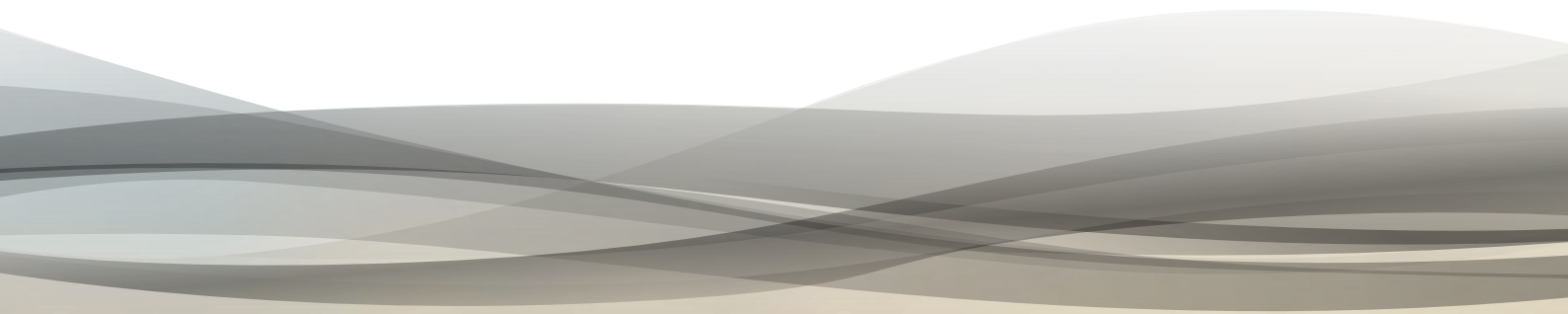


# Business Development Distribution



# Cybersecurity Services

## ACCESS RIGHTS ASSESSMENT

- Transparenz über Benutzer- und Berechtigungsstrukturen (AD, FILE, ERP, EXCHANGE, STORAGE)
- Verhinderung, dass Dritte auf kritische Informationen in Laufwerken & E-Mail-Postfächern (Vorstand, GF, Abteilungsleiter) zugreifen können

## CONTINUOUS SECURITY LAYER CONFIGURATION & VULNERABILITY ASSESSMENT

- Analyse der Konfigurationen der eingesetzten Securitytechnologien mit Optimierung derselben
- Durchführung von Penetrationstests der eingesetzten Securitytechnologien

## CYBERSECURITY SOLUTION DECISION AID SERVICES

- Entscheidungsunterstützungsmaßnahme in Form eines Experten-gesprächs mit einem Technologie-Analysten, wenn es darum geht, eine finale Produktentscheidung zu treffen

## DIGITAL FORENSIC SERVICES

- Sammlung, Analyse und Bewertung von relevanten elektronischen Beweisen auf Speichermedien mit möglicher Erläuterung des Vorfalls

## CERT-/CSOC-/SOC-READINESS ODER CONSULTING SERVICES

- Anpassung bestehender und Implementierung neuer organisatorischer Rollen, Prozesse und Schnittstellen und/oder Technologien
- Analyse des technischen und organisatorischen Aufbaus auf SOC-Eignung
- Überprüfung des Reifegrades eines Unternehmens für eine dedizierte Security-Organisationseinheit wie ein SOC / CERT
- Unterstützung bei der Auswahl und Grobkonzeption von SOC-relevanten Technologien sowie die Integration bestehender und Implementierung neuer Rollen / Prozesse

## CYBER ADVANCED WARNING SYSTEM

- Durch die Simulation der Auswirkungen von Exploits auf die eingesetzten Sicherheitstechnologien /-hersteller kann ein Frühwarnsystem implementiert werden, was zur Einleitung von entsprechenden schützenden Gegenmaßnahmen verwendet werden kann

## INCIDENT RESPONSE SERVICES

- Beseitigung von Sicherheitsrisiken bestimmter Angriffsobjekte
- Analyse von Angriffsvektoren
- Einleitung sog. Remediation-Prozesse
- Lösung von konkreten IT-Sicherheitsvorfällen, z. B. bekanntwerden neuer Sicherheitslücken in bestimmten Anwendungen oder Betriebs-systemen, neuartige Virenverbreitung, etc.
- Warnung vor Sicherheitslücken

