SYNOPSYS®

How Cyberthreats Can Become an Unwanted Real-Life Hollywood Blockbuster

Boris Cipot, Senior Security Engineer

Agenda

- Understand the threats in today's software supply chain to help identify the potential future risks
- Learn best practices for resolving issues that lead to software vulnerabilities
- See how can these problems be addressed, taking into account development organizations’ time pressures

A Hollywood blockbuster

Source: https://diehard.fandom.com/

Source: https://www.quora.com/What-is-used-for-hacking-in-the-movie-Live-Free-or-Die-Hard

Source: https://diehard.fandom.com/

This is our life

threatpost | Cloud Security | Malware | Vulnerabilities | InfoSec Insiders | Podcasts

Joker Trojans Flood the Android Ecosystem

Universal Health Services Ransomware Attack Impacts Hospitals Nationwide

The Ryuk ransomware is suspected to be the culprit.

A ransomware attack has shut down Universal Health Services, a Fortune-500 owner of a nationwide network of hospitals.

The attack occurred in the wee hours of the morning on Monday, according to reports coming in from employees on Reddit and other platforms.

Author
Tara Seals
September 28, 2020
11:32 am

IOT | MOBILE | SICHERHEIT

h Ransomw

Universitäten und K
gab es deswegen
che Einrichtunge
e Netzwerke wid

threatpost | Cloud Security | Malware | Vulnerabilities | InfoSec Insiders | Podcasts

2 More Hospitals Hit by Growing Wave of Ransomware Attacks, As Feds Issue Warning

Hospitals in New York and Oregon were targeted on Tuesday by threat actors who crippled systems and forced ambulances with sick patients to be rerouted, in some cases.

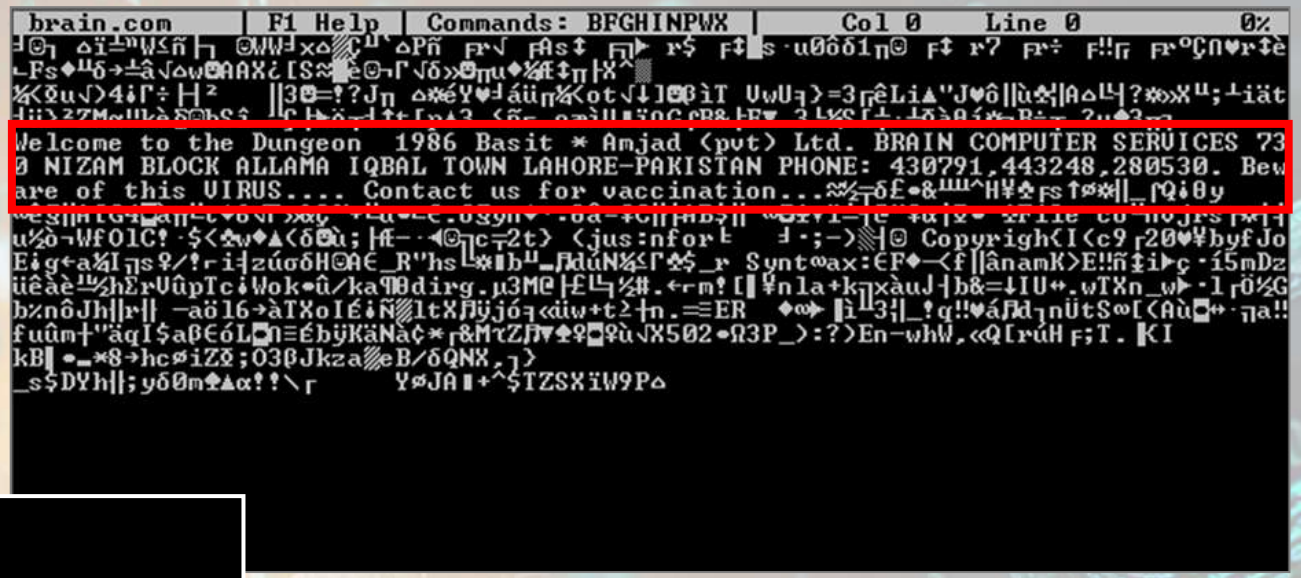
UPDATE

Two more hospitals were hit with ransomware attacks this week as a growing number of criminals target healthcare facilities during the COVID-19 pandemic. The troubling trend

Author
Tom Spring
October 28, 2020
5:43 pm

Malware from the past

Malware Authors were known



The infection was visible

Cybercriminals of the Past – Motivation: Fame

Chen Ing-Hau

1998

Joseph McElroy

Hacker attack on a U.S. government lab to use the network power to download movies and music from the Internet.

2003

Benny / 29A

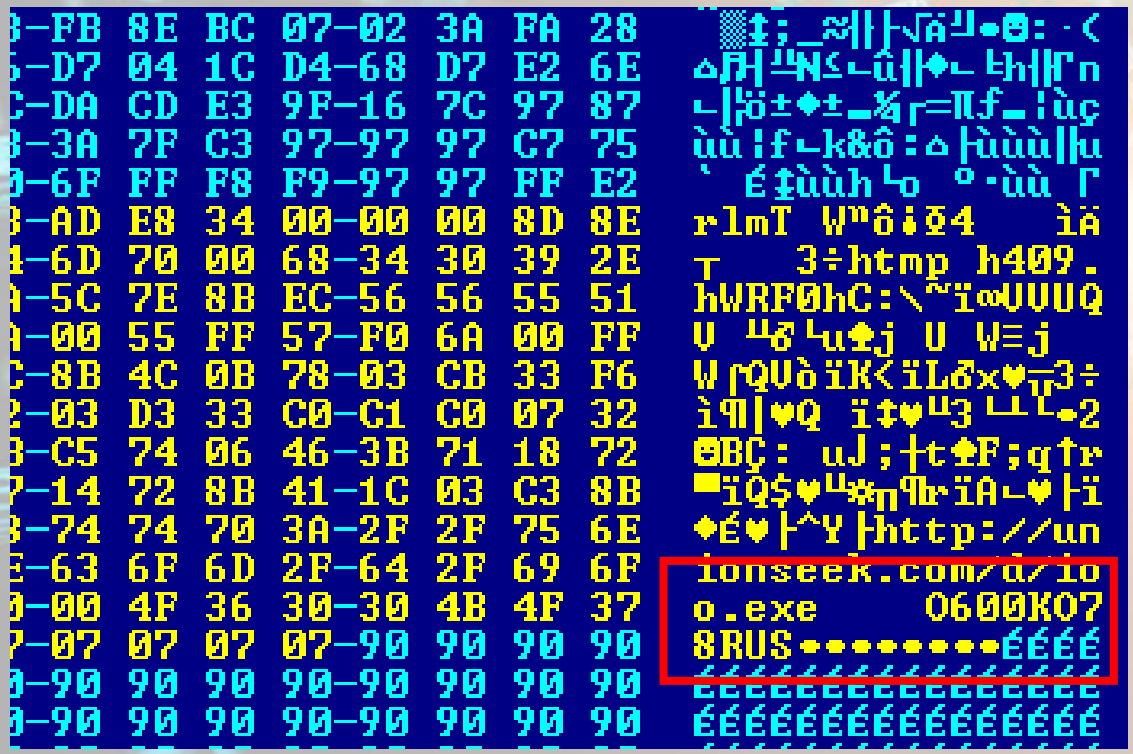
199x

Attacks were signed.

