Cyber-Security Produkte richtig bewerten

Stefan Wieczorek

2021-10-12

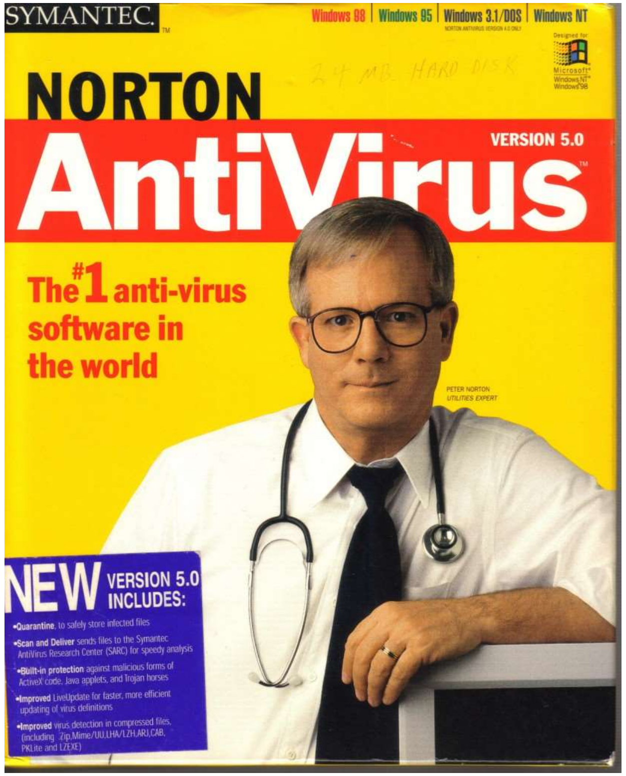
Deutsche Cyber-Sicherheitsorganisation GmbH

Joint Venture of Allianz SE, BASF SE, Bayer AG, and Volkswagen AG

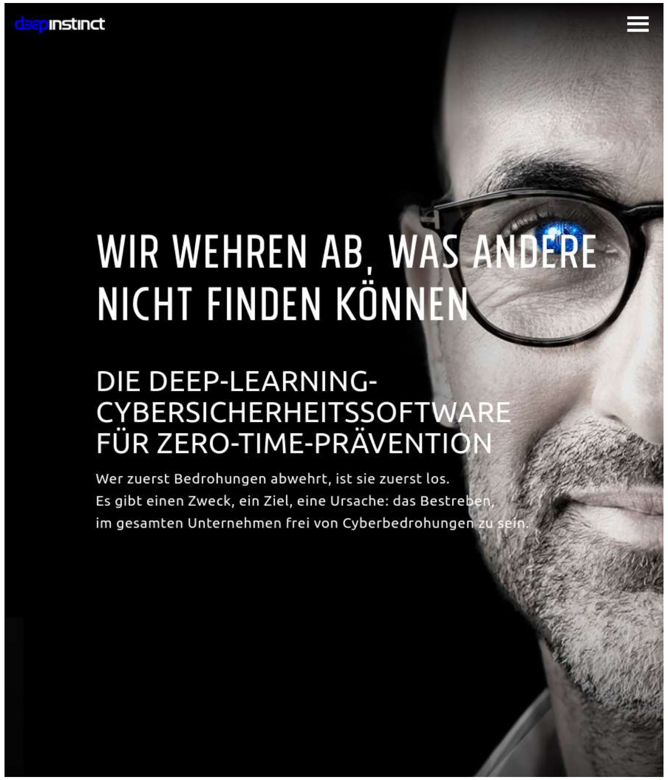
DCSO Security Technology

Surveys of **the IT-security market**
Tested over 90 IT-security products against customer use cases

Aufmerksamkeitsökonomie
IT-Vertrieb im Wandel



1998



2021

https://hampdencomputer.com/2014/09/antivirus-expired-playing-with-fire/
https://www.deepinstinct.com/de/

7 Schritte zum richtigen Produkt
Ein strukturierter Auswahlprozess erzeugt belastbare Entscheidungen

Der erste Schritt
Die richtigen Fragen finden

Use Cases
Was soll erreicht werden?

Funktionale

“Warum wird das Produkt angeschafft?”

- Sichtbarkeit
- Schutzwirkung
- Reaktionsfähigkeit
- Abdeckung der Umgebung
- Alarmierung

-> Unterschiedlich über Produktgruppen

Nicht-funktionale

“Was muss zum Betrieb erfüllt sein?”

- Dokumentation
- Backup / Restore
- Compliance / Betriebsrat
- Bedienbarkeit
- Performance

-> Ähnlich über Produktgruppen

Granularisierung
Use Cases testbar machen

5 User Stories → **30 Use Cases** → **300 Test Cases**

Vorstellungen | Anforderungen | Kriterien

☐	T78006	Does the product detect suspicious things while building the Kubecrusher-Container?		Failed
☐	T78003	Which basic security capabilities are provided in this lifecycle step?		Failed

Container Deployment (Image Registry) 5

Evaluation of product's integration with common container registries covering security checks for containers in the registry or when they are added to the registry.

☐	ID	Title	Assigned To	Status
☐	T77988	Does the product offer a detection point on registry level?		Passed
☐	T77989	Does the product offer enforcement points on registry level?		Failed
☐	T77916	Does the product support security checks for uploads of new containers in the container registry?		Passed
☐	T77990	Does the product checks for outdated/unused Layers/images?		Passed
☐	T78000	Which basic security capabilities are provided in this lifecycle step?		Failed

Container Runtime (Runtime Environment) 11

Evaluation of product's integration coverage of security checks at runtime of containers.

☐	ID	Title	Assigned To	Status
☐	T77994	Does the product offer a detection point for the container runtime environment?		Passed
☐	T77995	Does the product offer an enforcement point for the container runtime environment?		Failed
☐	T77996	Does the product recognize the exploitation of security vulnerabilities during runtime (Dynamic Vulnerability checks)?		Failed
☐	T77949	Does the product detect use of kubernetes commands from within a container?		Failed
☐	T77948	Does the product detect outgoing connections?		Failed
☐	T77997	Does the product evaluate (external) environment permissions on the container?		Failed
☐	T77991	Does the product checks for vulnerable (unwanted) definitions in the deployment?		Failed
☐	T77992	Does the product offer white/blacklisting approch for registry access?		Failed
☐	T77993	Does the product checks for "long running containers" ?		Failed
☐	T77918	Does the product check for binding incoming container traffic to a specific host interface?		Failed
☐	T78004	Which basic security capabilities are provided in this lifecycle step?		Failed

Container Decomissioning 0

Evaluation of product's supports for decommissioning of unsecure containers.

Testmanagement
Das richtige Tool

Testmanagement Tools

- Aus der Softwareentwicklung
- Übersicht über komplexe Projekte
- Testpläne, KPIs, Reports
- Dokumentation der Durchführung
- DCSO nutzt TestRail

||

Excel / Sheets online

- Einfach verfügbar
- Mehrnutzerfähig
- Manuelle Arbeit notwendig

Takeaways

- Nichtfunktionale Kriterien betrachten
- Anforderungen in granulare, testbare Kriterien aufbrechen
- Angemessenes Tooling verwenden

https://business-services.heise.de/security/security-loesungen/beitrag/in-sieben-schritten-zu-mehr-it-sicherheit-4080?source=wpnl

DCSO

Engineering Security.
Together.

DCSO Deutsche Cyber-Sicherheitsorganisation GmbH
EUREF-Campus 22
10829 Berlin

stefan.wieczorek@dcso.de