# Cybersecurity Services

## INDIVATOR OF COMPROMISE ASSESSMENT SERVICES

- Auffinden von noch unentdeckten Malware- oder ATP-Infektionen
- Untersuchung des Netzwerkverkehrs auf Anomalien wie z.B. der Versuch implementierte IT-Sicherheitsmaßnahmen aktiv zu umgehen
- Erkennung von ungewollten Datenabflüssen oder ungewöhnlichen eingehenden Datenverkehrs, z.B. mehrere GB-großer Download von Spielen

## OPERATING SYSTEM MIGRATION SERVICES

- Migration auf Windows 10 mit Übernahme von bestehenden Profilen

## SECURITY ASSESSMENTS

- Assessments von ATM, ICS, POS, TELCO, WLAN
- Erkennung und Beseitigung der Auswirkungen von Schwachstellen in Telekommunikationsnetzen, einschließlich der Hauptfunknetze (GSM, UMTS, LTE)
- Umfassendes Schwachstellen-Assessment von Geldautomaten und Kassensystemen zur Vermeidung von unberechtigten Geldabhebungen und unerwünschten Transaktionen

## SOCIAL ENGINEERING ATTACK SIMULATION SERVICES

- Überprüfung der Wirksamkeit von durchgeführten Security Awareness Kampagnen/Programmen
- Durchführung von entsprechenden Telefonkampagnen zur Erlangung von Passwörtern oder aktives Vorbeigehen an Zentralen zur Erlangung von sensitiven Informationen

## MALWARE ANALYSIS SERVICES

- Durchführung einer gründlichen Analyse der bereitgestellten Malware und Erstellung eines detaillierten Berichtes

## PENETRATION TESTING SERVICES

- Einhaltung von behördlichen Auflagen und Branchen- und Unternehmensnormen, z. B. PCI DSS
- Identifizierung der Schwachstellen innerhalb einer Infrastruktur
- Vermeidung von finanziellen und betrieblichen Verlusten und Image-Schäden durch Cyberangriffe

## SECURITY IMPROVEMENT PROGRAM SERVICES

- Bewertung der Effizienz von IT-Sicherheitslösungen
- Definition von neuen IT-Sicherheitsstrategien
- Identifikation von notwendigen IT-Sicherheits-Maßnahmen für ggf. notw. organisatorische Anpassungen / Richtlinien

## SOLUTION DESIGN SERVICES

- Konzeptionsdesign technologischer Lösungen für die Technologien AEP, BDS/BPS, DLP, EDR, IAM, PAM, SIEM, TI
- Unterstützung bei der Betriebseinführung / Übergabe
- Detailkonzeption einzelner Lösungsbausteine
- Unterstützung bei der Definition oder Bewertung von Ausschreibungen

# Klassisches Dienstleistungsspektrum



## Herstellerportfolio



# Business Development Portfolio

Hersteller	Lösungskategorie(n)	Zielgruppe	GESAMT-KOSTEN	GESETZES-KONFORMITÄT	RESSOURCEN-OPTIMIERUNG	SICHERHEITS-NIVEAU
ACCESSDATA	DF	5+ User	↓	↑	↑	↑
BeyondTrust	PAM, VMS	500+ User	↓	↑	↑	↑
COFENSE	CERT, SACBT, TI	2.000+ User	↓	↑	↑	↑
Fidelis Cybersecurity	BDS, BPS, CERT, DF, DLP, EDR	500+ User, 250MB/s	↓	↑	↑	↑
ivanti	EPP, ITSM, PMP, UEM	25+ User	↓	↑	↑	↑
KASPERSKY CyberSecurity	AEP, BDS, BPS, CERT, EDR, TI	500+ User	↓	↑	↑	↑
KASPERSKY Malwareprotection	EPP, MPP	5+ User	↓	↑	↑	↑
NSS LABS	CSVP	2.000+ User	↓	↑	↑	↑
PICUS SECURITY	CSVP	500+ User	↓	↑	↑	↑
solarwinds 8MAN	ARM	100+ User	↓	↑	↑	↑
RADAR SERVICES (MSP)	BDS, CERT, IDS, SIEM, SOC, VMS	25+ User	↓	↑	↑	↑
SailPoint The Power of Identity	IAM	2.000+ User	↓	↑	↑	↑
Vade Secure Predictive Email Defense	APP	25+ User	↓	↑	↑	↑

