Application Security

Continuous Security im Application Lifecycle

Beris Bachmeier - Security Consultant

claranet | Make modern happen®

PUBLIC
Verantwortlich: Claranet GmbH
Version 1.0 – 03.07.2025

Agenda

- **Cyber Security Prozess**
  Application Security im Cyber Security Prozess
- **Bedrohungslage**
  Überblick über die Bedrohungslage im Hinblick auf Applikationen und deren Bedeutung
- **Sichere Architektur & Entwicklung**
  Wie Methodik und sichere Entwicklungspraktiken Schwachstellen frühzeitig verhindern
- **Kontinuierliche Sicherheitsprüfung**
  Penetrationstests und Continuous Security Testing (CST) für nachhaltigen Schutz

claranet cyber security®

Cyber Security Prozess

- Die Realität stellt immer wieder neue Anforderungen
- Cyber Security ist kein Zustand, sondern ein Prozess, der kontinuierlich angepasst werden muss

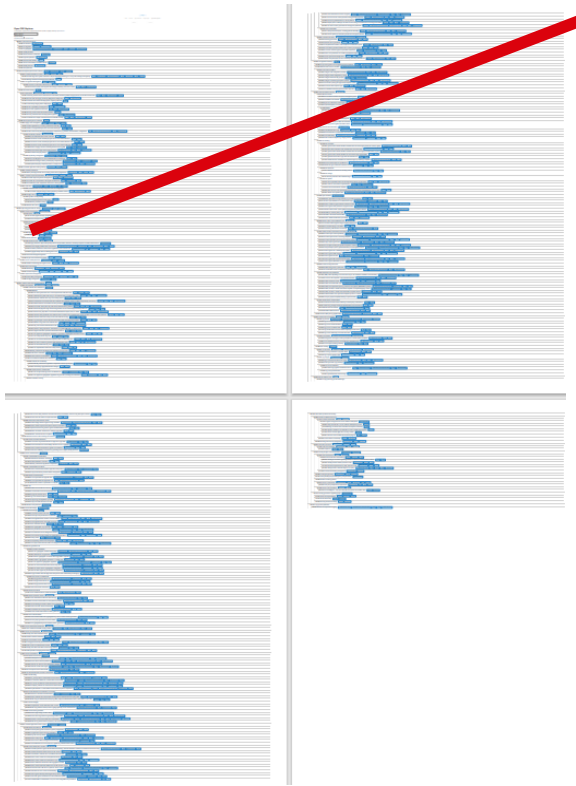
Dieser Prozess unterliegt einem Lebenszyklus

claranet | Make modern happen®

Definition: Application Security

Application Security ist ein weites Feld mit Verknüpfungen in unterschiedlichste Gebiete der Informationssicherheit

Auszug Open Common Requirement Enumeration



- 862-452: Operating processes for security [Cloud Controls Matrix] [ISO 27001] [NIST 800-53 v5]
  - 850-376: Facilities management [Cloud Controls Matrix]
    - 163-776: Backup [ISO 27001]
      - 257-117: Perform regular backups of important data and test restoration [CWE] [ASVS]
      - 614-353: Store backups securely [CWE] [ASVS]
    - 148-227: Endpoint management [Cloud Controls Matrix] [ISO 27001] [NIST 800-53 v5]
      - 007-274: Patching and updating system components [SAMM]
      - 286-500: OS security [Cloud Controls Matrix]
      - 872-574: Virus/malware protection [ISO 27001]
    - 157-587: Equipment management [ISO 27001] [NIST 800-53 v5]
      - 114-853: Maintenance [ISO 27001] [NIST 800-53 v5]
    - 522-616: Media protection [ISO 27001] [NIST 800-53 v5]
    - 467-784: Network security [ISO 27001] [NIST 800-53 v5]
      - 132-146: Apply defense-in-depth techniques/processes for protection, detection, and timely response to network-based attacks. [Cloud Controls Matrix]
      - 336-512: Ensure integrity of DNS entries and domains [OWASP Web Security Testing Guide (WSTG)] [Cloud Controls Matrix] [CWE] [OWASP Cheat Sheets] [ASVS] [ISO 27001]
      - 515-021: Sandbox, containerize and/or isolate applications at the network level [OWASP Proactive Controls] [CWE] [Cloud Controls Matrix] [ASVS] [ISO 27001]
      - 273-600: Segregate components of differing trust levels [Cloud Controls Matrix] [CWE] [ASVS]
    - 125-010: Password management systems
    - 234-282: Physical & environment protection [ISO 27001] [NIST 800-53 v5]
  - 247-250: Access control processes [Cloud Controls Matrix] [ISO 27001] [NIST 800-53 v5]
    - 623-347: Disallow shared high privileged accounts [NIST 800-63] [CWE] [ASVS] [OWASP Cheat Sheets]
  - 887-750: Detect and respond
    - 058-083: Monitoring [Cloud Controls Matrix] [ISO 27001] [NIST 800-53 v5] [SAMM]
    - 463-577: Incident response [Cloud Controls Matrix] [ISO 27001] [NIST 800-53 v5] [SAMM] [NIST SSDF]
  - 010-678: Improvement management
    - 732-148: Vulnerability management [Cloud Controls Matrix] [ISO 27001] [NIST 800-53 v5] [NIST SSDF] [SAMM]
    - 112-648: Change management [Cloud Controls Matrix] [ISO 27001]
- 636-660: Technical application security controls [NIST SSDF]

