



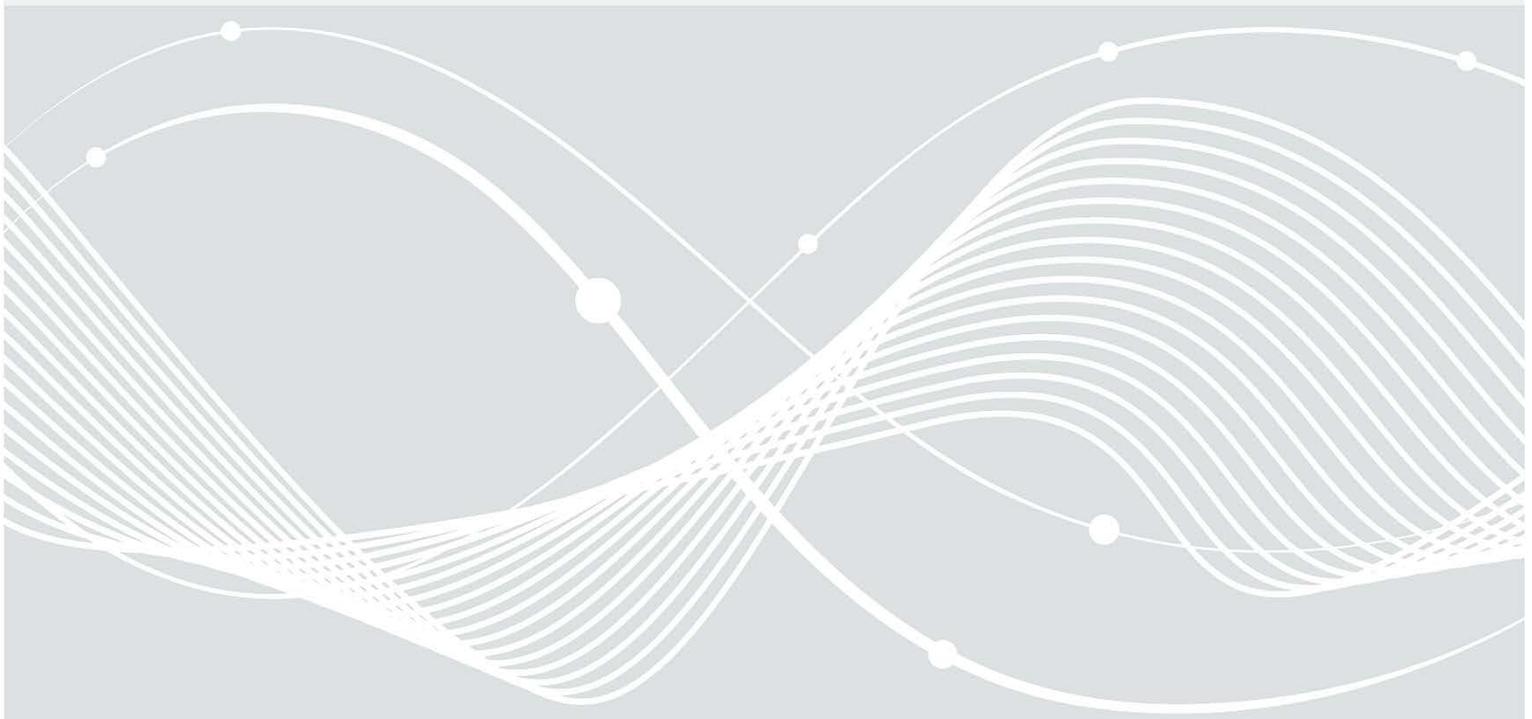
Bundesamt  
für Sicherheit in der  
Informationstechnik

Deutschland  
**Digital•Sicher•BSI•**

# Qualifizierte APT-Response Dienstleister

im Sinne § 3 BSIG

Stand: 07. November 2024



Bundesamt für Sicherheit in der Informationstechnik  
Postfach 20 03 63  
53133 Bonn  
Tel.: +49 22899 9582- 0  
E-Mail: [qdl@bsi.bund.de](mailto:qdl@bsi.bund.de)  
Internet: <https://www.bsi.bund.de>  
© Bundesamt für Sicherheit in der Informationstechnik 2024

