SECURITY SERIES

Supercharge Your Vulnerability Management

Maciej Halasz
Timesys Corporation

SECURE CONNECTIONS
FOR A SMARTER WORLD

EXTERNAL

Agenda

Keeping your products secure

- What are CVEs and why do I care?
- Security process, anyone?

Working with the right tools = success

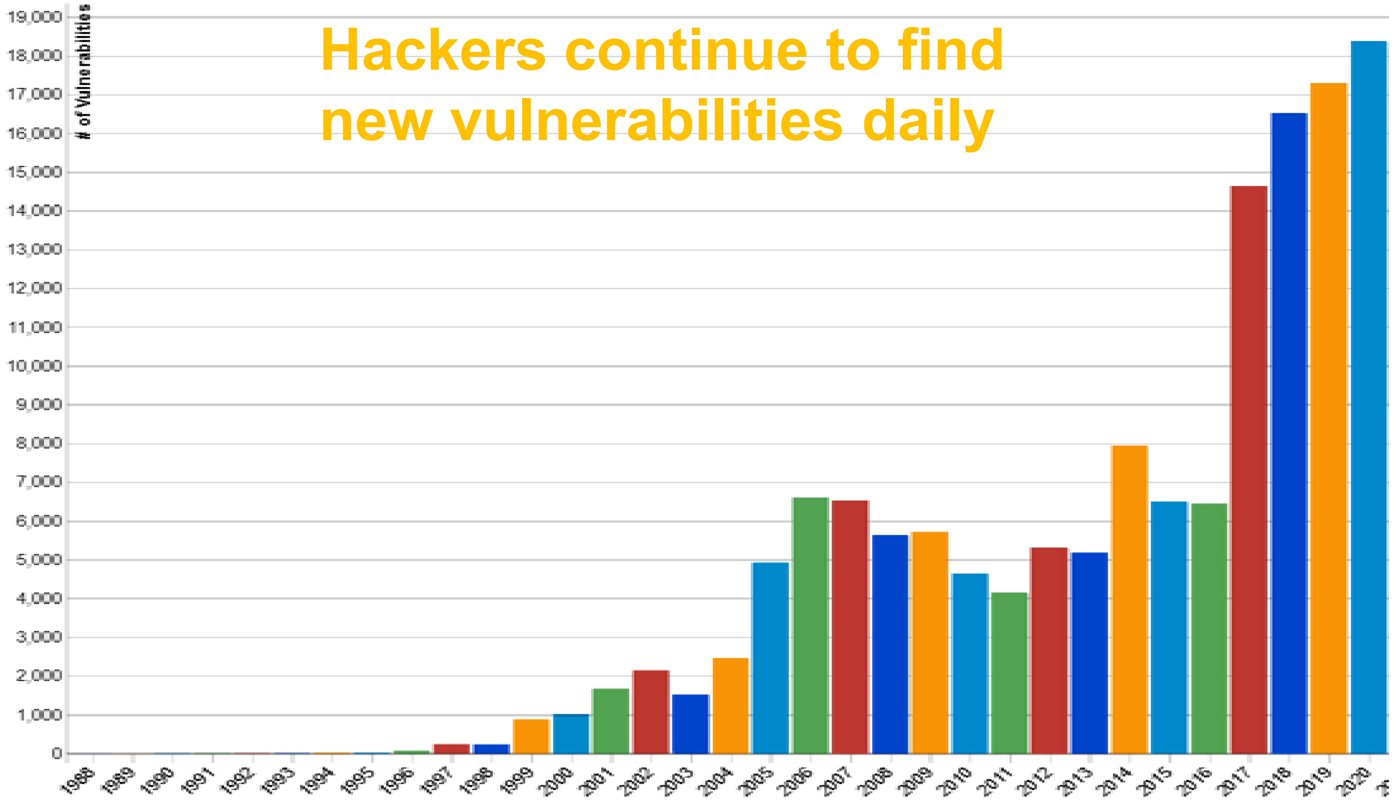
- SBOM
- Monitoring
  - License and policy alerts
- Triaging
  - Team collaboration
  - Tracking changes between releases
- Reporting
- Development process integration
  - Jira integration
  - APIs for a custom dashboard

Is keeping your product secure important?

NXP SECURE CONNECTIONS FOR A SMARTER WORLD

timesys

Device security and maintenance is key



Hackers continue to find new vulnerabilities daily

Reported vulnerabilities reached more than 19,000 in 2021
(avg. > 350 per week)

Source: nvd.nist.gov

Security requirements for application and OS are coming from all sides

- End device users are reporting problems
- You need to meet industry compliance requirements
- Your company has internal cybersecurity guidelines

Vulnerability CVE – Publicly recognized security issue

- CVE-ID (Common Vulnerabilities and Exposures)
- Description of the issue
- Estimated severity (CVSS - Common Vulnerability Scoring System)
  - Low to Critical, 0.0 to 10.0
- Estimated impact and domain scores
  - e.g. “Attack Vector”, “User Interaction”, “Scope”, “Confidentiality”, …
- Affected products, version numbers (CPEs - Common Platform Enumeration)
  - eg: cpe:2.3:a:openssl:openssl:1.1.0g:*:*:*:*:*:*:*
    - Key piece for automation
- List of reference links
  - Exploits, patches, bug entry, mitigation, advisories...
- Vulnerability Type (CWE - Common Weakness Enumeration)
  - e.g. “buffer overflow”, “pointer issues”

Example: CVE-2018-18074

Current Description

The Requests package before 2.20.0 for Python sends an HTTP Authorization header to an http URI upon receiving a same-hostname https-to-http redirect, which makes it easier for remote attackers to discover credentials by sniffing the network.

Known Affected Software Configurations

cpe:2.3:a:python-requests:requests:*:*:*:*:*:*:*:*

Up to (excluding) 2.20.0

Impact

CVSS v3.0 Severity and Metrics:

Base Score: 9.8 CRITICAL

Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Impact Score: 5.9

Exploitability Score: 3.9

Attack Vector (AV): Network

Attack Complexity (AC): Low

Privileges Required (PR): None

User Interaction (UI): None

Scope (S): Unchanged

Confidentiality (C): High

Integrity (I): High

Availability (A): High

Product security

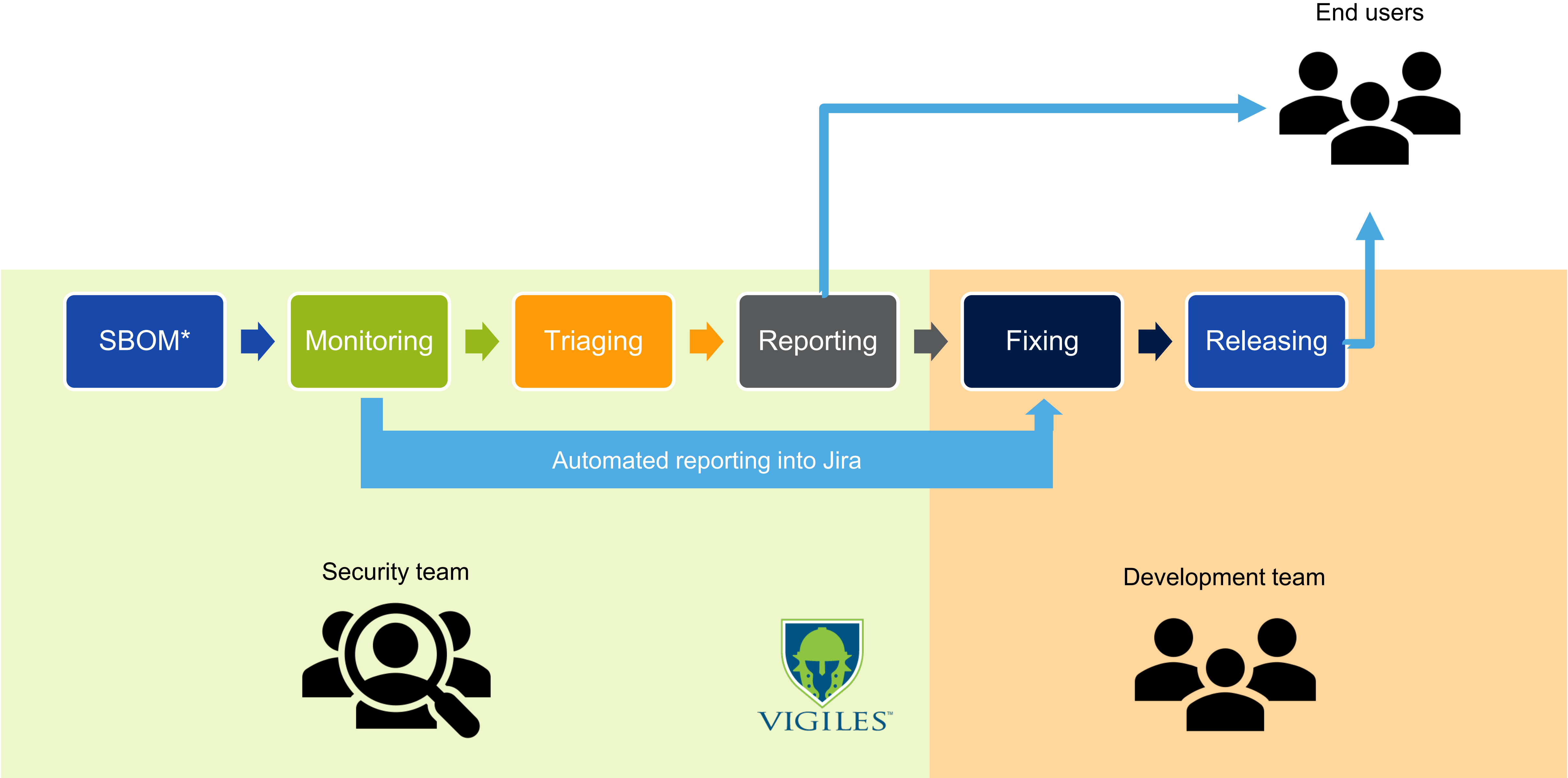
- … is a process … multiple processes

Compliance likes processes!!!

- Process of designing security features into the product
    - Take into account must have processor security requirements such as Secure boot + Secure key storage (HAB, CAAM)
- Process of monitoring software used in product for new security vulnerabilities
- Process of addressing desired vulnerabilities
- Process of servicing field deployed device for security

Each secure product needs security lifecycle – supported by multiple processes
TODAY we will focus on security maintenance!

Security maintenance process



* SBOM - Software Bill of Materials

Monitoring

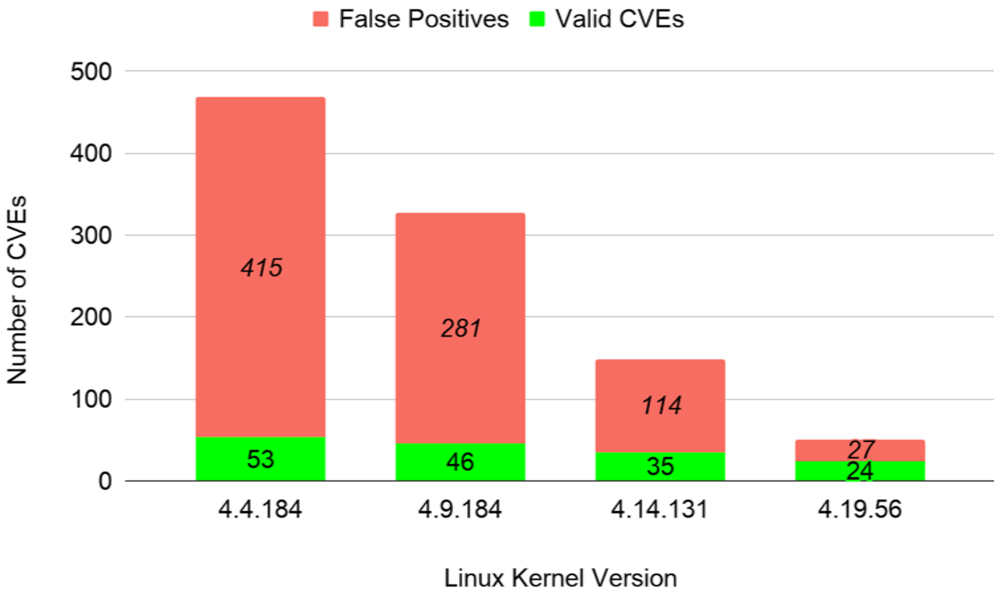
Software Bill of Materials (SBOM)

- Provides transparency on software used in a product
- Tracks specific software information including
  - Exact name
  - Version
  - Licensing
  - Patches applied
  - Configuration of components (optional)
- Is the subject of government mandated regulations and standardization
  - SPDX format - Software Package Data Exchange
  - https://ntia.gov/sbom
- Can be obtained directly from a build system or generated manually

Software Composition Analysis (SCA) tools — which ones to use?

Multiple options for SCA tools are available. Some have serious blind spots when it comes to embedded Linux and other open source, third-party software used in building embedded systems. These blind spots make security maintenance much harder and more complex.

- Binary scanners
  - No metadata in binaries about patching or configurations, so fixed or irrelevant vulnerabilities are still reported as active.
  - Sometimes a component or version cannot be determined based on a binary signature, so the SBOM is inaccurate.
- Source scanners
  - Cannot identify which packages are actually installed in a given product so they report all packages as installed.
  - Cannot collect build artifacts such as patches and kernel configurations so they result in highly inaccurate vulnerability reports.
- Build system scanners



Software Composition Analysis (SCA) tool for build systems — Vigiles

Vigiles addresses the SCA blind spots because it is integrated with your Yocto, Buildroot or Timesys Factory build system:

- **Extracts SBOM from build system to capture metadata**
  - Configurations enabled (e.g., drivers enabled in Linux kernel)
  - List of vulnerabilities already addressed in applied patches
  - Hardware platform information
- **Filters vulnerabilities based on more accurate SBOM**
  - Reporting “unfixed” vulnerabilities applicable to “your hardware platform” based on “enabled configurations”
  - Can cut reported vulnerabilities by **up to 75%** — huge reduction in level of effort

Feature	**Build system based**	**Binary scan**	**Source scan**
SBOM generation accuracy	Best	Good	Poor
Vulnerability metadata for generating accurate reports – based on patches applied, configurations and hardware info	Best	Poor	Good
Integration into the developer workflow	Best	Poor	Poor

