ทดสอบความปลอดภัยแอปพลิเคชันและบริหารความเสี่ยง

zcrX

ทดสอบแอปพลิเคชัน รู้ว่าควรแก้อะไรก่อน

zcrX ตรวจ source code ด้วย static application security testing (SAST) และทดสอบแอปพลิเคชันที่รันอยู่ด้วย dynamic application security testing (DAST) คอนโซลยังรวมความพร้อมด้านการเข้ารหัส ช่องโหว่ซอฟต์แวร์ และความน่าเชื่อถือของ dependency โดย Agent รายงาน posture จากโฮสต์และระบบบิลด์ที่ลงทะเบียน แล้วจัดลำดับการแก้ไขตามสัญญาณการใช้โจมตี ความรุนแรง และจำนวนโฮสต์ที่ได้รับผลกระทบ

พร้อมใช้งาน · Subscription รายปี ขอบเขตและใบเสนอราคาผ่านพาร์ทเนอร์ที่ได้รับอนุมัติ

ใครควรประเมิน zcrX · ทีมจัดการช่องโหว่ ทีมความปลอดภัยแอปพลิเคชันและวิศวกรรมแพลตฟอร์ม ผู้ให้บริการความปลอดภัยที่ดูแลหลายองค์กรลูกค้า และผู้บริหารความปลอดภัยที่วางแผนย้ายสู่การเข้ารหัสยุคหลังควอนตัม

รู้จักสัญญาณที่ใช้จัดลำดับ

CVE · Common Vulnerabilities and Exposures
รหัสและระเบียนอ้างอิงช่องโหว่ความมั่นคงปลอดภัยไซเบอร์ที่เปิดเผยต่อสาธารณะ [1]

CISA KEV · Known Exploited Vulnerabilities
บัญชีช่องโหว่ที่มีหลักฐานว่าถูกใช้โจมตีจริง จัดทำโดยหน่วยงานความมั่นคงปลอดภัยไซเบอร์และโครงสร้างพื้นฐานของสหรัฐฯ (CISA) [2]

EPSS · Exploit Prediction Scoring System
ค่าประมาณของ FIRST ว่าช่องโหว่ที่มี CVE จะถูกใช้โจมตีจริงภายใน 30 วันข้างหน้ามีโอกาสเท่าใด เป็นค่าความน่าจะเป็น ไม่ใช่คะแนนความรุนแรง [3]