Definition: Application Security

Sicheres Erstellen und Betreiben von Applikationen über den gesamten Lebenszyklus hinweg.

Erkennen und Beheben von Schwachstellen während

- Planung
- Development
- Release
- Deployment
- Betrieb
- Maintenance

Application Security ist relevant – auch wenn Applications nicht selbst entwickelt werden.

claranet | Make modern happen®

Bedrohungslage – Application Security

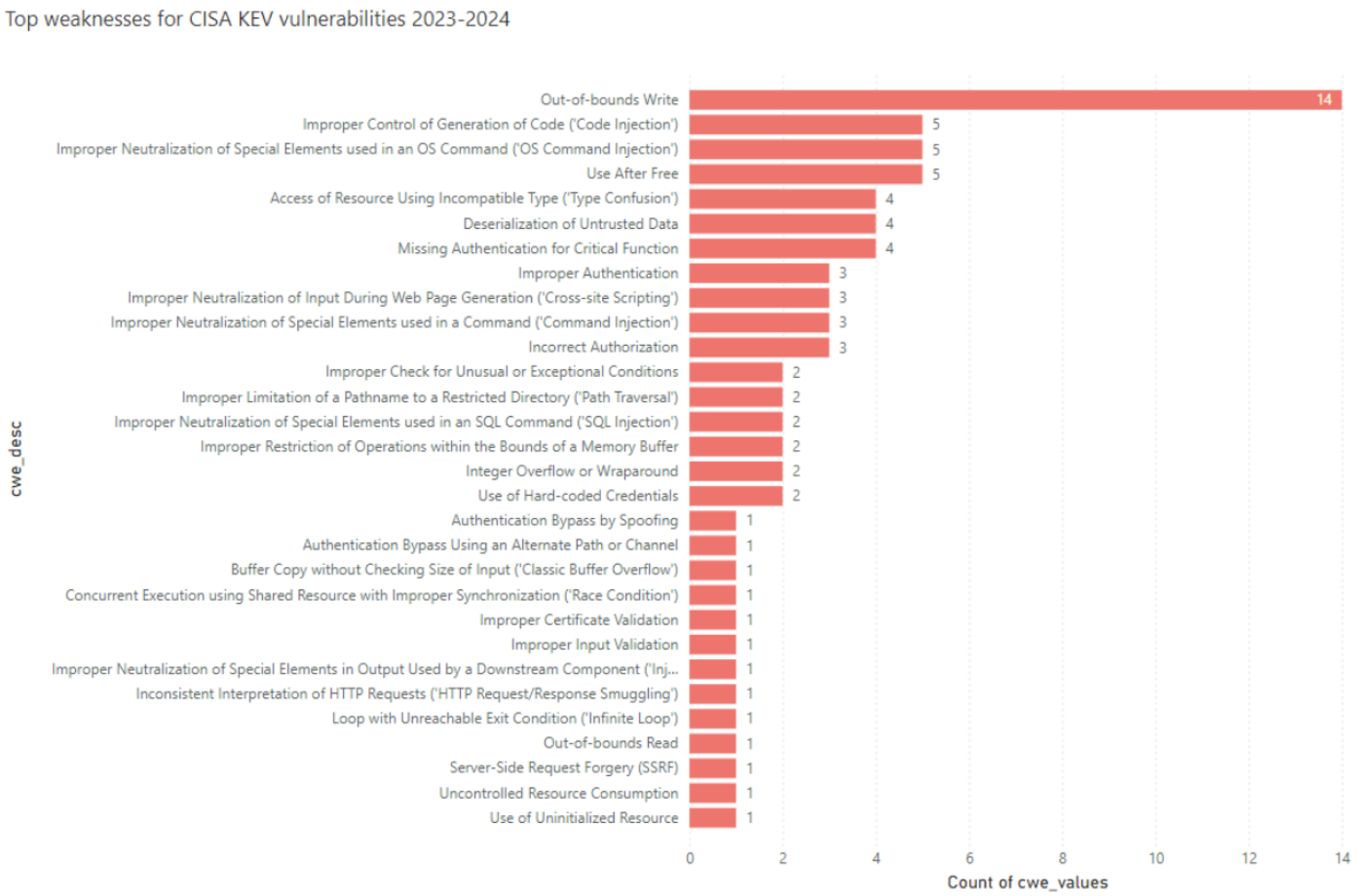
Wie sieht die Lage real aus?

