

SYNOPSYS®

AppSec

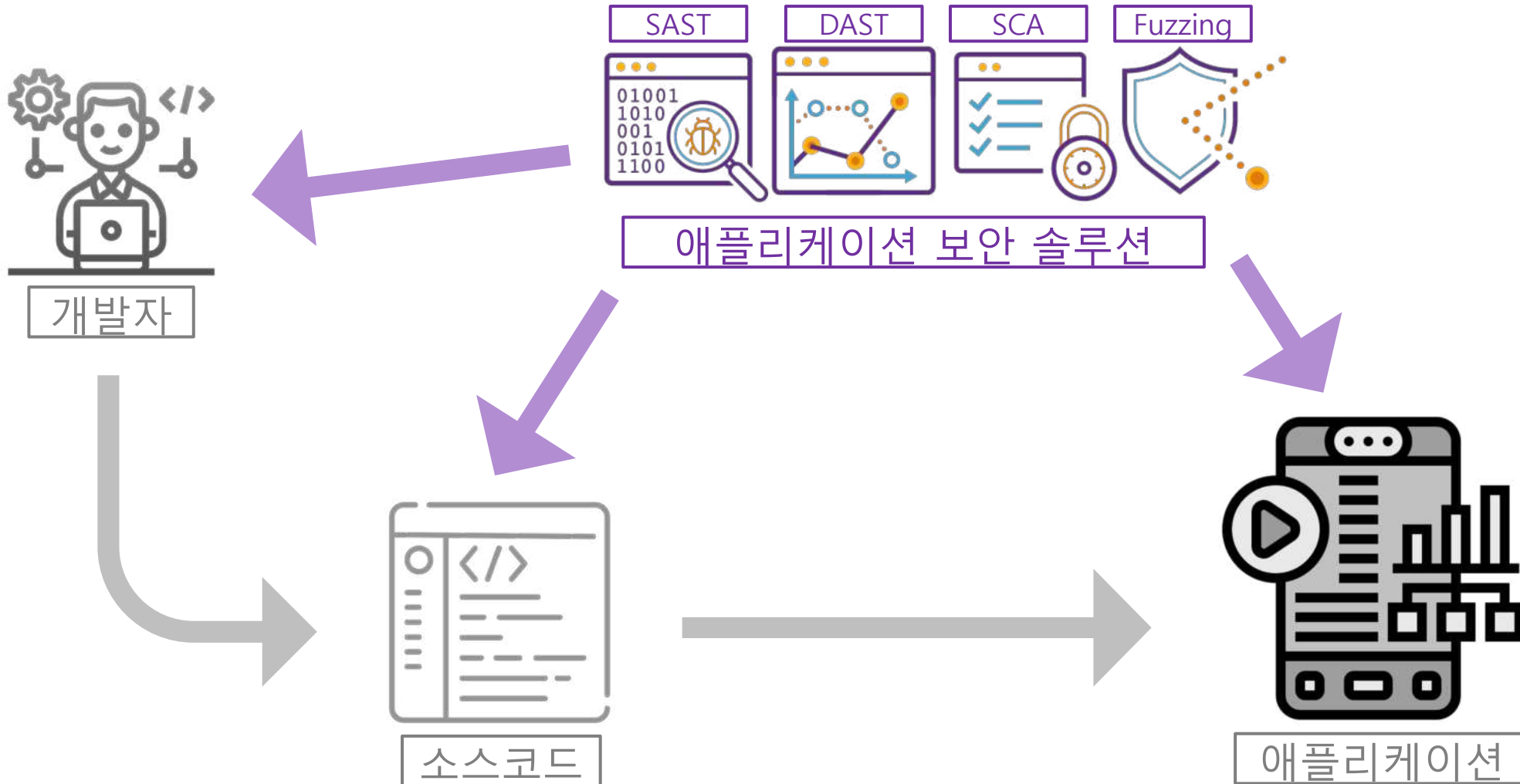
- of the AI, by the AI, for the AI

*AI시대의 애플리케이션 보안*

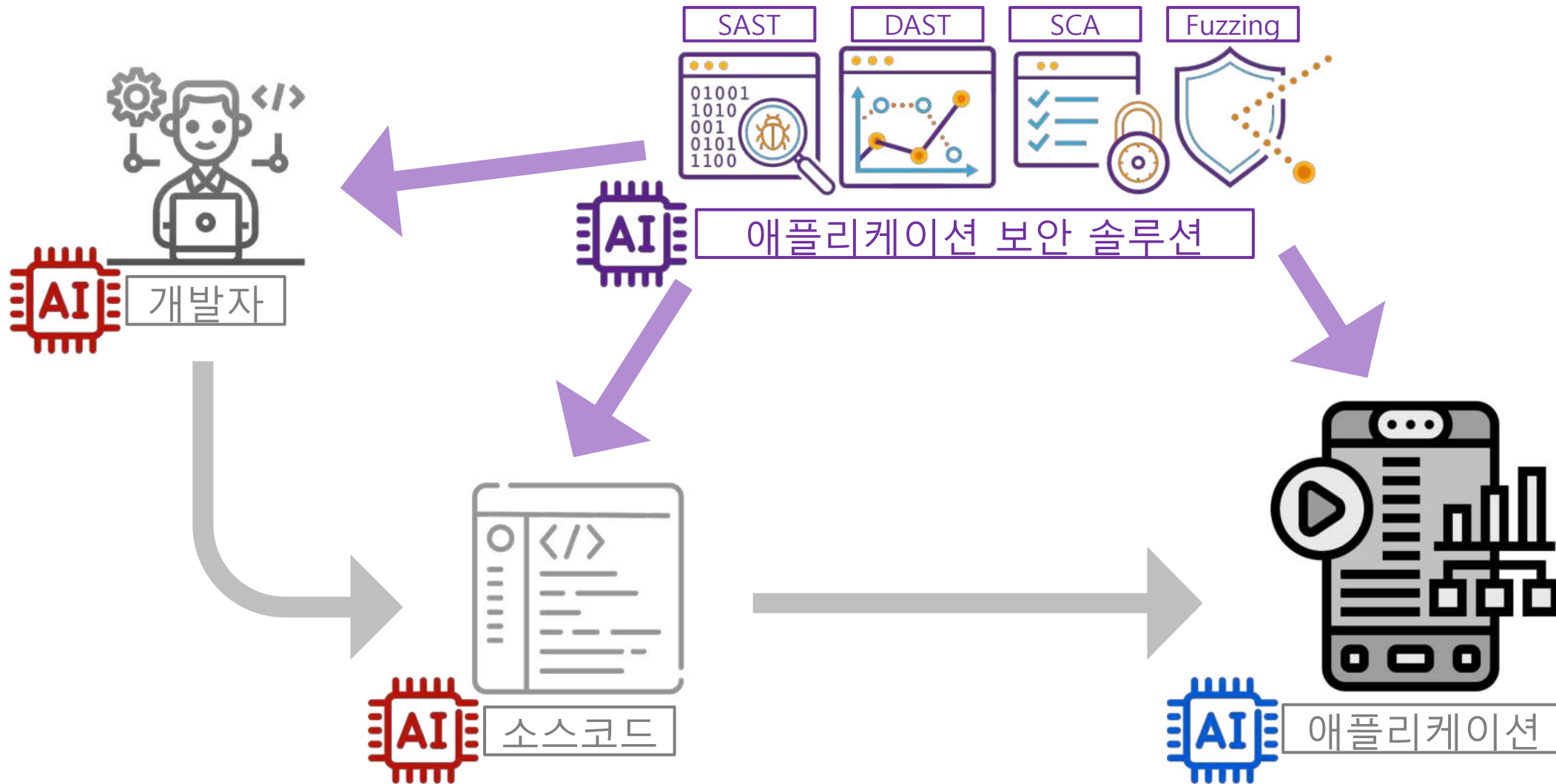
Synopsys Korea SIG, 제병주 부장

2024년 5월 28일

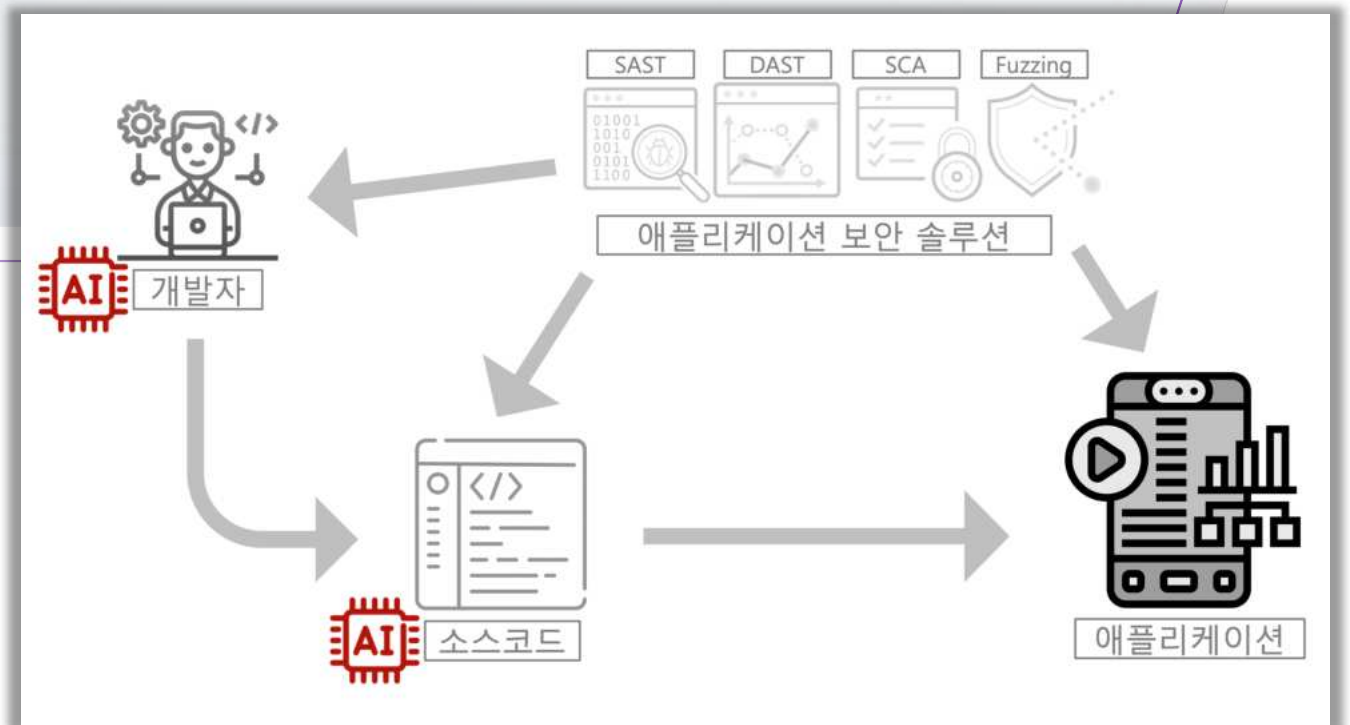
# 애플리케이션 보안의 일반적인 구성



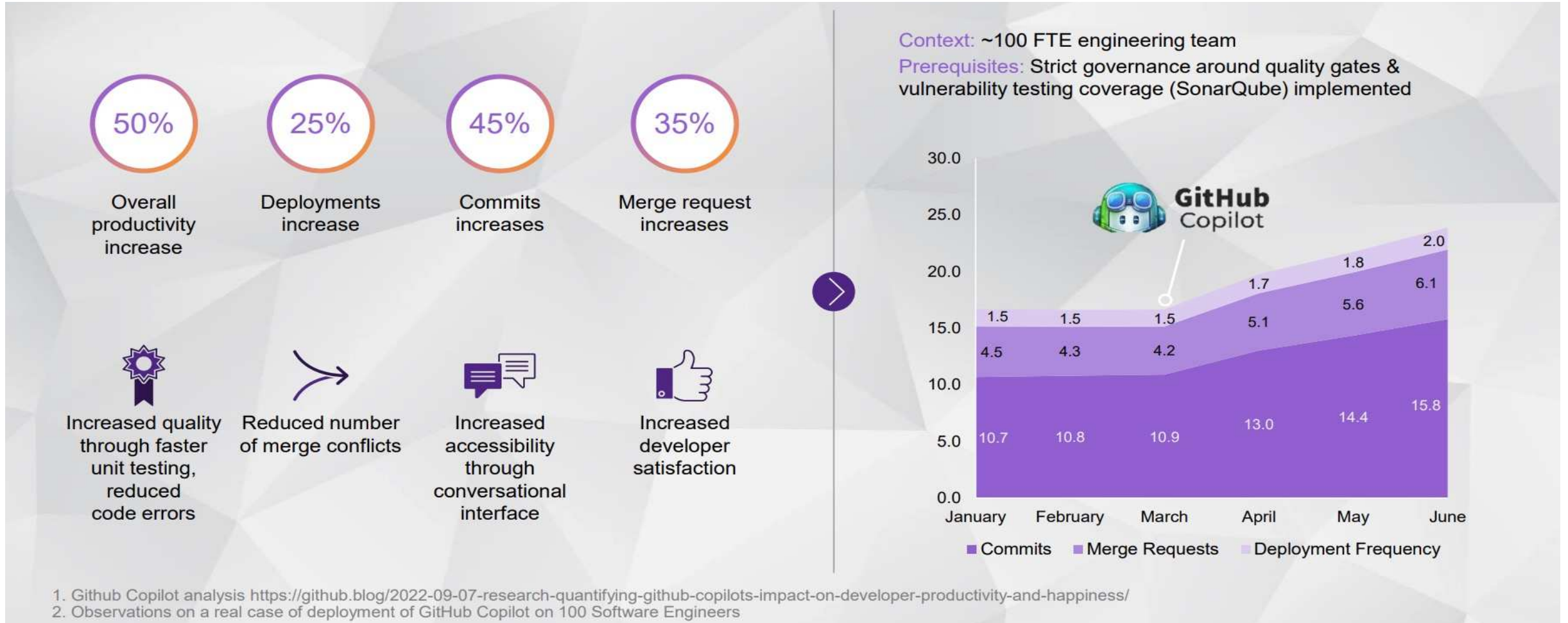
# 애플리케이션 보안에서 AI의 활용



# AI가 작성한 소스코드



# AI를 통해 개발 생산성이 급격하게 증가

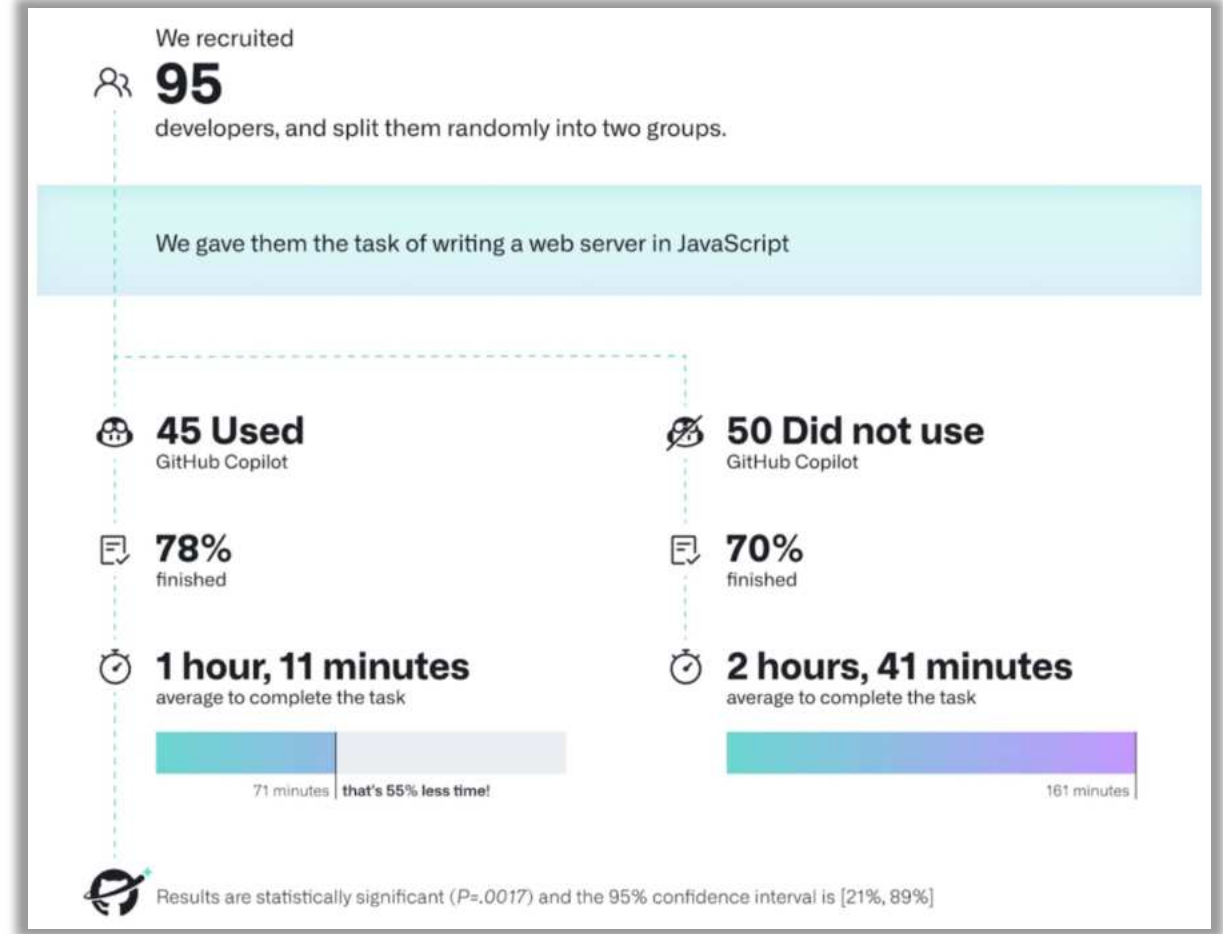


# AI를 통해 개발 생산성이 급격하게 증가

## 개발자가 체감하는 생산성 증가



## 프로젝트 완수에 걸리는 시간 감소



# AI가 작성한 소스코드에서 애플리케이션 보안

## AI가 작성한 코드는 사이버보안에 안전한가?

- 아직은 안전하지 않음
- AI가 보안 코딩을 한다 하더라도, 확인 및 안전을 위한 보안 활동이 필요
- 사람이 작성한 코드와 마찬가지로 애플리케이션 보안을 위한 활동이 필요

## AI가 작성한 코드는 오픈소스 라이선스를 준수하는가?

- 라이선스 위반이 가장 큰 문제
- AI를 통해 오픈소스 라이선스를 준수한다고 해도, 확인 작업이 필요
- Black Duck의 snippet scan을 통해 오픈소스 라이선스 위반 검출 가능



# Black Duck SCA를 통한 snippet analysis 예

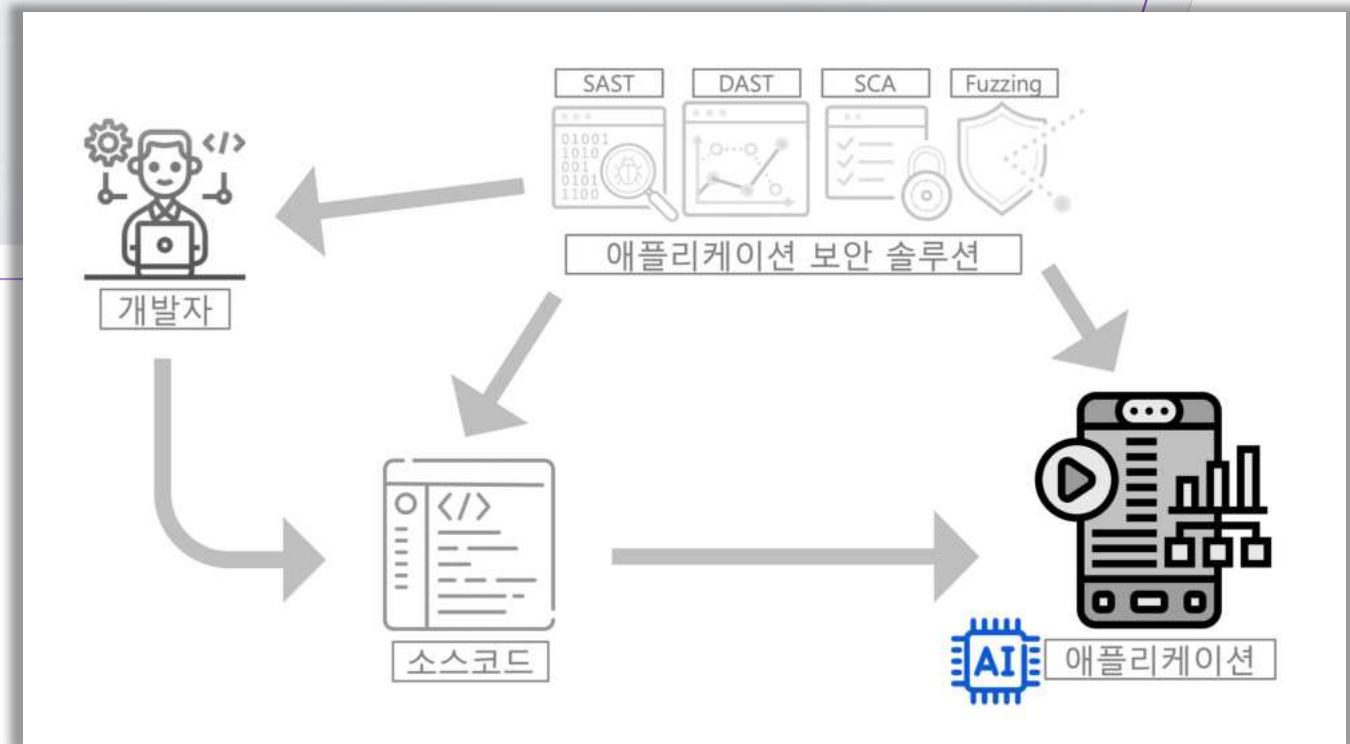
AI가 생성한 코드에서 오픈소스 라이선스 위험을 식별

Scanned File	Matched Component
<p>github-copilot-generated.c</p> <p>Scanned File Path: file:///Users/kadu/Downloads/github-copilot-snippet-scan/github-copilot-generated.c</p> <p>File Size: 3.83 KB</p> <p>(Line 88 to 99)</p>	<p>acado last_1_1_0_beta</p> <p>License: GNU Lesser