แหล่งนิยาม: [1] CVE Program · [2] CISA · [3] FIRST · [1] ↗ [2] ↗ [3] ↗

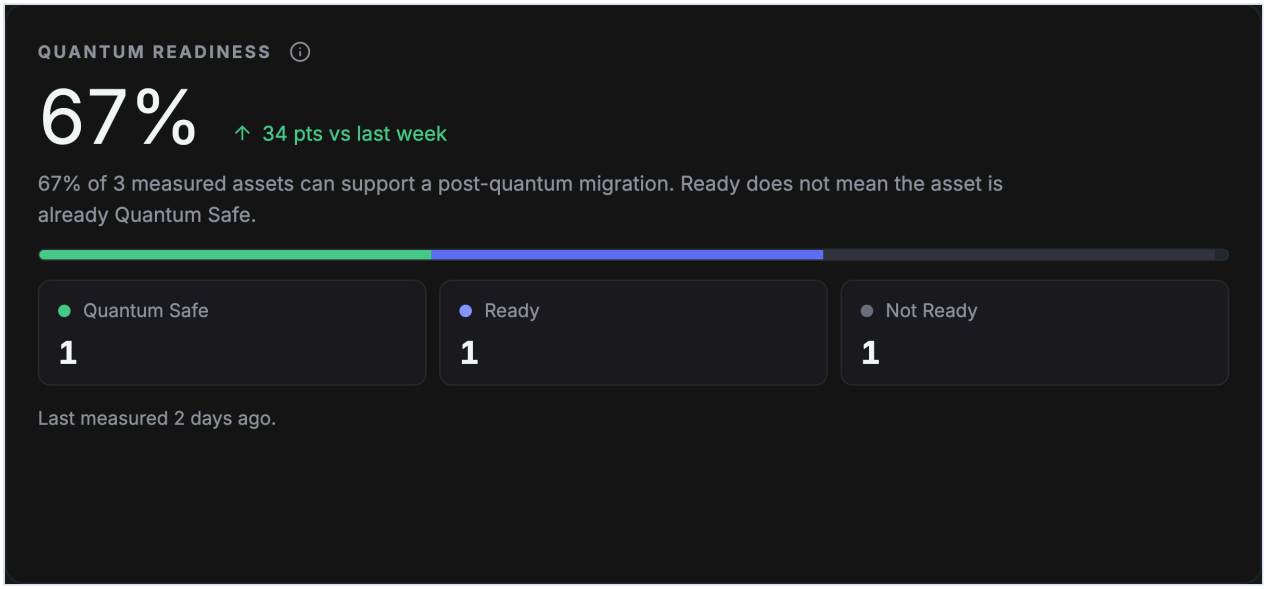
แต่ละมุมมองช่วยตัดสินใจเรื่องใด

Cryptography พร้อมสู่ Quantum	ติดตามรายการ certificate และ algorithm เทียบกับความพร้อม migration สู่ post-quantum
จัดลำดับการแก้ช่องโหว่	จัดลำดับการแก้ไขตามสถานะ CISA KEV, EPSS score และความรุนแรง ไม่ใช่จำนวน CVE ดิบ
Supply Chain ที่ยืนยันได้	ยืนยันที่มาของ dependency ด้วย cryptographic proof หรือการยืนยันจาก Agent ครอบคลุมหลาย ecosystem
มุมมองเดียวสำหรับ Provider	บริหาร posture ของทุก customer tenant ผ่านสิทธิ์การเข้าถึงแบบ delegated และ least-privilege

อ่านความพร้อมและลำดับการแก้ไข

01 / วางแผนย้ายระบบการเข้ารหัส

Cryptography posture: รายการ certificate และ algorithm ให้คะแนนเป็น quantum-safe, ready หรือ not ready



วิดเจ็ตความพร้อมด้านควอนตัมแบบเต็ม เก็บคำอธิบายสถานะและความต่างระหว่าง Ready กับ Quantum Safe ไว้ครบ เดโม — ข้อมูลตัวอย่าง ไม่ใช่ตัวเลขลูกค้าจริง คงหน้าจอภาษาอังกฤษตามต้นฉบับ เปิดหน้าจอเดโม ↗

> ลำดับด้านการเข้ารหัสสะท้อนความเร่งด่วนในการย้ายสู่ยุคหลังควอนตัม Ready ในตัวอย่างหมายถึงพร้อมสำหรับการย้าย ยังไม่ใช่ quantum-safe และยังประเมินความเร่งด่วนไม่ได้หากไม่มีบริบททางธุรกิจที่ระบุไว้

02 / ดูเหตุผลที่ต้องแก้รายการนี้ก่อน

- Software vulnerability posture: finding ระดับ host และ package จับคู่กับ CVE advisory, สถานะ CISA KEV และ EPSS score
- จัดลำดับการแก้ไขตาม KEV, score และจำนวน host ที่ได้รับผลกระทบ พร้อมเหตุผลของแต่ละลำดับ
- ติดตาม finding เทียบกับกรอบเวลาการแก้ไขตามความรุนแรงที่ประกาศไว้ และแจ้งเตือนเมื่อเลยกำหนด

Why it matters	Action
A critical advisory affects this package version; An affecting advisory is on CISA's Known Exploited Vulnerabilities catalog	View affected packages