European Union Agency for Cybersecurity
ENISA THREAT LANDSCAPE 2024:

“(..) **Exploiting vulnerabilities remains a favoured tactic** for State-nexus actors to infiltrate organisations.

Public applications continue to be a prime
target for actors(..) Their **main focus includes web applications** such as e-commerce platforms, collaboration tools and service desk software, alongside lingering vulnerabilities(..)”

Table 2: CWEs responsible for KEVs 2023-2024



Bedrohungslage – Application Security

VERIZON
Data Breach Investigations Report 2025
Initial Access Analysis

"(..) **exploitation of vulnerabilities being present in 20% of all breaches we analyzed – a 34% increase from last year**.."

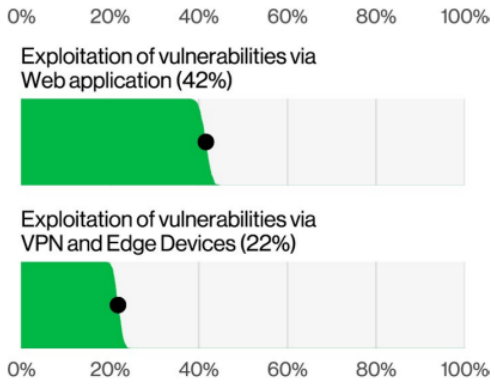
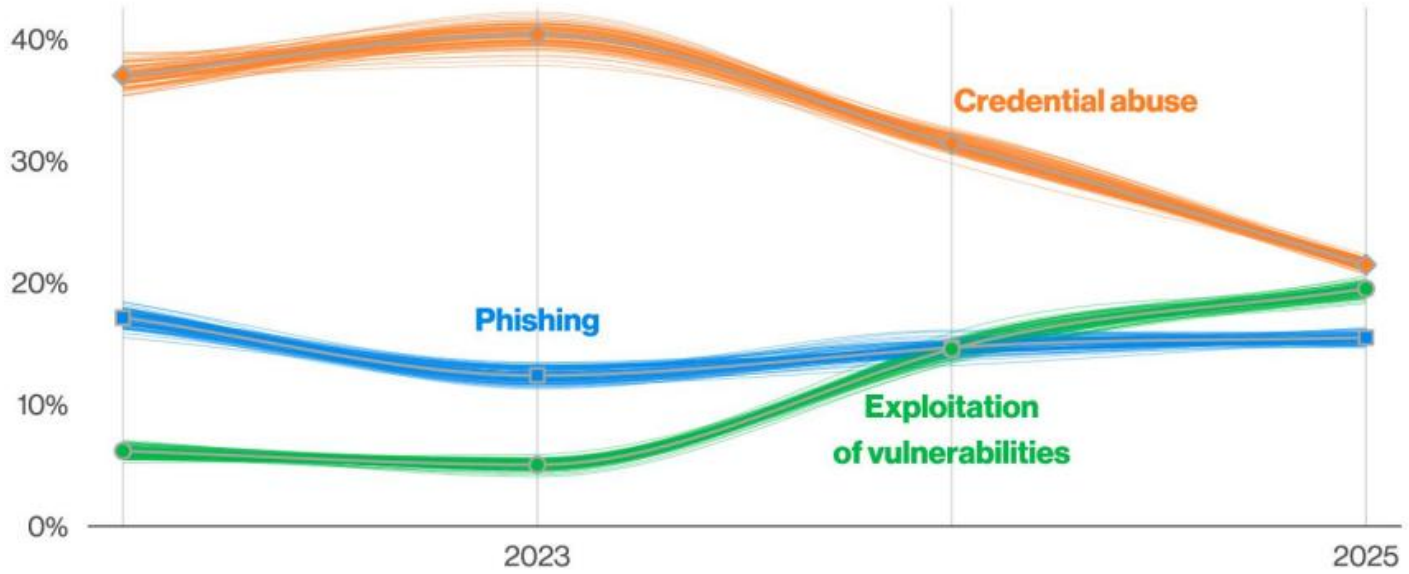


