RADAR SERVICES

DSGVO - Kontinuierliches IT Security Monitoring als Managed-Service für die Optimierung von IT-Sicherheit sowie Effizienzsteigerung des Risikomanagements

Sebastian Michels
Head of Partner Sales

Ren Gamper
Enterprise Security Architecture

500 Technology Fast 500 2016 EMEA WINNER Deloitte.

IT Security made in Europe

ECS EUROPEAN CYBER SECURITY ORGANISATION

Teilnehmer der Allianz für Cyber-Sicherheit

Im Mittelpunkt steht die
zeitnahe Erkennung von
IT-Sicherheitsvorfällen und -risiken.

EUROPÄISCHE WURZELN,
WELTWEIT IM EINSATZ.

100% IT-SECURITY MADE IN EUROPE.

4 KONTINENTE, AUF DENEN WIR EINGESETZT WERDEN.

170 LÄNDER, IN DENEN UNSERE KUNDEN TÄTIG SIND.

130 MITARBEITER.

SOCs:	WIEN (HQ)	BERLIN	Vaduz (BU)	DUBAI
BÜROs:	FRANKFURT	WARSCHAU	MOSKAU	

WIEN: DAS GRÖSSTE SOC
IN EUROPA.

188 PETABYTE DATEN.

24 BILLIONEN EVENTS.

260 MILLIONEN SCHWACHSTELLENINFORMATIONEN.

1,6 MILLIONEN IDENTIFIZIERTE INCIDENTS.

TECHNOLOGIE:

- MEHRSTUFIGE KORRELATION
- BREITES SPEKTRUM AN EREIGNISSEN
- MACHINE LEARNING
- INTERNE ENTWICKLUNG

Durchschnittsangaben pro Jahr

FOKUS: FORSCHUNG

FÜHREND IN EUROPA.

WIR SEHEN UNS ALS HERSTELLER MIT EINEM „MANAGED SECURITY SERVICE ANSATZ“

TEAM:
INTERNATIONAL
MIT SEHR
HOHER
FACHKOMPETEN
Z

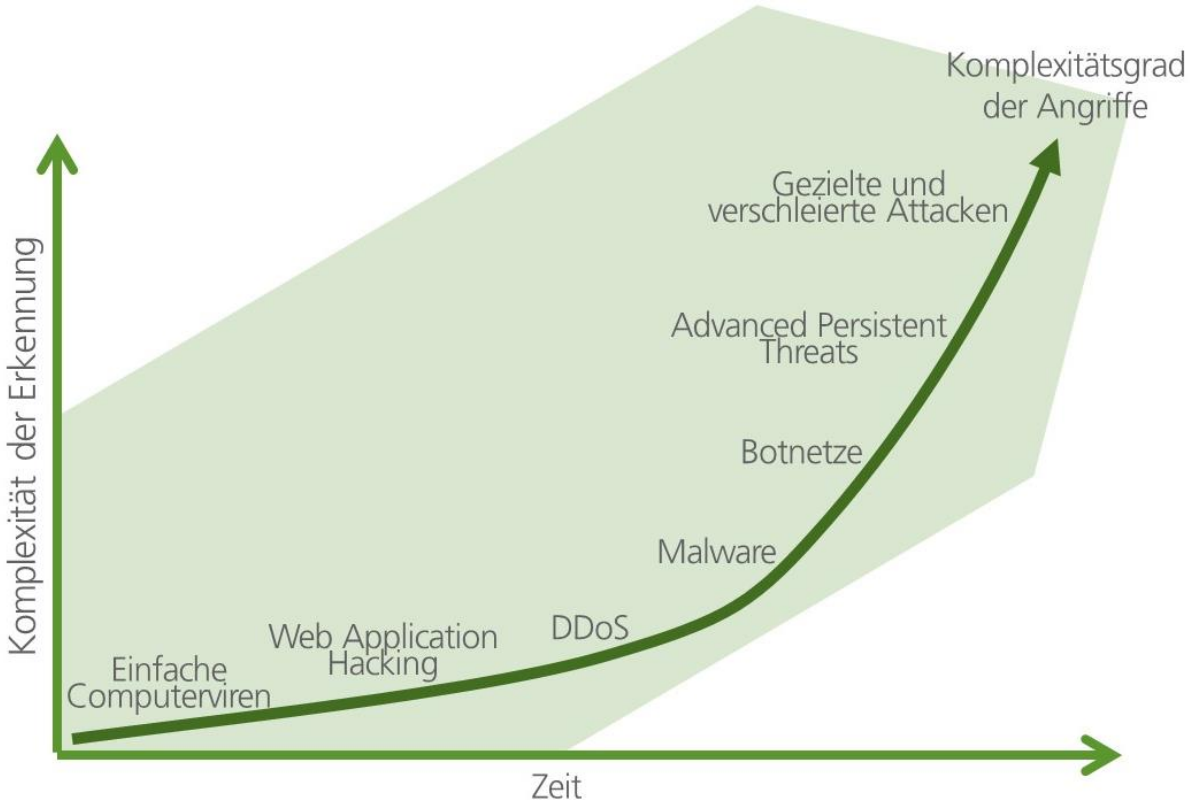
BEREICHE:
ADVANCED
CORRELATION &
RISIKOERKENNU
NG

ZIEL:
RISIKOÜBERBLIC
K AUF
KNOPFDRUCK

KUNDENVORTEI
L:
STÄNDIGES
EINFLIESSEN
DES
KNOWHOWS IN

10 Jahre
Research & Development

Wachsende Bedrohungen



Frankfurter Allgemeine
Wirtschaft
Mittwoch, 04. November 2015

Wirtschaftsspionage

Unternehmen schützen sich zu wenig vor der NSA

Geheimdienste wie die amerikanische NSA haben die Wirtschaft im Visier. Die getroffenen Sicherheitsmaßnahmen der Unternehmen sind unzureichend. Si... zu umgehen – ein leichtes Spiel.