Threats Have Evolved – Motivation: MONEY

Operating from the shadows

Signatures were rare...



... and encrypted in program code.

The infection was hidden to keep the infected computers running.

Modern Cyber Threat – Motivation: VARIOUS

MONEY

HACKTIVISM

POLITICS

What’s at stake

Transportation

- Air
- Train
- Car

Power services

- Nuclear power plants
- Power operator's network
- Governmental departments of energy networks

Infrastructure

- Police, phone services
- RPC-based SCADA networks
- Hospitals
- Airports
- Coast guard

Banks

- ATM networks
- Bank offices

What’s at stake

Transportation	Power	Infrastructure	Banks	Malware
• Air traffic control problems in USA	• Infected nuclear power plant in Ohio	• 911 phone services down in Seattle	• Bank of America's ATM network down	**Slammer** 2003
• Air Canada flights grounded • CSX trains stopped	• NY ISO power operator’s network infected	• Numerous RPC-based SCADA networks down	• Several Windows-based ATM networks infected	**Blaster** 2003
• Railcorp trains stopped in Australia • Delta flight problems • Delays with British Airways flights	• Hong Kong government’s department of energy networks infected	Infected: • Two hospitals in Sweden • EU commission • Heathrow airport • Coastguard U.K.	• Several banks shut down offices because of internal infections	**Sasser** 2004

How many attacks are happening now?

Unfortunately, more than can fit on this page

How many attacks are happening now

Source: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

January 2024: Hackers breached Global Affairs Canada's secure VPN in December 2023, allowing hackers to access sensitive personal information of users and employees. It affected staff emails, calendars, and contacts. It's unclear if classified information was compromised or lost. The hacker's identity is currently unknown.
January 2024: Russian hackers launched a ransomware attack against Sweden's only digital service provider for government services. The attack affected operations for 120 government offices and came as Sweden prepared to join NATO. Sweden expects disruptions to continue for several weeks.
January 2024: Microsoft announced that Russian hackers broke into its corporate systems. Hackers used a "password spray attack" to steal emails and documents from accounts of Microsoft's senior leadership, cybersecurity, and legal teams back in November 2023.
January 2024: Russian hackers attacked 65 Australian government departments and agencies and stole 2.5 million documents in Australia's largest government cyberattack. Hackers infiltrated an Australian law firm that worked with the government to gain access to government files.
January 2024: The Australian government identified and sanctioned Aleksandr Ermakov as the Russian hacker who breached Medibank, the country's largest private health insurance provider, in 2022. He stole information from 9.7 million current and former Medibank customers. This is the first time Australia has issued cyber sanctions against an individual since the framework was established in 2021. The U.S. and UK also sanctioned Ermakov.
January 2024: Russian agents hacked residential webcams in Kyiv to gather information on the city's air defense systems before launching a missile attack on Kyiv. Hackers changed the cameras' angles to gather information on nearby critical infrastructure facilities and stream the footage on YouTube. Ukraine has since ordered webcam operators in the country to stop live broadcasts.
December 2023: Israeli-linked hackers disrupted approximately 70% of gas stations in Iran. Hackers claimed the attack was in retaliation for aggressive actions by Iran and its proxies in the region. Pumps restored operation the next day, but payment issues continued for several days.
December 2023: Ukrainian state hackers crippled Russia's largest water utility plant by encrypting over 6,000 computers and deleting over 50 TB of data. Hackers claimed their attack was in retaliation for the Russian Kyivstar cyberattack.

December 2023: Russian hackers hit Ukraine's largest mobile phone provider, Kyivstar, disabling access to its 24 million customers in Ukraine. Hackers claim to have destroyed more than 10,000 computers and 4,000 servers, including cloud storage and backup systems. The attack began hours before President Zelenskyy met with President Biden in Washington D.C.
December 2023: Ukraine's military intelligence service (the GRU) claims to have disabled Russia's tax service in a cyberattack. According to the GRU, the attack destroyed the system's configuration files, databases, and their backups, paralyzing Russia's tax service.
November 2023: Suspected Chinese hackers launched an espionage campaign against Uzbekistan and the Republic of Korea. Hackers use phishing campaigns to gain access to their target's systems and decrypt their information.
November 2023: Chinese-linked hackers attacked Japan's space agency during summer 2023 and compromised the organization's directory. The agency shut down parts of its network to investigate the breach's scope. It claims it did not compromise critical rocket and satellite operations information.
November 2023: Chinese hackers compromised Philippine government networks beginning in August 2023. Hackers used phishing emails to imbed malicious code into their target's systems to establish command and control and spy on their target's activities.
November 2023: Trinidad and Tobago's Prime Minister Dr. Keith Rowley declared the latest ransomware attack against the country's telecommunications service to be a "national security threat." Hackers stole an estimated six gigabytes of data, including email addresses, national ID numbers, and phone numbers.
November 2023: Denmark suffered its largest cyberattack on record when Russian hackers hit twenty-two Danish power companies. The attack began in May 2023 and appeared to be aimed at gaining comprehensive access to Denmark's decentralized power grid. Hackers exploited a critical command injection flaw and continued to exploit unpatched systems to maintain access.
November 2023: Chinese cybercriminals targeted at least 24 Cambodian government networks, including the National Defense, Election Oversight, Human Rights, National Treasury, Finance, Commerce, Politics, Natural Resources and Telecommunications agencies. Hackers disguised themselves as cloud storage services to mask their data exfiltration. Initial research indicates the attack is part of a broader Chinese espionage campaign.

