Context-Aware Security Pipelines

Subtitle I

Agenda

1. **Introduction**

   If you want something new, you have to stop doing something old

2. **The Current Landscape**

   How decisions are made in the CVSS landscape

3. **Adding Context**

   Known Exploited Vulnerabilities (KEV) and Exploit Prediction Scoring System (EPSS)

4. **Prioritizing Risk**

   What do we do with these new frameworks and what problem do they solve?

5. **Putting it All Together**

   How security pipelines work and how applications are scanned for vulnerabilities

5. **Thank You + Q/A**

Introduction

Bacchus Jackson

Chief Mission Architect
Clarity Innovations

Former Air Force 480th ISRW Innovation Specialist responsible for standardizing Airmen Led development founded in Lean Startup principles.

Currently working with Engineers from Air Force Platform One on the Continuous Authorization and Verification Engine (batCAVE) for the Center for Medicaid and Medicare Services (CMS).

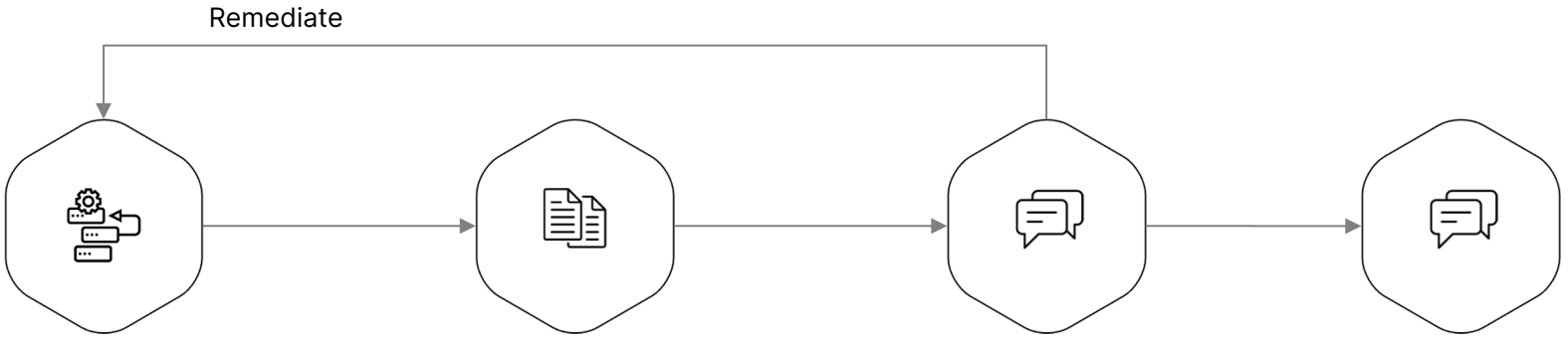
Mike Lanciano

Director of Engineering Growth
Clarity Innovations

Solutions architect with over a decade of supporting end to end solutioning across both the public and private sectors with a heavy focus in large scale data platforms for both the DoD and IC.

Passionate about organizational culture and cybersecurity outcomes that positively impact mission.

Pipeline without Context



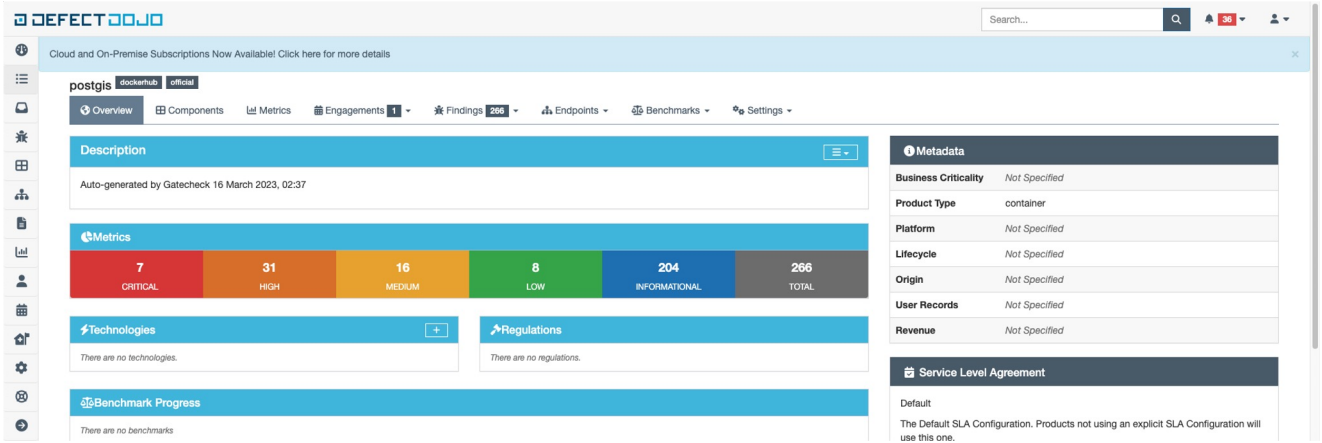
Scan Code and Dependencies for CWE and CVE signatures (SBOM)