ZDNet / Sicherheit / Virus

Computerviren legen Systeme mehrerer Kliniken in NRW lahm

von Björn Greif am 12. Februar 2016, 10:48 Uhr

Mehrere Kliniken in Nordrhein-Westfalen sind in jüngerer Vergangenheit Computerviren z... Opfer gefallen. Neuester Fall ist der des Lukaskrankenhauses in Neuss, dessen Systeme einen vorschnell geöffneten E-Mail-Anhang infiziert wurden. Nach Informationen von RP waren zuvor auch Kliniken in Essen, Köln und Mönchengladbach von ähnlichen Vorfälle betroffen.

ZEIT ONLINE

Wirtschaftsspionage

"Ein gnadenloser Krieg"

Der französische Geheimdienst schnüffelt ganz offiziell im Namen der Nation für seine Unternehmen – und eine eigens gegründete Schule lehrt den Beruf Wirtschaftsspion.

SPIEGEL ONLINE POLITIK

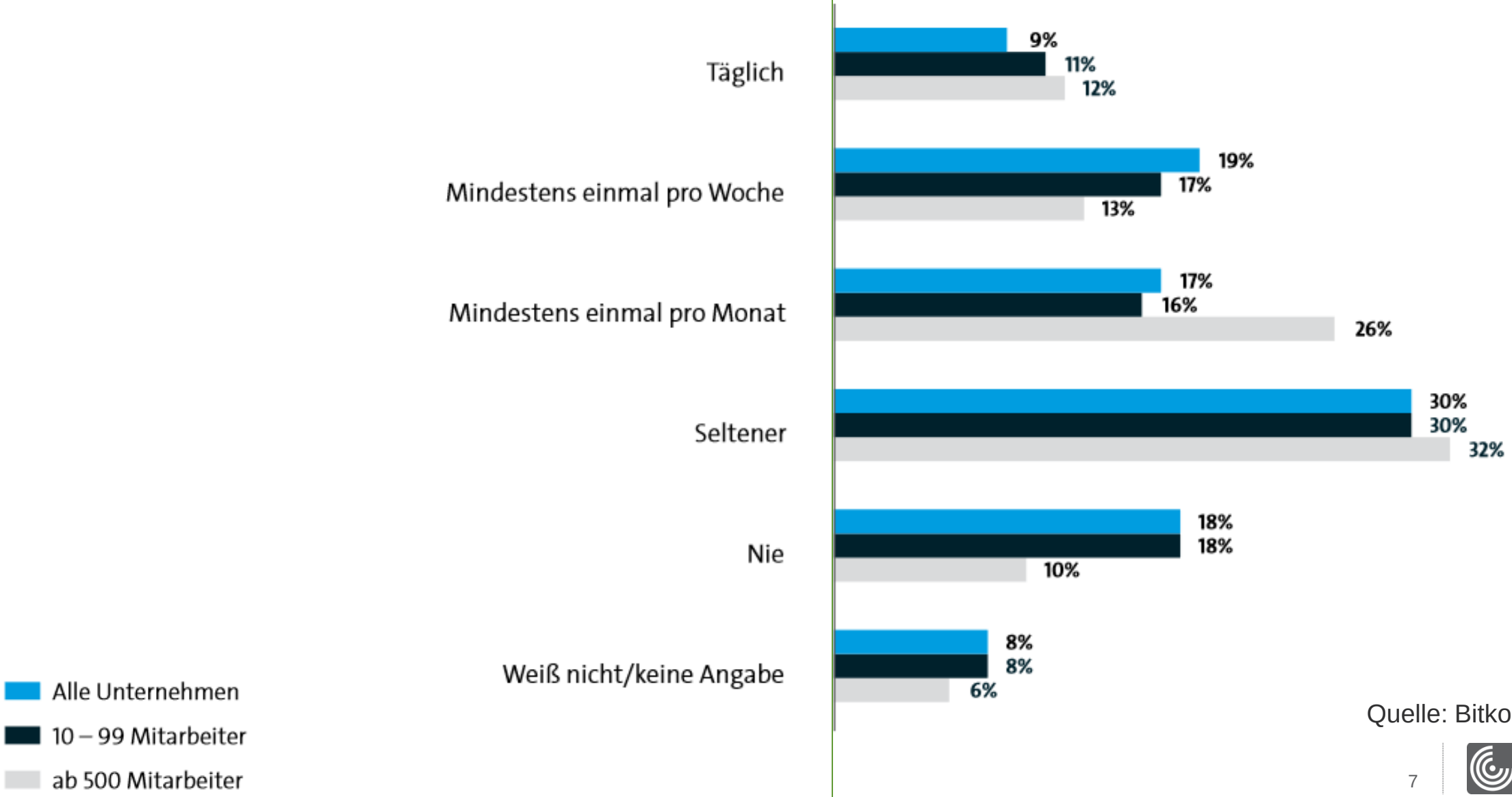
Abhör-Affäre: BND-Mitarbeiter erhärtet Verdacht auf Wirtschaftsspionage

In der NSA-Affäre sind weitere Indizien dafür aufgetaucht, dass der US-Geheimdienst deutsche Unternehmen ausgeforscht hat. Nach Informationen des SPIEGEL kannte ein BND-Mitarbeiter Suchbegriffe mit deutschen Firmennamen.