October 2023: Hacktivists stole 3,000 documents from NATO, the second time in three months that hacktivists have breached NATO's cybersecurity defenses. Hackers described themselves as "gay furry hackers" and announced their attack was retaliation against NATO countries' human rights abuses. NATO alleges the attack did not impact NATO missions, operations, or military deployments.
October 2023: Researchers discovered what appears to be a state-sponsored software tool designed for espionage purposes and used against ASEAN governments and organizations.
October 2023: Pro-Hamas and pro-Israeli hacktivists have launched multiple cyberattacks against Israeli government sites and Hamas web pages in the aftermath of Hamas' attacks on Israel on October 7th. Russian and Iranian hacktivists also targeted Israeli government sites, and Indian hacktivists have attacked Hamas websites in support of Israel.
October 2023: Vietnamese hackers attempted to install spyware on the phones of journalists, United Nations officials and the chairs of the House Foreign Affairs Committee and Senate Homeland Security and Government Affairs. The spyware was designed to siphon calls and texts from infected phones, and the unsuccessful deployment comes while Vietnamese and American diplomats were negotiating an agreement to counter China's growing influence in the region.
October 2023: New reporting reveals Chinese hackers have been targeting Guyana government agencies with phishing emails to exfiltrate sensitive information since February 2023.
October 2023: North Korean hackers sent malware phishing emails to employees of South Korea's shipbuilding sector. South Korea's National Intelligence Service suggested that the attacks were intended to gather key naval intelligence that could help North Korea build larger ships.
September 2023: Indian hacktivists targeted Canada's military and Parliament websites with DDoS attacks that slowed system operations for several hours. Hacktivists referenced Canadian Prime Minister Justin Trudeau's public accusation against India of killing Sikh independence activist Hardeep Singh Nijjar as motivation for the hack.
September 2023: Iranian hackers launched a cyberattack against Israel's railroad network. The hackers used a phishing campaign to target the network's electrical infrastructure. Brazilian and UAE companies were also reportedly targeted in the same attack.
September 2023: U.S. and Japanese officials warn that Chinese state-sponsored hackers placed modifying software inside routers to target government industries and companies located in both countries. The hackers use firmware implants to stay hidden and move around in their target's networks. China has denied the allegations.

SOME OF THE ATTACKS

How could it come so far?

Software development in the past

- Software development with proprietary source code
- Software complexity is still low
- Long development cycles
- No or limited connection to the Internet or other networks
- Few platforms to support

Modern software development is more of everything

Software development using proprietary and third-party source code → The software is very complex → Short development cycles → Support from many platforms

More code	More complexity	More velocity	More risk
Software is a business-critical infrastructure in organizations in all industries	Languages Platforms Open source Third-party license code Proprietary code Container Cloud	Agile Shift left Continuous integration Continuous delivery Continuous deployment DevOps	Connection to the internet or other networks

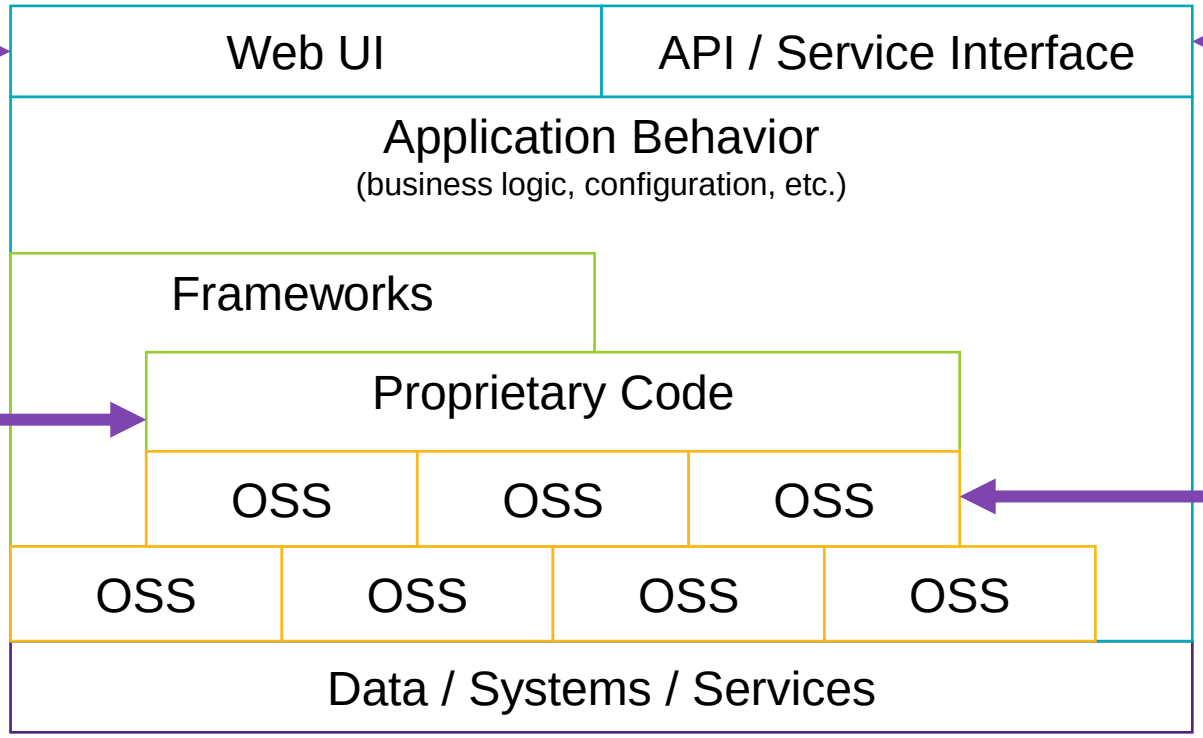
*Source: SAP

To simplify things, let's think about how apps are built

How do we integrate and automate all of this?

How do we know we've addressed exploitable vulnerabilities and data protection issues before we deploy?

How do we ensure the protocols our software serves aren't vulnerable to common hacks?



How can our developers produce code with fewer defects and security weaknesses (CWEs) without slowing down?

How do we track an manage open source use and the security and license compliance risks that come with it?