General Public License v3.0 only</p> <p>Release Date: Oct 6, 2013</p> <p>Matched File Path: /acado-e2ba77daa5171e589c105c794cbf23c4c8385dea/external_packages/csparse/cs_util.c</p> <p>Snippet Match: 17%</p> <p>(Line 2 to 13)</p>
<pre>86 } 87 88 /* allocate a sparse matrix (triplet form or compressed-column form) */ 89 cs *cs_sppalloc (int m, int n, int nzmax, int values, int triplet) 90 { 91     cs *A = (cs *) cs_calloc (1, sizeof (cs)); /* allocate the cs struct */ 92     if (!A) return (NULL); /* out of memory */ 93     A-&gt;m = m; /* define dimensions and nzmax */ 94     A-&gt;n = n; 95     A-&gt;nzmax = nzmax = CS_MAX (nzmax, 1); 96     A-&gt;nz = triplet ? 0 : -1; /* allocate triplet or comp.col */ 97     A-&gt;p = (int *) cs_malloc (triplet ? nzmax : n+1, sizeof (int)); 98     A-&gt;i = (int *) cs_malloc (nzmax, sizeof (int)); 99     A-&gt;x = values ? (double *) cs_malloc (nzmax, sizeof (double)) : NULL; 100     return ((!A-&gt;p    !A-&gt;i    (values &amp;&amp; !A-&gt;x)) ? cs_done (A, NULL, NULL, 0) 101           : A); 102 } 103 104 105  </pre>	<pre>1 #include "cs.h" 2 /* allocate a sparse matrix (triplet form or compressed-column form) */ 3 cs *cs_sppalloc (int m, int n, int nzmax, int values, int triplet) 4 { 5     cs *A = (cs *) cs_calloc (1, sizeof (cs)); /* allocate the cs struct */ 6     if (!A) return (NULL); /* out of memory */ 7     A-&gt;m = m; /* define dimensions and nzmax */ 8     A-&gt;n = n; 9     A-&gt;nzmax = nzmax = CS_MAX (nzmax, 1); 10    A-&gt;nz = triplet ? 0 : -1; /* allocate triplet or comp.col */ 11    A-&gt;p = (int *) cs_malloc (triplet ? nzmax : n+1, sizeof (int)); 12    A-&gt;i = (int *) cs_malloc (nzmax, sizeof (int)); 13    A-&gt;x = values ? (double *) cs_malloc (nzmax, sizeof (double)) : NULL; 14    return ((!A-&gt;p    !A-&gt;i    (values &amp;&amp; !A-&gt;x)) ? cs_sppfree (A) : A); 15 } 16 17 /* change the max # of entries sparse matrix */ 18 int cs_spprealloc (cs *A, int nzmax) 19 { 20     int ok, oki, okj = 1, okx = 1;</pre>

왼쪽의 AI가 생성한 코드가 오른쪽의 GNU 라이선스의 오픈소스와 동일함



# AI를 활용한 애플리케이션



# AI 관련 뉴스 헤드라인

**AI Vision: White House Sets Policy for Future of Artificial Intelligence**  
Artificial Intelligence promises transformative change, with the capacity to revolutionize industries and reshape the way we live, work, and... However, with great power comes even greater responsibility.