RADAR SERVICES

Häufigkeit der Angriffe

45% der Unternehmen verzeichnen monatlich **ernste** Angriffe

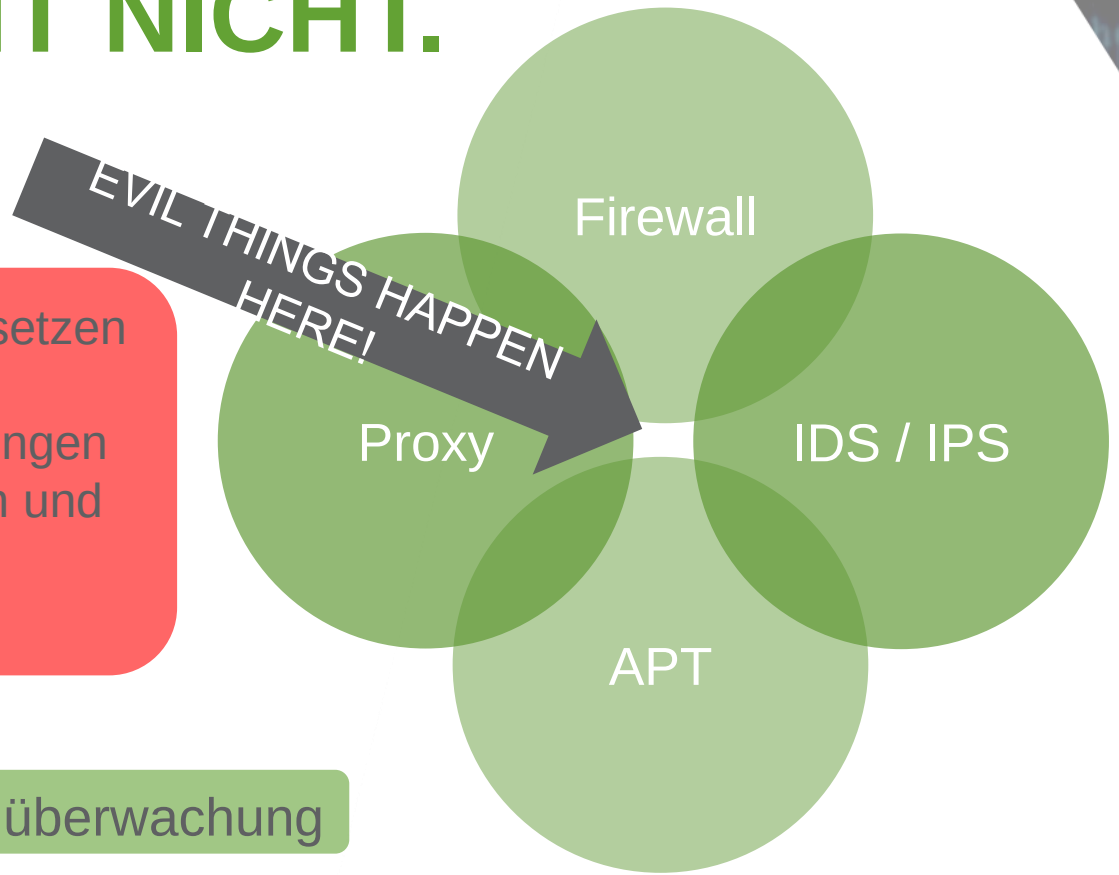


Quelle: Bitkom.de, n=1.074

RADAR SERVICES

Welche Maßnahmen müssten aus Ihrer Sicht ergriffen werden?

TECHNOLOGIE ALLEIN
REICHT NICHT.



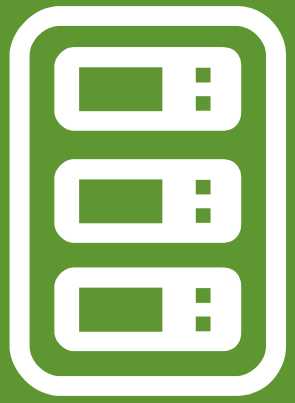
Wichtig: Wir ersetzen keine Security Prevention Lösungen – wir verarbeiten und ergänzen deren Informationen

