

DIGICERT STM

(SOFTWARE TRUST MANAGER)

- 소프트웨어 공급망 보호를 위한 플랫폼

나정주 지사장

Country Manager for Korea

digicert[®]





AGENDA








- DigiCert 소개
- 2025 사이버 보안 전망
- 소프트웨어 보안의 기본
- DigiCert STM (Software Trust Manager)
- DigiCert STM - Threat Detection
- 한국전자인증 (Crosscert) 소개










DIGICERT 소개

DigiCert – 혁신과 리더십의 역사

<p>2022</p> <p>DigiCert acquires DNS Made Easy in extending its leadership in Digital Trust with Enterprise-Grade managed DNS services</p> 	<p>2022</p> <p>DigiCert acquires Mocana providing complete end to end security management of IoT devices</p> 
--	--

<p>1995</p> <p>VeriSign becomes the first Certificate Authority</p> 	<p>2005</p> <p>DigiCert becomes founding member of the CA/Browser Forum</p> 	<p>2010</p> <p>Symantec acquires Verisign Authentication & rebrands the iconic trust seal</p> 	<p>2015</p> <p>DigiCert launches scalable IoT platform</p> 	<p>2017</p> <p>DigiCert acquires Symantec's Website Security business and reissues all certificates on DigiCert's trusted roots</p> 	<p>2019</p> <p>DigiCert acquires QuoVadis, the leading Qualified Trust Service Provider (QTSP) in the EU and Switzerland</p> 	<p>2021</p> <p>DigiCert launches industry changing TLS automation manager</p> 
---	--	--	---	--	---	--

<p>1997</p> <p>VeriSign becomes first international CA</p> 	<p>2003</p> <p>DigiCert founded based on the question, "Isn't there a better way?"</p> 	<p>2007</p> <p>DigiCert partners with Microsoft to develop first Multi-Domain certificate</p> 	<p>2013</p> <p>DigiCert builds the first CT log accepted by Google</p> 	<p>2016</p> <p>DigiCert acquires Verizon SSL/TLS business</p> 	<p>2018</p> <p>DigiCert's trusted roots become encryption foundation for enterprises worldwide</p> 	<p>2020</p> <p>DigiCert announces DigiCert ONE. The DigiCert ONE platform is a holistic approach to PKI management</p> 
---	---	---	---	--	---	---

DIGICERT – 디지털 신뢰를 위한 선도 기업

- 1등 Enterprize TLS/SSL 인증서를 발급하는 인증 기관
- DigiCert® Trust Lifecycle Manager wins the Next Gen Certificate Lifecycle Management Category Award in the 12th annual Global InfoSec Awards 2024
- “Fortune 500”의 88%와 Top 100 banks의 93%가 선호
- 매일 260억 개의 Web connection의 안전한 연결 보장
- 디지서트가 보호하는 글로벌 e커머스 트랜잭션 비중이 87%
- TLS/SSL, PKI & IoT 솔루션을 전세계 180여국가에서 제공
- 자동화 플랫폼인 “DigiCert TLM”, “DigiCert STM” 등 발표
- 2018년 10월 DigiCert-Gemalto-Isara 등과 양자 컴퓨팅 시대의 보안을 위한 PQC 파트너십 시작
- 세계 최초 “PQC test kit” 발표(DigiCert Secure Site Pro)



디지털 신뢰의 표준을 구축한 DIGICERT

신뢰 분야의 표준 구축을 위한 투자

- 기술과 업계 표준을 선도
- 연간 25건 이상의 감사



NIST



CableLabs®



전 세계적 범위, 현지에 적용된 서비스

- 180개 국가에 고객 보유
- 24시간 연중무휴, 세계 최고 수준의 지원



디지털 신뢰를 위한 PQC READY PLATFORM

digicert® ONE

Machines

Trust Lifecycle Manager

- Certificate lifecycle mgmt.
- Cryptographic inventory
- Ownership & notifications
- Delegation & workflows

Software

Software Trust Manager

- Code signing
- Secure key mgmt.
- SBOM management
- Malware/vuln. scanning

Devices

Device Trust Manager

- Tamperproof device Id.
- Device lifecycle mgmt.
- Over the air updates
- Developer SDK

Content

Document Trust Manager

- Digital signatures & seals
- EU Qualified, Adobe trusted
- Timestamping services
- Content provenance

Network

UltraDNS

- Authoritative DNS
- Traffic optimization
- DDoS protection
- API security / WAF