Modern application

=

Custom or proprietary code

+

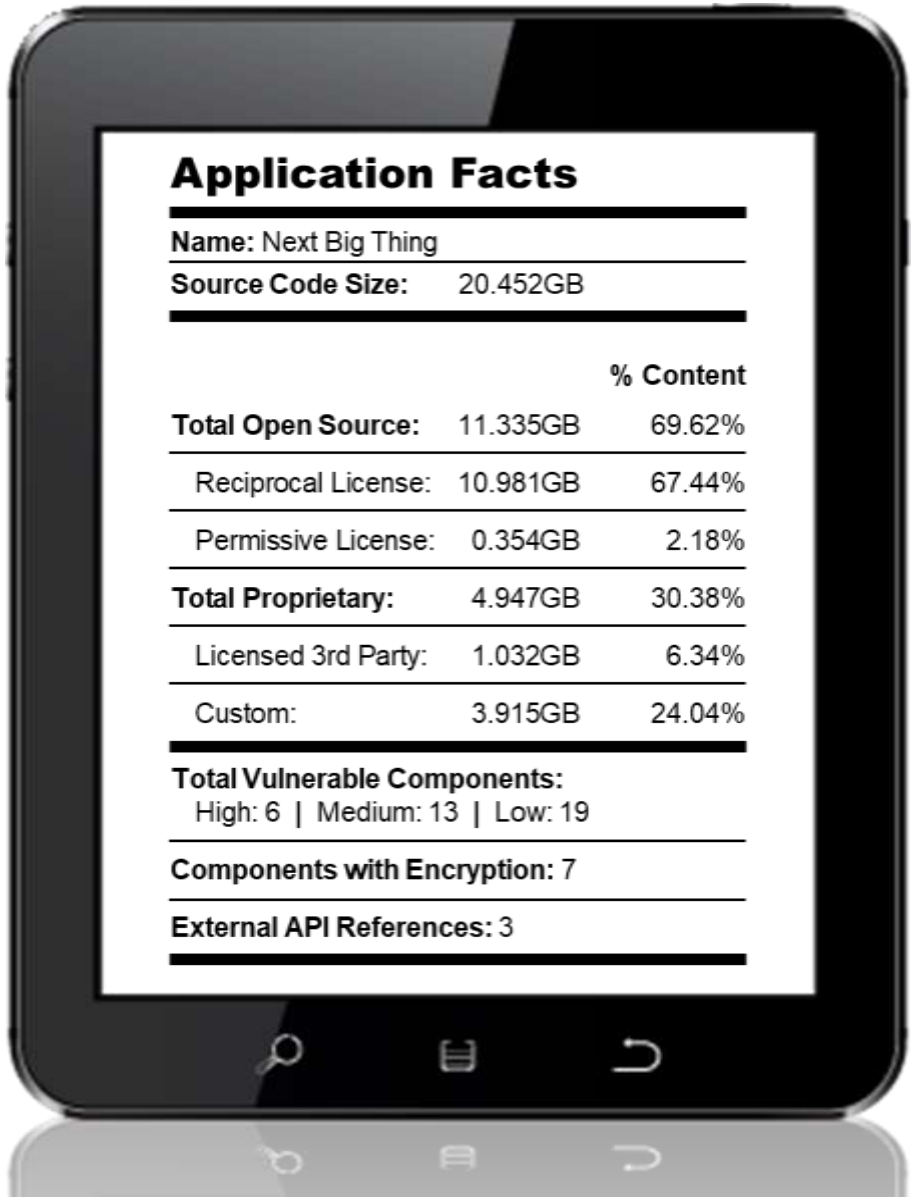
Open source components

+

API usage

+

Application behavior and configuration



Application Facts

Name: Next Big Thing

Source Code Size: 20.452GB

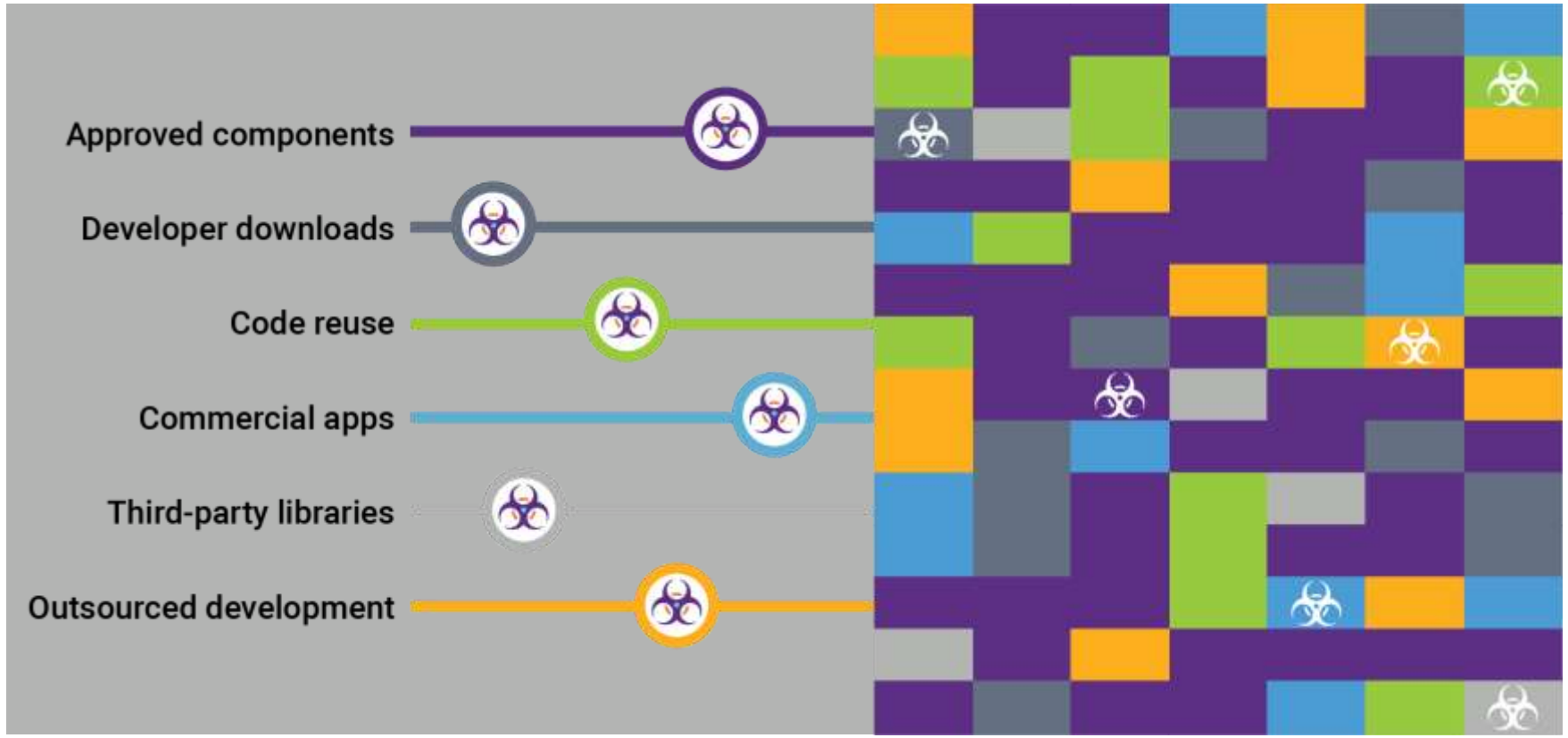
		% Content
Total Open Source:	11.335GB	69.62%
Reciprocal License:	10.981GB	67.44%
Permissive License:	0.354GB	2.18%
Total Proprietary:	4.947GB	30.38%
Licensed 3rd Party:	1.032GB	6.34%
Custom:	3.915GB	24.04%