**G7 Leaders Release AI Governance Code Same Day USA Signs AI Executive Order**  
Cindy Gordon Contributor @CEO, Innovation Leader Passionate about Modernizing via AI  
Oct 31, 2023, 10:46am EDT

**Gene**  
Under the radar, ethical issues are in the forefront.  
By George Lawton

Like other forms of AI, surrounding data privacy, potentially produce a set of infringements and harmful displacement are additional.

**G7**  
CANADA  
FRANCE  
GERMANY  
ITALY  
JAPAN  
UNITED KINGDOM  
UNITED STATES

The G7 leaders announced Monday that they had reached agreement on a set of international guiding principles on artificial intelligence.

## Biden Urges Congress to Take Action Following AI Order

Experts Praise Executive Order for Focusing on Security Risks Associated With AI

Chris Riotta (@chrisriotta) · October 30, 2023

Share Tweet Share Credit Eligible Get Permission



U.S. President Joe Biden in the White House on March 13, 2023 (Image: Shutterstock)

**AI SAFETY SUMMIT**  
HOSTED BY THE UK | 1-2 NOVEMBER 2023

AI Safety Summit attendees including world leaders and government officials.

U.S. Secretary of State Antony Blinken, German Economy and Climate Minister Robert Habeck, President of the European Commission Ursula von der Leyen, Britain's Prime Minister Rishi Sunak, Italy's Prime Minister Giorgia Meloni, United Nations Secretary-General Antonio Guterres, and others attend the AI Safety Summit in Blechley Park, near Milton Keynes, Britain, November 2, 2023.

# AI의 물결은 기대와 두려움을 불러옵니다!

## AI 기대와 두려움

- **빠르게 변화하는 생성형 AI 기술**
  - ✓ ChatGPT, Copilot
- **AI 가이드 레일을 둘러싼 글로벌 토론**
  - ✓ 히로시마 AI 프로세스 - G7 회원국 리더
- **AI 거버넌스**
  - ✓ AI 거버넌스 탐구를 위한 UN의 새로운 자문 기구 (2023년 10월 26일)
  - ✓ 미국 대통령의 **AI 행정명령** (2023년 10월 20일)
  - ✓ 영국 “**국제 AI 서밋**” (2023년 11월 2일)



### 참조:

- U.S. President Joe Biden has [issued an executive order](#) (EO) (October 30<sup>th</sup>, 2023)
- [Hiroshima AI Process.pdf \(mofa.go.jp\)](#) (May 2023 Japan)
- [Commission welcomes G7 leaders' agreement \(europa.eu\)](#) (May 2023)
- The United Nations [announced](#) a new [AI advisory board](#) (October 2023)
- [The AI Safety Summit 2023 - GOV.UK](#) (November 2023)

# AI 행정명령?



“

행정 명령은 **AI 안전 및 보안에 대한 새로운 표준을 확립**하고, 미국인의 개인 정보를 보호하고, 형평성과 시민권을 증진하고, 소비자와 근로자를 옹호하고, **혁신과 경쟁을 촉진**하고, 전 세계에서 미국의 리더십을 발전시키는 등의 작업을 수행합니다.

”

참조: <https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/>



# 미국 행정부의 AI관련 활동 웹사이트

<https://ai.gov>

An official website of the United States government [Here's how you know](#) ▾

AI.GOV Administration Actions Government Use of AI Research and Teach AI Bring your AI Skills to the U.S. Make Your Voice Heard Apply Now Español

PRESIDENT BIDEN

MAKING AI WORK FOR THE AMERICAN PEOPLE

JOIN THE NATIONAL AI TALENT SURGE

Apply Now

PLAY VIDEO

INTRODUCTION

AI is one of the most powerful technologies of our time. President Biden has been clear that we must take bold action to harness the benefits and mitigate the risks of AI. The Biden-Harris Administration has acted decisively to protect safety and rights in the age of AI, so that everyone can benefit from the promise of AI.

[Learn More about the Biden-Harris Administration's Actions](#)

<https://nairrpilot.org/>

NAIRR Pilot National Artificial Intelligence Research Resource Pilot

Current Opportunities ▾ NAIRR Secure Awarded Projects About

## The National Artificial Intelligence Research Resource (NAIRR) Pilot

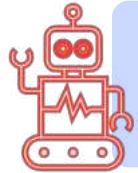
The NAIRR Pilot aims to connect U.S. researchers and educators to computational, data, and training resources needed to advance AI research and research that employs AI. Federal agencies are collaborating with government-supported and non-governmental partners to implement the Pilot as a preparatory step toward an eventual full NAIRR implementation.

- Spur innovation
- Increase diversity of talent
- Improve capacity
- Advance trustworthy AI

[Learn more about NAIRR Pilot](#) [Subscribe for updates](#)

# “안전하고 신뢰할 수 있는 AI”를 향한 여정

행정 명령의 일부 특징:



행정명령에는 “**강력한 AI 시스템의 개발자는 안전 테스트 결과를 미국 정부와 공유해야 한다**”고 명시



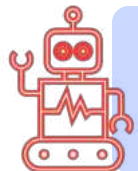
행정명령은 “**AI 시스템의 잠재적 위험으로부터 미국인을 보호**” 할 계획입니다.



“**새로운 AI 안전 및 보안 기준을 국방 생산법(1950)**”에 맞춰 조정



또한, “**의료, 정의 및 주택 분야의 형평성과 시민권, 차별 및 편견**”을 다루고 있습니다.



**NIST**는 모델이 대중에게 공개될 수 있도록 수행해야 하는 **AI 테스트 프레임워크**를 개발하고 있습니다.

참조: [https://www.fema.gov/sites/default/files/2020-03/Defense\\_Production\\_Act\\_2018.pdf](https://www.fema.gov/sites/default/files/2020-03/Defense_Production_Act_2018.pdf)

# 행정명령 14110 수행을 위한 NIST의 업무 및 일정

**NIST** Search NIST Menu

Information Technology /Artificial intelligence

## EXECUTIVE ORDER ON SAFE, SECURE, AND TRUSTWORTHY ARTIFICIAL INTELLIGENCE

**Executive Order Tasks**

- Generative AI
- Secure Software
- Synthetic Content
- Differential Privacy
- Biosecurity: Synthetic Nucleic Acid Sequencing
- Test, Evaluation and Red-teaming
- AI Standards

**Request for Information**

**Engage**

**FAQs**

AI @ NIST

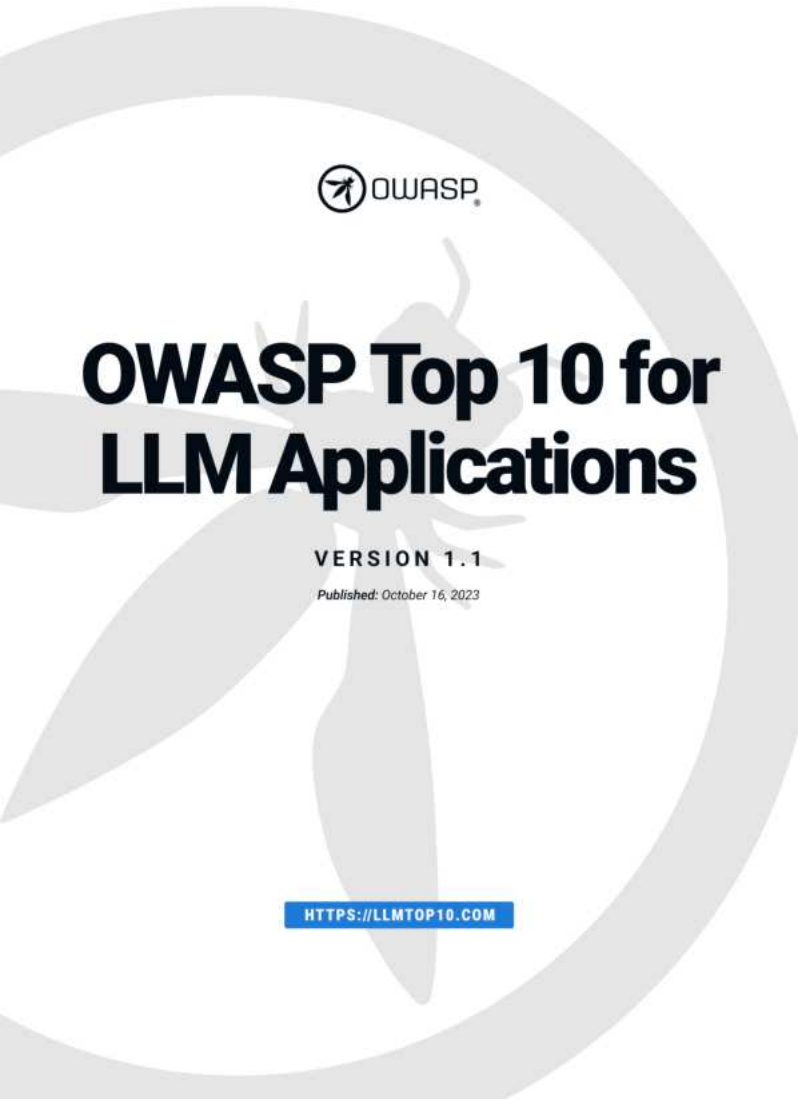
## NIST's Due Dates Under Executive Order 14110



