A MEDICAL DEVICE CYBERSECURITY TOOLBOX

Complying with FDA cybersecurity regulations requires a variety of processes and technologies. A hypothetical device vendor's approach to securing their product is analyzed, and leading tools identified.

Background:
The Food and Drug Administration (FDA) Postmarket Management of Cybersecurity in Medical Devices has asked medical device manufacturers to create a process to ensure medical devices are "secure by design", as well as quality systems that quickly identify and address vulnerabilities found once a device is released.

In this paper we propose a hypothetical medical device vendor's mature cybersecurity program, and analyze the processes and products that aid in their success.

READERS WILL LEARN

Whether you're a VP, Director, Engineering & Research Professional, or anyone else involved in ensuring cybersecurity best practices are maintained in medical devices, this will inform your decisions around product cybersecurity.

- Quality systems need to include cybersecurity considerations in the product design phase.
- Both internal and external cybersecurity signals need to be analyzed during the life of the product.
- Devices with security features at their core will minimize the overall cost of cybersecurity compliance.
- A variety of commercial tools exist to help address medical device cybersecurity effectively and efficiently.
- A list of tools and services being used by medical device vendors to meet and exceed the FDA's cybersecurity requirements are included as an appendix.

SECTION I: CYBERSECURITY PROCESSES START DURING DESIGN

FDA GUIDANCE REQUIRES BOTH PROCESSES & PRODUCTS

The FDA's Postmarket and Premarket Management of Cybersecurity in Medical Devices describes a mature approach to cybersecurity as consisting of both **Processes** (through which security is managed) and **Products** (technology features that improve the security of a device).

Example Process:	**Example Product:**
"Manufacturers should define, as part of their comprehensive cybersecurity risk management plan, the safety and essential performance of their device, the resulting severity of patient harm if compromised, and the risk acceptance criteria." *Postmarket Management of Cybersecurity in Medical Devices, section X.A.i*	"Manufacturers should consider the incorporation of design features that establish or enhance the ability of the device to detect and produce forensically sound postmarket evidence capture in the event of an attack." *Postmarket Management of Cybersecurity in Medical Devices, section X.B.iv*

These Processes and Products are most effective when implemented during the design phase of a medical device. While there are millions of medical devices in the field that have been designed without these considerations in mind, new products under development should have these Processes and Products in place.

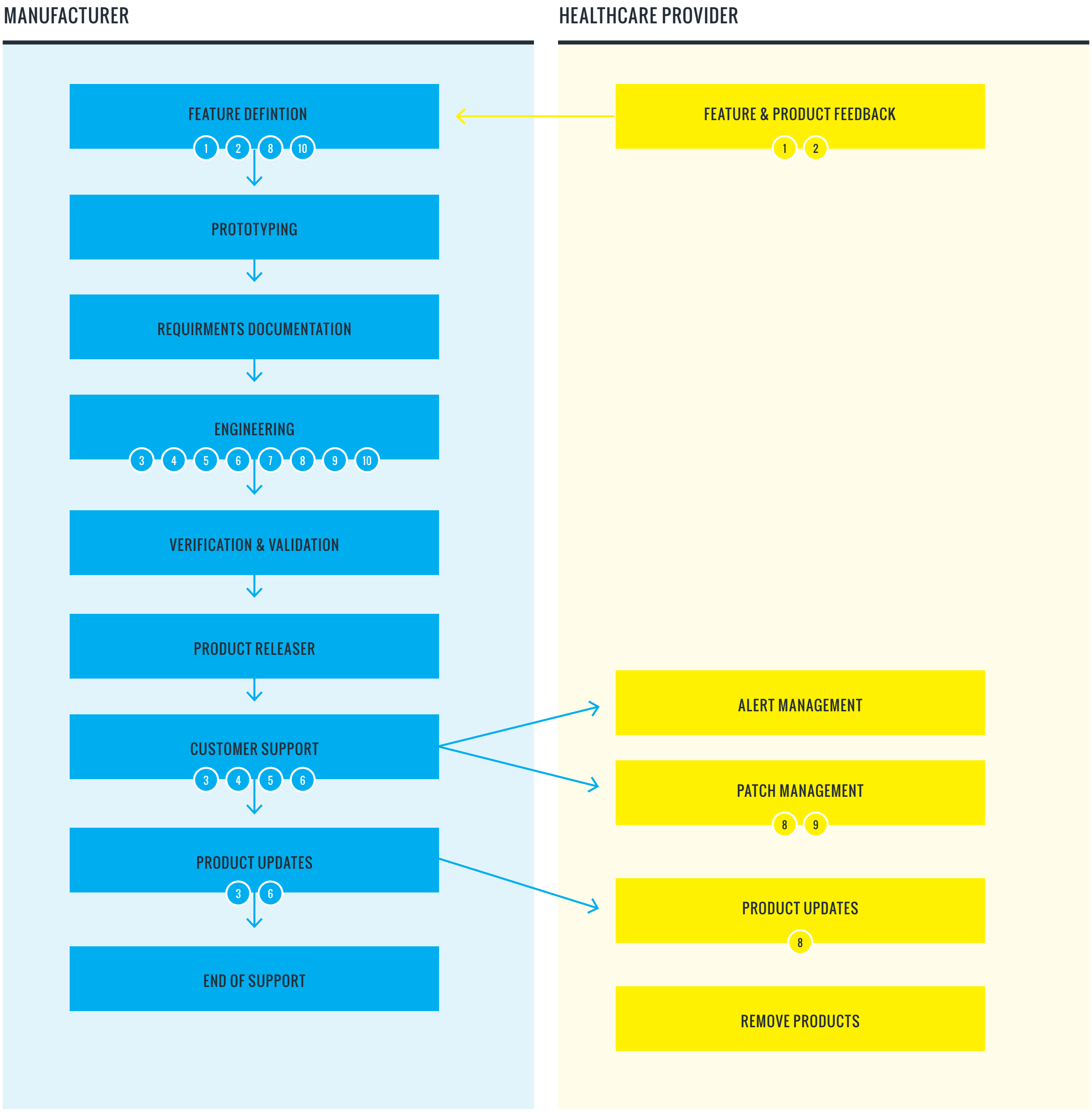
PREMARKET & POSTMARKET CYBERSECURITY REQUIREMENTS:

The FDA's premarket and postmarket guidance suggests the following be incorporated throughout the device lifecycle:

	Area	Guidance	Process or Product
1	**Device Safety & Performance Definition**	Define the safety and essential performance of their device, the resulting severity of patient harm if compromised, and the risk acceptance criteria.	**Process**
2	**Complaint Processing Process**	Analyze complaints, returned product, service records, and other sources of quality data to identify existing and potential causes of nonconforming product or other quality problems.	**Process**
3	**Cybersecurity Signal Processing**	Actively identify cybersecurity signals that might affect their product, and engage with the sources that report them.	**Process**
4	**Vulnerability Processing**	Characterize and assess identified vulnerabilities. Consider factors such as remote exploitability, attack complexity, threat privileges, actions required by the user, exploit code maturity, and report confidence.	**Process**
5	**Risk Analyses**	Conduct cybersecurity risk analyses that include threat modeling for each of their devices and to update those analyses over time.	**Process**
6	**Threat Source Processing**	Analyze possible threat sources.	**Process**
7	**Mitigation Assessment**	Determine if the risk of patient harm presented by the vulnerability are adequately controlled by existing device features and/or manufacturer defined compensating controls (i.e., residual risk levels are acceptable).	**Product**
8	**Forensic Evidence Generation**	Incorporate design features that establish or enhance the ability of the device to detect and produce forensically sound postmarket evidence captured in the event of an attack.	**Product**
9	**Horizontal Impact Analysis**	Have a process to assess the impact of a cybersecurity signal horizontally (i.e., across all medical devices within the manufacturer's product portfolio and sometimes referred to as variant analyses) and vertically (i.e., determine if there is an impact on specific components within the device).	**Product**
10	**Device Design Controls**	Implement device-based features, i.e. device design controls, as a primary mechanism to mitigate the risk of patient harm.	**Process**
11	**Coordinated Vulnerability Disclosure**	Adopt a coordinated vulnerability disclosure policy and practice that includes acknowledging receipt of the vulnerability to the vulnerability submitter within a specified time frame.	**Process**

EXAMPLE DEVICE DESIGN PROCESS

The eleven recommendations from the FDA must be embedded in the device design process to ensure industry leading practices are sustainable. While there are a variety of development approaches, rooted in different methodologies (such as ISO/IEC/IEEE 12207:2017), a typical manufacturer's design process labeled with FDA requirements, may look like the following:



MANUFACTURER

FEATURE DEFINTION 1 2 8 10

PROTOTYPING

REQUIRMENTS DOCUMENTATION

ENGINEERING 3 4 5 6 7 8 9 10

VERIFICATION & VALIDATION

PRODUCT RELEASER

CUSTOMER SUPPORT 3 4 5 6

PRODUCT UPDATES 3 6

END OF SUPPORT

HEALTHCARE PROVIDER

FEATURE & PRODUCT FEEDBACK 1 2

ALERT MANAGEMENT

PATCH MANAGEMENT 8 9

PRODUCT UPDATES 8

REMOVE PRODUCTS

1 Device Safety & Performance Definition

2 Complaint Processing Process

3 Cybersecurity Signal Processing

4 Vulnerability Processing

5 Risk Analyses

6 Threat Source Processing

7 Mitigation Assessment

8 Forensic Evidence Generation

9 Horizontal Impact Analysis

10 Device Design Controls

11 Coordinated Vulnerability Disclosure

SECTION II: SIGNALS COME FROM BOTH INSIDE & OUTSIDE THE COMPANY

While many device vendors have seen cybersecurity as an internal, confidential regulatory compliance process, the FDA has made it clear that “cybersecurity signals” may originate from outside the vendor’s organization, and these signals need to be continually evaluated for both impact and mitigation on a vendor’s device.

COMMON SOURCES OF SIGNALS:

INTERNAL CYBERSECURITY SIGNALS

Features developed are tested to confirm they meet the requirements established and focus on performance, quality and functional capabilities. This has traditionally occured after development is complete, but best-practice methodologies are employing continuous testing. Testing the application against security policy using several methods, including static, dynamic, software composition analysis, and manual penetration testing can offer an inventory of signals to be addressed.

“TECHNICAL DEBT”

As engineers turn technical requirements into code, some lower-priority features may fail to be completed before deadlines. Engineers may also choose to implement a feature quickly, while noting that the implementation of that feature could be improved in the future. Collectively, choosing a path that will require future rework is referred to as “Technical Debt”.

If this Technical Debt leads to increased cybersecurity risk, the risk should be evaluated before the product is released. If the risk is deemed acceptable, future engineering efforts may need to address this security-related technical debt. The implications of these Technical Debt items should be reevaluated from time to time, to ensure that the Risk posed doesn’t become Uncontrolled.[1]

PERFORMING A CODE REVIEW

While developing the requirements established in collaboration with the business and customers, developers should find and resolve vulnerabilities in the code. Tools such as Static Code Analysis (SCA) can be used during the design phase to identify coding errors and design flaws that may create vulnerabilities. A popular SCA tool used by medical device vendors is Coverity by Synopsys.

PENETRATION TESTING

Penetration testing aims to simulate what an adversarial hacker would do if they were trying to hack your device. This testing usually happens in a controlled setting, and the end product is a list of recommendations of how to make it more difficult for a “bad guy” to hack your device. These recommendations need to be prioritized by their relative risk, and fed back into the engineering process in the form of new requirements.

Devices should be subjected to both internal and external penetration testing as part of the product development process. While larger organizations may have their own “Red Team” penetration testing engineers, other vendors will find it more feasible to use a “pen testing” firm, such as Whitescope, or the Phobos Group.

CONTROLLED RELEASE

Moving away from manual releases to automated processes brings a level of predictability that reinforces the use of security best practices during development. Plans for change management, should any bugs or enhancements be identified at this stage, should be in place to embed security. Disaster recovery requirements should also be identified.

[1] Postmarket Management of Cybersecurity in Medical Devices, Section IV.J

EXTERNAL CYBERSECURITY SIGNALS

A major focus of the FDA's Postmarket Cybersecurity Guidance for Medical Devices is vendors' approach to cybersecurity signals that originate outside their organization. In the past, some organizations have seen engagements with these outside sources as somehow exposing them to additional liability; "If we don't know about the problem, we can't be held responsible for its existence." The FDA's position is clear—a vendor must analyze these external sources to comply with safety regulations.

VULNERABILITIES IN THIRD-PARTY SOFTWARE

Most commercial software (and firmware) contains at least some third party software, either in the form of commercial tools (like Windows and SQL Server), or open source libraries (like Apache and OpenSSL). These components are being continually tested for cybersecurity issues by other users, customers, and researchers. This results in periodic patches and upgrades of these component libraries. A medical device vendor needs to analyze these vulnerabilities to assess applicability and the risk they pose to their products' essential performance.

It should be noted that the periodic discovery of vulnerabilities in third-party software is widely accepted as improving a product's cybersecurity posture, especially when compared to a product whose various software functions are not being continually subjected to security testing. The "Security by Obscurity" approach of using only proprietary software that is never tested for vulnerabilities will almost certainly result in a product that is more susceptible to intrusion than a product using commercial and open source components.