Figure 17. Select exploitation of vulnerabilities vector enumerations in non-Error, non-Misuse breaches



claranet | Make modern happen®

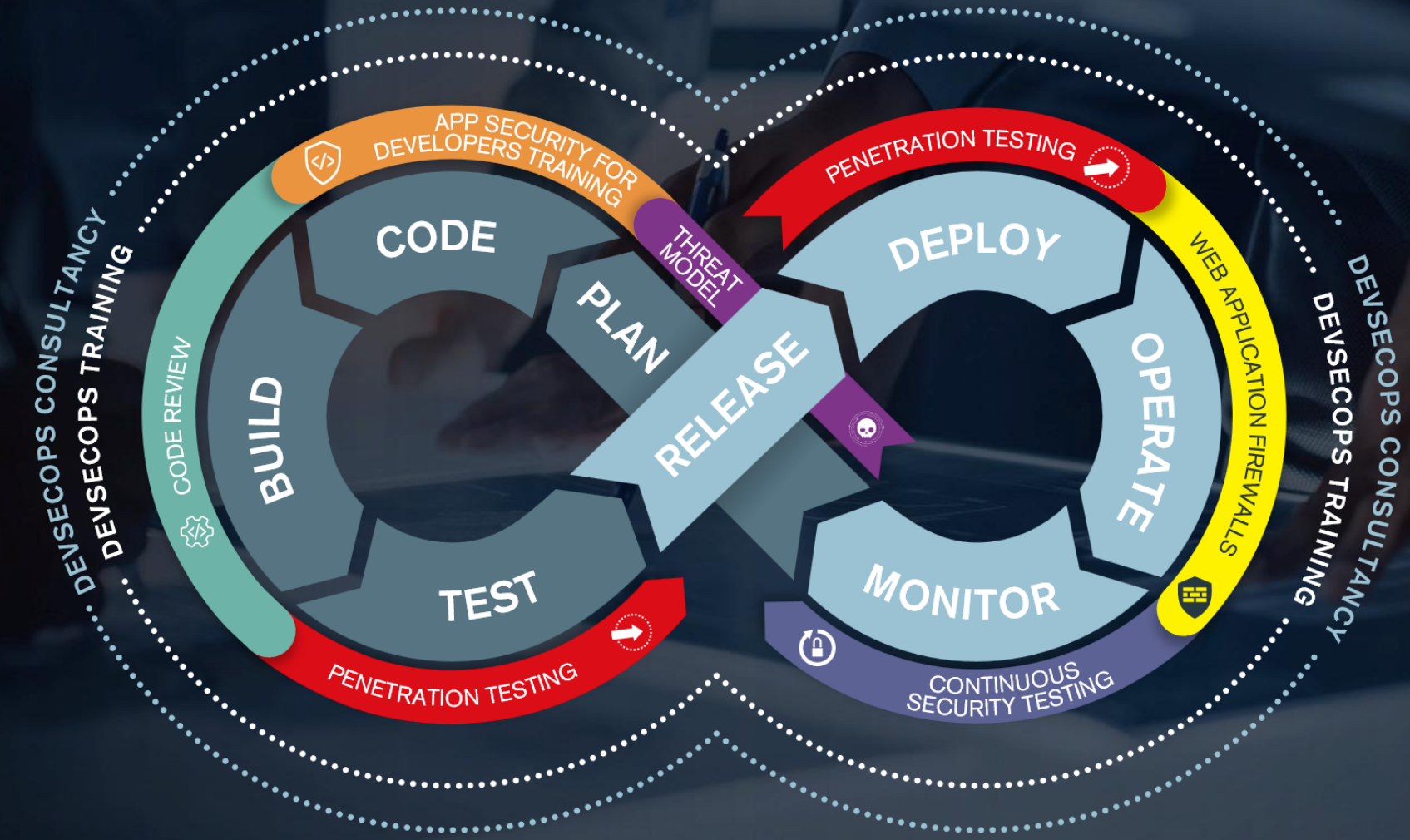
Application Lifecycle - Application Security

INFINITE LOOP – APPLICATION LIFECYCLE

- AppSec? DevSecOps?

Application Lifecycle – Application Security

CONTINUOUS SECURITY



Sichere Architektur und Entwicklung

Was kann schiefgehen? Was können wir dagegen tun?

Cyber Security beginnt bereits in der PLAN Phase

- Systematische Modellierung
- Potentielle Bedrohungen feststellen

Threat Modeling

- Wichtiger Ansatz zur Analyse des Aufbaus
- Identifizieren und Visualisieren der wichtigsten Bedrohungen und Risiken
- Nicht nur auf Applikationen anwendbar

Sichere Architektur und Entwicklung

Entspricht unsere Umsetzung entsprechenden Sicherheitsanforderungen?