참조: <https://www.nist.gov/artificial-intelligence/executive-order-safe-secure-and-trustworthy-artificial-intelligence>



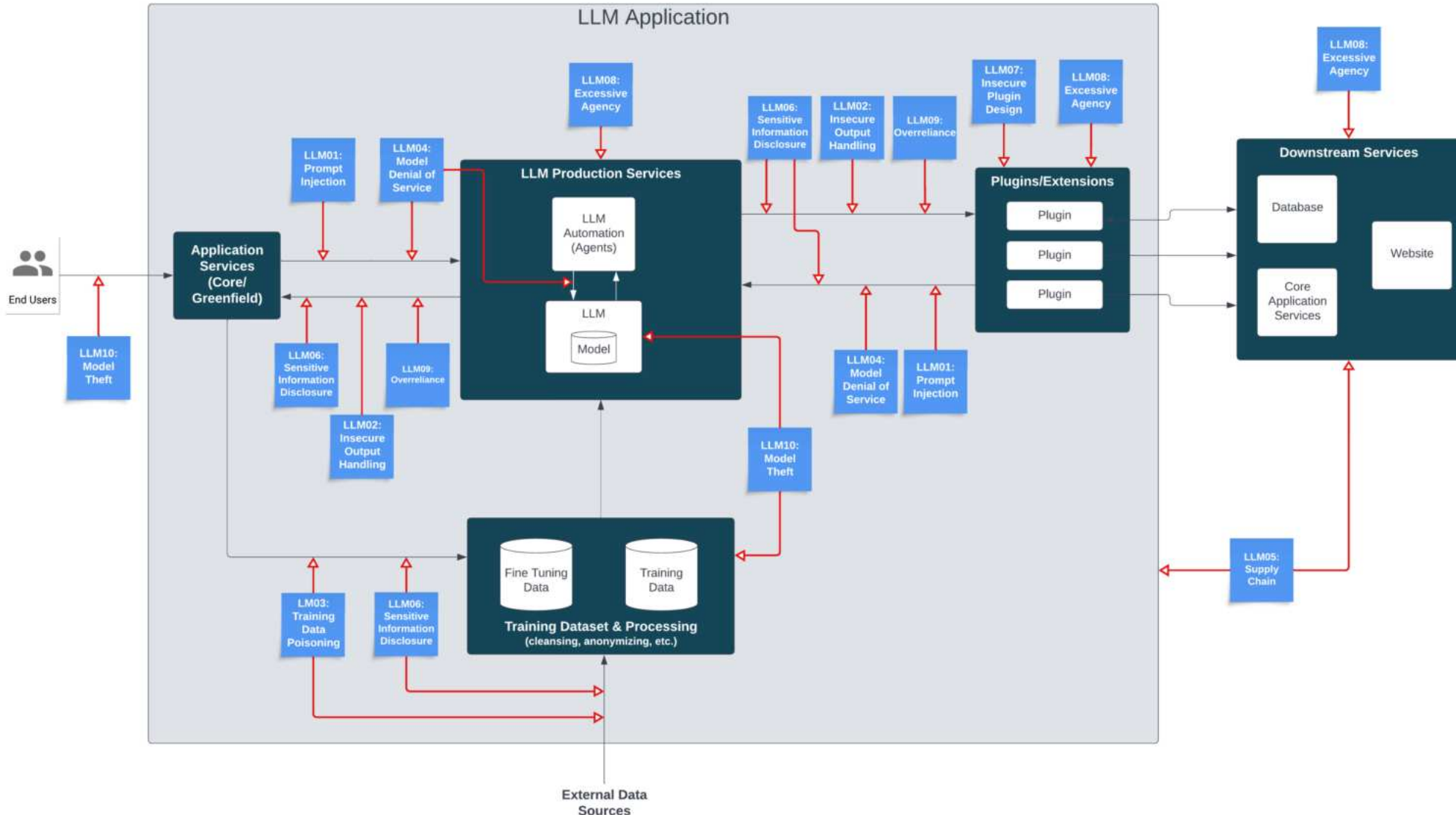
# OWASP Top 10 for LLM Applications



<p><b>LLM01</b></p> <h3>Prompt Injection</h3> <p>This manipulates a large language model (LLM) through crafty inputs, causing unintended actions by the LLM. Direct injections overwrite system prompts, while indirect ones manipulate inputs from external sources.</p>	<p><b>LLM02</b></p> <h3>Insecure Output Handling</h3> <p>This vulnerability occurs when an LLM output is accepted without scrutiny, exposing backend systems. Misuse may lead to severe consequences like XSS, CSRF, SSRF, privilege escalation, or remote code execution.</p>	<p><b>LLM03</b></p> <h3>Training Data Poisoning</h3> <p>This occurs when LLM training data is tampered, introducing vulnerabilities or biases that compromise security, effectiveness, or ethical behavior. Sources include Common Crawl, WebText, OpenWebText, &amp; books.</p>	<p><b>LLM04</b></p> <h3>Model Denial of Service</h3> <p>Attackers cause resource-heavy operations on LLMs, leading to service degradation or high costs. The vulnerability is magnified due to the resource-intensive nature of LLMs and unpredictability of user inputs.</p>	<p><b>LLM05</b></p> <h3>Supply Chain Vulnerabilities</h3> <p>LLM application lifecycle can be compromised by vulnerable components or services, leading to security attacks. Using third-party datasets, pre-trained models, and plugins can add vulnerabilities.</p>
<p><b>LLM06</b></p> <h3>Sensitive Information Disclosure</h3> <p>LLMs may inadvertently reveal confidential data in its responses, leading to unauthorized data access, privacy violations, and security breaches. It's crucial to implement data sanitization and strict user policies to mitigate this.</p>	<p><b>LLM07</b></p> <h3>Insecure Plugin Design</h3> <p>LLM plugins can have insecure inputs and insufficient access control. This lack of application control makes them easier to exploit and can result in consequences like remote code execution.</p>	<p><b>LLM08</b></p> <h3>Excessive Agency</h3> <p>LLM-based systems may undertake actions leading to unintended consequences. The issue arises from excessive functionality, permissions, or autonomy granted to the LLM-based systems.</p>	<p><b>LLM09</b></p> <h3>Overreliance</h3> <p>Systems or people overly depending on LLMs without oversight may face misinformation, miscommunication, legal issues, and security vulnerabilities due to incorrect or inappropriate content generated by LLMs.</p>	<p><b>LLM10</b></p> <h3>Model Theft</h3> <p>This involves unauthorized access, copying, or exfiltration of proprietary LLM models. The impact includes economic losses, compromised competitive advantage, and potential access to sensitive information.</p>

참조: <https://owasp.org/www-project-top-10-for-large-language-model-applications/>