NXP Presents Vigiles*: Keeping your Linux BSP Secure

www.nxp.com/vigiles

On-demand security monitoring for more secure systems

- NXP takes great care to ensure the BSP releases use recent software when rolled out
  - As time goes on, new CVEs are reported, and developers customize BSPs to meet product requirements, resulting in possible exposure to security issues
  - Staying secure is a process that must be implemented by your engineering team
- Vigiles enables you to quickly and efficiently analyze security issues and take action
  - Automatically scans for and identifies vulnerabilities specific to your projects and software components
  - Produces highly accurate security reports, which combined with a very low false positive rate provides you with product ongoing security management that is streamlined and highly efficient

Features

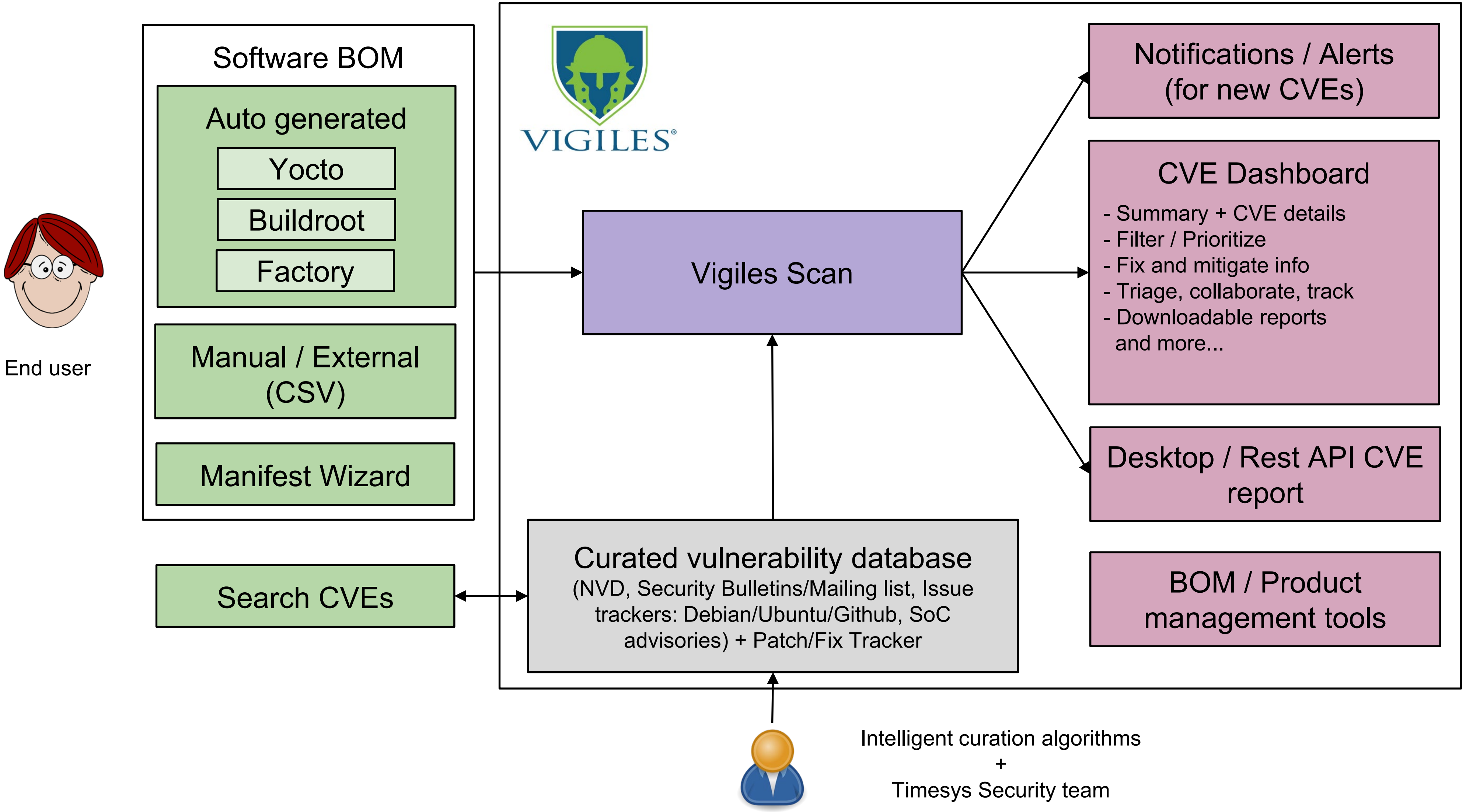
- On-demand vulnerability reports
- Automatic alerts for newly discovered CVEs
- Filtering CVEs by severity and whitelisting non-issues
- Provides direct link to fixes
- Can be bundled with Pro-Support for assistance

Benefits

- Maintain strong product security throughout your product lifecycles
- Bring more secure products to market faster
- Make security a key product differentiator
- Works with ANY Yocto based BSP
- Start for free

** Vigiles is powered by a third-party vendor*

Vigiles high-level architecture overview



Software BOM

Auto generated

Yocto

Buildroot

Factory

Manual / External (CSV)

Manifest Wizard

End user

Search CVEs

VIGILES®

Vigiles Scan

Notifications / Alerts (for new CVEs)

CVE Dashboard

- Summary + CVE details
- Filter / Prioritize
- Fix and mitigate info
- Triage, collaborate, track
- Downloadable reports and more...

Desktop / Rest API CVE report

BOM / Product management tools

Curated vulnerability database (NVD, Security Bulletins/Mailing list, Issue trackers: Debian/Ubuntu/Github, SoC advisories) + Patch/Fix Tracker

Intelligent curation algorithms
+
Timesys Security team

Generating an SBOM from Yocto Project with Vigiles

- Vigiles is enabled with a Yocto metalayer (meta-timesys)
- Easily used with NXP Yocto Project
  - Can be added to any NXP Yocto BSP (https://github.com/TimesysGit/meta-timesys)

```
RELEASE=thud
git clone https://github.com/TimesysGit/meta-timesys.git -b $RELEASE
```

  - Comes pre-integrated into NXP’s Yocto BSP — starting from Yocto “Thud” (https://source.codeaurora.org/external/imx/imx-manifest/)

Generating an SBOM from Yocto Project with Vigiles

- Step 1: Configure your Yocto build for scanning with Vigiles (in conf/local.conf)

```
INHERIT += "vigiles"

VIGILES_KEY_FILE = "/tools/timesys/linuxlink_key"
```

- Step 2: Finetune the scanning results by pointing to your Linux kernel configuration

