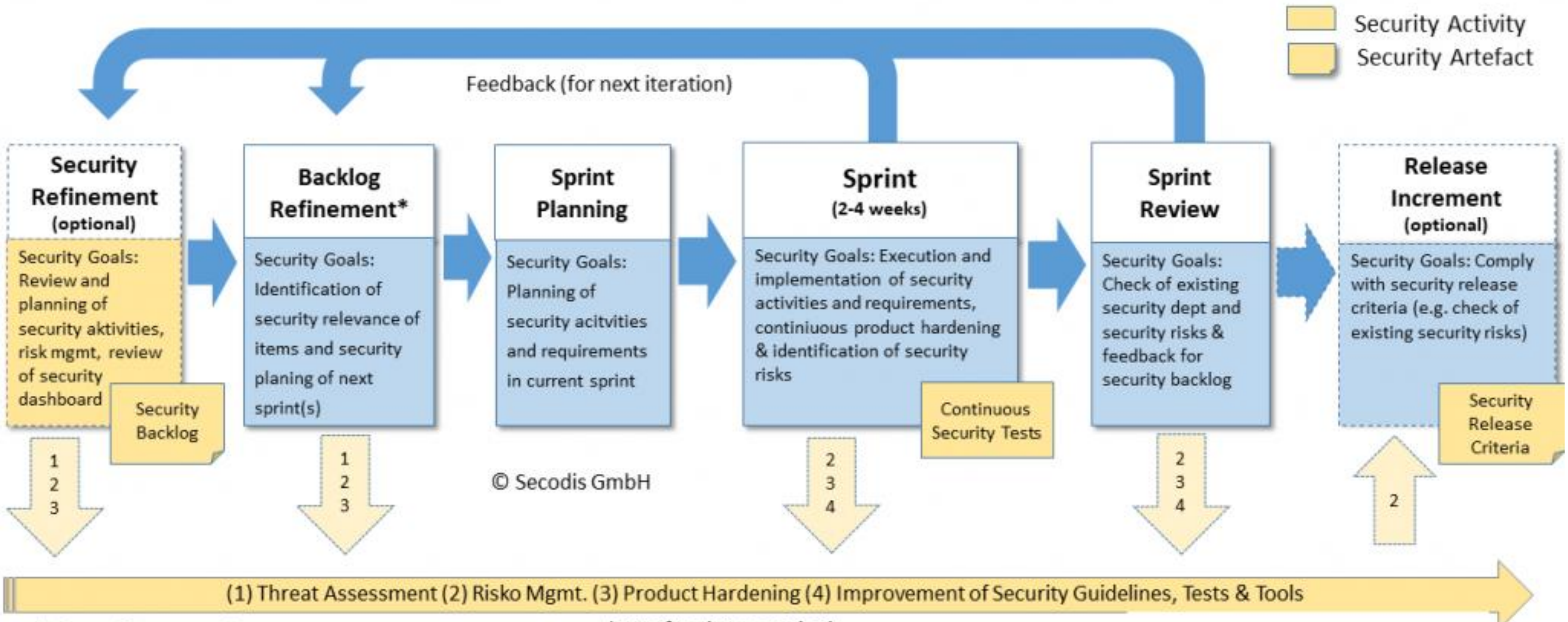
Common best practices and frameworks

- OWASP
  - Top 10
  - ASVS
- Cloud Security Alliance (CSA)
- CIS

Technology

- Vendor documentation
- Best practices
- Guidelines

Secure agile practices



Security Activity

Security Artefact

Feedback (for next iteration)

Security Refinement (optional)

Security Goals: Review and planning of security aktivities, risk mgmt, review of security dashboard

Security Backlog

1 2 3

Backlog Refinement*

Security Goals: Identification of security relevance of items and security planing of next sprint(s)

1 2 3

Sprint Planning

Security Goals: Planning of security acitvities and requirements in current sprint

© Secodis GmbH

Sprint (2-4 weeks)