# OWASP Top 10 for LLM Applications 데이터 흐름도



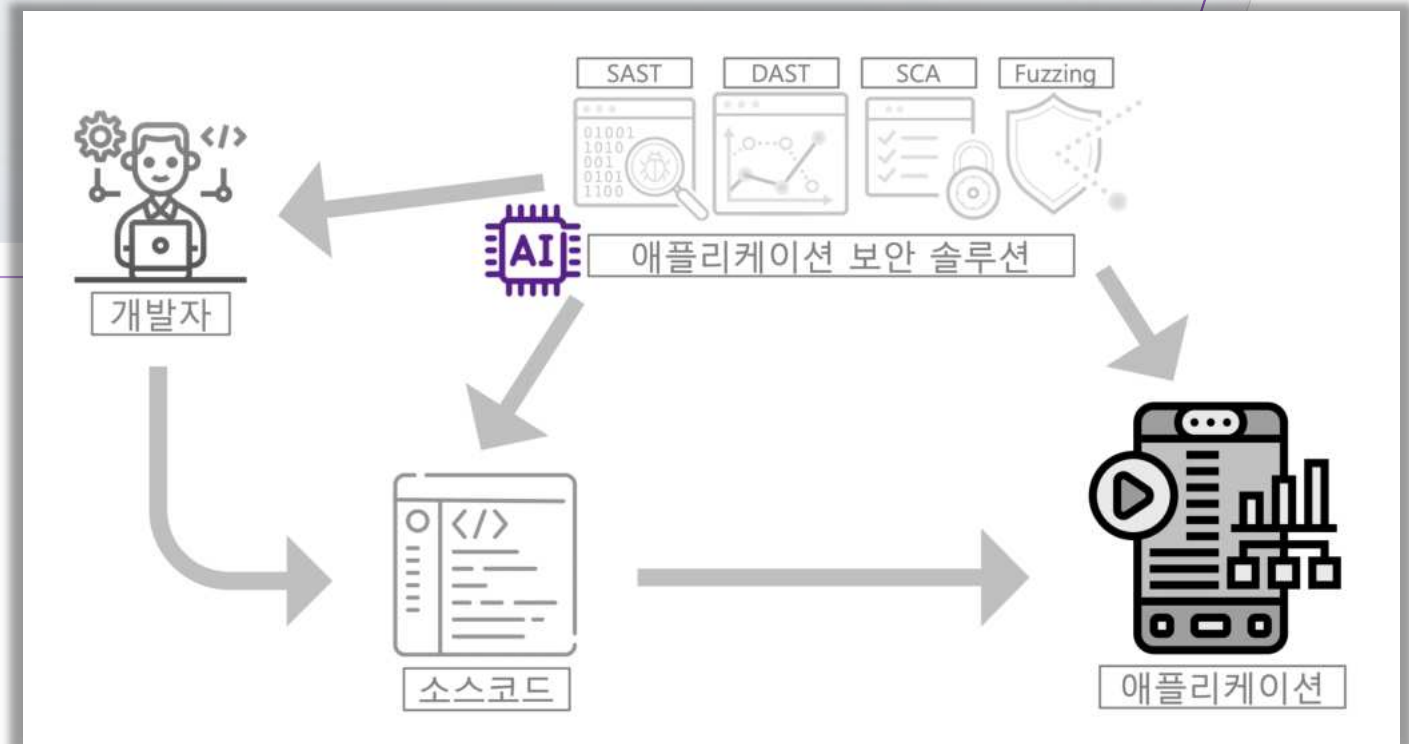
# OWASP Top 10 for LLM Applications 항목

LLM01 프롬프트 주입	LLM02 안전하지 않은 출력처리	LLM03 학습 데이터 중독	LLM04 Denial of Service 모델	LLM05 공급망 취약점
LLM06 민감한 정보 누출	LLM07 안전하지 않은 플러그인 디자인	LLM08 과도한 권한의 LLM 에이전시	LLM09 과도한 LLM 의존	LLM10 모델 도난

# OWASP Top 10 for LLM Applications 항목별 예방조치

<b>LLM01</b> 프롬프트 주입 DAST	<b>LLM02</b> 안전하지 않은 출력처리 SAST	<b>LLM03</b> 학습 데이터 중독 ???	<b>LLM04</b> Denial of Service 모델 DAST	<b>LLM05</b> 공급망 취약점 SCA
<b>LLM06</b> 민감한 정보 누출 ARA	<b>LLM07</b> 안전하지 않은 플러그인 디자인 SAST	<b>LLM08</b> 과도한 권한의 LLM 에이전시 ???	<b>LLM09</b> 과도한 LLM 의존 ARA	<b>LLM10</b> 모델 도난 ARA

# AI를 활용한 보안 솔루션



# 보안 솔루션에서 AI 활용 방안

## EXPLANATION

왜 보안취약점이 발생하는 지에 대해 일반적인 설명이 아니라 해당 문제에 맞춤형 설명을 제공

## FIX GUIDE

어떻게 보안취약점을 해결하는 지에 대해 가이드를 제공

## FIX CODE

보안취약점을 해결한 코드를 생성하여 제시

## FP REMOVAL

애플리케이션 보안 도구에서 가장 문제가 되는 '오탐'을 AI를 활용하여 사전에 제거

## CORRELATION

발견된 보안취약점 중에서 동일한 원인에 의해 발생한 문제들을 묶어서 하나의 아이템으로 표시

### Source Code

The finding occurs in [gitrepo/routes/vulnCodeSnippet.ts](#) on line 94

```
82 }
83 } catch (error) {
84   const statusCode = setStatusCode(error)
85   res.status(statusCode).json({ status: 'error', error: utils.ge
86   return
87 }
88 const vulnLines: number[] = snippetData.vulnLines
89 const neutralLines: number[] = snippetData.neutralLines
90 const selectedLines: number[] = req.body.selectedLines
91 const verdict = getVerdict(vulnLines, neutralLines, selectedLine
92 let hint
93 if (fs.existsSync('./data/static/codefixes/' + key + '.info.yml'
94   const codingChallengeInfos = yaml.load(fs.readFileSync('./data
95   if (codingChallengeInfos?.hints) {
96     if (accuracy.getFindItAttempts(key) > codingChallengeInfos.h
97     if (vulnLines.length === 1) {
```



# Polaris Assist: AI를 활용한 가이드 제공

The screenshot displays the Synopsys Polaris interface for a project named 'Example Application'. The main view shows a list of issues with columns for Issue Type, Location, Filename/Orig, Tool Type, Triage Status, CWE, Vulnerability ID, Jira ID, Fix-By, and First Detected. One issue, 'Insufficient Session Expiration', is highlighted. Below the list, the 'Issue Details' section shows the location 'src/main/java/org/owasp/webgoat/webwolf/jwt/JWTToken.java' and the first detected date 'Feb 15, 2024 10:36 AM'. A red box highlights a button labeled 'AI Insight powered by Polaris Assist'.

Issue Type	Location	Filename/Orig	Tool Type	Triage Status	CWE	Vulnerability ID	Jira ID	Fix-By	First Detected
Improper Resource Shutdown or Release	src/main/java/org/...	SqlInjection...	SAST	Not Triaged	CWE-4...		PD-85		Oct 19, 202...
<b>Insufficient Session Expiration</b>	src/main/java/org/...	JWTToken.ja...	SAST	Not Triaged	CWE-6...		PD-85		Feb 15, 202...
Improper Resource Shutdown or Release	src/main/java/org/...	VulnerableT...	SAST	Not Triaged	CWE-4...		PD-85		Oct 17, 202...



SaaS 기반으로  
SAST, SCA, DAST  
테스트를  
통합 제공하는  
Synopsys SIG의  
차세대 솔루션



# Polaris Assist

The screenshot shows the Synopsys interface for 'Example Application' in 'Project One' on the 'main (default)' branch. The 'Issues' tab is active, displaying a table of security issues. The table has columns for Issue Type, Location, Filename/Orig, Tool Type, and Triage Status. Three issues are listed:

Issue Type	Location	Filename/Orig	Tool Type	Triage Status
Improper Resource Shutdown or Release	src/main/java/org/...	SqlInjection...	SAST	Not Triaged
Insufficient Session Expiration	src/main/java/org/...	JWTTokenja...	SAST	Not Triaged
Improper Resource Shutdown or Release	src/main/java/org/...	VulnerableT...	SAST	Not Triaged

Below the table, the 'Issue Details' tab is selected, showing the location: 'src/main/java/org/owasp/webgoat/webwolf/jwt/JWTToken.java'. The 'First Detected' date is 'Feb 15 2024 10:36 AM' and the tool used is 'Coverity'.

The screenshot shows the detailed view of the 'Insufficient Session Expiration' issue. The 'Issue Details' tab is active, displaying the following information:

- Location:** src/main/java/org/owasp/webgoat/webwolf/jwt/JWTToken.java
- First Detected:** Feb 15 2024 10:36 AM
- Tool:** Coverity

The 'Contributing Code Events' tab is also active, showing a code snippet:

```
124 new JwtConsumerBuilder()
125     .setSkipAllValidators()
126     .setVerificationKey(new HmacKey(secretKey.getBytes(UTF_8)))
127     .setRelaxVerificationKeyValidation()
128     .build();
129 try {
```

Below the code, the 'Issue Summary' section states: "'JwtConsumerBuilder' ignores expiration time by default, making JSON web tokens valid forever and allowing attackers a longer window to exploit. CWE-613."

The 'Code Analysis' section provides a functional description:

- This code snippet defines a private method called "validateSignature".
- The method takes two parameters - "secretKey" and "jwt".
- It uses the "hasText" method to check if the "secretKey" is not null or empty.
- It creates an instance of "JwtConsumer" using the "JwtConsumerBuilder" class.
- The "setSkipAllValidators" method is called to skip all JWT validation checks.
- It sets a verification key using the "setVerificationKey" method.
- The "setRelaxVerificationKeyValidation" method is called to relax verification key validation.
- Finally, the "build" method is called to build and return the "JwtConsumer" object.
- The method then tries to verify the JWT using this object and the "try" block.
- If verification fails, an exception is thrown.