Total Vulnerable Components:
High: 6 | Medium: 13 | Low: 19

Components with Encryption: 7

External API References: 3

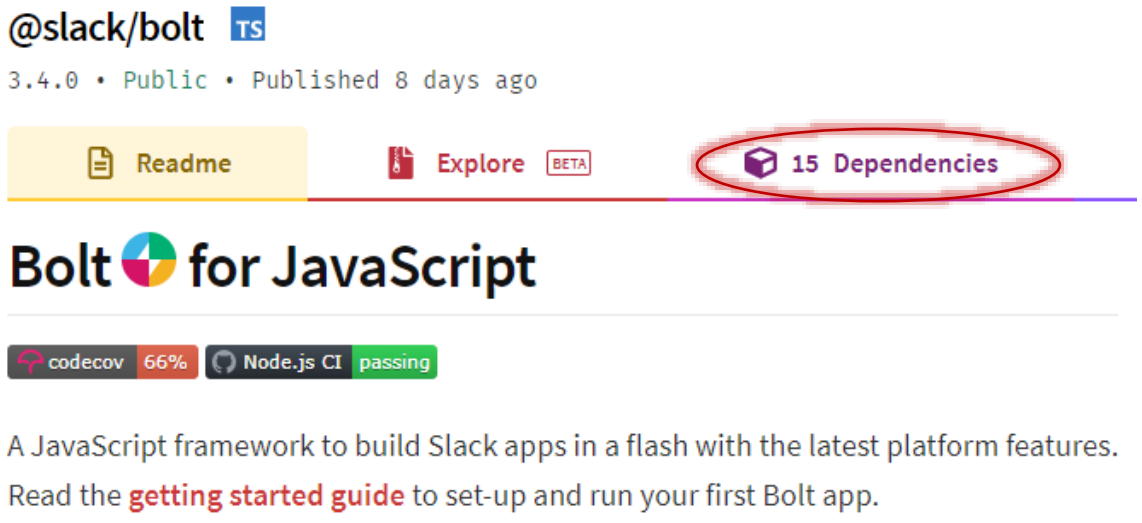
Open source components are third-party components



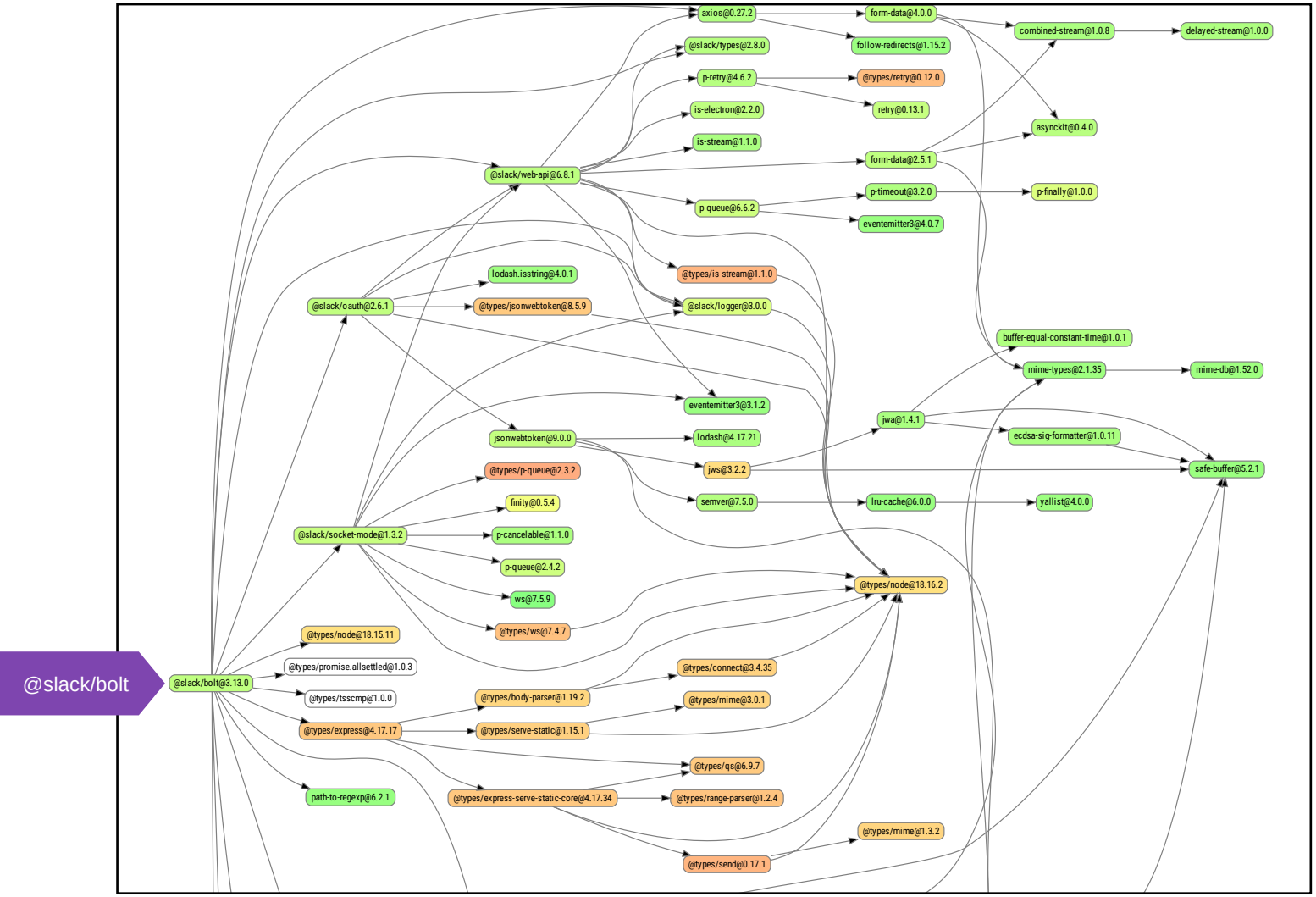
Example:
Integrate Slack and Instagram in one app