24/7 Systemüberwachung

24/7 Schutz vor bisher unbekannten Angriffsmustern

Pay-as-you-grow OPEX Model

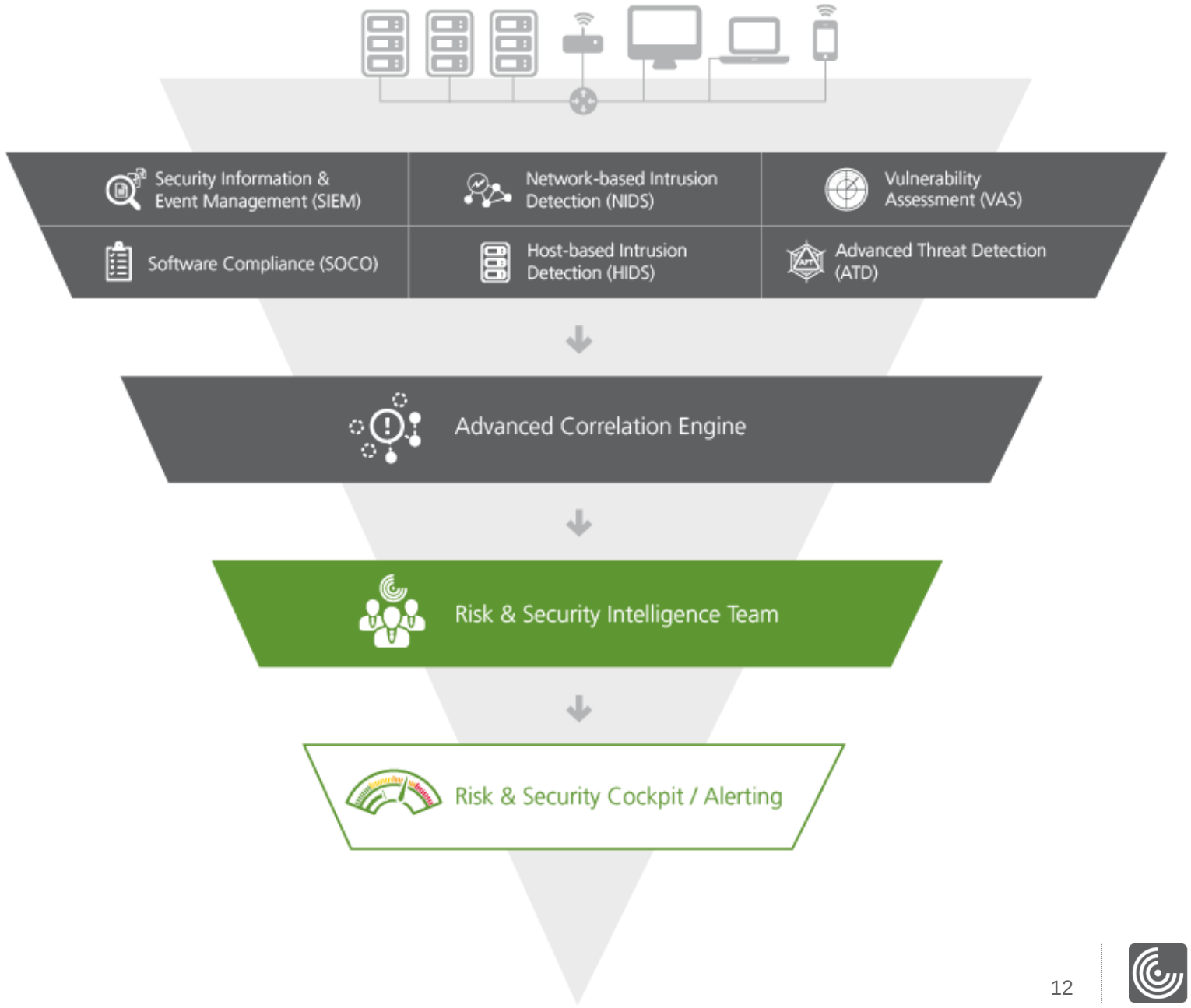
Next Generation Managed Security Services:



Ihre Daten
verlassen niemals
Ihr Unternehmen.

Mehrstufige Erkennung in modularer Architektur.

RADARSERVICES
DAS SYSTEM.



RADAR SERVICES

RADARSERVICES
DAS RESULTAT.

22 757 261 076
möglicherweise sicherheitsrelevante Ereignisse/90 Tagen

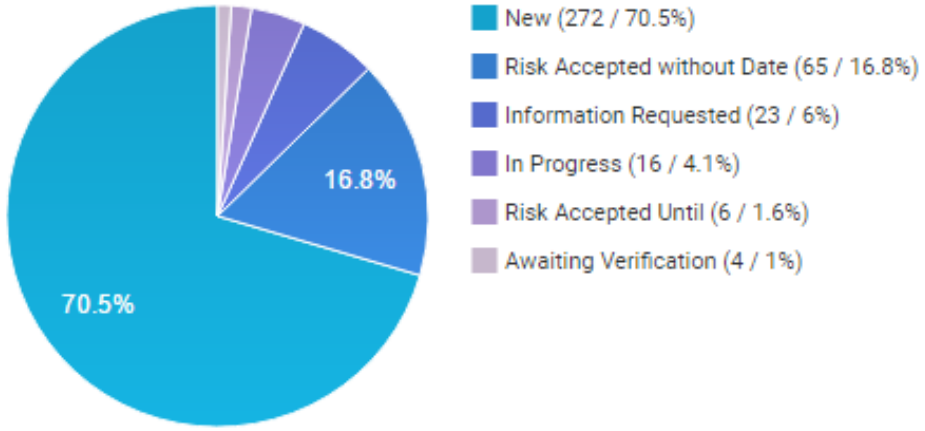
793 678
8.800 Alarme/Tag // 10 Alarme pro Sekunde

204
Krit. Attacken // 2 von 3 false positives

74
< 1 krit. Attacke/Tag

RADAR SERVICES

Incident Status Overview (excluding closed)

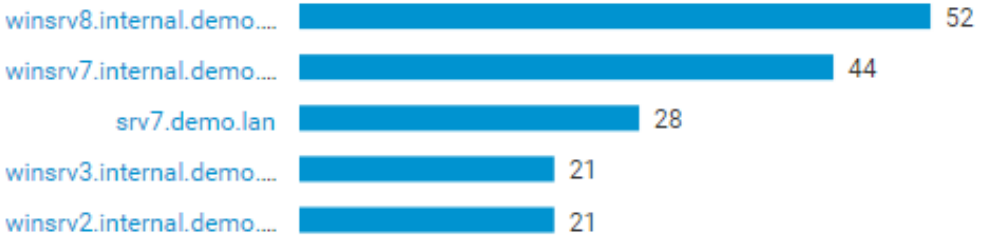


Incidents - Status by Risk Level

Download CSV

Status	High Risk	Medium Risk	Low Risk	No Risk	Total
All Open	55	100	158	2	315
New	12	100	158	2	272
In Progress	16	-	-	-	16
Information Requested	23	-	-	-	23
Awaiting Verification	4	-	-	-	4
Risk Accepted	32	14	25	-	71
Risk Accepted without Date	26	14	25	-	65
Risk Accepted Until	6	-	-	-	6
Closed	16	19	39	-	74
Total	103	133	222	2	460