The 'Weakness' section states: "CWE-613, Ignoring expiration time in JSON web token. Impact: Attackers have a longer window to exploit stolen tokens due to their indefinite validity."

The 'Fix Suggestion' section provides the corrected code snippet:

```
124     JwtConsumerBuilder()
        .setSkipAllValidators()
        .setVerificationKey(new HmacKey(secretKey.getBytes(UTF_8)))
        .setRelaxVerificationKeyValidation()
        .build();
```

At the bottom, a note states: "AI-generated content may be incorrect."

# SRM: 오탐 확률 / 여러 도구의 결과 통합

The screenshot displays the Synopsys Software Risk Manager (SRM) interface. At the top, it shows '14,416 total findings (533 types from 35,150 results)'. The main area is a table of findings with columns for ID, Project, Type, Tool, CWE, Location, Finding..., Triage Stat..., Assigne..., Predicted Status, and Jira Issue. The table lists various vulnerabilities, such as 'Vulnerable Component' and 'Command Injection', with associated tools like Black Duck and ESLint. On the left, there are filter panels for 'Policy Violations', 'Fix-by Urgency', 'Type', and 'Project', each with a 'Select All' button and a list of items to filter by.

ID	Project	Type	Tool	CWE	Location	Finding...	Triage Stat...	Assigne...	Predicted Status	Jira Issue
224762	WebGoat	Vulnerable Component	3 active results from Black Duck / Sec...	1352	Components/spring-boot-starter-se...	Existing	Not Tr...	U...	False Positive 67.6%	
224761	WebGoat	Vulnerable Component	3 active results from Black Duck / Sec...	1352	Components/spring-boot-starter-ao...	Existing	Not Tr...	U...	False Positive 67.6%	
224758	WebGoat	Vulnerable Component	3 active results from Black Duck / Sec...	1352	Components/spring-boot-starter-js...	Existing	Not Tr...	U...	False Positive 67.6%	
224757	WebGoat	Vulnerable Component	3 active results from Black Duck / Sec...	1352	Components/spring-boot-starter-ac...	Existing	Not Tr...	U...	False Positive 67.6%	
224754	WebGoat	Vulnerable Component	5 active results from Black Duck / Sec...	1352	Components/spring-webmvc:5.3.21	Existing	Not Tr...	U...	False Positive 48.9%	
224752	WebGoat	Vulnerable Component	5 active results from Black Duck / Sec...	1352	Components/spring-aspects:5.3.21	Existing	Not Tr...	U...	False Positive 48.9%	
224751	WebGoat	Vulnerable Component	37 active results from Black Duck / Se...	1352	Components/xstream:1.4.5	Existing	Not Tr...	U...	False Positive 59.5%	
224746	WebGoat	Vulnerable Component	5 active results from Black Duck / Sec...	1352	Components/spring-orm:5.3.21	Existing	Not Tr...	U...	False Positive 48.9%	
224745	WebGoat	Vulnerable Component	3 active results from Black Duck / Sec...	1352	Components/spring-boot-autoconfi...	Existing	Not Tr...	U...	False Positive 67.6%	
37346	Microser...	Vulnerable Component	3 active results from Black Duck / Sec...	937	Components/derby:10.11.1.1	New	To Be ...	U...	To Be Fixed 3.1%	(P man) POC...
246891	Microser...	Spring LDAP:2.3.3.REL...	2 active results from Black Duck / Ope...		Components/spring-ldap-core:2.3.3...	New	To Be ...	U...	False Positive 14.3%	
246749	webgoat	Command Injection	1 active result from ESLint / Security / ...77		goatAsyncErrorHandler.js:20	New	Not Tr...	U...	False Positive 32.6%	
246746	webgoat	Cross-site Scripting (X...	1 active result from ESLint / XSS / No L...	79	goatAsyncErrorHandler.js:19	New	Not Tr...	U...	False Positive 50.0%	
246702	webgoat	Command Injection	1 active result from ESLint / Security / ...77		clientSideFiltering.js:30	New	Not Tr...	U...	False Positive 32.7%	
246701	webgoat	Cross-site Scripting (X...	1 active result from ESLint / XSS / No ...	79	clientSideFiltering.js:31	New	Not Tr...	U...	False Positive 66.3%	



## Software Risk Manager

여러 종류의  
애플리케이션 보안  
도구의 결과를  
통합하여 보여주는  
On-prem 기반의  
ASPM 솔루션

\* ASPM : Application Security Posture Management

# SRM: 오탐 확률

SYNOPSYS SOFTWARE RISK MANAGER v2024.3

14,416 total findings (533 types from 35,150 results)

Filters: All findings, Q Search, Policy Violations, Fix-by Urgency, Type, Project

Findings: Displaying 14,416 matching findings

ID	Project	Type	Tool	CWE	Location	Finding...	Triage Stat...	Assign...	Predicted Status	Java Issue
224762	WebGoat	Vulnerable Component	3 active results from Black Duck / Sec...	1352	Components/spring-boot-starter-se...	Existing	Not Tr...	U...	False Positive 67.6%	
224761	WebGoat	Vulnerable Component	3 active results from Black Duck / Sec...	1352	Components/spring-boot-starter-ao...	Existing	Not Tr...	U...	False Positive 67.6%	
224758	WebGoat	Vulnerable Component	3 active results from Black Duck / Sec...	1352	Components/spring-boot-starter-js...	Existing	Not Tr...	U...	False Positive 67.6%	
224757	WebGoat	Vulnerable Component	3 active results from Black Duck / Sec...	1352	Components/spring-boot-starter-ac...	Existing	Not Tr...	U...	False Positive 67.6%	
224754	WebGoat	Vulnerable Component	5 active results from Black Duck / Sec...	1352	Components/spring-webmvc:5.3.21	Existing	Not Tr...	U...	False Positive 48.9%	
224752	WebGoat	Vulnerable Component	5 active results from Black Duck / Sec...	1352	Components/spring-aspects:5.3.21	Existing	Not Tr...	U...	False Positive 48.9%	
224751	WebGoat	Vulnerable Component	37 active results from Black Duck / Sec...	1352	Components/xstream:1.4.5	Existing	Not Tr...	U...	False Positive 59.5%	
224746	WebGoat	Vulnerable Component	5 active results from Black Duck / Sec...	1352	Components/spring-orm:5.3.21	Existing	Not Tr...	U...	False Positive 48.9%	
224745	WebGoat	Vulnerable Component	3 active results from Black Duck / Sec...	1352	Components/spring-boot-autoconfi...	Existing	Not Tr...	U...	False Positive 67.6%	
37346	Microser...	Vulnerable Component	3 active results from Black Duck / Sec...	937	Components/derby:10.11.1.1	New	To Be ...	U...	To Be Fixed 3.1%	POC-2
246891	Microser...	Spring LDAP:2.3.3.REL...	2 active results from Black Duck / Ope...		Components/spring-ldap-core:2.3.3...	New	To Be ...	U...	False Positive 14.3%	
246749	webgoat	Command Injection	1 active result from ESLint / Security / ...77		goatAsyncErrorHandler.js:20	New	Not Tr...	U...	False Positive 32.6%	
246746	webgoat	Cross-site Scripting (X...	1 active result from ESLint / XSS / No L...	79	goatAsyncErrorHandler.js:19	New	Not Tr...	U...	False Positive 50.0%	
246702	webgoat	Command Injection	1 active result from ESLint / Security / ...77		clientSideFiltering.js:30	New	Not Tr...	U...	False Positive 32.7%	
246701	webgoat	Cross-site Scripting (X...	1 active result from ESLint / XSS / No ...	79	clientSideFiltering.js:31	New	Not Tr...	U...	False Positive 66.3%	



... Predicted Status ▾ Jir

False Positive 67.6% -
False Positive 67.6% -
False Positive 67.6% -
False Positive 67.6% -
False Positive 48.9% -
False Positive 48.9% -
False Positive 59.5% -
False Positive 48.9% -
False Positive 48.9% -
False Positive 67.6% -
To Be Fixed 3.1% (P)
False Positive 14.3% -
False Positive 32.6% -
False Positive 50.0% -
False Positive 32.7% -
False Positive 66.3% -

# SRM: 여러 도구의 결과 통합

SYNOPTIS SOFTWARE RISK MANAGER v2024.3

14,416 total findings (533 types from 35,150 results)

Filters: All findings

Q Search: e.g. some/file.txt

Policy Violations: DISASTIG (2,449 - 17%), panchen-demo-policy (15 - 0.1%), Varun BD Policy Test (36 - 0.2%), Vulnerable to XSS (124 - 0.9%), None (11,916 - 82.7%)

Fix-by Urgency: Overdue (2,464 - 17.1%), Due Soon (0 - 0%), On Track (0 - 0%), No Fix-by Set (11,952 - 82.9%)

Type: "Java Concurrency in Practice" book annotat..., [] is better written in dot notation (22 - 0.2%), A class with only private constructors should..., Abstract class does not contain any abstract..., AD\_No\_Exploit (1 - < 0.1%), Alert malloous code (1 - < 0.1%), Always specify the columns in an INSERT sta...