Vulnerabilities found in third party software, like commercial operating systems (e.g. Windows) and common open source libraries (e.g. OpenSSL) can be the root cause of a vulnerability in a medical device. It is important to be alerted when the community finds these vulnerabilities, and to assess how they impact the security of your device. One such vulnerability monitoring tool is SelectEvidence by Nova Leah.

CUSTOMER / USER FEEDBACK

FDA guidance requires that device vendors "analyze complaints, returned product, service records, and other sources of quality data" to detect possible vulnerabilities. In other words, when a customer states that their device isn't functioning as expected, vendors need to determine if a cybersecurity breach could be the root cause.

HDOs frequently have their own staff dedicated to securing their hospital networks, and these individuals may find vulnerabilities in the medical devices they are using. There should be a mechanism by which the technical detail of these vulnerabilities can be shared with the engineering team for evaluation and remediation.

CYBERSECURITY RESEARCHERS

Perhaps the most sensitive aspect of medical device cybersecurity is the way in which vulnerabilities identified by security researchers are handled by medical device vendors. In decades past, vendors may have seen a researcher independently testing their product as a violation of the device's intended use, or even its licensing agreements. The initial response from the vendor may have been to pursue legal action against the researcher. However, the Digitial Millenium Copyright Act (DMCA) put forth a specific provision allowing independent researchers to assess the cybersecurity posture of medical devices. Also, the FDA has described interactions between vendors and researchers in their 2016 Postmarket Guidance.[3] It is clear that a formal plan for addressing the findings of security researchers needs to be adopted by medical device vendors.

MedCrypt's recent whitepaper analyzing ICS-CERT advisories found that ~35% of advisories mentioned a researcher as the party originally identifying the vulnerability. The consensus among medical device vendors most active in cybersecurity disclosures is that these researchers play an important part in our ecosystem, and generally have benevolent intentions. Failing to manage these relationships deliberately can have costly implications both for the vendor and the researcher.

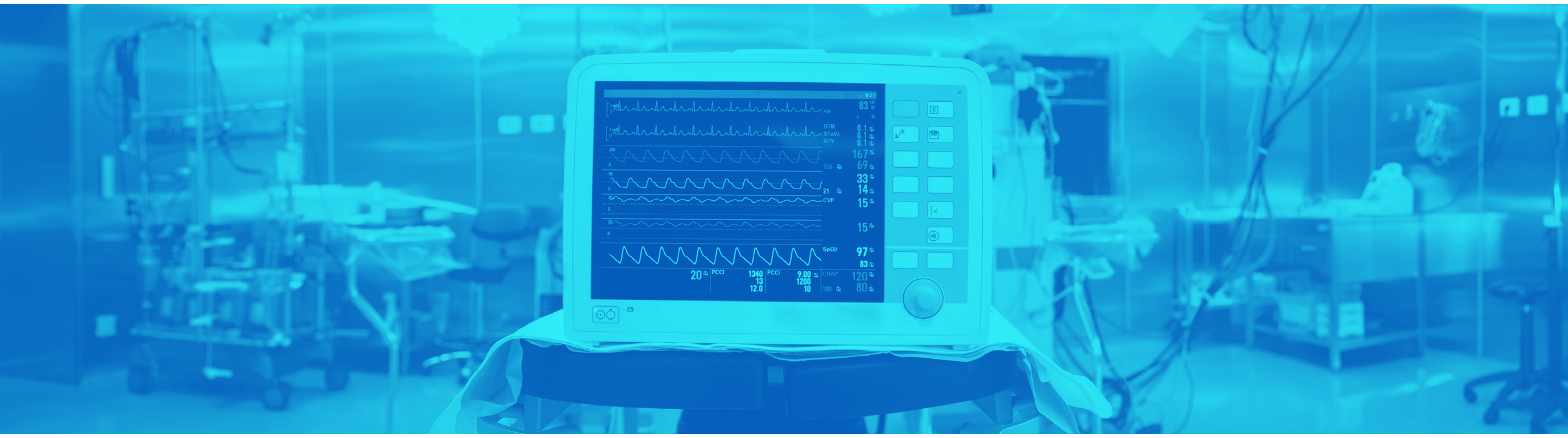
[2] Postmarket Management of Cybersecurity in Medical Devices, Section X.A.ii

[3] Postmarket Management of Cybersecurity in Medical Devices, Section V.B

REGULATORY COMPLIANCE

Regional governmental regulations and organizations, including OWASP, HIPAA, Department of Defense, FDA, NIST800-53 and ISO/IEC27001, should be assessed for security considerations. The FDA Guidance allows for a vendor to classify a vulnerability as a "Controlled Risk", and not issue a software update if there is a Compensating Control in place. The existence of this vulnerability needs to be documented in a quality system, so that it can be addressed in the future. Many quality systems will track this as a bug in a system like Jira, but some commercial vulnerability inventory systems are available, including Unified Security Management by Alien Vault.