Policy and Governance

Integrations and Automation

DigiCert CertCentral

DigiCert Private CA

Other Certificate Authorities

2025 사이버 보안 전망

2025년 사이버 보안 전망



AI 기반의 피싱 공격 급증



자동화와 암호화
민첩성이 필수 요소



PQC : 양자 내성 암호
(Post Quantum
Cryptography)의 부상



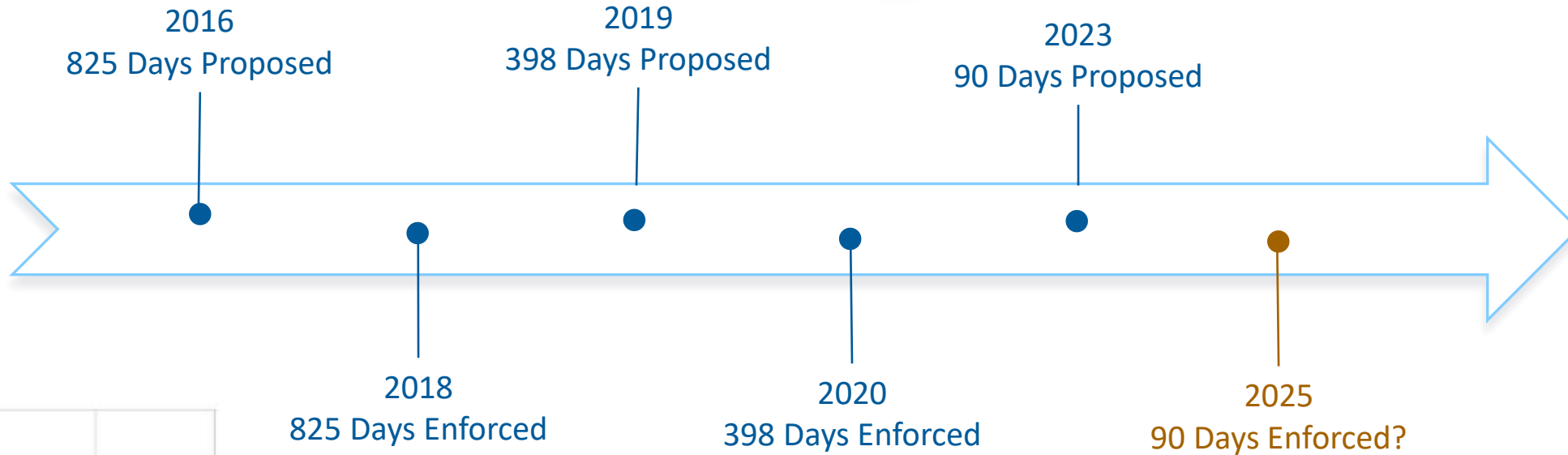
인증서 관리
수작업 시대 종료



디지털 콘텐츠
출처 확인의 보편화

PQC 및 GOOGLE의 90일 인증서 제안

- PQC imminent
 - PQC transition efforts have begun
- Google's 90-day proposal



Automation is the key!

소프트웨어 보안의 기본

Code Signing & Keylocker

CODE SIGNING 이란?

Definition

- A security technology that allows software developers to prove the origin and integrity of their code through a digital signature.

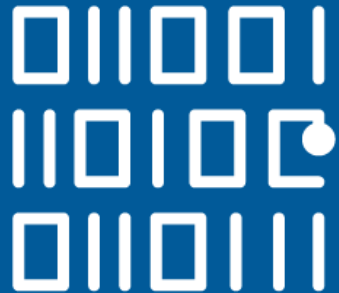
Importance

- **Enhance Security:** Protects users and systems from malicious code or malware.
- **Building Trust:** Provides software reliability to users, encouraging installation and use
- **Compliance:** Essential for meeting various industry standards and regulatory requirements

How it works

- **Signing Process:**
 - The developer applies a digital signature to the code using a private key.
 - The user verifies the validity of the signature using the public key.
- **Integrity Verification:** Ensures that the code has not been modified during transmission or distribution

KEY LOCKER란?



Cloud-based key protection for OV and EV code signing certificates

- **Providing a Secure Key Repository:** Stores sensitive cryptographic keys in a secure environment to prevent unauthorized access and leaks.
- **Managing Key Lifecycle:** Efficiently manages the entire lifecycle of keys, from creation, distribution, and rotation to disposal.
- **Access Control and Permission Management:** Precisely controls access rights for users and applications to the keys.