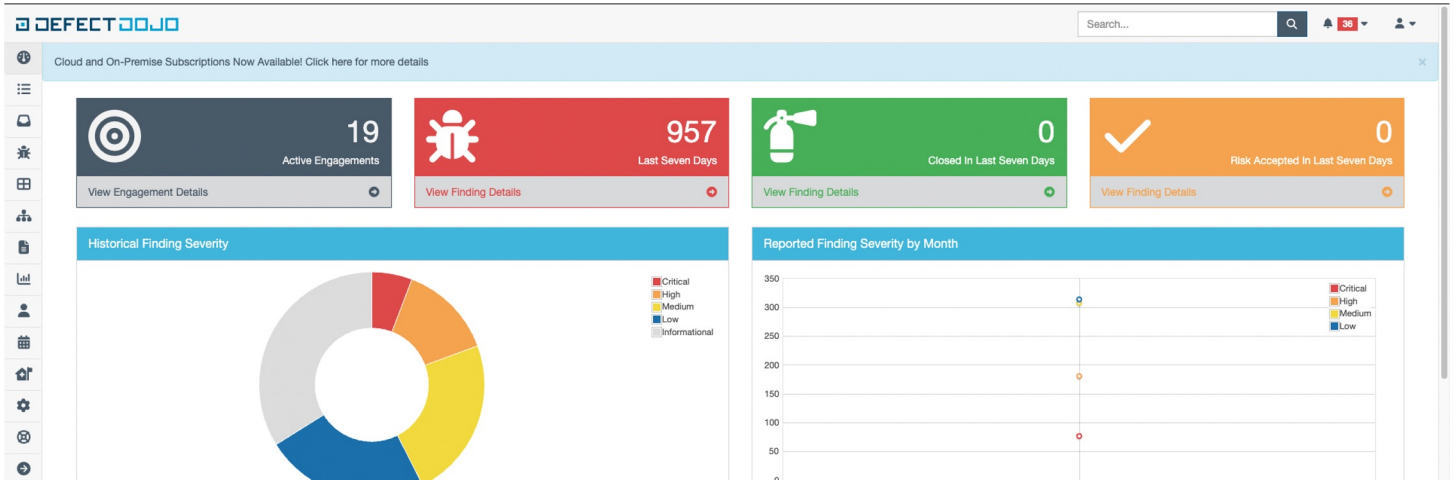
Scoring of Findings using Qualitative Analysis (i.e. CVSS)

Organizational Threshold Validation for Deployment (e.x. 0 Criticals or Highs)

Deliver Value

Great Until...


DEFECTDOJO
Search...
Cloud and On-Premise Subscriptions Now Available! Click here for more details
postgis
dockerhub
official
Overview
Components
Metrics
Engagements 1
Findings 266
Endpoints
Benchmarks
Settings
Description
Auto-generated by Gatecheck 16 March 2023, 02:37
Metrics
7 CRITICAL
31 HIGH
16 MEDIUM
8 LOW
204 INFORMATIONAL
266 TOTAL
Technologies
There are no technologies.
Regulations
There are no regulations.
Benchmark Progress
There are no benchmarks
Metadata
Business Criticality Not Specified
Product Type container
Platform Not Specified
Lifecycle Not Specified
Origin Not Specified
User Records Not Specified
Revenue Not Specified
Service Level Agreement
Default
The Default SLA Configuration. Products not using an explicit SLA Configuration will use this one.


DEFECTDOJO
Search...
Cloud and On-Premise Subscriptions Now Available! Click here for more details
19 Active Engagements
View Engagement Details
957 Last Seven Days
View Finding Details
0 Closed In Last Seven Days
View Finding Details
0 Risk Accepted In Last Seven Days
View Finding Details
Historical Finding Severity
Critical
High
Medium
Low
Informational
Reported Finding Severity by Month
350
300
250
200
150
100
50
Critical
High
Medium
Low

CVSS at a Glance

- **Exploitability**
  - Attack Vector
  - Complexity
  - Privileges
  - User Interaction
- **Scope**
  - Propagation
- **Impact**
  - Confidentiality, Integrity, Availability
- **Exploit/Code Maturity***
- **Remediation***
  - Is there a patch?
- **Confidence**