Top 5 Assets by Open Incidents



Open Incidents by Risk Type

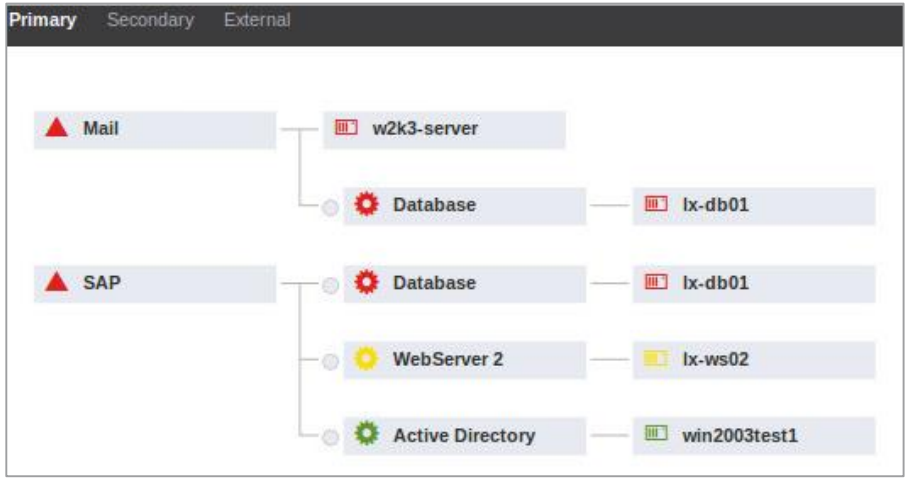
Top 5: Network Anomaly

CUSTOMIZED REPORTS

RISIKODARSTELLUNG EN.

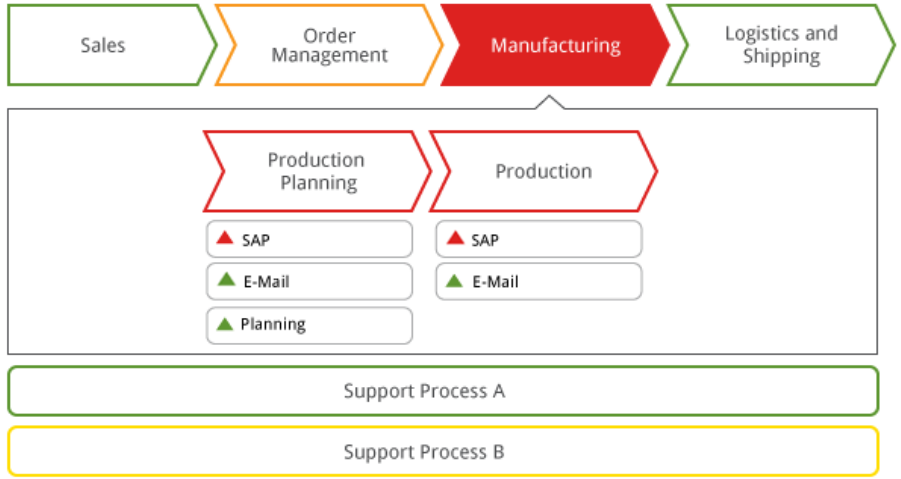
SERVICE VIEW

- Welche IT Services werden benötigt?
- Wie wichtig sind diese?
- Welche Risiken bestehen für die Services?
- Warum sind sie Risiken ausgesetzt?
- Welche Abhängigkeiten bestehen zwischen Services untereinander und zu Assets?



BUSINESS PROCESS VIEW

- Welche Geschäftsprozesse sind durch die Sicherheitsprobleme gefährdet?



CUSTOMIZED REPORTS IM FOKUS.

IT-Leader Report
05.10.2013 - 18.10.2013

MONTHLY REPORT

RADAR SERVICES

GLOBAL RISK SCORE

Risk Score

9.2

Risk Score Progression

INCIDENTS IN REPORTING PERIOD

No. of **NEW** Incidents in Reporting Period

No. of **CLOSED** Incidents in Reporting Period

No. of **NEW** vs. **CLOSED** Incidents in Reporting Period

Risk Level	Status New	Status Closed	Delta
Low	2	0	2
Medium	1	0	1
High	2	1	1
Total	5	1	4

Interpretations

New incidents delivered from vulnerability scans and network anomalies. Few incidents have been closed. More customer activity on RIC interface recommended.