CODE und BUILD Phasen

- Motivation und Befähigung der Entwicklungsteams
- Überprüfung des Source Codes

Trainings for AppSec & DevSecOps

- Praktische Fähigkeiten
- Techniken und Tools, um sicher zu entwickeln
- DevSecOps-Bewusstsein schaffen

Code Review

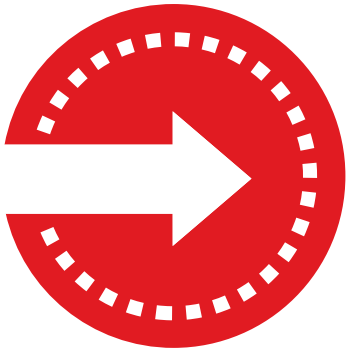
- Überprüfung des Source Code durch dedizierte Security Experts
- Enge Zusammenarbeit mit den Dev-Teams

Kontinuierliche Sicherheitsprüfungen

Sind Applications und Systeme im Betrieb angreifbar ? (3rd Party oder selbstentwickelt)
Unerwartete Schwachstellen vorhanden, die vorab nicht aufgefallen sind?
Wie ist dem Auftreten und der Ausnutzung von Schwachstellen schnellstmöglich zu begegnen?

The Challenge of Continuous Security Testing

Wie dieser Herausforderung meistens begegnet wird



Penetration Testing

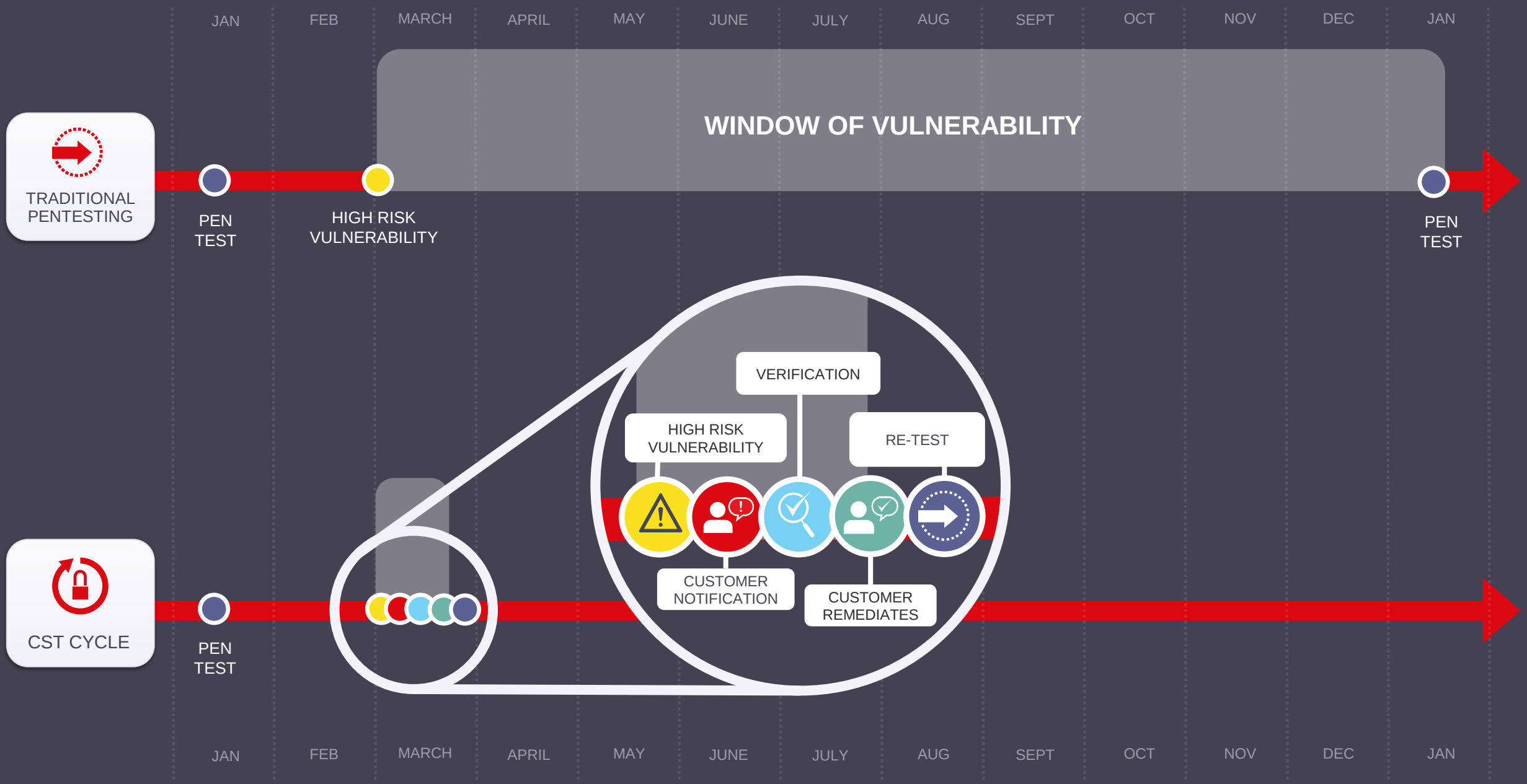
- Detailliert, aber eng gefasst
- Momentaufnahme
- Re-Tests bei vielen Anwendungen und hoher Dynamik aufwendig

