DCSO
ENGINEERING SECURITY

DCSO: Cyber Security Trends im Test

Stefan Wieczorek

Fast Lane IT-Forum, Berlin, 12. Oktober 2017

DCSO Gründer

DCSO Übersicht

Security Solutions	Cyber Defense Services	Govern. Risk & Compliance
Technology Scouting and Evaluation	**Threat Intelligence** (Operational TI, Reports)	**TISAX® Audit Platform**
Joint Projects / Prototyping (DCSO::Labs)	**Internet Monitoring**	**Cloud Vendor Assessment Community**
	Threat Detection & Hunting	**Information Risk Assessment Process**
	Incident Response	

Professional Services: Architecture, Integration, PoCs, GRC Consulting

Threat Intelligence Sharing Platform: Members share threat indicators and trends

Sharing between DCSO Members: Threats, Techn. Experience, Future Security Architecture

Technology Scouting and Evaluation (TSE) hilft beim…

1. …vorbereiten einer **Übersicht über den IT-Security Markt** entlang definierter Fähigkeiten
2. …tested zentralisiert und unvoreingenommen **funktionale und nichtfunktionale** Aspekte
3. …teilt das **Wissen und die Erfahrungen** aller DCSO TSE Kunden und begeleitet PoCs
4. …reduziert für jeden Kunden von TSE **Zeit und Aufwand** für die Produktauswahl

DCSO ENGINEERING SECURITY

Wie finde ich ein gutes (Security) Produkt?

DCSO ENGINEERING SECURITY

Wann suche ich ein gutes Security Produkt?

Übliche Trigger für die Evaluation von Produkten

Key Account Manager von <security company> hat ein tolles, neues Angebot

Gartner, Kuppingercole oder ein anderer Analyst veröffentlicht einen neuen Quadraten/Wave/Report

…und manchmal sieht das Marketing einfach sehr vielversprechend aus

Wo wir von Marketing reden…

[…] Next Generation Platform to provide the broadest enterprise visibility and accurate detection of advanced threats & evasion techniques, and zero-day attacks by utilizing behavioral analytics, machine learning, and Long-Data Security-Analytics.

By coupling sophisticated math and machine learning with a unique understanding of a hacker's mentality, […] provides the technology and services to be truly predictive and preventive against advanced threats

[…] prevents advanced attacks and zero-days when and where they happen – at your endpoints and in real time, with zero false positives and no performance degradation.

Vernünftige Trigger für die Evaluation von Produkten

Neue Lösungen / Architekturen müssen abgesichert werden (Office 365, Mac, BYOD)

Ein bestehendes Produkt ist nicht mehr ausreichend oder erwünscht

Neue technologische Entwicklungen könnten bestehende Lösungen obsolet machen

---

Es existiert ein echter Bedarf

DCSO ENGINEERING SECURITY

Schritte einer Produktevaluation

Schritt 1: Initiale Phase

Ein Abteilungsleiter war mit einem **Vertriebler der UberCyber** Golf spielen

Der Abteilungsleiter ist von den **Vorteilen von UberCyber überzeugt**

Das Produkt soll **schnellstens evaluiert und beschafft** werden

üblich

In der Firma soll die **Nutzung von Clouddiensten abgesichert** werden

Anforderungen werden erarbeitet

Eine **Recherche** ergibt **mehrere vielversprechende Produkte**, unter anderem UberCyber

sinnvoll

Schritt 2: Vorbereiten der Teststellung

Der Vertriebler installiert UberCyber auf einem Server **im Produktivnetz**

Der Hersteller richtet das Produkt in einer **„üblichen Konfiguration“** ein

Mit UberCyber werden **Ziel und Dauer** der Testellung definiert und **dokumentiert**