The anticipated change to the FDA pre-market guidance, further recommended by the Office of Inspector General (OIG) emphasizes the collaboration of regulators and various stakeholders . The OIG report confirms devices are scrutinized by the FDA to ensure compliance with guidance requirements. But even in the absence of FDA scrutiny, device vendors are seeing higher levels of product security as mandatory to compete in the marketplace.



SECTION III: IT'S CHEAPER TO SECURE THAN TO FIX

Some organizations may feel that investing in a "Secure by Design" development process is overly expensive, and that it may be cheaper to deal with cybersecurity issues that may arise only when absolutely necessary, and as part of a regular software update. However it is becoming increasingly clear that addressing certain types of vulnerabilities once a device is in the field can be prohibitively expensive, and in some cases impossible. Devices that have security considerations as part of their design inputs will face fewer objections from customers' CIOs and CISOs, will face fewer recalls, and face fewer regulatory hurdles.

Some of the security considerations that should be part of the design process can be achieved through organizational processes. For example, code reviews can find many security issues before they make it to the product, and don't require additional tools or equipment; only additional engineering time. Other considerations may be best addressed by commercial products. As vendors determine how to design and maintain their device security posture, a build, buy, partner assessment should be completed to accomplish efficient and effective security interventions.

MedCrypt's whitepaper analyzing ICS-CERT vulnerabilities found that two classes of vulnerabilities accounted for 66% of disclosures: user authentication, and software code errors. Vendors may choose to use commercial user authentication tools, such as Okta, in order to decrease the likelihood of these vulnerabilities. Static Code Analysis tools, like those sold by Synopsys, may be helpful in identifying code issues or bugs during the development phase.

Other vulnerabilities may be prevented by adding encryption into various areas of the product. Public Key Infrastructure tools, like those sold by Digicert, allow devices to authenticate other endpoints. Encryption tools like those sold by MedCrypt make it easy to secure data and instructions generated by devices, as well as verify the integrity of clinical data received from these devices.

Finally, devices deployed in the field should incorporate intrusion detection features, such as those offered by MedCrypt, or Symantec's Critical System Protection. This allows a device vendor to respond to a cybersecurity incident more quickly, and without having to rely on their customers' monitoring their network traffic for unusual activity.

SECTION IV: CONCLUSION

As medical devices incorporate connectivity into their essential performance, vendors face increasing cybersecurity challenges. These challenges range from new regulatory requirements, to unsolicited vulnerability disclosures by members of the community. Vendors need both Processes and Product features geared toward ensuring their devices function safely and effectively, regardless of the security of the network on which the devices function.

There are several commercial software tools and service offerings to help medical device vendors prosper in this new era of medical device connectivity. Vendors should identify functions and features that are best accomplished through proprietary means, and rely on commercial offerings for the rest. Our industry's products will benefit from the "communal knowledge" that comes from shared technology tools and platforms.

DISCLOSURES

The authors of this paper are employed by MedCrypt Inc, a medical device cybersecurity software provider.

Thank you.
Mike Kijewski, CEO
mike@medcrypt.co

APPENDIX A

The following is a short list of tools and services used by medical device vendors to address the cybersecurity posture of their devices.

Vendor	Product	Description	Line
AlienVault	Unified Security Management	Vulnerability Management	https://www.alienvault.com/solutions/vulnerability-management
Atlassian	Jira	Bug / ticket tracking	https://www.atlassian.com/software/jira
Digicert	Digicert PKI	PKI, Certificate Authority	https://www.digicert.com/internet-of-things/healthcare/
MedCrypt	Guardian, Overwatch	Endpoint encryption, behavior monitoring	https://www.medcrypt.co
Nova Leah	SelectEvidence	Risk management compliance suite	https://novaleah.com
Okta	Okta	Cloud-based User Authentication	https://www.okta.com
Phobos Group		Penetration Testing	https://phobos.io
Symantec	Critical System Protection	Lightweight security client for IoT	https://www.symantec.com
Synopsys	Coverity	Static Code Analysis	https://www.synopsys.com/software-integrity/security-testing/static-analysis-sast.html
WhiteScope		Penetration Testing Services	https://whitescope.io