Security Goals: Execution and implementation of security activities and requirements, continiuous product hardening & identification of security risks

Continuous Security Tests

2 3 4

Sprint Review

Security Goals: Check of existing security dept and security risks & feedback for security backlog

2 3 4

Release Increment (optional)

Security Goals: Comply with security release criteria (e.g. check of existing security risks)

Security Release Criteria

2

(1) Threat Assessment (2) Risko Mgmt. (3) Product Hardening (4) Improvement of Security Guidelines, Tests & Tools

(out of Sprint execution)

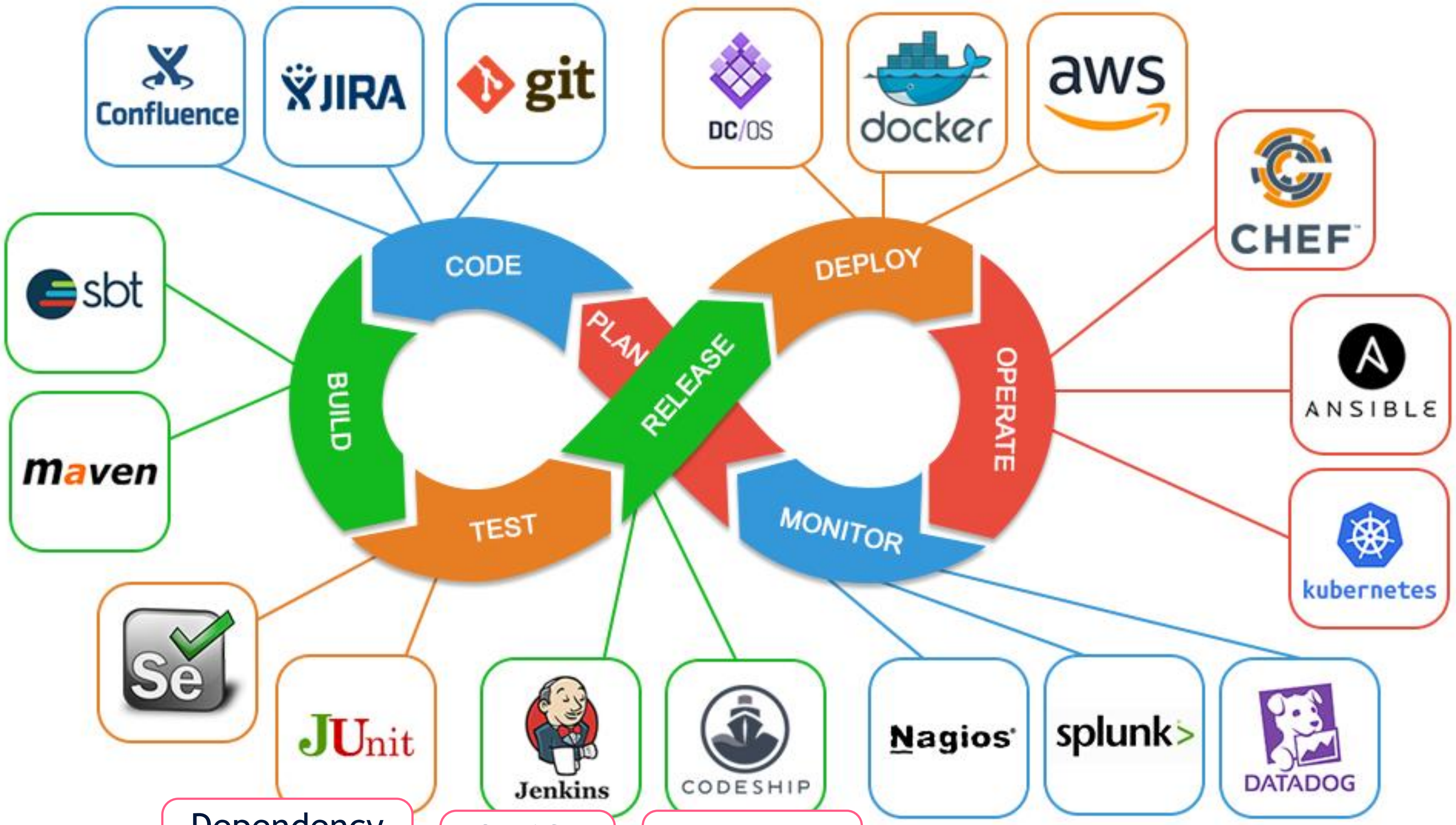