No. of Incidents changed Status to

Average Throughput Time (in Days)

Average Retention Time (in Days) per Incident Status

Risk Level Legend
None Low Medium High

Page 1 / 11

IT-Leader Report
05.10.2013 - 18.10.2013

MONTHLY REPORT

RADAR SERVICES

SERVICES

Most Critical Services
Mail
Domain
Database 2
WebServer 2
DMZ Firewall
Website
Database

Mail

Risk Score

10.0

Risk Score Progression

Statistics

SAP

Risk Score

0.0

Risk Score Progression

Statistics

Domain

Risk Score

8.0

Risk Score Progression

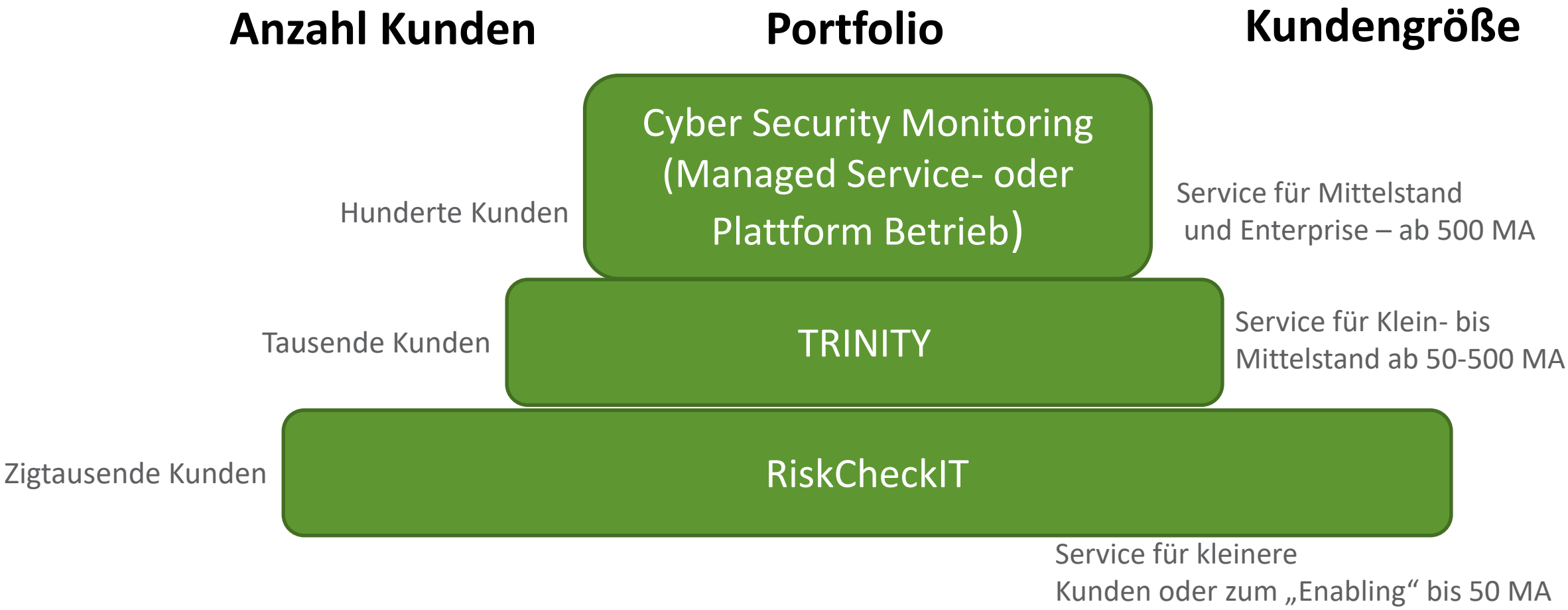
Statistics

Risk Level Legend
None Low Medium High

Page 4 / 11

RADAR SERVICES

PORTFOLIO



RADAR SERVICES

RADARSERVICES PORTFOLIO

RadarServices Serviceprodukte	Erläuterung	Wesentliche Merkmale
Cyber Security Monitoring	Das Flaggschiff-Serviceprodukt von RadarServices – ganzheitliche Cyber Security Risikoerkennung mit mehrstufigem Analyseansatz	- On-Premise (Anti-Cloud) - Höchstmögliche Analysetiefe durch Cyber Security Expertenteam - Monatliche Kunden Jour-Fixes
Trinity	Die Cyber Security Risikoerkennung basierend auf RadarCloud und einer Sensorhardware vor Ort beim Endkunden	- RadarCloud-basierte Datenhaltung und Risikoanalyse - Weitreichende, automatische Korrelation - Kombination von Risikoerkennungs-Werkzeugen und fragenbogenbasierter Selbstbeurteilung
RiskCheckIT	Die portalbasierte Cyber Security Monitoring Lösung für Private, Kleinst- und Kleinunternehmen	- Risikoanalyse über RadarCloud - Keine Sensorhardware beim Endkunden - Kombination von Risikoerkennungs-Werkzeugen und vereinfachter fragenbogenbasierter Selbstbeurteilung

IHR NUTZEN BEI EINSATZ UNSERES SERVICES -1-

» **Managed SOC Team des Kunden:** **Werkzeuge für** Risikoerkennung und –management + **Prozesse + Menschliche Security Intelligenz** - bis das Risiko behoben wurde

» **Wirtschaftlicher- und effektiver Security Ansatz:** **Effizienter Ressourceneinsatz** (keine Personalsuche, Aufbau und Anstellung von eigenem Personal zum SOC Betrieb nötig) **+ Keine Hard- und Software Anschaffungen** (OPEX-Modell), integrierte eigenentwickelte oder angepasste Open Source Werkzeuge zur Darstellung von **Security Incidents** und deren Auswirkungen auf **die Risiken der**

