CYTRES

XDR+

Prozessübersicht

1. Cloud-Security

    1.1. Passives Cloud-Scanning

        1.1.1. HTTP-Header
        1.1.2. Transportverschlüsselung
        1.1.3. Software-Versionen / EoL
        1.1.4. Offenlegung von Informationen
        1.1.5. Konfigurationsfehler
        1.1.6. Sensitive Dateien und Ordner

    1.2. Automatisierter Cloud-Penetrationstest

        1.2.1. Cross-Site-Scripting (XSS)
        1.2.2. SQL-Injection
        1.2.3. XML External Entities (XXE)
        1.2.4. Fehler in der Zugriffskontrolle
        1.2.5. Unsichere Deserialisierung
        1.2.6. Remote-Code-Execution (RCE)
        1.2.7. Denial-of-Service (DoS)
        1.2.8. Cross-Site-Request-Forgery (CSRF)
        1.2.9. Speicherkorruptionen
        1.2.10. Nutzung von Komponenten mit bekannten Schwachstellen

2. Endpoint-Security

    2.1. Anti-Malware: Statisch, signaturbasiert
    2.2. Anti-Malware: Dynamisch, KI-basiert
    2.3. Anti-Phishing: Statisch, signaturbasiert
    2.4. Anti-Phishing: Dynamisch, KI-basiert
    2.5. Anti-Exploit / Anomalieerkennung
    2.6. Anti-PUP / Softwareüberwachung
    2.7. Lokales Schwachstellen-Scanning: CVE
    2.8. Lokales Schwachstellen-Scanning: Zero-Day-Exploits
    2.9. Netzwerk Schwachstellen-Scanning: CVE
    2.10. Netzwerk Schwachstellen-Scanning: Zero-Day-Exploits
    2.11. Offene Updates / Automatische Aktualisierung

3. Software-Security

    3.1. Automatisierte Identifikation von Speicherkorruptionen

        3.1.1. Buffer-Overflow
        3.1.2. Heap-Overflow

        3.1.3. Stack-Overflow
        3.1.4. Integer-Overflow
        3.1.5. Use-After-Free
        3.1.6. Double-Free
        3.1.7. Format-String
        3.1.8. NULL-Pointer-Dereferenzierung

    3.2. Automatisierte Erzeugung von PoC-Exploits
    3.3. Automatisierte Software-Patches

4. API-Security

    4.1. Protokollbasiertes Fuzzing
    4.2. Automatisierte Erzeugung von PoC-Exploits

5. Sonstiges

    5.1. Schwachstellenmanagement
    5.2. Benutzerverwaltung
    5.3. Entwickler-API