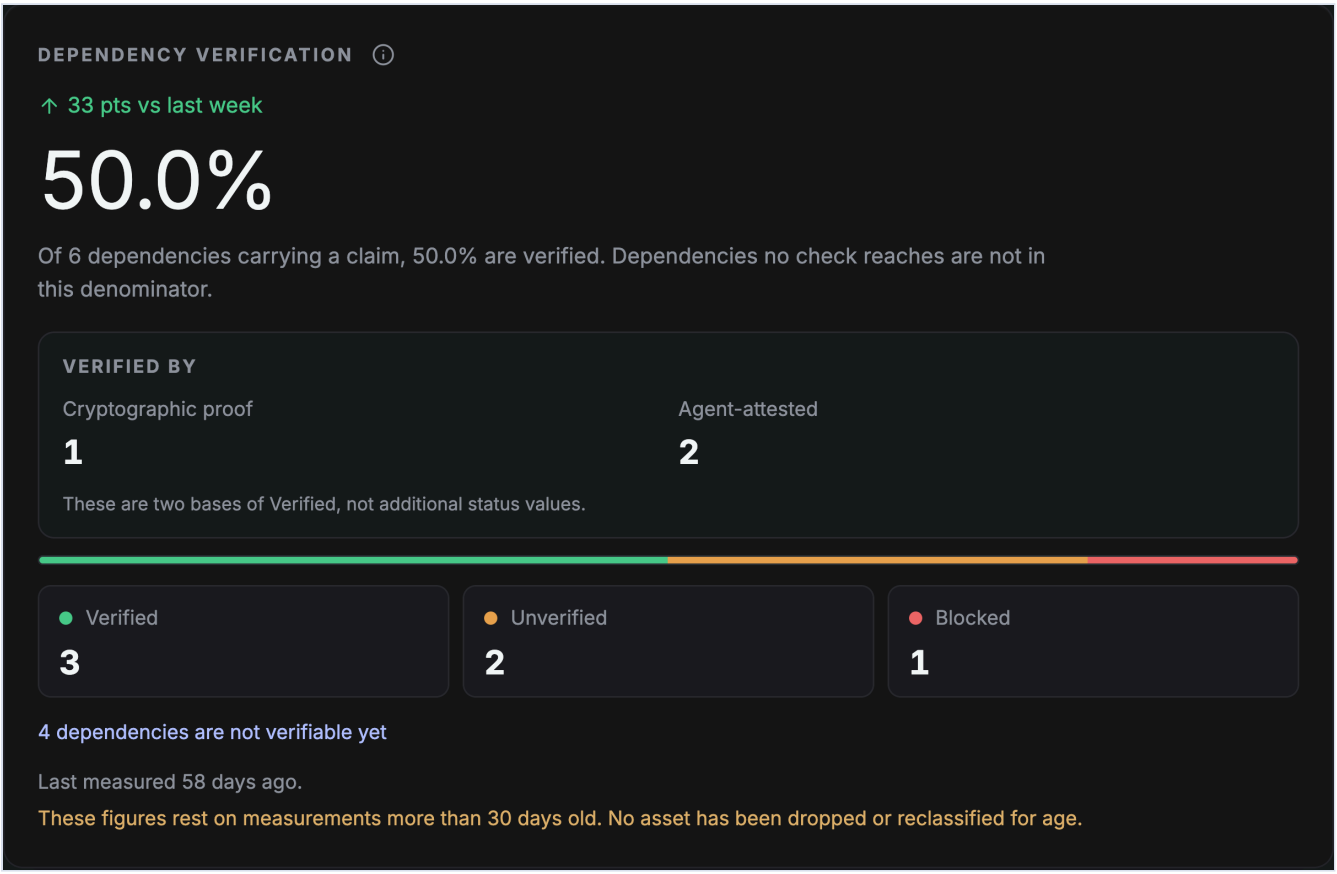
คอลัมน์ “Why it matters” และ “Action” ของหนึ่งแถวที่จัดลำดับไว้ แสดงเหตุผลเรื่องช่องโหว่ระดับวิกฤตและการอยู่ใน KEV ครบถ้วน ไม่ใช่ผลลัพธ์ที่วัดจากลูกค้าจริง เดโม — ข้อมูลตัวอย่าง ไม่ใช่ตัวเลขลูกค้าจริง คงหน้าจอภาษาอังกฤษตามต้นฉบับ เปิดหน้าจอเดโม ↗