IHR NUTZEN BEI EINSATZ UNSERES SERVICES -2-

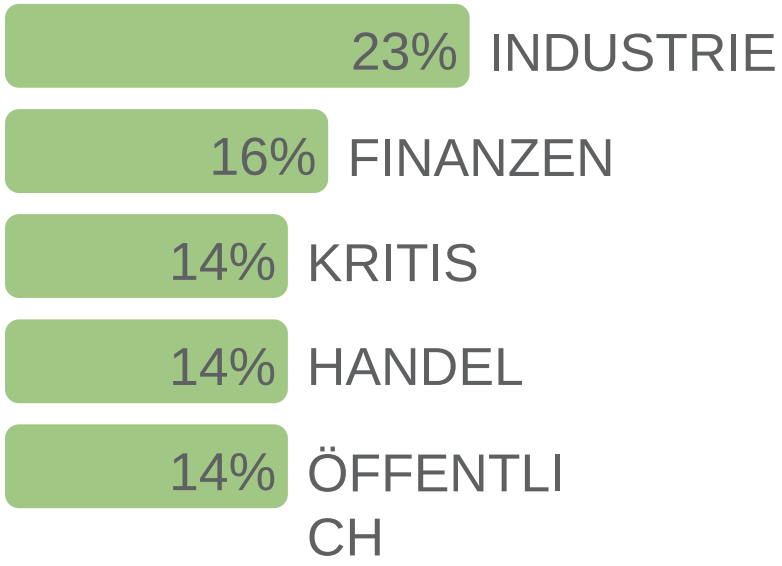
» **Mehrstufige Informationsverdichtung: Automatische Risikoerkennungsmodule**, **Cross Korrelation** der Incidents, **menschliche** Nachanalyse, Darstellung der verdichteten Ergebnisse im **Risk- und Security Cockpit** Kompetenz - **Technologie alleine reicht hier nicht mehr!**

» ***Integrierter Workflow:*** **keine Insellösungen, integrierte Module mit Cross-Korrelation, ein Dashboard** zu Risikodarstellung

» ***Europäische Lösung*: kein Patriot Act, keine backdoors, Daten verlassen nicht das Unternehmen des Kunden (Flagship)**

MIT SICHERHEIT ERFOLGREICH: ÜBER UNSERE KUNDEN.

UNTERNEHMEN NACH BRANCHEN



UNTERNEHMEN NACH GRÖSSE (ANZ.

RADAR SERVICES

RadarServices als Teil der Lösung. Beispiele für Sicherstellung der Einhaltung der DSGVO

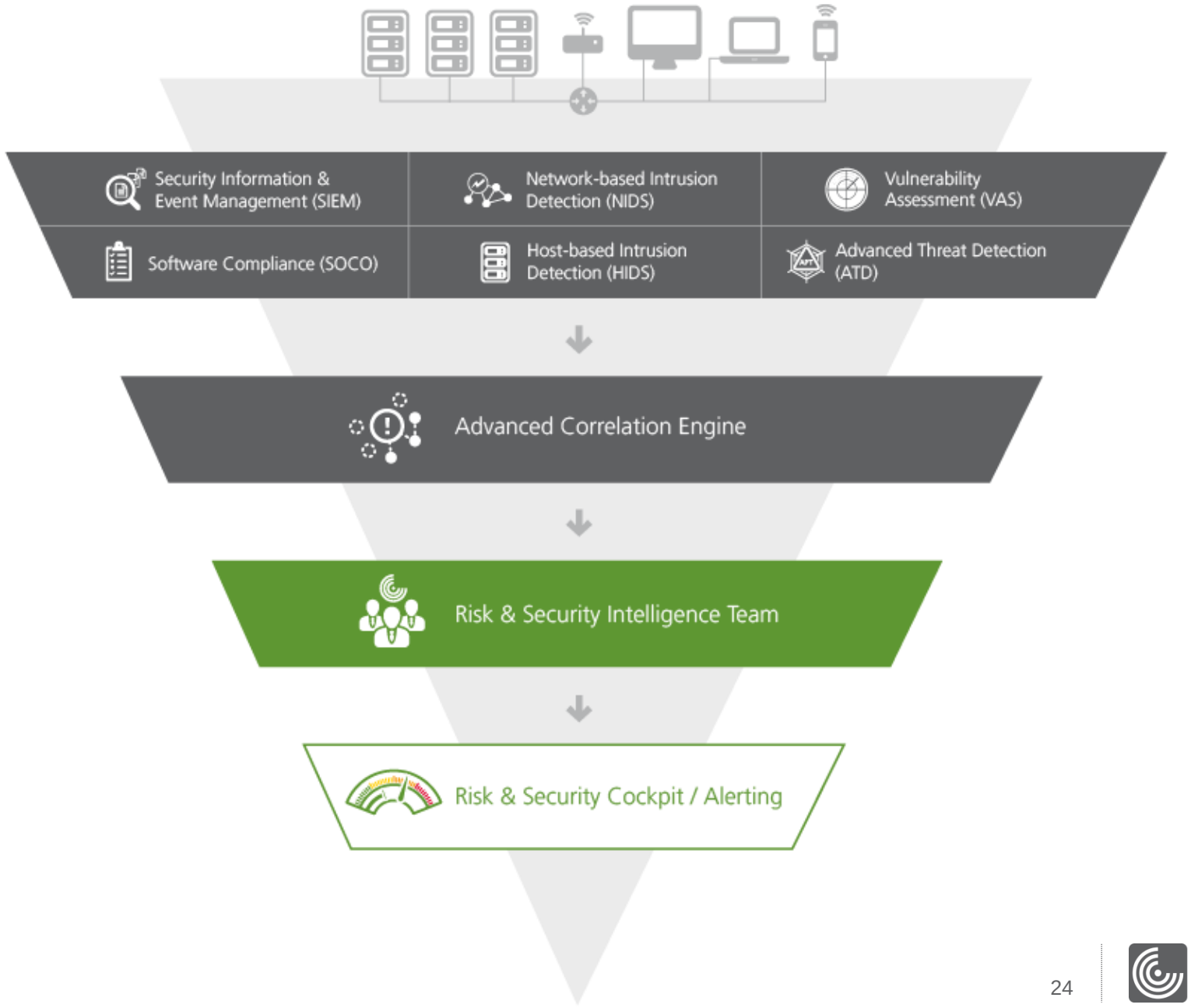
Artikel 24 DSGVO

» …

» (1) **Der Verantwortliche setzt** unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen **geeignete technische und organisatorische Maßnahmen** um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

» …

RADARSERVICES
DAS SYSTEM.