Vulnerability Scanners

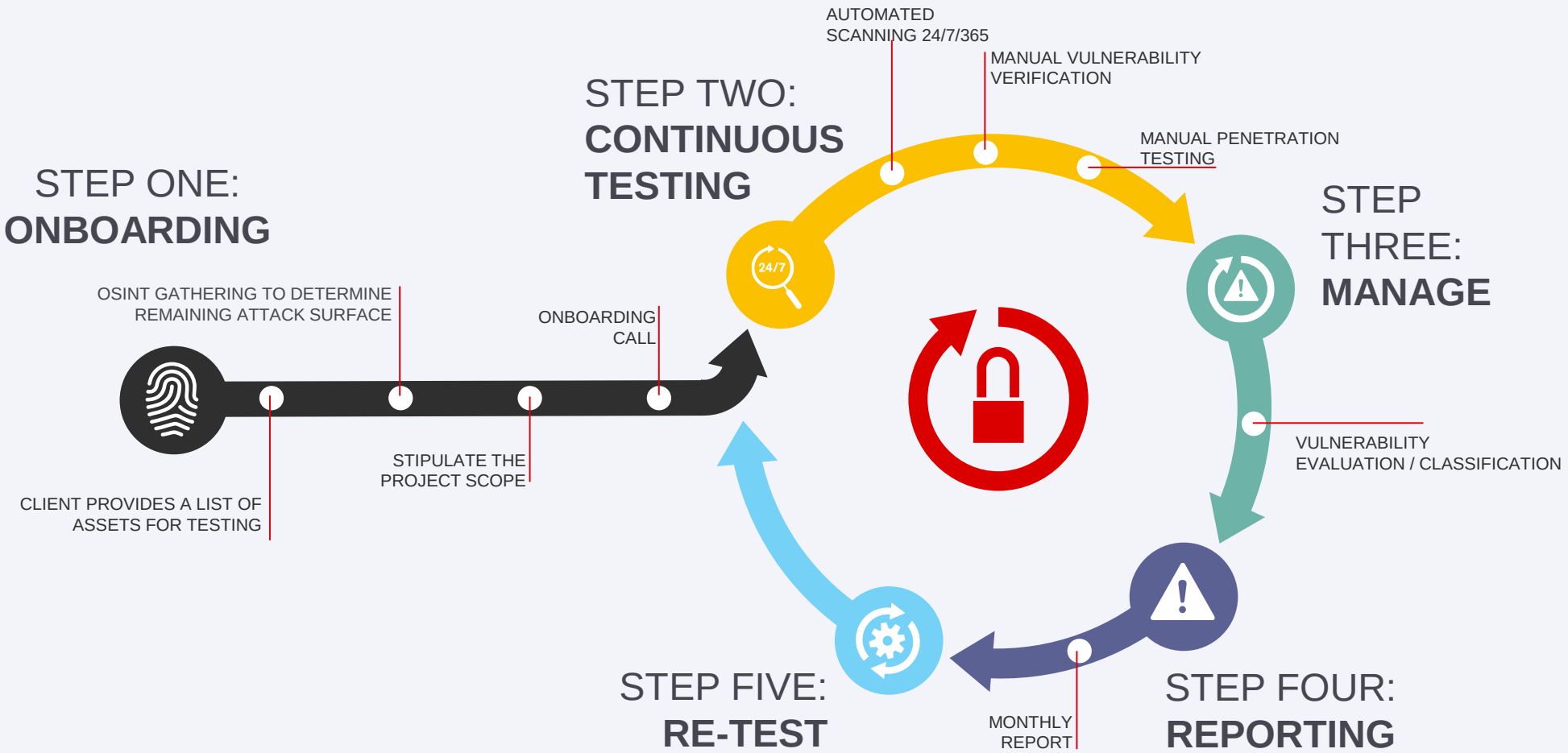
- Schnell, aber oberflächlich
- Können nicht ausreichend Kontext liefern
- Hohe Aufwände in der Verifizierung

Crowdsourced pentesting/bug bounties

- Konzentriert sich auf schnelle Erfolge
- Wenig/keine direkte Kommunikation mit Hunters
- Keine Kenntnis, ob und wann die eigenen Applikationen getestet werden