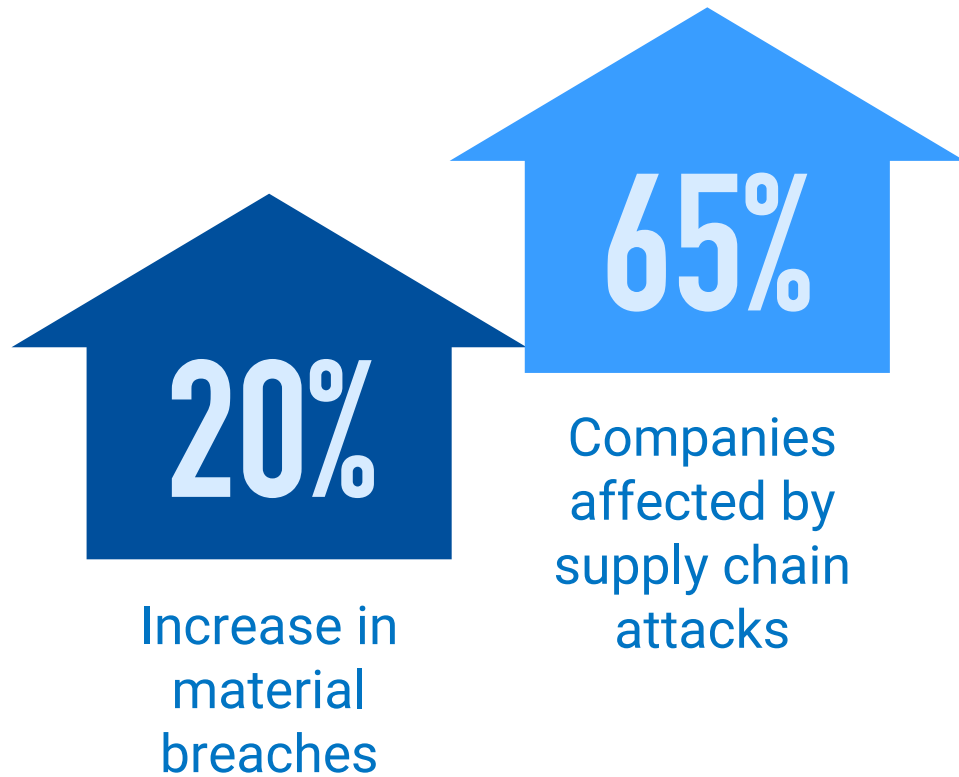
DIGICERT® STM

STM (Software Trust Manager)