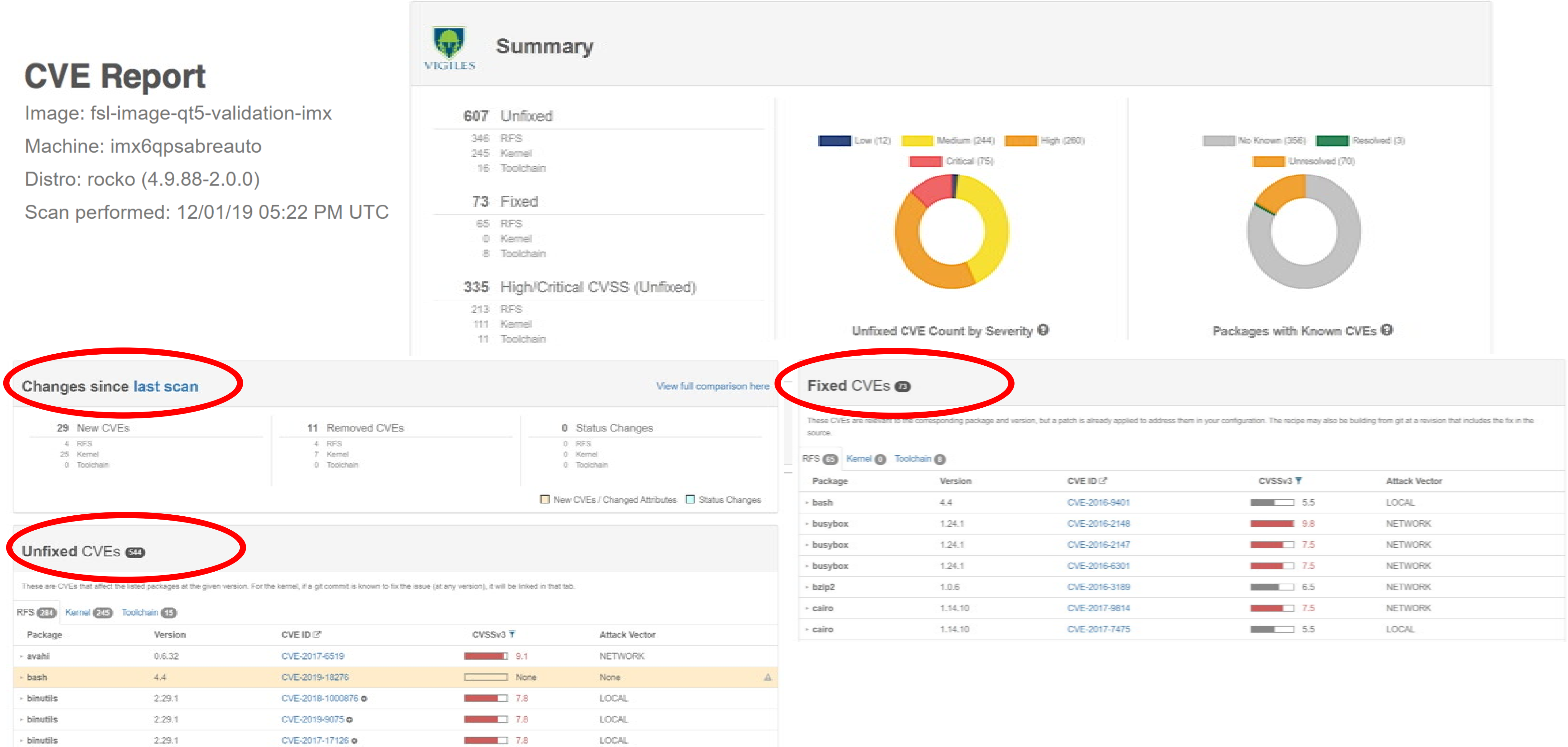
```
VIGILES_KERNEL_CONFIG = "/projects/kernel/linux-5.4-ts+imx-1.0/.config"
```

- Step 3: Run the scan

```
$ bitbake -c vigiles_check core-image-minimal
```

- Step 4: Look at the report locally
- Step 5: Look at the details, analyze and triage using Vigiles online UI

Vigiles: On-Demand Report



CVE Report

Image: fsl-image-qt5-validation-imx

Machine: imx6qpsabreauto

Distro: rocko (4.9.88-2.0.0)

Scan performed: 12/01/19 05:22 PM UTC

VIGILES

Summary

607	Unfixed
346	RFS
245	Kernel
16	Toolchain
73	Fixed
65	RFS
0	Kernel
8	Toolchain
335	High/Critical CVSS (Unfixed)
213	RFS
111	Kernel
11	Toolchain

Unfixed CVE Count by Severity

Packages with Known CVEs

Changes since last scan

View full comparison here

29	New CVEs		11	Removed CVEs		0	Status Changes
4	RFS		4	RFS		0	RFS
25	Kernel		7	Kernel		0	Kernel
0	Toolchain		0	Toolchain		0	Toolchain

□ New CVEs / Changed Attributes □ Status Changes

Unfixed CVEs 544

These are CVEs that affect the listed packages at the given version. For the kernel, if a git commit is known to fix the issue (at any version), it will be linked in that tab.

RFS 284 Kernel 245 Toolchain 15

Package	Version	CVE ID	CVSSv3	Attack Vector	
avahi	0.6.32	CVE-2017-6519	9.1	NETWORK	
bash	4.4	CVE-2019-18276	None	None	⚠
binutils	2.29.1	CVE-2018-1000876	7.8	LOCAL	
binutils	2.29.1	CVE-2019-9075	7.8	LOCAL	
binutils	2.29.1	CVE-2017-17126	7.8	LOCAL	

Fixed CVEs 73

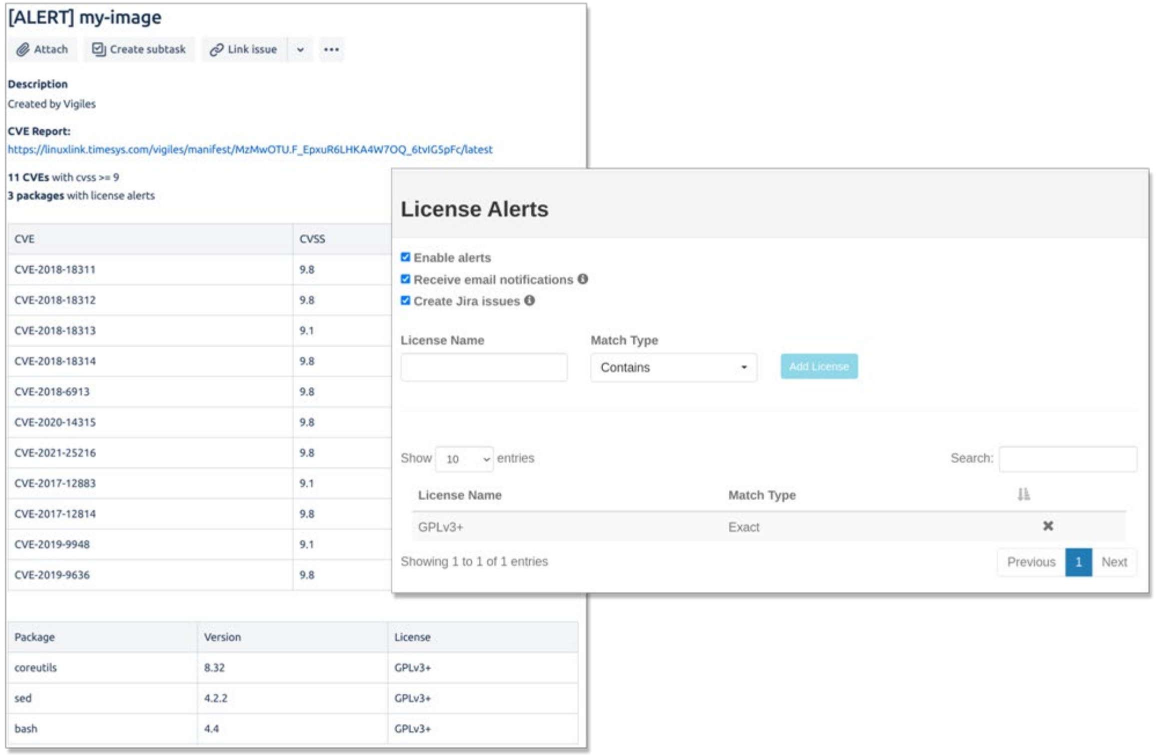
These CVEs are relevant to the corresponding package and version, but a patch is already applied to address them in your configuration. The recipe may also be building from git at a revision that includes the fix in the source.