RADAR SERVICES

Artikel 32 DSGVO:

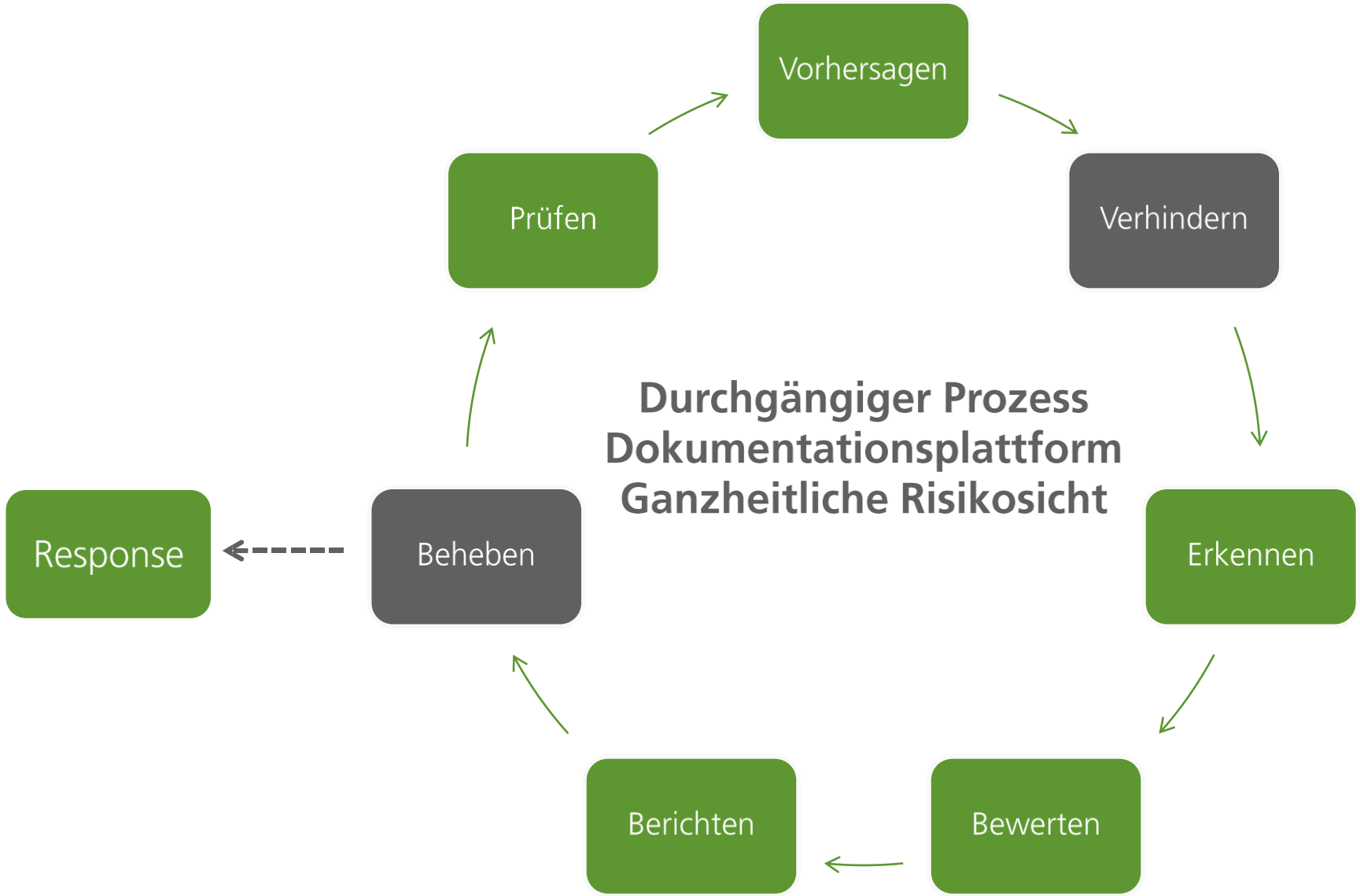
» …

» b) die **Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit** der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer **sicherzustellen**;

» d) **ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen** zur Gewährleistung der Sicherheit der Verarbeitung.

» …

PROCESSES.
RISK ANALISYS
WORKFLOW.



Kunde

RadarServices

RADAR SERVICES

Artikel 33 DSGVO:

» …

» (1) Im Falle **einer <u>Verletzung des Schutzes</u> personenbezogener Daten <u>meldet</u>** der Verantwortliche **unverzüglich und möglichst binnen 72 Stunden**, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

» …

RADAR SERVICES

VIELEN DANK.

T. +43 (1) 929 12 71-0
sales@radarservices.com
www.radarservices.com

© 2016 RadarServices Smart IT-Security GmbH

500 | Technology Fast 500 2016 EMEA WINNER Deloitte.

IT Security made in Europe

ECS EUROPEAN CYBER SECURITY ORGANISATION

Teilnehmer der Allianz für Cyber-Sicherheit