## BEGRIFFSBESTIMMUNGEN:

**AEP** ADVANCED ENDPOINT PROTECTION  
**APP** ANTIPHISHING PLATFORM  
**ARM** ACCESS RIGHTS MANAGEMENT  
**BDS** BREACH DETECTION SYSTEMS  
**BPS** BREACH PREVENTION SYSTEMS  
**CERT** COMPUTER EMERGENCY RESPONSE TEAM  
**CSVP** CONTINUOUS SECURITY VALIDATION PLATFORM

**DC** DATA CLASSIFICATION  
**DF** DIGITAL FORENSICS  
**DLP** DATA LEAKAGE PREVENTION  
**DRM** DIGITAL RIGHTS MANAGEMENT  
**EDR** ENDPOINT DETECTION & RESPONSE  
**EPP** ENDPOINT PROTECTION PLATFORMS  
**IAM** IDENTITY AND ACCESS MANAGEMENT  
**IDS** INTRUSION DETECTION SYSTEM

**MPP** MALWARE PROTECTION PLATFORM  
**PAM** PRIVILEGED ACCESS MANAGEMENT  
**PMP** PATCH MANAGEMENT PLATFORM  
**SACBT** SECURITY AWARENESS COMPUTER-BASED TRAINING  
**SIEM** SECURITY INFORMATION & EVENT MANAGEMENT  
**SOC** SECURITY OPERATIONS CENTER  
**UEM** UNIFIED ENDPOINT MANAGEMENT  
**VMS** VULNERABILITY MANAGEMENT SYSTEM



## Essential Security

Technologien, die jedes Unternehmen einsetzen sollte, um einen grundlegenden Schutz der IT zu unterstützen.

**Produkt:** 8MAN

8MAN ist eine führende Lösung für Access Rights Management (ARM) in Microsoft- und virtuellen Server-Umgebungen und schützt damit Unternehmen vor unberechtigten Zugriffen auf sensible Daten.

**Produkt:** Patchmanagement

Umfassendes Patchmanagement für Windows, Linux, MacOS, Unix sowie virtuelle Infrastrukturen.

**Produkt:** Application & Device Control

Granulare Anwendungs- & Schnittstellenkontrolle reduziert die Gefahren vor unbekanntem Bedrohungen.

**Produkt:** Endpoint Security for Business

Sicherheitstechnologien für Endpunkte und umfangreiche Systemmanagement-Funktionen – und all das in einer einzigen, integrierten Verwaltungskonsole.

**Produkt:** Hybrid Cloud Security

Schutz von physischen, virtualisierten & Cloud-Infrastrukturen.

**Produkt:** Security for File, Mail & SharePoint

Zentraler Malware-Schutz über verschiedene Betriebssysteme hinweg.

**Produkt:** Security for Storage

Schutz vor Ransomware- & Malware-Angriffen auf NetApp-Storage-Systeme.

**Produkt:** Vade Secure

Vade Secure bietet Lösungen, die die Nutzer vor komplexen E-Mail-Angriffen wie Spear-Phishing, Phishing, Malware und Ransomware schützt.

## Beteiligte Hersteller





## IT Asset & Service Management

Technologien, die Geschäftsprozesse mit technischen Lösungen unterstützen und dessen Ausführung optimieren.



**Produkt:** Desktop- & Server-Management

Management von Konfigurationen, dem Lebenszyklus von Software sowie Lizenzen; Software-Paketierung & Citrix Servermanagement.



**Produkt:** IT-Assetmanagement

Inventur- & Lebenszyklus-Management von bekannten & unbekanntem Unternehmenswerten (IT).



**Produkt:** IT-Service-Management

Automatisierung von Workflows, Beseitigung von manuellen Prozessen mit höherer Effizienz sowie Compliance durch Cloud-optimiertes ITSM-Service-Management.



**Produkt:** Service Desk

Service Desk bietet Change- und Configuration-Management für zügige und effiziente Change-Behandlungen.



**Produkt:** Unified EndPoint Management

Endpunkt- und Benutzerprofilverwaltung mit Erkennung aller Geräte, die mit dem Netzwerk verbunden werden.