*Aka Backlog Grooming

Dev Environment

Hardened environment

- Threat modeling => which are the main threats of the dev enviroment
- Data classification => where to store sensitive data?
- Access rights => how needs to gain access to where?

huld Security and continuous integration



OpenVAS/GVM, Nessus

Dependency Track

OWASP ZAP

SAST
SonarQube, ...

huld Security analysis & testing

Static Analysis—identifies the exact location of weaknesses by analyzing the software without executing it.

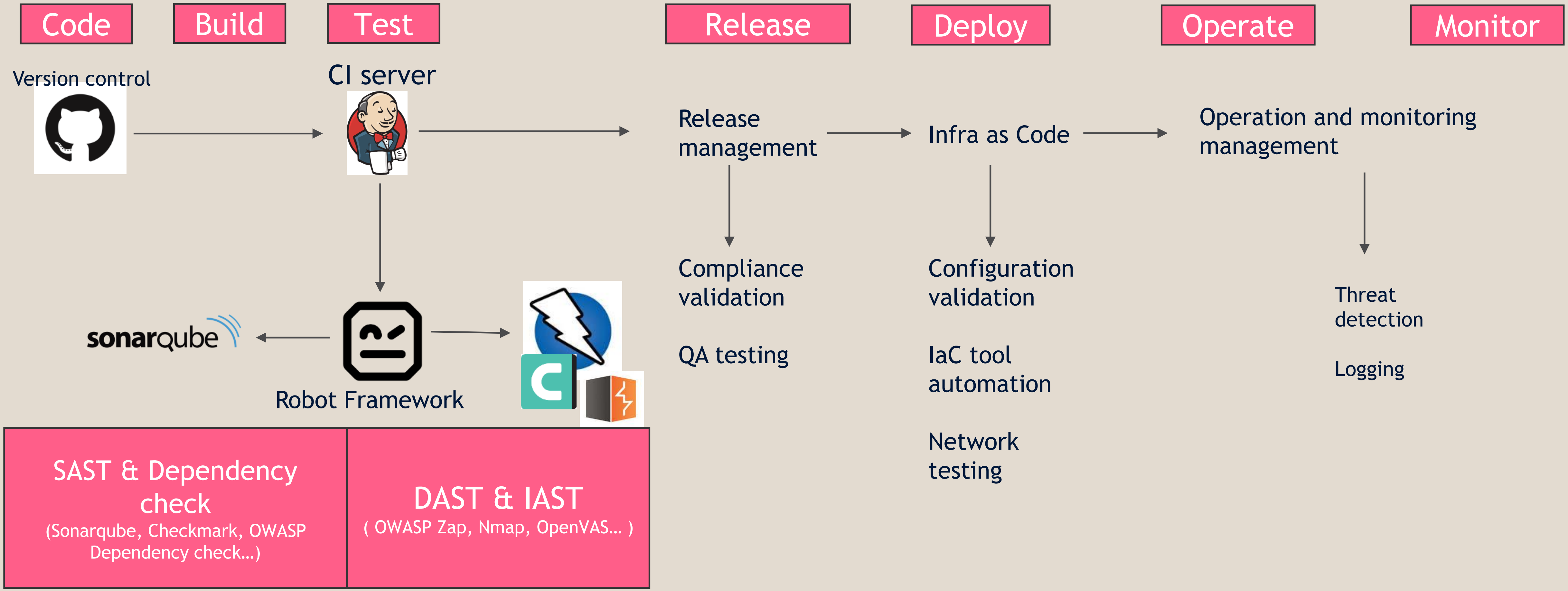
Dynamic Analysis—identifies weaknesses by running the software, helping find infrastructure flaws and patch errors.