RFS 65 Kernel 0 Toolchain 8

Package	Version	CVE ID	CVSSv3	Attack Vector
bash	4.4	CVE-2016-9401	5.5	LOCAL
busybox	1.24.1	CVE-2016-2148	9.8	NETWORK
busybox	1.24.1	CVE-2016-2147	7.5	NETWORK
busybox	1.24.1	CVE-2016-6301	7.5	NETWORK
bzip2	1.0.6	CVE-2016-3189	6.5	NETWORK
cairo	1.14.10	CVE-2017-9814	7.5	NETWORK
cairo	1.14.10	CVE-2017-7475	5.5	LOCAL

Notifications and Alerts

- **Notifications** - allow you to stay on-top of new vulnerabilities reported for already uploaded SBOMs.
  - Email sent with vulnerability digest
  - Selectable cadence: Daily, Weekly, Monthly
- **Alerts**
  - CVEs exceeding CVSS score threshold — alert on specific score CVEs (e.g. high and critical)
  - Non-authorized license types — alert when new/updated software in SBOM violates company security policy
  - Raise a Jira issue for alerts to help engineering stay on-top of security issues



[ALERT] my-image

Description
Created by Vigiles

CVE Report:
https://linuxlink.timesys.com/vigiles/manifest/MzMwOTU.F_EpxuR6LHKA4W7OQ_6tvIG5pFc/latest

11 CVEs with cvss >= 9
3 packages with license alerts

CVE	CVSS
CVE-2018-18311	9.8
CVE-2018-18312	9.8
CVE-2018-18313	9.1
CVE-2018-18314	9.8
CVE-2018-6913	9.8
CVE-2020-14315	9.8
CVE-2021-25216	9.8
CVE-2017-12883	9.1
CVE-2017-12814	9.8
CVE-2019-9948	9.1
CVE-2019-9636	9.8

Package	Version	License
coreutils	8.32	GPLv3+
sed	4.2.2	GPLv3+
bash	4.4	GPLv3+

License Alerts

☑ Enable alerts
☑ Receive email notifications
☑ Create Jira issues

License Name:
Match Type: Contains

Show 10 entries   Search:

License Name	Match Type	
GPLv3+	Exact	✖

Showing 1 to 1 of 1 entries

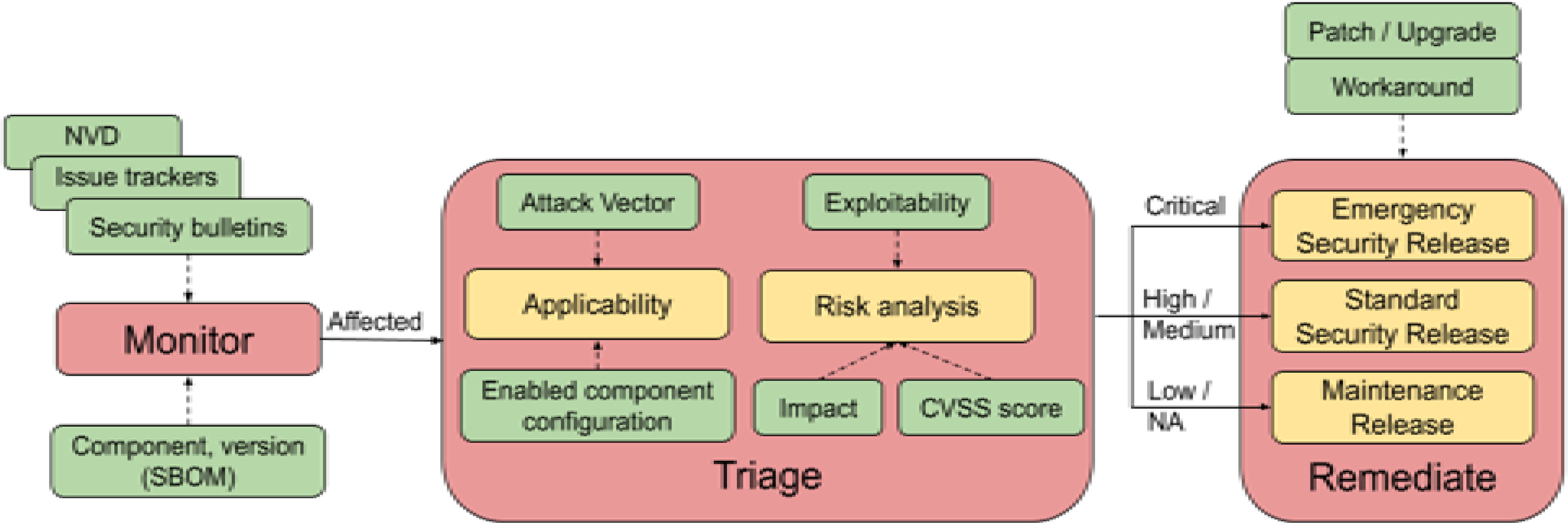
Hands-On

Monitoring Summary

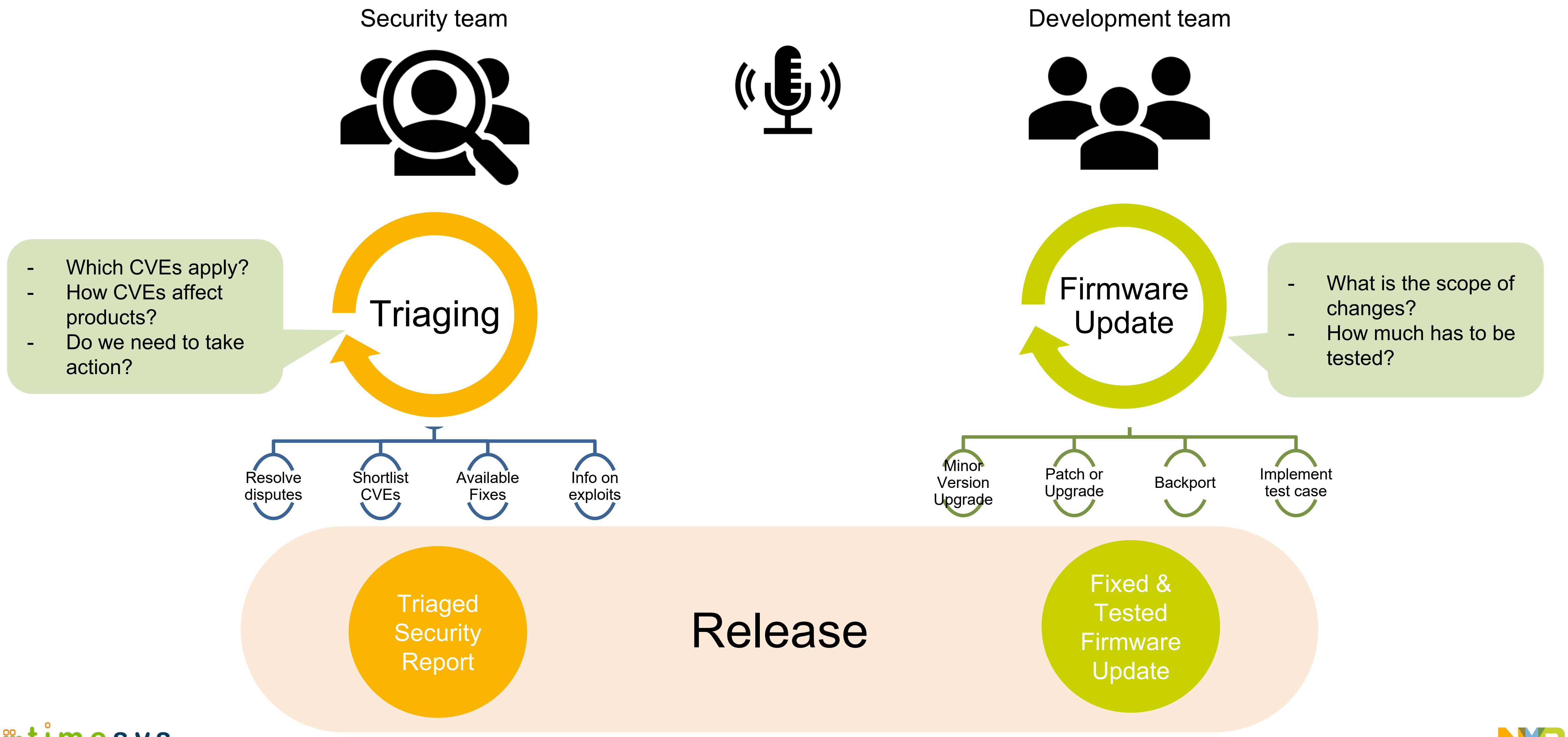
- Monitoring options for SBOMs in Vigiles include:
  - Email notification on new vulnerabilities reported against specific SBOM
    - Daily, Weekly or Monthly cadence
  - Build system/CI triggered rescan
  - Manual rescan
  - Alerts, based on CVSS scoring
- Vigiles highlights deltas between scans for easy identification of new issues

Triaging

Triaging process — Security Impact Assessment



Triaging and Fixing



Security team

Development team

- Which CVEs apply?
- How CVEs affect products?
- Do we need to take action?

Triaging

Resolve disputes

Shortlist CVEs

Available Fixes

Info on exploits

Firmware Update

- What is the scope of changes?
- How much has to be tested?

Minor Version Upgrade

Patch or Upgrade

Backport

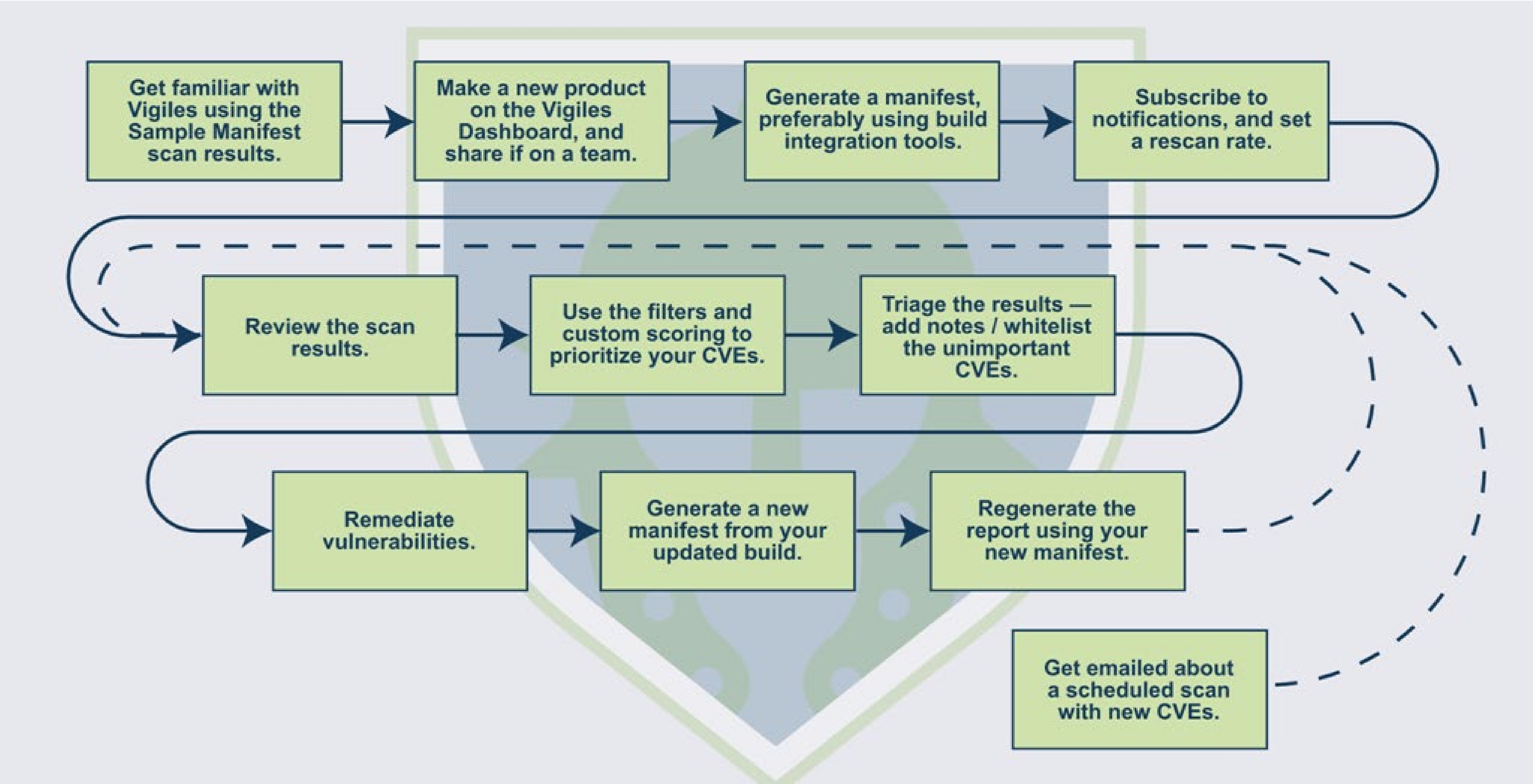
Implement test case

Triaged Security Report

Release

Fixed & Tested Firmware Update

Recommended workflow



Get familiar with Vigiles using the Sample Manifest scan results.

Make a new product on the Vigiles Dashboard, and share if on a team.

Generate a manifest, preferably using build integration tools.

Subscribe to notifications, and set a rescan rate.

Review the scan results.

Use the filters and custom scoring to prioritize your CVEs.

Triage the results — add notes / whitelist the unimportant CVEs.