> มุมมองซอฟต์แวร์ยังแยกรายการตามอายุเทียบกับกรอบเวลาแก้ไขที่ประกาศไว้ ต้นฉบับมีทั้งโฮสต์ที่ยังไม่ได้ประเมินและแพ็กเกจที่ยังไม่มีวิธีแก้ ทั้งสองสถานะไม่ได้ยืนยันว่าระบบปลอดภัย

ตรวจสอบที่มาของส่วนประกอบซอฟต์แวร์

03 / แยกหลักฐานยืนยันออกจากข้อมูลที่ยังขาด

Supply-chain posture: ยืนยันที่มาของ dependency ด้วย cryptographic proof หรือการยืนยันจาก Agent ครอบคลุม npm, PyPI, Go และ Maven



วิดเจ็ตยืนยันส่วนประกอบครบทั้งฐานคำนวณ หลักฐานสองแบบ และสถานะ การยืนยันจาก Agent กับหลักฐานทางการเข้ารหัสเป็นสองวิธีของ Verified ไม่ใช่สถานะเพิ่ม วัดล่าสุด 58 วันก่อน คงคำเตือนว่าข้อมูลวัดเกิน 30 วัน และไม่มีการตัดส่วนประกอบออกหรือเปลี่ยนสถานะเพราะอายุข้อมูล เดโม — ข้อมูลตัวอย่าง ไม่ใช่ตัวเลขลูกค้าจริง คงหน้าจอภาษาอังกฤษตามต้นฉบับ เปิดหน้าจอเดโม ↗

> ในตัวอย่างนี้ ส่วนประกอบที่ยังไม่มีการตรวจเข้าถึงจะไม่รวมในฐานคำนวณการยืนยัน สถานะ Unverified, Blocked และ Not verifiable yet แยกจากกัน ตัวเลขเปอร์เซ็นต์ในตัวอย่างไม่ได้ยืนยันความครอบคลุมของระบบคุณ

ขอบเขตที่ควรประเมินร่วมกับพาร์ทเนอร์

npm · PyPI · Go · Maven · Linux host · Container image

ยืนยันที่มาของ dependency ด้วย cryptographic proof หรือการยืนยันจาก Agent พร้อมความครอบคลุมของแต่ละ ecosystem และจำนวนช่องโหว่ที่ทราบ

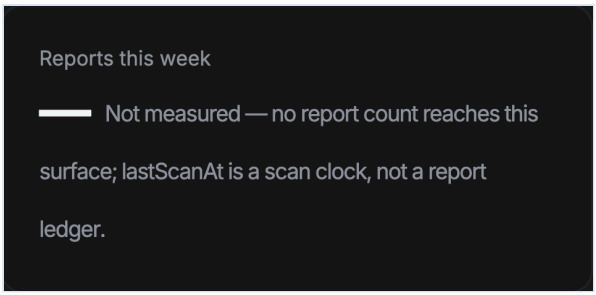
> ภาพรวมที่อนุมัติระบุระบบนิเวศและประเภทสินทรัพย์เหล่านี้ไว้ ต้องให้พาร์ทเนอร์ตรวจสอบรุ่นระบบปฏิบัติการ อิมเมจ และระบบบิลด์ที่ใช้จริง รายการนี้ไม่ได้รับรองว่าเข้ากันได้กับทุกสภาพแวดล้อม