Context Matters

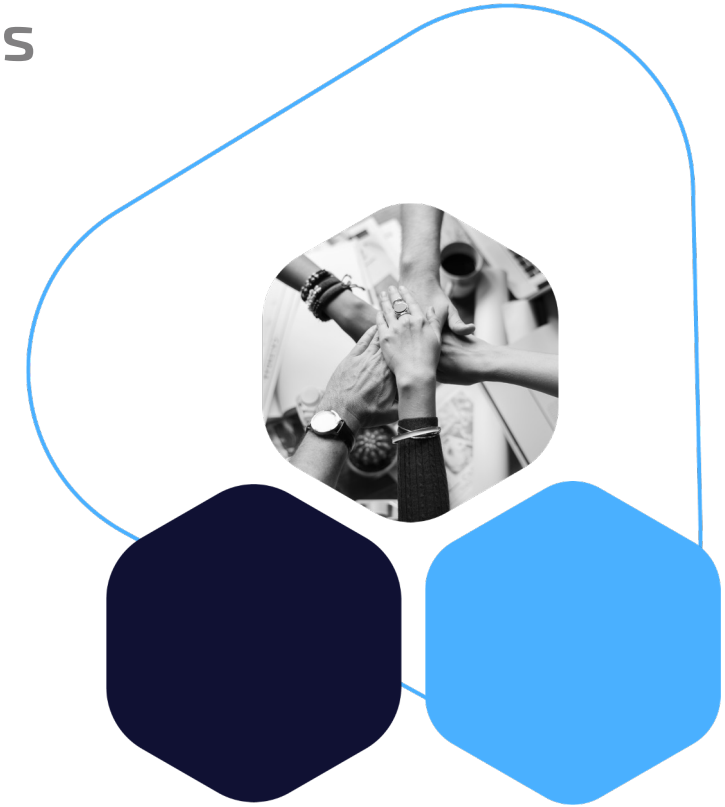
Sustainable and proactive risk management is about contextualizing the **impact** and **probability of risk** to your overall mission. Currently used frameworks are often considering only **qualitative impact**.

“Attackers do not rely only on ‘critical’ vulnerabilities to achieve their goals; some of the most widespread and devastating attacks have included multiple vulnerabilities rated ‘high’, ‘medium’, or even ‘low’. “

-CISA, Binding Operational Directive 22-01

Known Exploited Vulnerabilities (KEV)

- **Catalog Selection Criterion**
  - #1 Assigned CVE ID
  - #2 Active Exploitation
  - #3 Clear Remediation Guidance
- **Data Source and Publish Frequency**
  - JSON, CSV, Bulletin
  - CISA Website
- **Cross Referencing**
  - Syft SBOM -> Grype -> Gatecheck

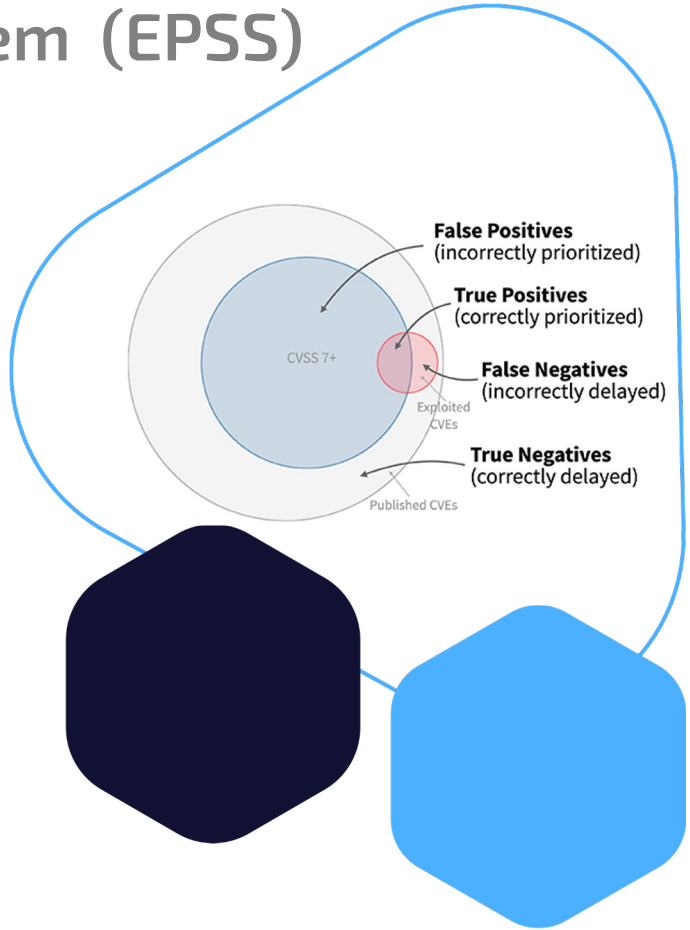


CISA Recommendation

“CISA strongly recommends all stakeholders include a requirement to immediately address KEV catalog vulnerabilities as part of their vulnerability management plan. Doing so will build collective resilience across the cybersecurity community.”