- 소프트웨어 공급망 보호를 위한 플랫폼

증가하는 위협

데이터 유출 및 공급망 공격에 대한 노출 증가



USD \$9.4m

Cost per data breach

USD \$14m

Cost of failed audit / compliance

47%

of consumers say they have switched vendors because of loss of trust

악성코드와 공급망

Malware is being embedded in the SDLC in novel & hidden ways

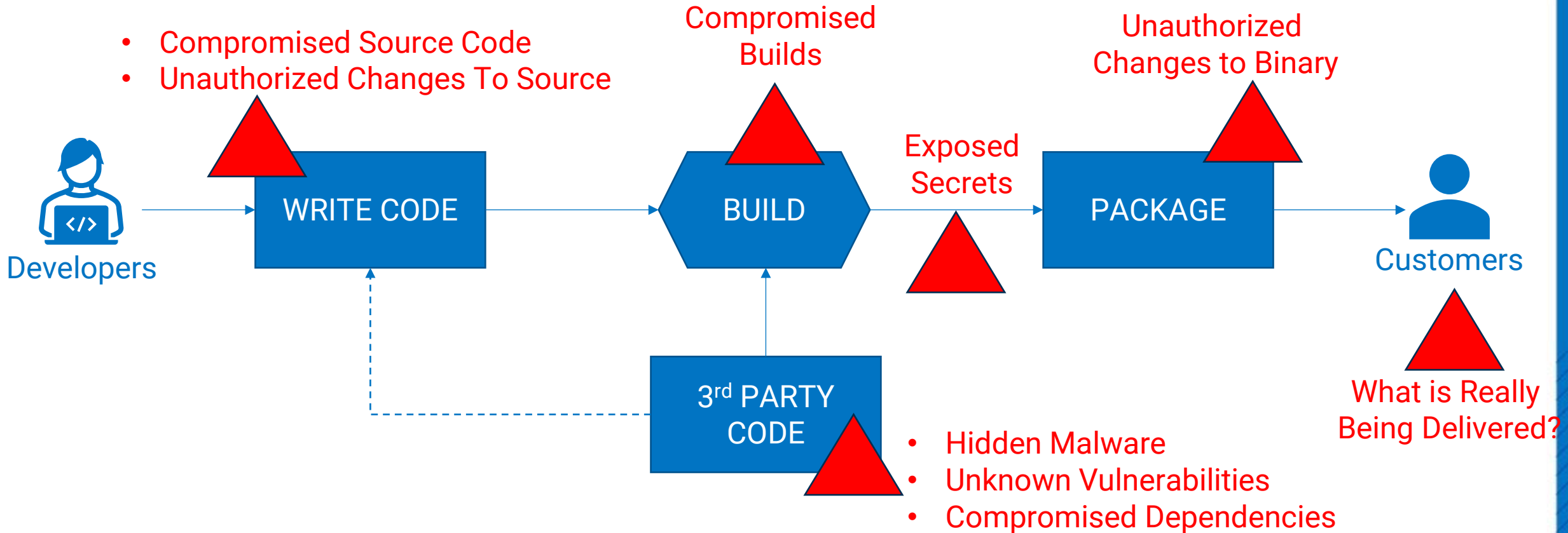
- Compromise of build platforms
- Exploitation of poor code signing hygiene
- Hidden in 3rd party open-source and commercial software
- Exploitation of insecure software engineering practices

The collage features several key elements:

- MSI Logo:** A large, stylized logo for MSI (Micro-Star International) in white on a black background.
- BleepingComputer Article:** A news snippet titled "Hackers compromise 3CX desktop app in a supply chain attack" by Sergiu Gatan, dated March 29, 2023. The article includes a 3CX logo and a brief description: "A digitally signed and trojanized version of the 3CX Voice Over Internet Protocol (VOIP) desktop reportedly being used to target the company's customers in an ongoing supply chain attack. 3CX is a VoIP IPBX software development company whose 3CX Phone System is used by more than 600,000 companies worldwide and has over 12 million daily users."
- Hacker News Article:** A snippet titled "Malware Attack on CircleCI Engineer's Laptop Leads to Recent Security Incident" by Ravie Lakshmanan, dated Jan 14, 2023. The text below reads: "DevOps platform CircleCI on Friday disclosed that unidentified threat actors compromised an employee's laptop and leveraged malware to steal their two-factor authentication-backed credentials to breach the company's systems and data last month."
- LOG4J Logo:** The logo for the Log4j vulnerability, featuring the text "LOG4J" and a red circular icon with a white '3' and a red arrow.
- CircleCI Logo:** The logo for CircleCI, consisting of a white circle with a dot inside, followed by the text "circleci".
- Malwarebytes Labs:** A small logo in the top right corner of the collage.

넓은 공격 표면을 가진 SDLC

Attacks Can, and Do, Happen Anywhere During This Process



디지털 신뢰를 위한 PQC READY PLATFORM

digicert® ONE

Machines

Trust Lifecycle Manager

- Certificate lifecycle mgmt.
- Cryptographic inventory
- Ownership & notifications
- Delegation & workflows

Software

Software Trust Manager

- Code signing
- Secure key mgmt.
- SBOM management
- Malware/vuln. scanning

Devices

Device Trust Manager

- Tamperproof device Id.
- Device lifecycle mgmt.
- Over the air updates
- Developer SDK

Content

Document Trust Manager

- Digital signatures & seals
- EU Qualified, Adobe trusted
- Timestamping services
- Content provenance

Network

UltraDNS

- Authoritative DNS
- Traffic optimization
- DDoS protection
- API security / WAF

Policy and Governance

Integrations and Automation

DigiCert CertCentral

DigiCert Private CA

Other Certificate Authorities

SOFTWARE TRUST MANAGER

Software Trust Manager is a digital trust solution that protects the **integrity of software-based products across the software supply chain** through the combination of threat and vulnerability detection, secure code signing, and SBOM generation.