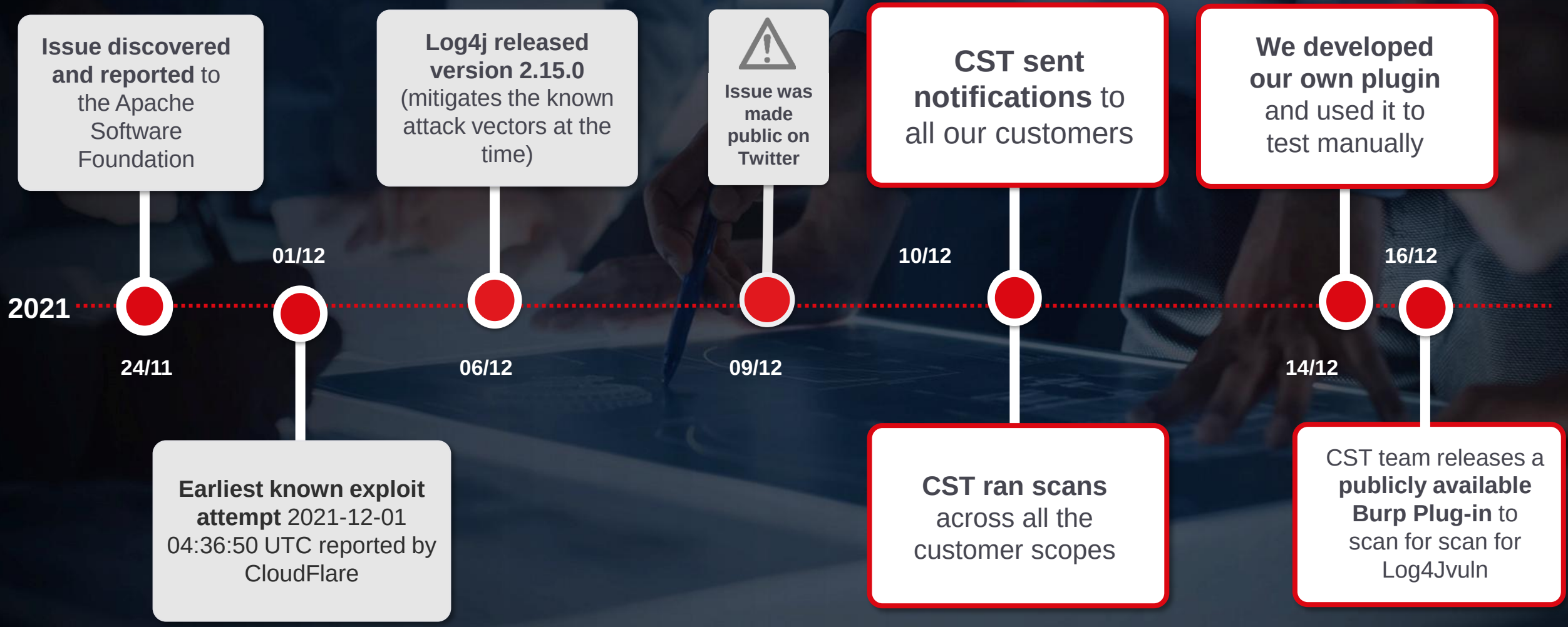

JAN
FEB
MARCH
APRIL
MAY
JUNE
JULY
AUG
SEPT
OCT
NOV
DEC
JAN
WINDOW OF VULNERABILITY
TRADITIONAL PENTESTING
PEN TEST
HIGH RISK VULNERABILITY
PEN TEST
CST CYCLE
PEN TEST
VERIFICATION
HIGH RISK VULNERABILITY
RE-TEST
CUSTOMER NOTIFICATION
CUSTOMER REMEDIATES
JAN
FEB
MARCH
APRIL
MAY
JUNE
JULY
AUG
SEPT
OCT
NOV
DEC
JAN

The Continuous Security Testing Cycle



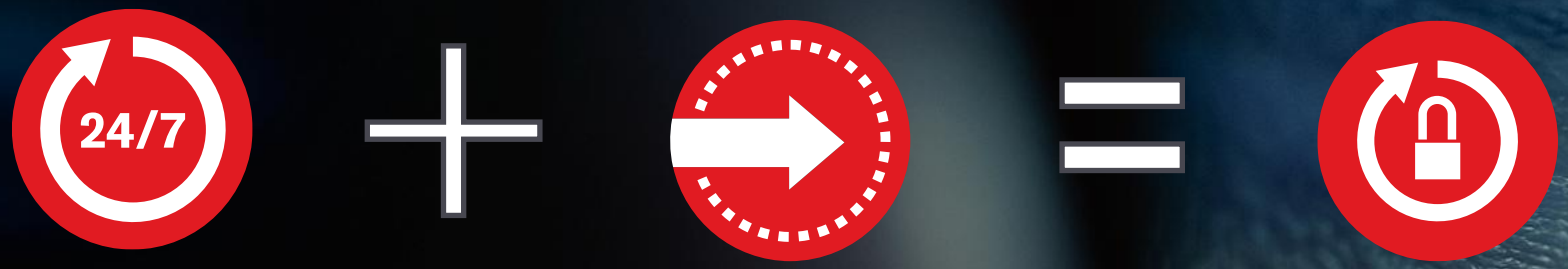
claranet | Make modern happen®

Zero Day Monitoring, Log4Shell Case Study



Best of both worlds

Combine the speed of automation with the expertise of a team of penetration testers.