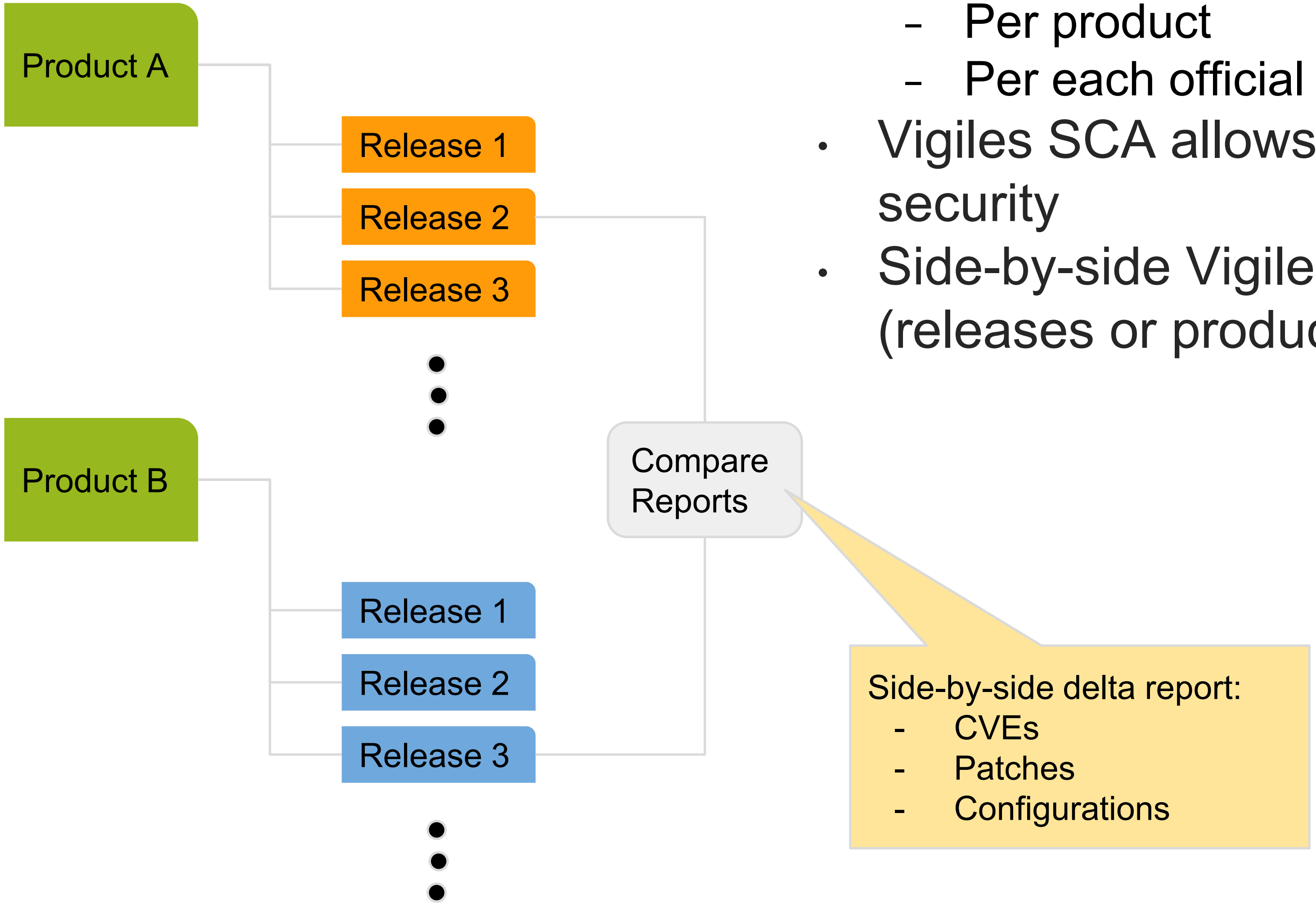
Remediate vulnerabilities.

Generate a new manifest from your updated build.

Regenerate the report using your new manifest.

Get emailed about a scheduled scan with new CVEs.

Vigiles is aligned with product releases



Side-by-side delta report:

- CVEs
- Patches
- Configurations

- Security information can be tracked:
  - Per product
  - Per each official release
- Vigiles SCA allows for independent tracking of security
- Side-by-side Vigiles reports for 2 different scans (releases or products)

Apply triage to other products/releases

- Leverage triage information across products and releases
  - Don’t have to redo triage on common product parts
  - Can focus on triaging delta
  - Simple import interface

- If in triage you identify specific license violation issue or security vulnerability you can look for this issue across all your products and releases using “manifest package search”

Team collaboration on Products in Vigiles

- Support for Products and Releases
- Teams can share Product SBOMs for collaboration
- Each team member triage actions are tagged for traceability
- Triage information from one product SBOM can be used with another product SBOM
- Build system and automated CI can be treated as a separate team member

Hands-On

Reporting

Security info that follows releases

- Each release can have an associated security report which includes:
  - Applicable, unfixed CVEs
  - Triage information
- Formats supported:
  - Summary PDF or Excel
  - Detailed PDF or Excel
  - Delta reports
- Possible use:
  - Track per product release security info
  - Disclose information on product security to end users of a product