DIGITAL
TRUST FOR
SOFTWARE
SUPPLY
CHAIN
INTEGRITY

- Secured storage for code signing keys
- Role and policy-driven approach to code signing access
- Deep threat and vulnerability analysis
- Software bill of materials and risk report generation for compliance

소프트웨어 공급망 전체를 보호하는 STM

Threat detection, code signing & SBOM in a unified security workflow



- 25B+ threat database
- Complete binary scanning
- Low impact to CI/CD

- Secured private keys
- Role-based access control
- Enterprise-wide visibility and signing policy

- Deep binary decomposition
- 3rd party & open source
- Regulatory compliance

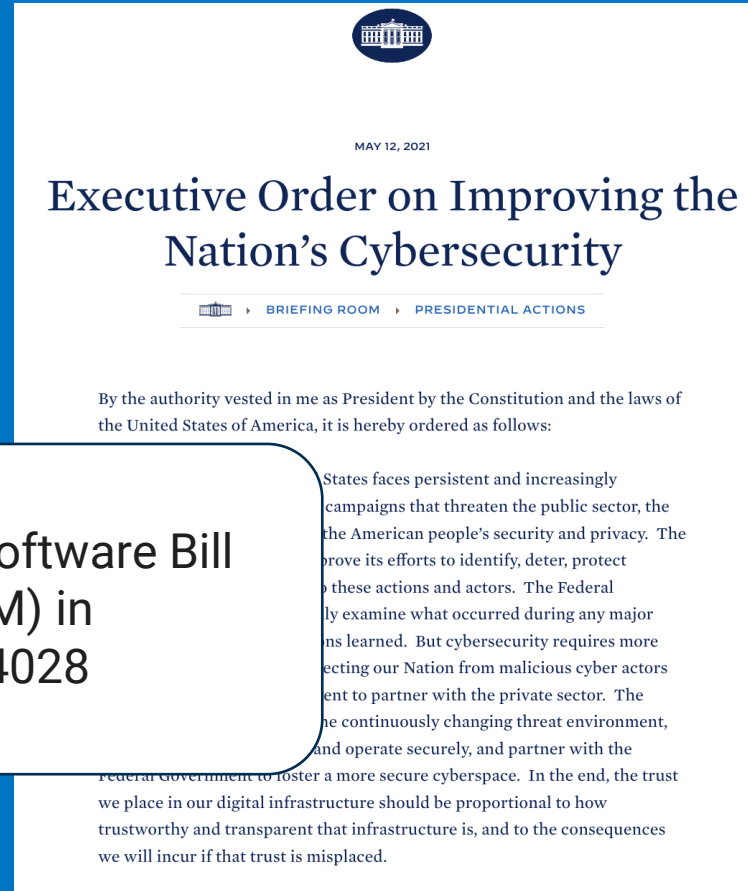
DIGICERT STM - THREAT DETECTION

위협 탐지

투명성 제고를 위해 SBOM이 규제화 되고 있다



Requirement for Software Bill of Materials (SBOM) in Executive Order 14028



“By 2026, at least **60%** of organizations procuring mission-critical software solutions will mandate SBOM disclosures in their license and support agreements, up from less than 5% in 2022.”

– Gartner

SOFTWARE BUILD OF MATERIALS

Whats an SBOM?

A Software Bill of Materials (SBOM) is a formal record containing the details and supply chain relationships of various components used in building software. These components, including libraries and modules, can be open source or proprietary, free or paid, and the data can be widely available or access-restricted.