**Produkt:** User Workspace Manager

Workspace-Managementlösung für die personalisierte Bereitstellung und Verwaltung von Desktops mit Automatisierung von Betriebssystem-Migrationen.

Beteiligter Hersteller



Technologien, die die Durchsetzung von Richtlinien, Gesetzen und internen Vorschriften fördern.



**Produkt:** E-Discovery

AccessData bietet Technologien für die Erfassung und Vorlage von Beweisen bei Rechtsstreitigkeiten oder Ermittlungen.



**Produkte:** Forensic Toolkit (FTK), Quin-C

Die Feststellung eines Tatbestandes & des Täters durch Erfassung, Analyse & Auswertung digitaler Spuren ist eine AccessData Kernkompetenz!



**Produkt:** Retina CS (Vulnerability Management)

BeyondTrust Retina CS ist eine Vulnerability-Management-Lösung, um Organisationen eine kontextsensitive Schwachstellenanalyse und Risikoanalyse zu bieten.



**Produkt:** PowerBroker PAM

Unified Privileged Access Management-Lösungen, die Insider-Risiken durch Sichtbarkeit und Kontrolle reduzieren. Diese Plattformen sind integrierte Lösungen, die Kontrolle über alle privilegierten Konten und Benutzer hinweg bieten.



**Produkt:** PowerBroker Auditing & Security Suite

BeyondTrust PowerBroker Auditing & Security Suite bietet zentralisierte Echtzeit-Änderungsüberwachung. Damit bietet sie die Möglichkeit, z.B. Active Directory-Objekte oder -Attribute wiederherzustellen und hilft, Berechtigungen in der Windows-Infrastruktur zu etablieren und durchzusetzen.



**Produkt:** Picus Assessment

Simulation von Angriffen auf Security-Gateways, MailSecurity & EndPoint-Security.



**Produkte:** IdentityIQ (onPremise), IdentityNOW (Cloud)

Vereinheitlicht Identity-Management-Prozesse für Cloud-, Mobile- und On-Premise-Anwendungen in komplexen und hybriden IT-Umgebungen.



**Produkt:** SecurtiyIQ

Analyse von Berechtigungsstrukturen in AD, FileServer, MailServer, Storage, SAP, usw.

## Beteiligte Hersteller







## Cyberthreat Detection & Prevention

Technologien, die bei der Entdeckung von gezielten Angriffen und Erschwerung von Datenabfluss unterstützen.

**Produkt:** Cerberus

Malware Threat-Hunting ist eine AccessData Technologie für Incident Response Teams.

**Produkt:** Cofense Reporter

Erkennung und Reaktion auf E-Mail-basierenden Bedrohungen & Angriffen

**Produkte:** Fidelis Network, Fidelis Endpoint

Fidelis Lösungen bieten eine ganzheitliche CyberThreat Detection & -Prevention Plattform für Netzwerk & Endgeräte. Sie ermöglichen eine hohe Sichtbarkeit, durch Analyse von Daten- Sitzungen im Netzwerk, in Prozessen und Speicher sowie Dateien auf dem Endgerät. Dies hilft bei der Erkennung und Verhinderung von Sabotage oder Datenabfluss.

**Produkt:** Anti Targeted Attack Platform (KATA)

Mit einer einzigartigen Kombination aus Technologie und Services, die durch führende Security-Intelligence-Lösungen gestützt werden, ermöglicht es Unternehmen, das Risiko zu mindern, gezielte Angriffe schon früh zu erkennen, mit Angriffen in nahe Echtzeit umzugehen und den Schutz vor künftigen Angriffen zu verbessern.

**Produkt:** Industrial Security (KICS)

Malware Threat-Hunting ist eine AccessData Technologie für Incident Response Teams.

**Produkt:** Radar Risk & Security Cockpit

Bedarfsgerechte Darstellung von Risiko-Informationen für kritische Geschäftsprozesse, IT-Services und rechtliche sowie regulatorische Anforderungen.

**Produkte:** Governance for Files

Zentrale Verwaltung & Kontrolle des Zugriffs auf unstrukturierte Daten einschließlich Datenklassifizierung.

## Beteiligte Hersteller





# Advanced Response Techniques & Threat Intelligence

Technologien / Services, die die Arbeit von CERTs/SOCs optimieren.