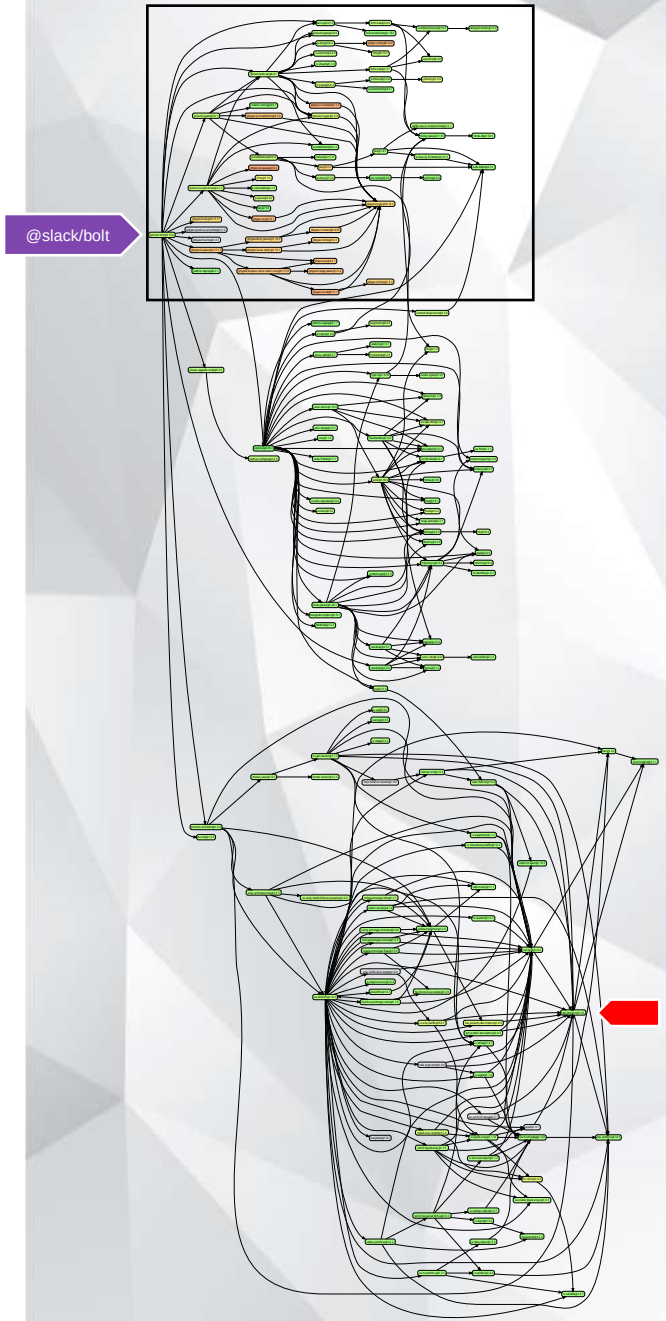
```
"dependencies": {
        "@slack/bolt": "^3.2.0",
        "axios": "^0.21.1",
        "dotenv": "^8.2.0",
        "get-pixels": "^3.3.2",
        "image-size": "^0.9.3",
        "instagram-private-api": "^1.43.3",
        "sharp": "^0.27.1",
        "snoowrap": "^1.22.0"
}
```

8 Declared (Dependencies)



Dependences: @slack/bolt





Dealing with end-of-life and vulnerabilities can be challenging

request DT

2.88.2 • Public • Published a year ago

Readme | Explore BETA | 20 Dependencies

Deprecated!

As of Feb 11th 2020, request is fully deprecated
In fact, none have landed for some time.

For more information about why request is de
refer to this issue.

Open **Request's Past, Present and Future** #3142
mikeal opened this issue on Mar 30, 2019 · 394 comments

Maintenance Mode

Here's the plan.

- `request` will stop accepting new features.
- `request` will stop considering breaking changes.

o merge fixes in a timely fashion, no promises though.
e into master will be published. I've already built this for

e collaborators and enforce 2fa, because commit rights will

245 656 204 233

CVE-2020-28282 Detail

Description

Prototype pollution vulnerability in 'getobject' version 0.1.0 allows an attacker to cause a denial of service and may lead to remote code execution.

Severity CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 9.8 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