Machine readable with popular formats
CycloneDX and SPDX

Sited in many regulations

Required by FDA and will be required by PCI-DSS

Focus is on generation

No real focus on benefits and operational use

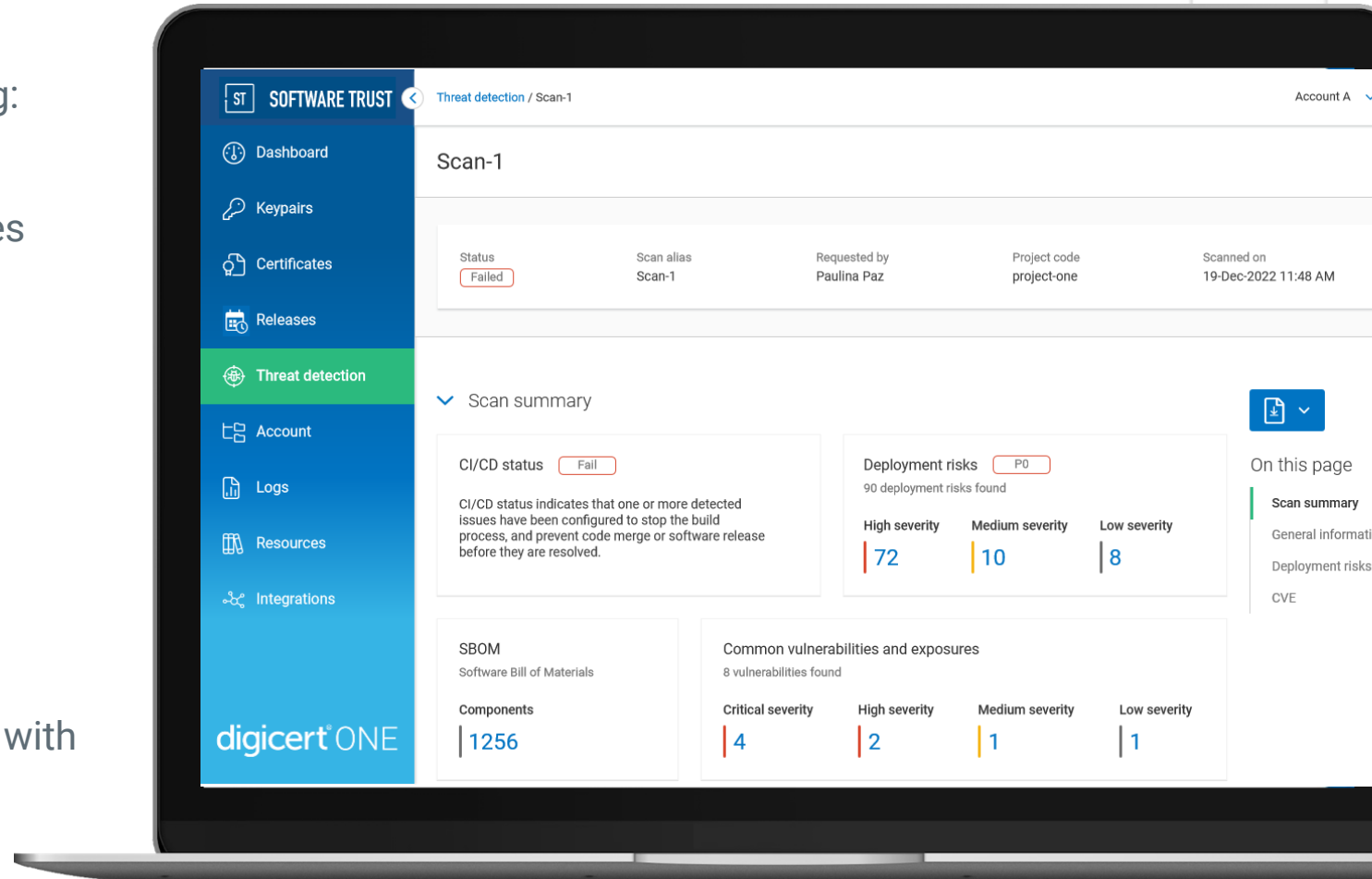


SOFTWARE TRUST MANAGER THREAT DETECTION

Software Supply Chain Integrity

Threat and vulnerability detection and reporting:

- Detect malware in large and complex binaries
- See deeper into software dependencies
- Prevent threats from reaching production
- Find exposed secrets before release
- Track improvements with each build
- Take a policy driven approach to releasing software with confidence
- Comply with emerging regulatory standards with SBOM and risk assessment reports