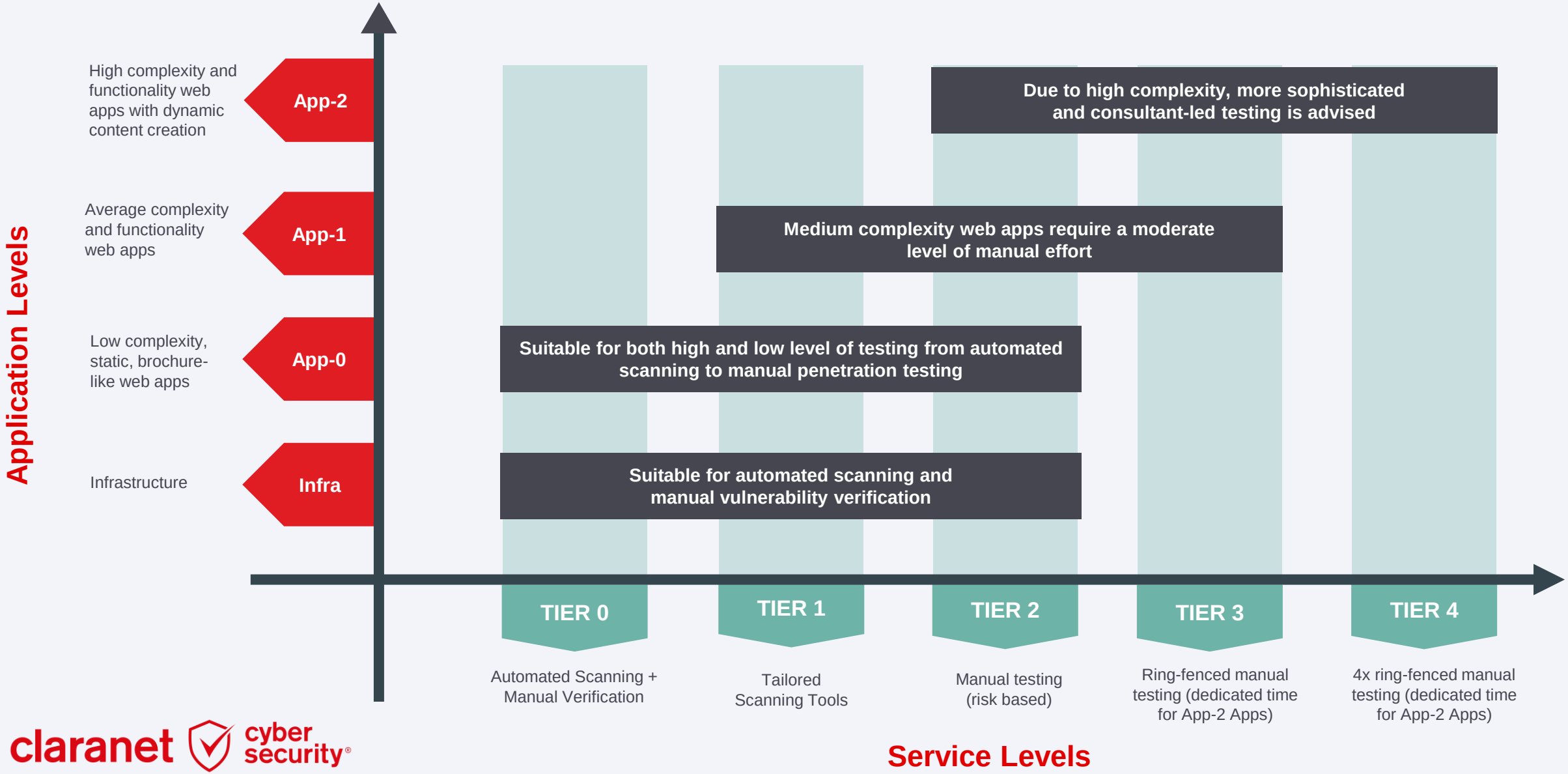


24/7 Automated Scanning

Manual Penetration Testing

Continuous Security Testing

Tailored to your needs



claranet cyber security®