Software Supply Chain Security Cheat Sheet

BLUBRACKET

Source code is considered by many to be an organization's most valuable asset. It has also become the most sought-after cyber asset to attack. According to a Cyentia 2021 report, 42% of all financial losses from cyber attacks are caused by software supply chain vulnerabilities or code related threats. These add up to many billions of dollars each year.

Software development for the modern enterprise takes place with code originating from several teams spread across the globe. Writing code is no longer a monolithic affair and developers can utilize pre-designed libraries of software functions to speed up the development process.

According to BluBracket, here are three key steps you need to know in order to protect your organization from software supply chain attacks

1

STEP 1

Lock down access to your code repositories with 2FA/MFA. Make code contributors digitally sign code.

2

STEP 2

Protect your Code Environments by applying patches. Identify configuration vulnerabilities

3

STEP3

Automate scanning and detection of security threats and vulnerabilities contained in code – current and historical

How to Proceed: Questions to ask at each step:

Step 1: Code Access

Where does your code live and who has access?

- Hint: How can I manage Access and Identity Risks?
- Hint: How can I prevent Code Leaks?

Step 2: Securing Code Environments

Securing the configuration of your git repos and cloud infrastructure

- Hint: How to avoid Git Misconfigurations
- Hint: How to identify Infrastructure as Code (IaC) violations

Step 3: What threats should I look for in code content

Securing the configuration of your git repos and cloud infrastructure

- Hint: Can I detect Secrets in
- Code?
- Hint: Prevent exfiltration of PII
- Hint: How to Identify and emove Non-inclusive Language

Access & Identity Vulnerabilities

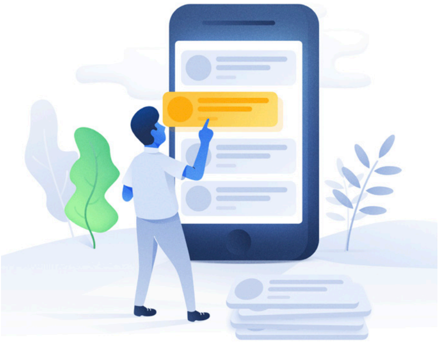
Access can be a viable threat to your most critical assets: control who has access to your code - reduce exposure to external and insider threats.

BluBracket Identifies / Removes Encryption Keys, API Tokens, passwords etc. from code

Code Leaks

Developers inadvertently expose code when they replicate code to external repositories. Valuable IP gets into the wrong hands

BluBracket scans public repositories for code fingerprints that may have leaked into the extended universe



Git Misconfigurations

Use of insecure default configs, un-patched applications exposes huge risks as code is deployed. Attack vector for malicious threat actors – external and insiders as well.

BluBracket scan software components, libraries, and application frameworks for vulnerable misconfigurations

Infrastructure as Code

Infrastructure is becoming the new attack vector as code replaces manual configurations. Attackers can bring down entire applications by targeting infrastructure.

BluBracket looks for secrets and misconfigurations in IaC prior to deployment

Secrets in Code

Access can be a viable threat to your most critical assets: control who has access to your code - reduce exposure to external and insider threats.

BluBracket Identifies / Removes Encryption Keys, API Tokens, passwords etc. from code

Protecting PII

Developers inadvertently expose code when they replicate code to external repositories. Valuable IP gets into the wrong hands

BluBracket scans public repositories for code fingerprints that may have leaked into the extended universe

Use of Non-Inclusive Language

Developers inadvertently expose code when they replicate code to external repositories. Valuable IP gets into the wrong hands

BluBracket scans public repositories for code fingerprints that may have leaked into the extended universe

About Blubracket

BluBracket is a code security solution that integrates with existing processes to mitigate risks in your code, environments, and pipelines unlike legacy tools which provide limited risk coverage and slow down development. BluBracket is headquartered in Palo Alto, California • www.blubracket.com