Exploit Prediction Scoring System (EPSS)

- **Data Sources**
  - MITRE's Published CVEs
  - CVSS v3 vectors in the base score National Vulnerability Database (NVD)
- **Scoring Methodology**
  - probability score between 0 and 1 (0% and 100%)
- **Efficiency & Coverage**
  - [True/False] [Negative/Positive]
- **Cross Referencing**
  - Syft SBOM -> Grype -> Gatecheck



Real World Examples

The WP Remote Users Sync plugin for WordPress is vulnerable to Server Side Request Forgery via the 'notify_ping_remote' AJAX function.

CVSS - 8.5 (High), EPSS 0.1%, KEV: Not Listed

Ivanti Endpoint Manager Mobile (EPMM), formerly MobileIron Core, through 11.10 allows remote attackers to obtain PII, add an administrative account, and change the configuration because of an authentication bypass, as exploited in the wild in July 2023.

CVSS - 10.0 (Critical), EPSS (96.5%), KEV: Listed

Context Drives Priority

With KEV and EPSS we know more:

- “Critical” does not imply “Exploitable”.
- We have a 30-day temporal contextual quantifiable risk.

So we can not prioritize our backlog of security chores.

“Past research has shown that firms are able to fix between 5% and 20% of known vulnerabilities per month. Secondly, only a small subset (2%-7% of published vulnerabilities are ever seen to be exploited in the wild).“

- FIRST

Developer and App Sec Fatigue

Trudging through a mountain of security vulnerabilities and tracing through false positives and low-probability exploits **reduces delivery** and makes the problem feel **intractable**.

Quantitative Tunnel Vision

Without the ability to contextually prioritize, all risk is created equal. You may inadvertently be running out the clock to reduce your overall risk and ignoring riskier items. ~15% of KEVs are **Mediums**.

Humans as the Loop

The inability to sort and contextualize the large buckets of information outside CVSS means you are limited by the manual intervention of humans and their domain knowledge of the applied problem.

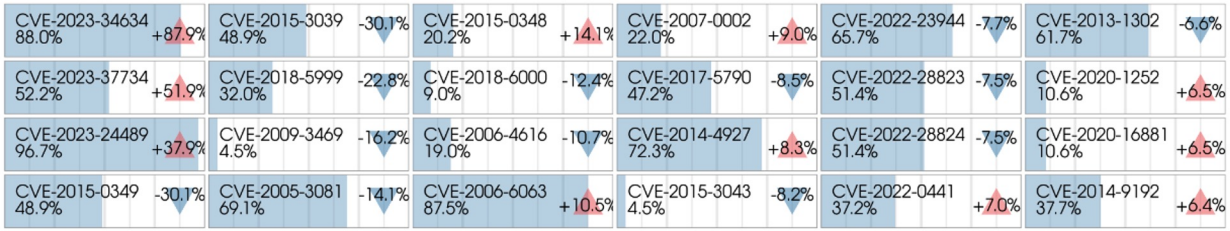
Expensive Confidence

All activities that don’t provide true security outcomes have an impact to cost, schedule, and performance. Similarly they provide a false sense of completion based security and not real-time temporal risk.

But There's More. Context Is Temporal.

CVEs with shifting EPSS scores

EPSS scores can shift around because of new information (e.g CPE data is available now, an exploit is published, etc)



Source: https://first.org/epss/data_stats, 2023-08-18

The automation and inclusion of these frameworks is made infinitely more valuable through strong **asset cataloging** (what's critical), **software bill of materials** (what's in the environment), **continuous scanning** (how long ago), and **runtime verification** (what I built is what is running).

Putting it All Together

We know that we want the intersection of CVSS+EPSS+KEV as well as the ability to apply that context to the whole lifecycle, Development to Operations. How are other organizations accomplishing this?

Context Aware Pipeline

EPSS
Exploit Prediction Scoring System

Pipeline Run

- Image Build
- SBOM Generation
- Vulnerability Scan
- Secrets detection
- Static Code Analysis

Gatecheck Bundle

- Security artifacts bundle
- Bundle Signature

Gatecheck Export

- S3 Security Data Lake
- Defect Dojo
- Summary Output

Gatecheck Validate

- KEV Catalog Deny Rule
- EPSS Allow & Deny Rules
- Threshold Rules

Deploy

- Attestation Verification
- GitOps Deployment

Thank you!

Questions?