Hands-On

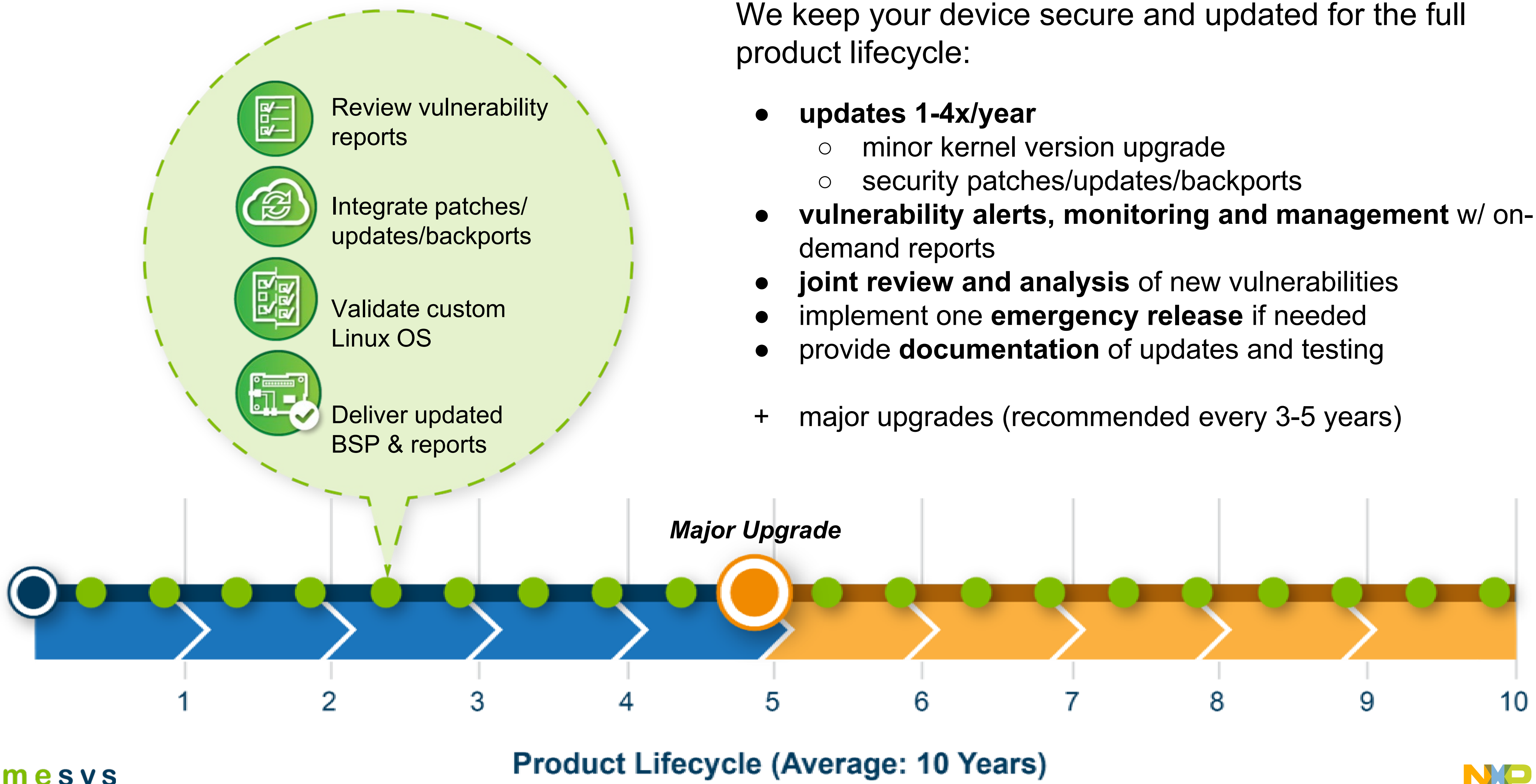
Engineering Process Integration

Engineering process integration

- Separate process possibly involving separate team
- Jira is a commonly used system for tracking issues
- Vigiles offers Jira integration
  - Automatic reporting of CVE issues as Jira issues
  - Brings visibility to security issues to engineering team
  - Becomes part of the engineering sprint planning
- Vigiles API
  - Integration with company’s CI system for automation including, e.g.:
    - Create a new folder
    - Set folder name
    - Associate SBOM with release tag/version
  - Custom dashboard for all security information in one place approach

Hands-On

Long-term security updates and maintenance for Linux OS/BSPs



Review vulnerability reports
Integrate patches/ updates/backports
Validate custom Linux OS
Deliver updated BSP & reports
Major Upgrade
1
2
3
4
5
6
7
8
9
10
Product Lifecycle (Average: 10 Years)

We keep your device secure and updated for the full product lifecycle:

- **updates 1-4x/year**
  - minor kernel version upgrade
  - security patches/updates/backports
- **vulnerability alerts, monitoring and management** w/ on-demand reports
- **joint review and analysis** of new vulnerabilities
- implement one **emergency release** if needed
- provide **documentation** of updates and testing

+ major upgrades (recommended every 3-5 years)

Takeaways

Establishing a process of monitoring and triaging vulnerabilities is of utter importance

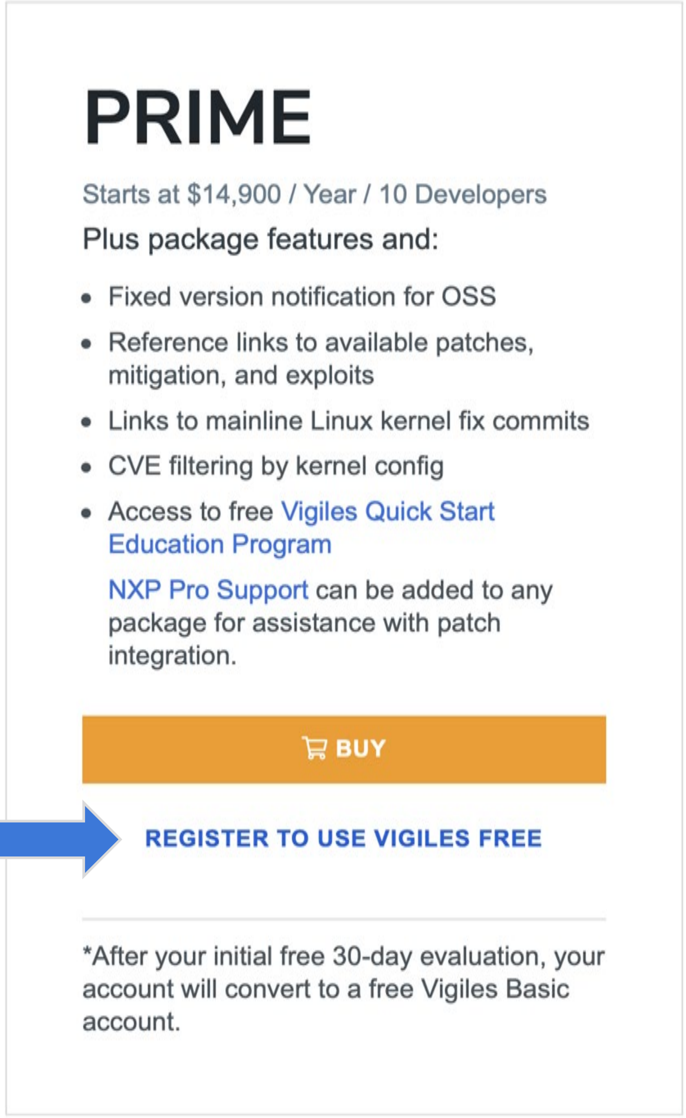
Automation is your friend = less effort and less time

Benefits of using NXP Vigiles:

- Superior vulnerability data
- Optimized for embedded systems
  - Kernel config triage option reduces triage effort by 4x
- Intuitive prioritization and powerful filtering mechanisms
- Collaboration
- BSP Maintenance if you prefer to have your BSP maintained by us

GOLD PARTNER NXP

www.nxp.com/vigiles



PRIME

Starts at $14,900 / Year / 10 Developers

Plus package features and:

- Fixed version notification for OSS
- Reference links to available patches, mitigation, and exploits
- Links to mainline Linux kernel fix commits
- CVE filtering by kernel config
- Access to free Vigiles Quick Start Education Program

NXP Pro Support can be added to any package for assistance with patch integration.

*After your initial free 30-day evaluation, your account will convert to a free Vigiles Basic account.

timesys

NXP

Call to Action

- Upcoming new Vigiles features:
  - SPDX Format Support
  - OpenWRT integration (generate/upload SBOM)
- Try Vigiles Prime today (https://www.timesys.com/register-nxp-vigiles/)
- Talk to us about your security needs

Previous Webinars

SECURE CONNECTIONS
FOR A SMARTER WORLD

timesys

Previous Webinars

Most Recent

- Security Standards Are Evolving; Is Your Company? Create Your Own Device Security Roadmap

Secure By Design Series

- Securing Embedded Linux Devices: Pitfalls to Avoid
- Software integrity and data confidentiality: Establishing secure boot and chain of trust on i.MX processors
- Trusted Execution Environment: Getting started with OP-TEE on i.MX processors
- Linux Kernel Security: Overview of Security Features and Hardening
- Designing OTA Updates for secure embedded Linux systems

Stay Secure (Vigiles) Series

- Software Security Management: Cutting through the vulnerability storm with NXP Vigiles
- BSP security maintenance: Best practices for vulnerability monitoring & remediation
- Full Life Cycle Security Maintenance of Embedded Linux BSPs
- Best practices for triaging Common Vulnerabilities & Exposures (CVEs) in embedded systems

For More Information and to Become More Secure

Timesys is an embedded Linux security expert and NXP Gold Partner.
To discuss your project, please contact us at sales@timesys.com

Use this link to go to Services for securing your device

Thank You!

Q&A

NXP

SECURE CONNECTIONS
FOR A SMARTER WORLD

timesys