Project: APAC (4 - < 0.1%), Microservice1 [roller] (2,806 - 19.5%), Microservice2 [roller] (2,000 - 13.9%)

Findings: Displaying 14,416 matching findings

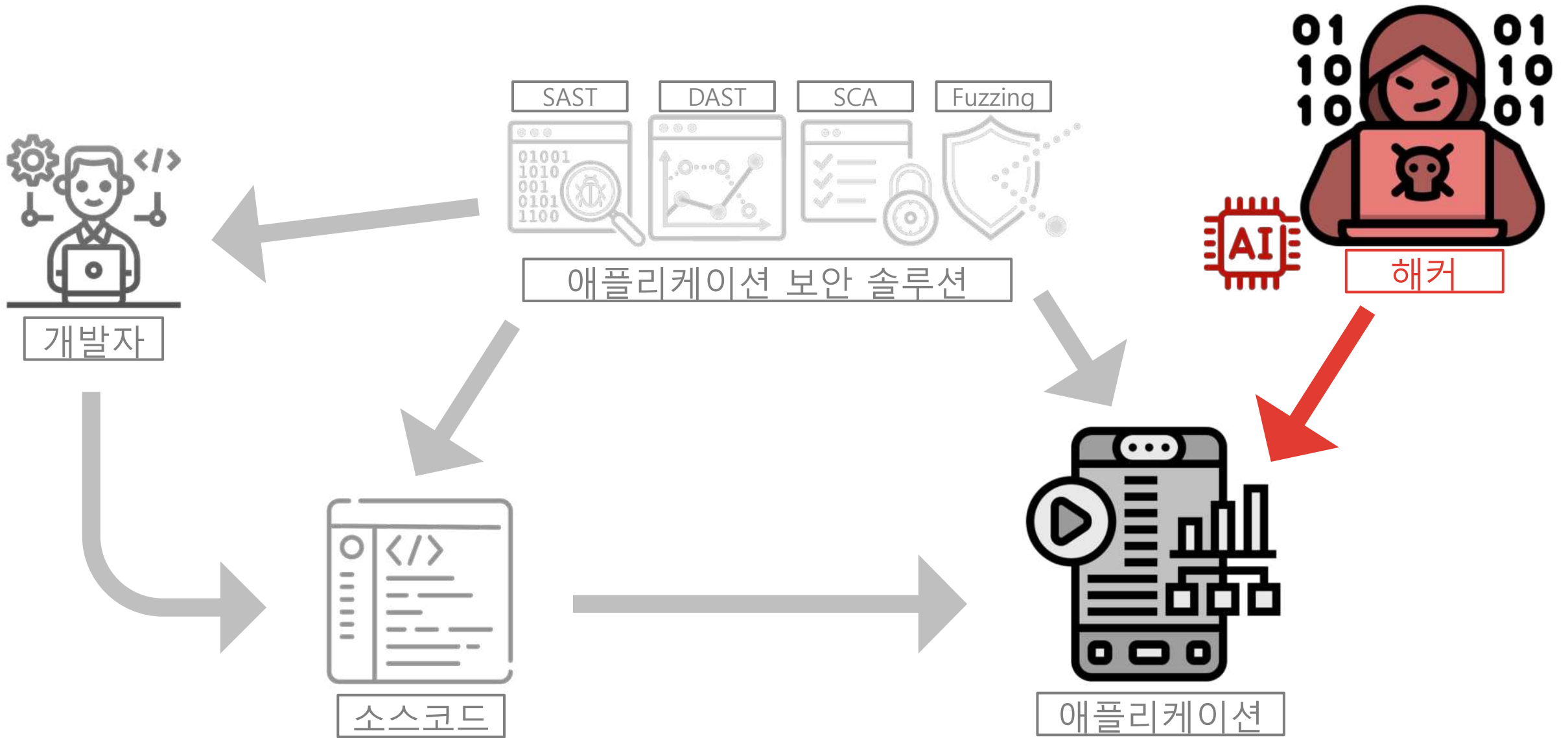
ID	Project	Type	Tool	CWE	Location	Finding...	Triage Stat...	Assigne...	Predicted Status	Jira Issue
224762	WebGoat	Vulnerable Component	3 active results from Black Duck / Sec...	352	Components/spring-boot-starter-se...	Existing	Not Tr...	U...	False Positive 67.6%	
224761	WebGoat	Vulnerable Component	3 active results from Black Duck / Sec...	352	Components/spring-boot-starter-ao...	Existing	Not Tr...	U...	False Positive 67.6%	
224758	WebGoat	Vulnerable Component	3 active results from Black Duck / Sec...	352	Components/spring-boot-starter-js...	Existing	Not Tr...	U...	False Positive 67.6%	
224757	WebGoat	Vulnerable Component	3 active results from Black Duck / Sec...	352	Components/spring-boot-starter-ac...	Existing	Not Tr...	U...	False Positive 67.6%	
224754	WebGoat	Vulnerable Component	5 active results from Black Duck / Sec...	352	Components/spring-webmvc:5.3.21	Existing	Not Tr...	U...	False Positive 48.9%	
224752	WebGoat	Vulnerable Component	5 active results from Black Duck / Sec...	352	Components/spring-aspects:5.3.21	Existing	Not Tr...	U...	False Positive 48.9%	
224751	WebGoat	Vulnerable Component	37 active results from Black Duck / Sec...	352	Components/xstream:1.4.5	Existing	Not Tr...	U...	False Positive 59.5%	
224746	WebGoat	Vulnerable Component	5 active results from Black Duck / Sec...	352	Components/spring-orm:5.3.21	Existing	Not Tr...	U...	False Positive 48.9%	
224745	WebGoat	Vulnerable Component	3 active results from Black Duck / Sec...	352	Components/spring-boot-autoconfi...	Existing	Not Tr...	U...	False Positive 67.6%	
37346	Microser...	Vulnerable Component	3 active results from Black Duck / Sec...	37	Components/derby:10.11.1.1	New	To Be ...	U...	To Be Fixed 3.1%	(P man) POC-2...
246891	Microser...	Spring LDAP:2.3.3.RE...	2 active results from Black Duck / Ope...		Components/spring-ldap-core:2.3.3...	New	To Be ...	U...	False Positive 14.3%	
246749	webgoat	Command Injection	1 active result from ESLint / Security / ...	77	goatAsyncErrorHandler.js:20	New	Not Tr...	U...	False Positive 32.6%	
246746	webgoat	Cross-site Scripting (XSS)	1 active result from ESLint / XSS / No I...	89	goatAsyncErrorHandler.js:19	New	Not Tr...	U...	False Positive 50.0%	
246702	webgoat	Command Injection	1 active result from ESLint / Security / ...	77	clientSideFiltering.js:30	New	Not Tr...	U...	False Positive 32.7%	
246701	webgoat	Cross-site Scripting (XSS)	1 active result from ESLint / XSS / No ...	89	clientSideFiltering.js:31	New	Not Tr...	U...	False Positive 66.3%	

Tool
3 active results from Black Duck / Sec...
3 active results from Black Duck / Sec...
3 active results from Black Duck / Sec...
3 active results from Black Duck / Sec...
5 active results from Black Duck / Sec...
5 active results from Black Duck / Sec...
37 active results from Black Duck / Se...
5 active results from Black Duck / Sec...
3 active results from Black Duck / Sec...
3 active results from Black Duck / Sec...
.. 2 active results from Black Duck / Ope...
1 active result from ESLint / Security / ..
1 active result from ESLint / XSS / No I...
1 active result from ESLint / Security / ..
1 active result from ESLint / XSS / No ...





애플리케이션 보안에서  
제일 많이 AI가 활성화 된 분야는...?



## Summary

*AI가 소프트웨어 개발 전반에서 활성화되는 시대,  
애플리케이션 보안은 더욱 더 사이버보안을 위해  
주요해 지고 있습니다.*

*다각적이면서 엄격하고 효율적인 애플리케이션  
보안 활동과 이를 위한 애플리케이션 보안 솔루션이  
필요합니다.*



Thank You