Why open source monitoring is important

Three dimensions of risk in open source software

1 Legal risk

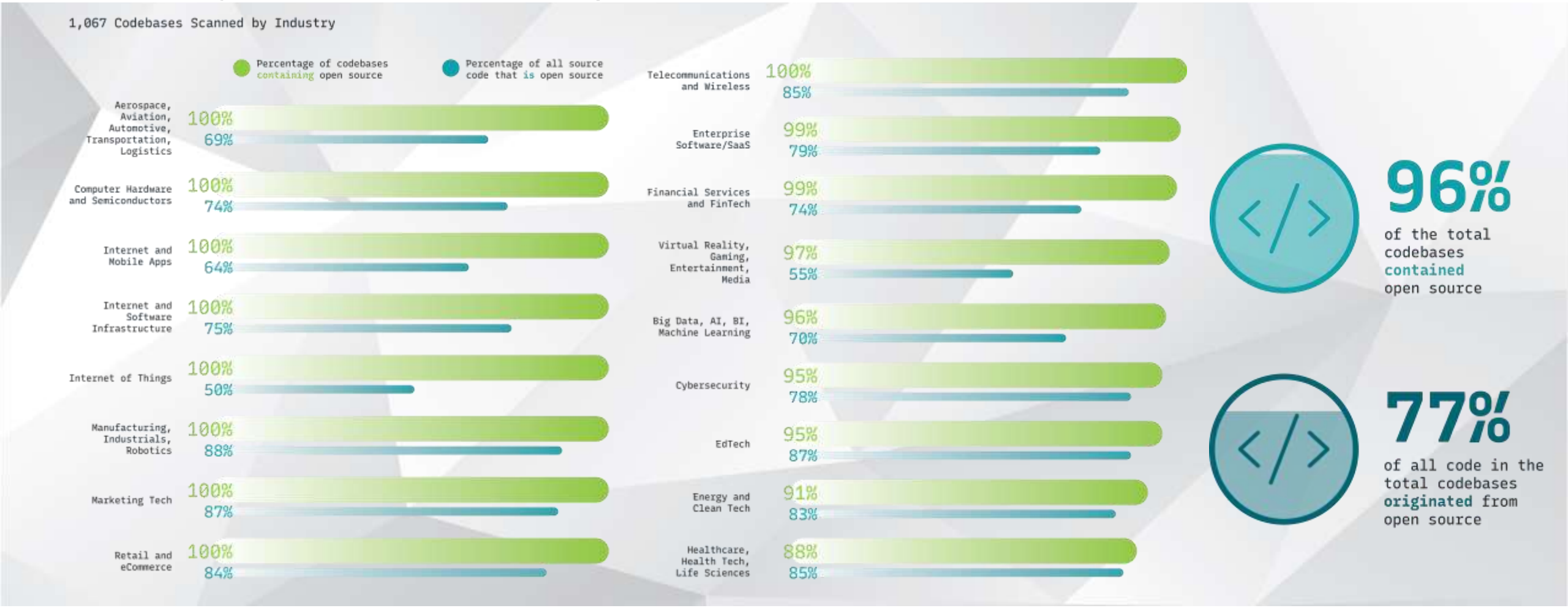
2 Security risk

3 Operational risk

OSSRA 2024

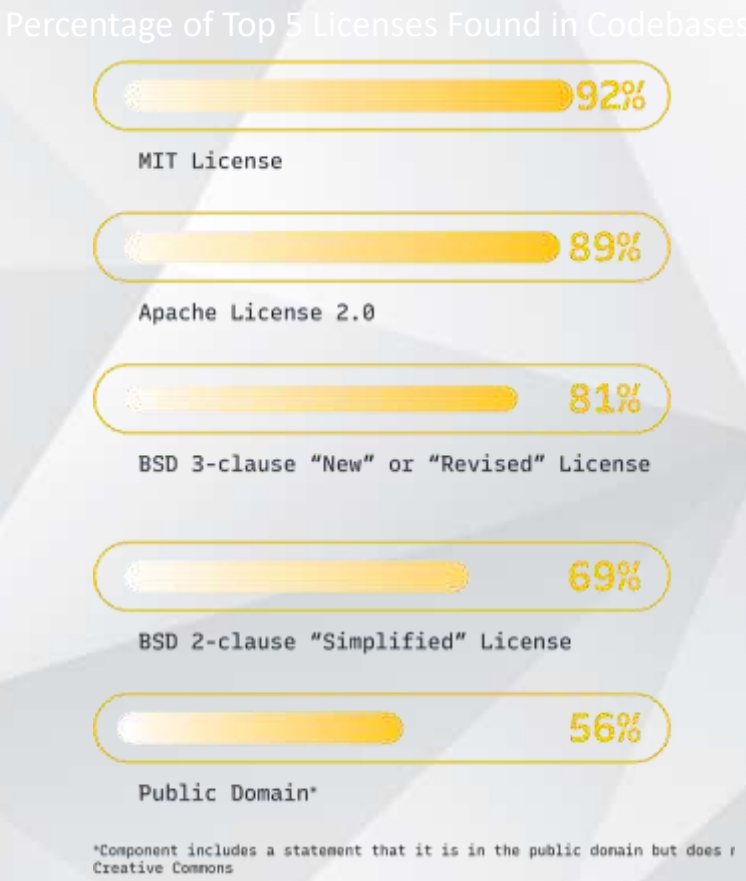
Shared reuse and collaboration fuels innovation

Percentage of codebase that is open source



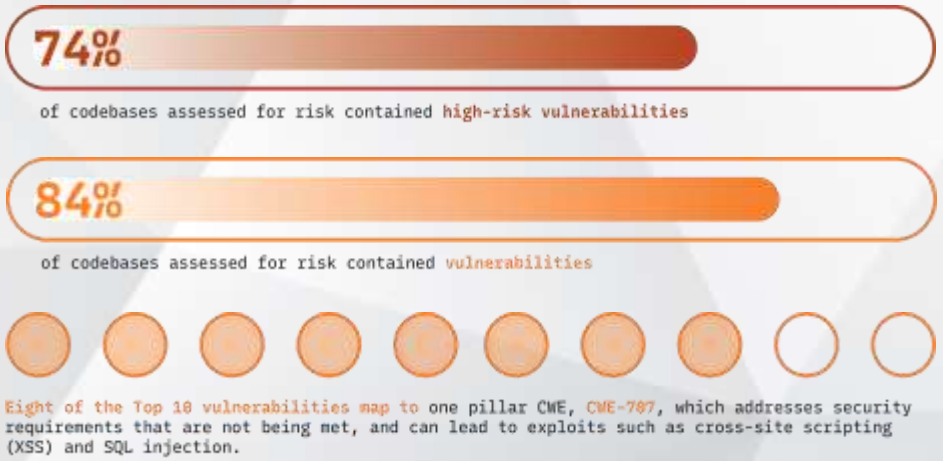
Open source license compliance remains critical

OSSRA 2024



Open source compliance remains critical

OSSRA 2024



84% of codebases contained at least one open source vulnerability

lab lab ai

How to improve your work with ChatGPT

OpenAI

new native group

NEXTG

Bard AI

How to resolve the issue

MAY 12, 2021

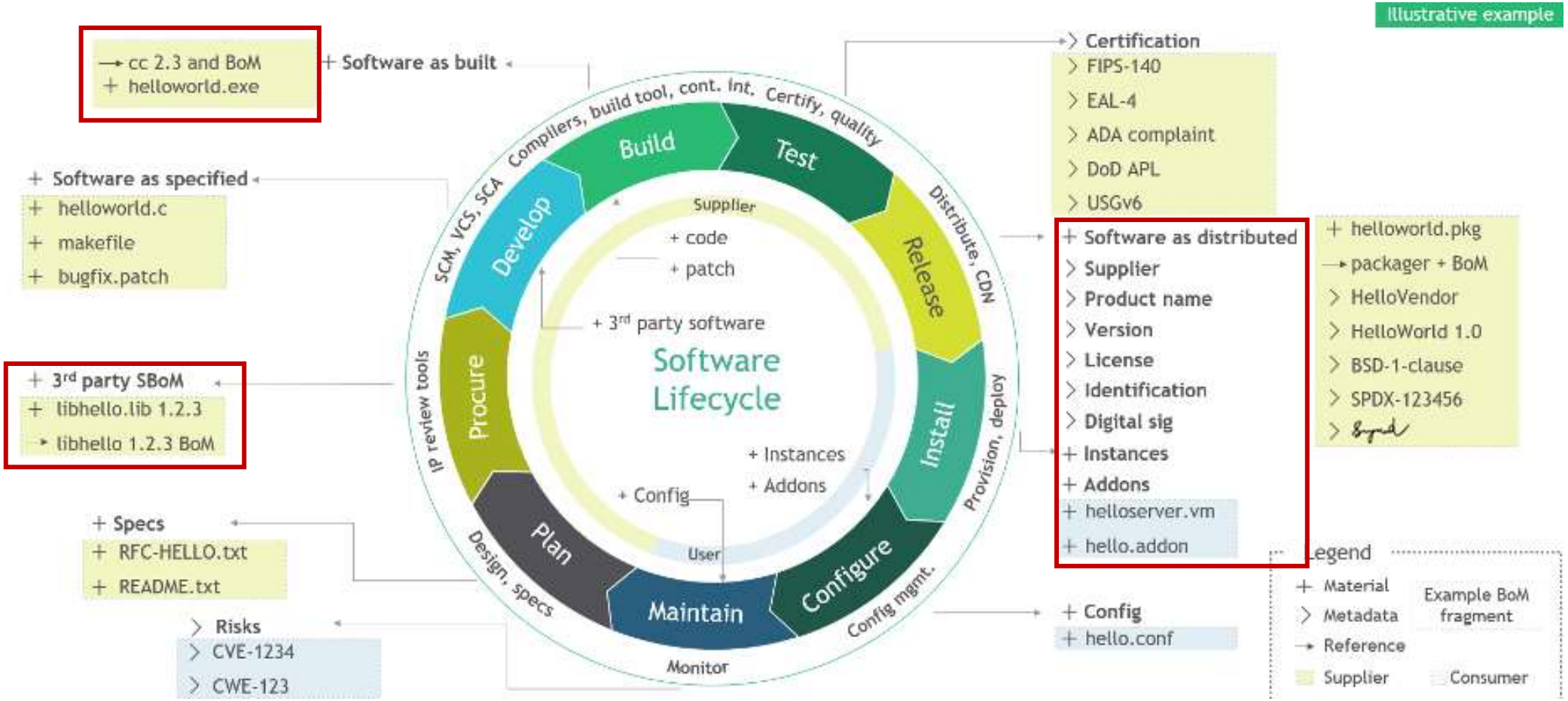
Executive Order on Improving the Nation's Cybersecurity