SOFTWARE BUILD OF MATERIALS

```
1  {
2    "$schema": "http://cyclonedx.org/schema/bom-1.4.schema.json",
3    "bomFormat": "CycloneDX",
4    "specVersion": "1.4",
5    "version": 1,
6    "serialNumber": "urn:uuid:69b2e23e-e48c-4323-a2cd-7b791785c721",
7    "metadata": {
8      "timestamp": "2023-08-30T16:40:00.883Z",
9      "component": {
10       "type": "application",
11       "name": "https://github.com/CortezFrazierJr/my_recipe_book.git",
12       "version": "418bed3e334f2c1b2d4de973e069037dc2faf60e",
13       "bom-ref": "custom+32098/github.com/CortezFrazierJr/my_recipe_book$418bed3e334f2c1b2d4de97",
14       "description": "Project uploaded via Provided Builds from fossa-cli",
15       "licenses": [
16         {
17           "license": {
18             "id": "ISC",
19             "text": {
20               "content": "SVNDIExpY2Vuc2UKQ29weXJpZ2h0ICChjKSAyMDA0LTIwMTAgYnkgSW50ZXJ1ZXQgU31zdG",
21               "contentType": "text/plain",
22               "encoding": "base64"
23             }
24           }
25         }
26       ]
27     },
28     "authors": [
29       {
30         "name": "FOSSA, Inc.",
31         "email": "support@fossa.com"
32       }
```

```
373  {
374     "type": "library",
375     "name": "@codemirror/search",
376     "version": "6.5.2",
377     "bom-ref": "pkg:npm/%40codemirror/search@6.5.2",
378     "author": "mail@adrianheine.de, marijn@haverbeke.berlin",
379     "description": "Search functionality for the CodeMirror code editor",
380     "licenses": [
381       {
382         "license": {
383           "id": "MIT",
384           "text": {
385             "content": "TU1UIExpY2Vuc2UKCkNvcHlyaWdodCAoQykgMjAxOC0yMDIxIGJ5IE1hcmlqb2IyYXZlcmJ1a2",
386             "contentType": "text/plain",
387             "encoding": "base64"
388           }
389         }
390       }
391     ],
392     "copyright": "2018-2021 by Marijn Haverbeke <marijn@haverbeke.berlin> and others",
393     "purl": "pkg:npm/%40codemirror/search@6.5.2"
394   },
395   {
396     "type": "library",
397     "name": "@codemirror/state",
398     "version": "6.2.1",
399     "bom-ref": "pkg:npm/%40codemirror/state@6.2.1",
400     "author": "mail@adrianheine.de, marijn@haverbeke.berlin",
401     "description": "Editor state data structures for the CodeMirror code editor",
402     "licenses": [
```

SUCCESS STORY: LEADING GLOBAL TECHNOLOGY COMPANY

UP TO 1.3 MILLION SIGNINGS

CENTRALIZED MANAGEMENT, KEY
SECURITY AND CONTROLS,
AUTOMATED WORKFLOWS



Challenge

- Distributed development teams across the globe
- High volume of signings such as 100000+ files being signed
- 10,000 signing events a year.



Solution:

- Centralized key and certificate management, secure key generation and storage
- Integration with CertCentral certificate issuance
- Fine-grained access controls with separation of duties
- Reporting and audit controls, tracking of all signing activities



Results

- Improved security of private key
- Reduced disruptions from improved business workflows

디지털 신뢰를 위한 PQC READY PLATFORM

digicert® ONE

Machines

Trust Lifecycle Manager

- Certificate lifecycle mgmt.
- Cryptographic inventory
- Ownership & notifications
- Delegation & workflows

Software

Software Trust Manager

- Code signing
- Secure key mgmt.
- SBOM management
- Malware/vuln. scanning

Devices

Device Trust Manager

- Tamperproof device Id.
- Device lifecycle mgmt.
- Over the air updates
- Developer SDK

Content

Document Trust Manager

- Digital signatures & seals
- EU Qualified, Adobe trusted
- Timestamping services
- Content provenance

Network

UltraDNS

- Authoritative DNS
- Traffic optimization
- DDoS protection
- API security / WAF

Policy and Governance

Integrations and Automation

DigiCert CertCentral

DigiCert Private CA

Other Certificate Authorities

한국전자인증

Digicert Platinum Elite Partner



□ 전자서명인증사업 최고의 파트너쉽

- Digicert Platinum Elite Partner
- DV/OV/EV SSL 인증서 국내시장 점유율 50% 이상
- 코드사인 인증서 발급 및 기술지원
- 토스 및 포스코 등 기업 전용 인증서 발급 서비스 제공 경험

□ 24년 검증된 전문인증기관

- 자체 PKI 기술로 구현한 전자서명인증 Total 솔루션 (RootCA/CA/RA/OCSP/TSA)
- 국제 FIDO Alliance 1.0 & FIDO2 인증 기술 보유 (KB국민은행, KB국민카드, 토스 등에 FIDO 공급)
- 인증기관 최초 클라우드 인증서비스 시작 (2017.10 ~)

□ 다양한 보안 응용솔루션 보유

- 전자문서 전자서명 솔루션
- 전자입찰, 계약, 전자세금계산서 솔루션
- 전자문서 PDF 생성, 전자인감.이미지 삽입 솔루션
- 개인정보보호 솔루션, 암호 키 관리 솔루션

감사합니다.

digicert[®]