รู้ว่าวัดอะไรแล้ว และใครมีสิทธิ์เข้าถึง

Agent และขอบเขตการวัด

ติดตั้ง Agent น้ำหนักเบาบน host และระบบ build เพื่อสแกนต่อเนื่อง

รายการ Agent แสดงตัวที่ลงทะเบียน สถานะการทำงาน และผลการวัดแต่ละด้านของโฮสต์ โฮสต์ที่ไม่มี Agent ถือว่ายังไม่มีการวัด ไม่ใช่ถือว่าปลอดภัย

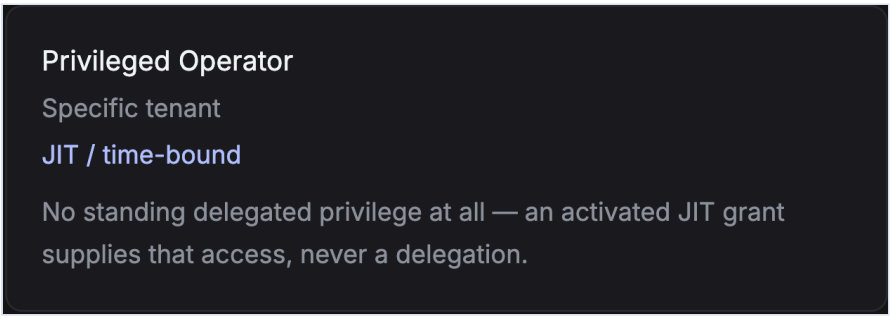


วิดเจ็ต “Reports this week” แบบเต็ม ตัวอย่างระบุ Not measured ชัดเจน และแยกเวลาสแกนออกจากบัญชีจำนวนรายงาน เดโม — ข้อมูลตัวอย่าง ไม่ใช่ตัวเลขลูกค้าจริง คงหน้าจอภาษาอังกฤษตามต้นฉบับ เปิดหน้าจอเดโม ↗

จำกัดสิทธิ์ตามขอบเขตของลูกค้าแต่ละราย

Provider control plane แบบ multi-tenant พร้อมสิทธิ์เข้าถึงแบบ delegated, least-privilege และจำกัดเวลา (JIT) ต่อ customer tenant

หน้าจัดการของผู้ให้บริการรองรับหลายองค์กรลูกค้า แยกขอบเขตข้อมูล (tenant) และมอบสิทธิ์เท่าที่จำเป็น มีทั้งนโยบายอนุมัติล่วงหน้าและอนุมัติเมื่อจำเป็นหรือ just-in-time (JIT) ซึ่งจำกัดระยะเวลาเข้าถึง



ส่วนบทบาท Privileged Operator แบบเต็ม ในเดโมนี้ สิทธิ์เกิดจาก JIT grant ที่เปิดใช้แล้ว การมอบหมายเพียงอย่างเดียวไม่ให้สิทธิ์ ต้นฉบับยังมีสถานะรอลูกค้าอนุมัติ เดโม — ข้อมูลตัวอย่าง ไม่ใช่ตัวเลขลูกค้าจริง คงหน้าจอภาษาอังกฤษตามต้นฉบับ เปิดหน้าจอเดโม ↗

เก็บรายละเอียดสำหรับงานปฏิบัติการ

- ติดตาม product lifecycle และวันหมดอายุการสนับสนุน (EOL) ของแต่ละซอฟต์แวร์
- Export CSV สำหรับ finding, dependency และ fleet ของ Agent

> CSV คือไฟล์ค่าที่คั่นด้วยจุลภาค ส่วน EOL คือการสิ้นสุดอายุผลิตภัณฑ์ มุมมองทั้งสามขยายชุดผลิตภัณฑ์ zcr ด้วยการวัดต่อเนื่องผ่าน Agent ไม่ใช่สแกนเพียงครั้งเดียว

> พาร์ทเนอร์ดูแลการสนับสนุนด่านแรก โดย zcr สนับสนุนพาร์ทเนอร์อีกชั้น เงื่อนไขการสนับสนุนเฉพาะต้องตรวจสอบร่วมกัน

เตรียมข้อมูลก่อนประเมินขอบเขต

คำถามก่อนเริ่มประเมิน

zcrX เปิดให้ใช้งานหรือยัง?