**Produkt:** Cofense Triage

Malware Threat-Hunting ist eine AccessData Technologie für Incident Response Teams.

**Produkte:** Fidelis ELEVATE

Fidelis ELEVATE bietet eine einzigartige Plattform zur Optimierung der Arbeit von dedizierten Security-Organisationseinheiten wie CERTs und SOC. Mit automatisierter Validierung, Untersuchung, Korrelation und aggregierte Darstellung von Sicherheitsvorfällen, befähigt es richtige Entscheidungen zu treffen und dadurch schneller auf Vorfälle reagieren zu können.

**Produkt:** Intelligence Reporting

APT oder kundenspezifische Berichte über Bedrohungen mit vollständigen technischen Details bereits erfolgte oder anstehende Angriffe.

**Produkt:** Threat Data Feeds (KL SIS)

Anreicherung und Verstärkung von bestehenden Netzwerksicherheitslösungen, darunter SIEM-Systeme, Firewalls, IPS/IDS, Anti-APT und Sandbox-/Simulationsverfahren, durch umfassende laufend aktualisierte Daten, die wichtige Einblicke in Cyberbedrohungen und gezielte Angriffe liefern.

**Produkt:** Threat Intelligence Portal (KTP)

Kaspersky Threat Intelligence Portal liefert das gesamte Wissen, das Kaspersky Lab über Cyber-Bedrohungen und deren Beziehungen erworben hat, in Form eines benutzerfreundlichen Web-Portals. Das Ziel ist es, Sicherheitsteams mit möglichst vielen Daten zu versorgen und so Cyber-Angriffe frühzeitig zu erkennen und Auswirkungen auf das Unternehmen zu reduzieren.

**Produkt:** Cyber Advanced Warning System (CAWS)

Das CAWS ist die weltweit erste und einzige „Security-as-a-Service“ (SaaS) Anwendung, mit der aktive Exploits entdeckt, ihre IT-Sicherheits-Level metrisch bewertet und aktuelle Unternehmensbedrohungen kontinuierlich aufgezeigt werden können.

**Produkte:** Security Testing

NSS Labs bietet die branchenweit größten und umfassendsten Bewertungen von Funktionen für Sicherheitsprodukte der Enterprise-Klasse. Ziel ist eine weitgehend herstellerneutrale, faktenbasierte und objektive sicherheitstechnische Bewertung anzubieten.

**Produkt:** PICUS Security

Die Lösung von Picus hilft Unternehmen, sich auf neue Cyberbedrohungen vorzubereiten, indem sie die Effektivität der bestehenden Sicherheitslösungen (Netzwerk und Endgerät) kontinuierlich mit realen und aktuellen Cyber-Angriffsmustern überwacht und misst.

## Beteiligte Hersteller



## Cybersecurity Consulting Enablement

Welche Technologien / Services optimieren die Ressourcen von CyberSecurity Consultants?

 ectacom

**Produkt:** Cybersecurity Assessment Services

Aufbau von Cybersecurity Assessment Skills unter Einbeziehung von bestimmten Technologien.

 ectacom

**Produkte:** Cybersecurity Skills Development

Aufbau von generischen Cybersecurity Skills für die Bewältigung von vertrieblichen & technischen Aufgaben.

 ectacom

**Produkt:** Digitale Forensik Services

Aufbau von Grundlagenwissen im Bereich Digitaler Forensik mit Spezialisierungsmöglichkeit (AccessData).

 ectacom

**Produkt:** SOC-Consulting Enablement

Aufbau von SOC-Consulting-Wissen für die Durchführung von SOC-Beratungen.

 ectacom

**Produkt:** Solution Design Enablement

Schaffung von Grundlagen & Expertenwissen für das Design & die Konzeption von maßgeschneiderten Lösungen.