Vulnerability Scanning—injects malicious inputs against running software to check how the program reacts. Mostly used to scan applications with a web interface.

Fuzzing—involves giving invalid, random data to a program, to check for access protocols and file formats. The test helps find bugs that humans often miss by generating random input and try all possible variations.

Third-party penetration testing—the tester simulates an attack to discover coding or system configuration flaws, and discover vulnerabilities a real attacker can exploit. It is required that the tester is an external party not connected to the team.

Security Test Automation



Code

Build

Test

Release

Deploy

Operate

Monitor

Version control

CI server

Robot Framework

sonarqube

SAST & Dependency check

(Sonarqube, Checkmark, OWASP Dependency check…)

DAST & IAST

(OWASP Zap, Nmap, OpenVAS…)

Release management

Compliance validation

QA testing

Infra as Code

Configuration validation

IaC tool automation

Network testing

Operation and monitoring management

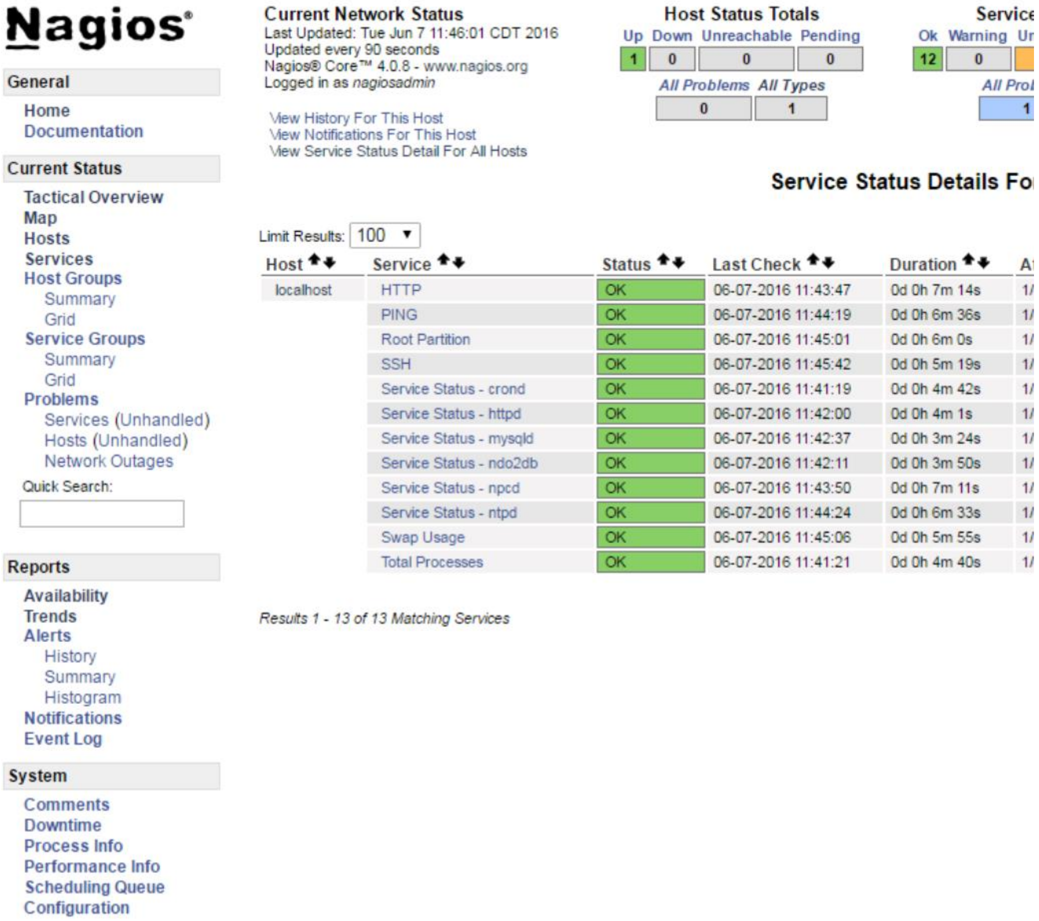
Threat detection

Logging

DevOps monitoring

Traditional network and service monitoring versus advanced application monitoring