พร้อมใช้งานแล้ว เป็น subscription รายปี พาร์ทเนอร์ของคุณจะยืนยันขอบเขต ใบเสนอราคา และการประเมินทางเทคนิค

zcrX ต้องติดตั้งซอฟต์แวร์บนทุก host ไหม?

zcrX ติดตั้ง Agent น้ำหนักเบาบน host และระบบ build ที่คุณลงทะเบียนไว้ host ที่ไม่มี Agent จะขึ้นว่าไม่มีการวัด ไม่ใช่ถือว่าปลอดภัย

zcrX จัดลำดับว่าจะแก้อะไรก่อนอย่างไร?

จัดลำดับตามสถานะ CISA Known Exploited Vulnerabilities (KEV), EPSS score, ความรุนแรง และจำนวน host ที่ได้รับผลกระทบ ไม่ใช่จำนวน finding ดิบ

zcrX บริหารหลาย customer พร้อมกันได้ไหม?

ได้ zcrX มี provider control plane พร้อมสิทธิ์เข้าถึงแบบ delegated และ least-privilege ต่อแต่ละ customer tenant ออกแบบมาสำหรับ channel partner ที่ดูแลลูกค้าหลายราย

นำข้อมูลเหล่านี้ไปคุยกับพาร์ทเนอร์ที่ได้รับอนุมัติ

สินทรัพย์และการอนุญาต	ระบุแอปพลิเคชัน สภาพแวดล้อมที่อนุญาตให้ทดสอบ โฮสต์ ระบบบิลด์ และรุ่นของระบบนิเวศ พร้อมผู้อนุมัติการทดสอบและการติดตั้ง Agent
ขอบเขตลูกค้า	ระบุ tenant เจ้าของข้อมูล และผู้อนุมัติของลูกค้า ตกลงสิทธิ์ที่ต้องมอบหมายและระยะเวลาเข้าถึง
หลักฐานที่ต้องตรวจ	เลือกตัวอย่างช่องโหว่ สถานะการย้าย หลักฐานที่มา ไฟล์ CSV และกรณีที่ยังไม่ทราบผลหรือยังไม่มีการวัด
ตรวจสอบสภาพแวดล้อม	ให้พาร์ทเนอร์ยืนยัน OS/รุ่น ทรัพยากร เส้นทางเครือข่าย สิทธิ์ติดตั้ง ความจุ และสิทธิ์เข้าถึงที่จำเป็น เอกสารนี้ยังไม่ได้ยืนยันรายละเอียดเหล่านี้
เงื่อนไขและการส่งมอบ	ยืนยันรุ่น แพ็กเกจ ราคา สกุลเงิน หน่วย รอบบิล ภาษี วันที่มีผล การสนับสนุน และหน้าที่ส่งมอบในข้อเสนอของพาร์ทเนอร์

ชมเดโมทางเทคนิค

เดโมสาธารณะแสดง posture ทั้งสามด้าน สำหรับ SAST/DAST ให้ตกลงแอปพลิเคชันและสภาพแวดล้อมทดสอบกับพาร์ทเนอร์ของคุณ

ปรึกษาขอบเขตการใช้งาน

ใช้รายการตรวจสอบตกลงขอบเขตติดตั้งและสิ่งที่ต้องยืนยัน แล้วรับข้อเสนอและใบเสนอราคาจากพาร์ทเนอร์ การทำสัญญาและส่งมอบดำเนินการผ่านพาร์ทเนอร์ที่ได้รับอนุมัติ

นัดประเมินผ่านพาร์ทเนอร์ที่ได้รับอนุมัติ ↗ เปิดเดโมข้อมูลตัวอย่าง ↗

เดโม — ข้อมูลตัวอย่าง ไม่ใช่ตัวเลขลูกค้าจริง คงหน้าจอภาษาอังกฤษตามต้นฉบับ