Eine **isolierte Umgebung** wird vorbereitet

Das Produkt wird **durch den Kunden** mit dem Vertriebler **installiert**

Der Kunde richtet das Produkt mit Hilfe der **Dokumentation ein**

Schritt 3: Produktevaluation

Durch den Vertriebler werden die Funktionen von UberCyber **demonstriert**

Dem Kunden werden **fehlende Features asap™** versprochen

Jedes Testing des Kunden **sollte im Beisein eines UberCyber Engineer** stattfinden

Es wird bereits am **Anfang ein Telefonat mit dem CTO** von UberCyber angeboten

Administratoren des Kunden testen UberCyber mit Hilfe der Dokumentation **ohne das Beisein eines Vertrieblers**

Der Test erfolgt nach **definierten Kriterien (ff)**

Testkriterien

- Trennung in **funktionale** und **nichtfunktionale** Tests
- Basierend auf den **realen Gegebenheiten**
- **Nicht** notwendigerweise **präzise**
- Üblicher Umfang: 200 – 400 Testfälle

Direkt die Funktion betreffend
- % erkannte Malware bei AV
- Qualität einer Verschlüsselung
- Unterstütze Cloud Services

Andere Aspekte
- Bedienbarkeit
- Dokumentation
- Sicherheit
- Integrationsfähigkeit

Testkategorien (Nichtfunktional) 1

- **Administration**
  - Vorkonfigurierte Templates / Policies
  - Workflow von Administratoren
- **Dokumentation**
  - Verfügbarkeit, Durchsuchbarkeit, Sprachen
  - Qualität
  - Schulungsangebote
  - Andere Medien
- **Compliance**
  - Zertifizierungen und Datenschutz
  - GDPR (General Data Protection Regulation) Umsetzbarkeit
  - Rollen und Rechte Management
  - Audit-Logging

Testkategorien (Nichtfunktional) 2

- **Enterprise Readiness**
  - Architektur und Integrationen (IPv6 Tauglichkeit ?)
  - Hochverfügbarkeit
  - Backup / Restore
- **Lifecycle**
  - Installation / Update / Deinstallation
- **Usability**
  - Für den Administrator
  - Für den Endnutzer
- **Sicherheit**
  - Low hangig fruits abgrasen (XSS, SQL Injection, HTTPs MITM)
  - Prozeduren abklopfen
  - Ergeben Architektur und Hersteller ein schlüssiges Bild?

Testkategorien Funktional

- Ca. **50% des Testumfanges**
- Abhängig von der **Produktkategorie**
- **Use-Case** orientiert arbeiten
- Fehlende Funktionen beim Hersteller anfragen
  - Teilweise über Integrationen möglich
  - Kundenprojekte zur Entwicklung von Funktionen geschätzt

Schritt 4: Roundup und Auswahl

Der Abteilungsleiter erklärt die Auswahl für **beendet**

Ein Vertrag wird abgeschlossen: UberCyber wird **zum Listenpreis** beschafft!

Alle Tests wurden **abgeschlossen**

Auf **Basis der Evaluation** wird die **Entscheidung** getroffen**,** UberCyber und ergänzende Produkte zu **beschaffen**

Durch den **vergleichenden Test** kann bei UberCyber **ein Rabatt** erzielt werden

Tips n‘ Tricks

- **Messen** besuchen und Visitenkarten sammeln
- **Überblick** über bereits eingesetzte Produkte **gewinnen**
- **Synergien** zwischen Produkten nutzen
- **Testmanagement Tools** > Excel

3 Takeaways

1. Nicht von Herstellern drängen lassen
2. Nichtfunktionale Aspekte beachten
3. Testing zahlt sich aus

Stefan Wieczorek
IT Security Analyst
DCSO GmbH
Mob: +49 151 43157869
Mail: stefan.wieczorek@dcso.de

Paul Weise
Head of Tech Scouting & Evaluation
DCSO GmbH
Mob: +49 151 414 457 44
Mail: paul.weise@dcso.de

DCSO Deutsche Cyber-Sicherheitsorganisation GmbH
Rosenthaler Straße 40 (Hackesche Höfe)
10178 Berlin