- Nagios
  - Host and service monitoring
  - Manual configuration
  - Plugin architecture to add targets
- Dynatrace
  - Application performance insights
  - Dynamic configuration by the agent
  - Limited number of supported technologies



Current Network Status
Last Updated: Tue Jun 7 11:46:01 CDT 2016
Updated every 90 seconds
Nagios® Core™ 4.0.8 - www.nagios.org
Logged in as *nagiosadmin*

View History For This Host
View Notifications For This Host
View Service Status Detail For All Hosts

Host Status Totals

Up	Down	Unreachable	Pending
1	0	0	0

All Problems	*All Types*
0	1

Service

Ok	Warning	Ur
12	0	

All Prol
1

Service Status Details Fo

Limit Results: 100 ▼

Host	Service	Status	Last Check	Duration	A
localhost	HTTP	OK	06-07-2016 11:43:47	0d 0h 7m 14s	1/
	PING	OK	06-07-2016 11:44:19	0d 0h 6m 36s	1/
	Root Partition	OK	06-07-2016 11:45:01	0d 0h 6m 0s	1/
	SSH	OK	06-07-2016 11:45:42	0d 0h 5m 19s	1/
	Service Status - crond	OK	06-07-2016 11:41:19	0d 0h 4m 42s	1/
	Service Status - httpd	OK	06-07-2016 11:42:00	0d 0h 4m 1s	1/
	Service Status - mysqld	OK	06-07-2016 11:42:37	0d 0h 3m 24s	1/
	Service Status - ndo2db	OK	06-07-2016 11:42:11	0d 0h 3m 50s	1/
	Service Status - npcd	OK	06-07-2016 11:43:50	0d 0h 7m 11s	1/
	Service Status - ntpd	OK	06-07-2016 11:44:24	0d 0h 6m 33s	1/
	Swap Usage	OK	06-07-2016 11:45:06	0d 0h 5m 55s	1/
	Total Processes	OK	06-07-2016 11:41:21	0d 0h 4m 40s	1/

Results 1 - 13 of 13 Matching Services

Other considerations - Push versus pull updates

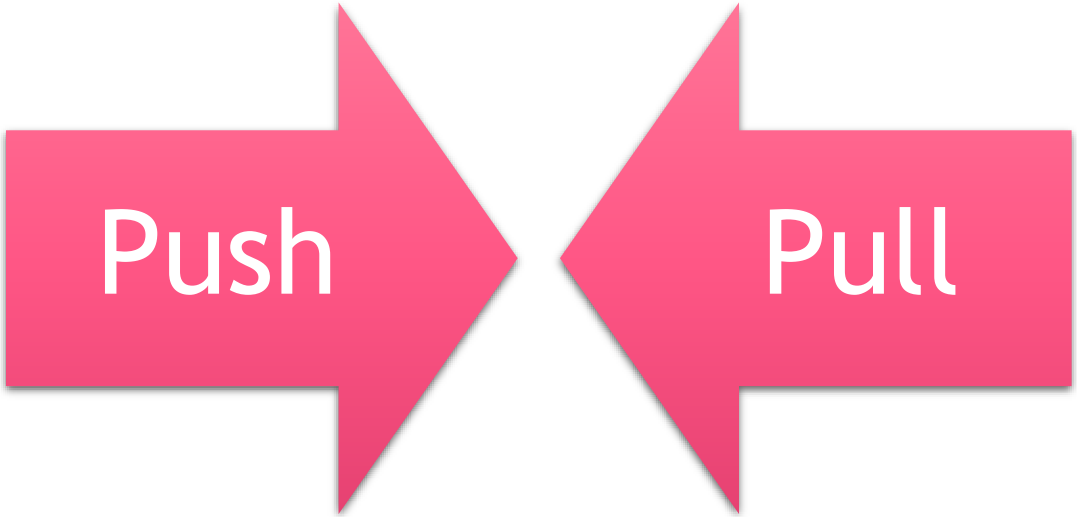
Planned updates versus immediate updates