Beteiligter Hersteller

 ectacom



trusted it-advisor – anywhere and anytime

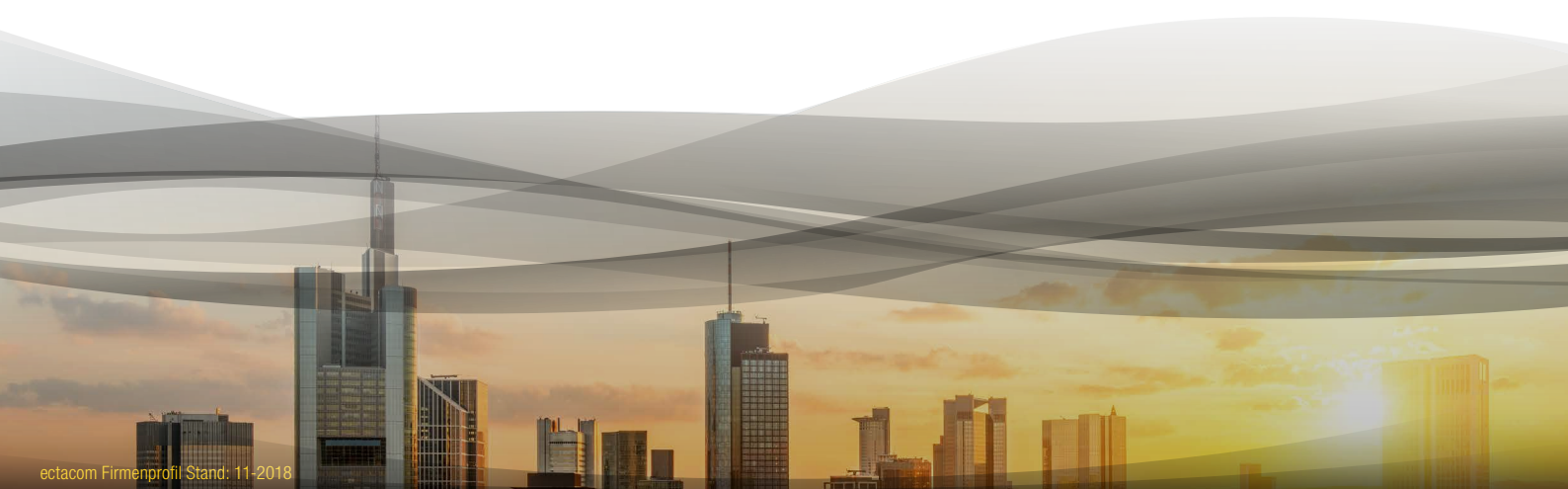
Unsere Mission ist es, mithilfe technologisch führender Hersteller Unternehmen jeglicher Größe und Branche nachhaltig vor bekannten und neuartigen Bedrohungen zu schützen, die Einhaltung von Compliance zu unterstützen sowie die Effizienz eingesetzten IT-Ressourcen signifikant zu erhöhen!

Die ectacom GmbH ist ein unabhängiger Business Development Distributor für komplexe IT-Lösungen und spezialisierte Dienstleistungen.

Unsere Mission ist es, Fachhändler beim generischen Wachstum mithilfe technologisch führender Hersteller zu unterstützen. Dabei realisieren wir signifikante Optimierungen bei der Generierung von Umsatz mit Bestands- und Neukunden und kurbeln den Verkauf von Dienstleistungen unserer Partner an.

Wir verstehen uns einerseits als Business Developer für visionäre Technologien, andererseits als Sourcing-Experte und Technologie-Enabler für unsere Partner. Diesen bieten wir jederzeit Zugang zu aktuellen Markt- und Technologieentwicklungen und unterstützen sie bei der Erschließung neuer Märkte und margenträchtiger Geschäftspotenziale.

Anerkannte IT-Experten, Integratoren und Consulting-Firmen vertrauen seit Jahren auf unsere Expertise für Technologie und Services. Komplexere technische Expertise, Produktevaluierungen, Installation, Konfigurations- und Einrichtungs-Services sowie Support-Dienstleistungen runden unser Business Development Profil ab.

A background image of a city skyline at sunset, with several skyscrapers and a warm, golden glow from the setting sun. The image is partially obscured by a large, semi-transparent, wavy graphic element that spans across the middle of the page.

ectacom Firmenprofil Stand: 11-2018

**ectacom HQ München:**  
T: +49 8102 8952-0

**ectacom Wien:**  
T: +43 664 4220555

**ectacom Linz:**  
T: +43 664 4526252

**ectacom Polska sp.z.o.o:**  
T: +48 501 295580

Mehr Informationen finden Sie unter  
[www.ectacom.com](http://www.ectacom.com)