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must

Executive Order 14028

Improving the country's cybersecurity

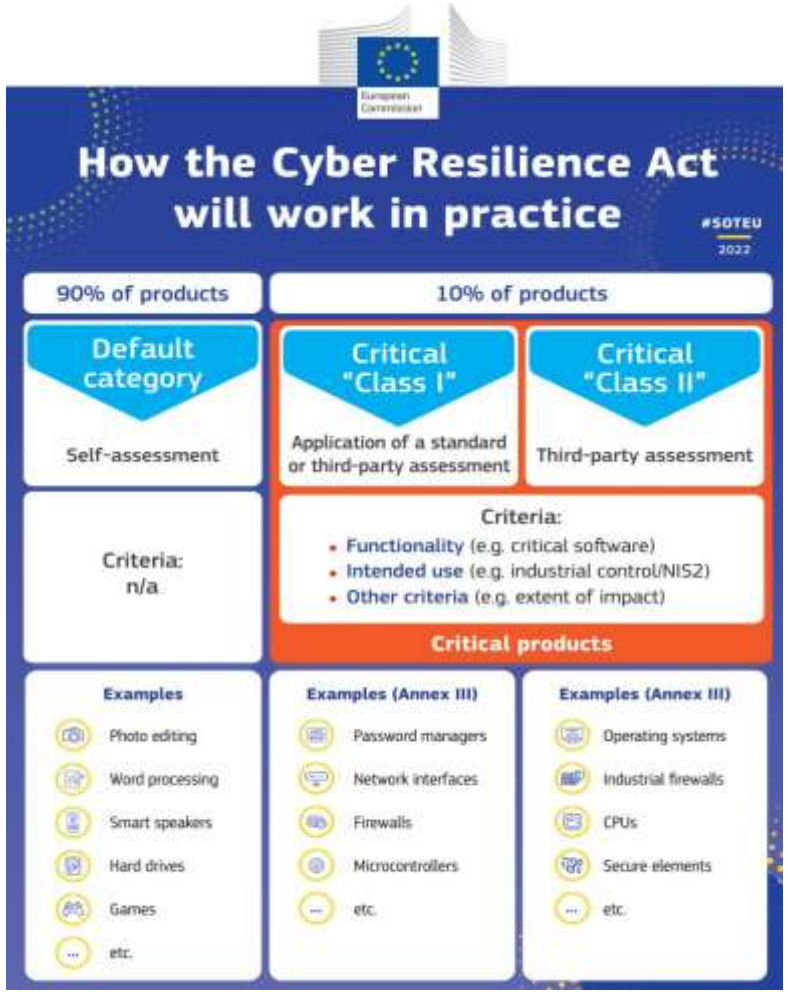


Cybersecurity - EU Regulations

- Cyber Resilience Act

SBOM Subject to a mandate

"Manufacturers of products with digital elements shall: (1) identify and document the vulnerabilities and components contained in the product, including by creating a software bill of materials in a commonly used and machine-readable format..."



The “One Tool to Rule Them All” legend

Focus on the whole range of capabilities

STATIC CODE ANALYSIS

DYNAMIC CODE ANALYSIS

INTERACTIVE CODE ANALYSIS

SOFTWARE COMPOSITION ANALYSIS

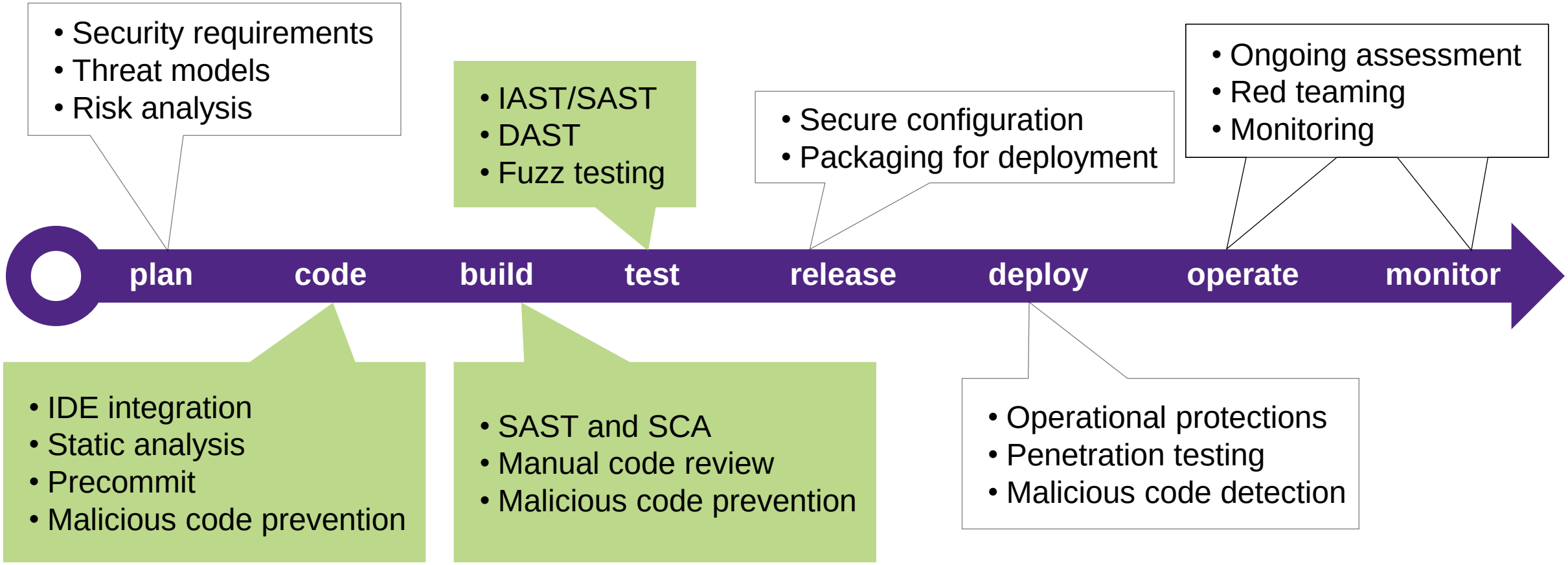
RUNTIME ANALYSIS

PEN TESTING

EDUCATION

MANAGED SERVICES

So much to do, so little time



Take on the challenge

- Planning, vigilance, and information-gathering is key
- Identify untrustworthy source code wherever it is
- Develop procedures for problem remediation
- Call it what you want (SecDevOps, DevSecOps, DevOpsSec) but security is crucial in your DevOps culture
- Integrate the procedures at every step of your process

BSIMM 14

Thank You