Open source component updates are not pushed to users automatically

Automatic update decreases risk of usage of outdated, vulnerable versions of software

Consider security risks of automatic updates

- Operating environments are hardly ever identical
- Rollback procedure automation



Push

Pull

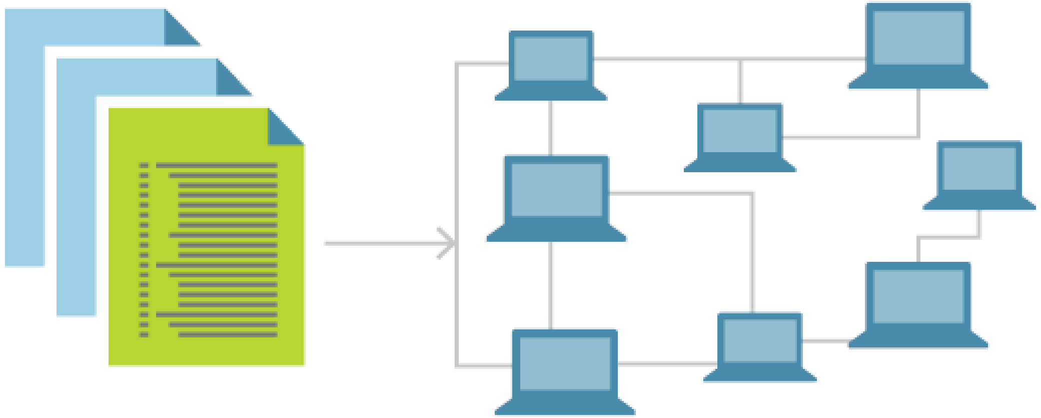
Other considerations - Infrastructure as Code (IaC)

Automated infrastructure building

- Automated security checks
- Configuration validation
- Ensure resources
- Faster redeployment

Prevent human errors

Utilize tools like Docker and Kubernetes



Other considerations - Server misconfiguration

Server misconfiguration is OWASP Top 10 threat

Hardening guidelines help to setup secure settings

Common misconfiguration flaws:

- Not using HTTP security headers or other HTTP security issues
- Default passwords (force changing initial passwords)
- Security settings unintentionally changed

huld

Coding

OWASP

OWASP TOP-10 (Good start!)

1. A01 Broken Access Control
2. A02 Cryptographic Failures
3. A03 Injection
4. A04 Insecure Design
5. A05 Security Misconfiguration
6. A06 Vulnerable and Outdated Components
7. A07 Identification and Authentication Failures
8. A08 Software and Data Integrity Failures
9. A09 Security Logging and Monitoring Failures
10. A10 Server Side Request Forgery (SSRF)

OWASP Verification standards (Advanced!)

1. ASVS (Application Security Verification Standard)
2. ISVS (IoT Security Verification Standard)
3. MASVS (Mobile Application Security Verification Standard)

SEI CERT Top-10

1. **Validate input.**
2. Heed compiler warnings.
3. Architect and design for security policies.
4. Keep it simple.
5. Default deny.
6. **Adhere to the principle of least privilege.**
7. Sanitize data sent to other systems.
8. Practice defense in depth.
9. Use effective quality assurance techniques.
10. **Adopt a secure coding standard.**

Thanks!
Q&A

huld

Beyond tomorrow