---

# Inhalt

1	Hintergrund .....	5
2	Verfahren.....	6
3	Qualifizierte APT-Response-Dienstleister .....	7
3.1	@-yet GmbH.....	7
3.2	Airbus Protect GmbH .....	7
3.3	Antago GmbH.....	7
3.4	Arctic Wolf Networks Germany GmbH.....	7
3.5	BDO Cyber Security GmbH.....	7
3.6	Bechtle AG.....	7
3.7	BFK edv-consulting GmbH.....	7
3.8	BlackBerry Deutschland GmbH.....	8
3.9	CERTAINTY Holding GmbH .....	8
3.10	Cirosec GmbH.....	8
3.11	Cisco Talos Incident Response.....	8
3.12	Code Blue GmbH.....	8
3.13	Corporate Trust Business Risk & Crisis Management GmbH .....	8
3.14	CrowdStrike.....	8
3.15	DCSO Deutsche Cyber-Sicherheitsorganisation GmbH.....	9
3.16	Deloitte GmbH .....	9
3.17	Deutsche Telekom Security GmbH .....	9
3.18	DigiFors GmbH .....	9
3.19	Dr. Michael Gorski Consulting GmbH .....	9
3.20	ERNW Research GmbH .....	9
3.21	ETAS GmbH.....	9
3.22	EY GmbH & Co. KG Wirtschaftsprüfungsgesellschaft .....	10
3.23	Eye Security GmbH .....	10
3.24	GDATA Advanced Analytics GmbH .....	10
3.25	glueckkanja AG.....	10
3.26	Grant Thornton AG Wirtschaftsprüfungsgesellschaft .....	10
3.27	HiSolutions AG.....	10
3.28	HvS-Consulting GmbH.....	10
3.29	intersoft consulting services AG .....	11
3.30	InfoGuard AG.....	11
3.31	KPMG AG Wirtschaftsprüfungsgesellschaft .....	11
3.32	LEITWERK AG.....	11
3.33	Mandiant Deutschland GmbH .....	11

---

3.34	Microsoft Deutschland GmbH .....	11
3.35	NCC Group GmbH.....	11
3.36	Northwave.....	12
3.37	NVISO GmbH.....	12
3.38	Oneconsult Deutschland AG .....	12
3.39	Orange Cyberdefense Germany GmbH .....	12
3.40	Palo Alto Networks.....	12
3.41	pco GmbH & Co. KG.....	12
3.42	PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft.....	12
3.43	QGroup GmbH .....	13
3.44	Rapid7 Germany GmbH.....	13
3.45	r-tec IT Security GmbH .....	13
3.46	SEC Consult Unternehmensberatung GmbH .....	13
3.47	Sophos Technology GmbH .....	13
3.48	SVA System Vertrieb Alexander GmbH.....	13
3.49	SySS GmbH .....	13
3.50	Trend Micro Incident Response.....	13
3.51	Verizon Deutschland GmbH .....	14
3.52	Wipro.....	14
3.53	WithSecure GmbH.....	14
4	Leistungsmerkmale.....	15
4.1	24x7 Erreichbarkeit .....	15
4.2	ISO27001-Zertifizierung der Institution .....	15
4.3	Hauptsitz des Dienstleisters in der EU .....	15
4.4	Sichere Aufbewahrungsmöglichkeiten.....	15
4.5	APT-Dienstleistungen durch eigene Mitarbeitende.....	15
4.6	Weitere Dienstleistungsangebote.....	15
4.7	Technische Ausstattung .....	16
5	Gegenüberstellung der Leistungsmerkmale der einzelnen APT-Response-Dienstleister .....	17

# 1 Hintergrund

Das BSI hat gemäß § 3 BSIG die Aufgabe, Betreiber Kritischer Infrastrukturen auf deren Ersuchen bei der Sicherung ihrer Informationstechnik zu beraten und zu unterstützen. Hierzu kann auch auf qualifizierte Sicherheitsdienstleister verwiesen werden.

Angriffe auf Unternehmen nehmen in der letzten Zeit stark zu, sowohl in der Anzahl, als auch in der Intensität der Bedrohungen. Der Schaden, welcher dabei entsteht, verursacht bei den betroffenen Unternehmen nicht nur große wirtschaftliche Schäden, sondern auch einen Reputationsverlust, wenn Dienste nicht zur Verfügung stehen oder ein Datenabfluss zu verzeichnen war. Zur Verbesserung der Abwehr oder zur Bewältigung eines erfolgreichen Angriffs bedarf es vielfältig der Unterstützung externer Dienstleister, die in ihrem jeweiligen Tätigkeitsgebiet ein hohes Spezialwissen erlangt haben.

Mit der Benennung von themenspezifischen Qualitätskriterien und der Identifikation geeigneter Dienstleister möchte das BSI betroffenen Unternehmen eine Hilfestellung bei der Suche und Auswahl geeigneter Dienstleister bieten, um die Unternehmen im Ernstfall von einem eigenen zeitintensiven Rechercheaufwand zu entlasten. Gleichzeitig soll auf diese Weise ein gewisses Qualitätsniveau in der jeweiligen Branche etabliert werden.

Zur Identifikation von qualifizierten Sicherheitsdienstleistern für die Abwehr von APT-Angriffen hat das BSI Kriterien<sup>1</sup> veröffentlicht, die betroffene Betreiber Kritischer Infrastrukturen bei der Auswahl von geeigneten Dienstleistern unterstützen sollen.

Die Dienstleister, die anhand der Kriterien mit der Hilfe des in Kapitel 2 beschriebenen Verfahrens gefunden wurden, sind in diesem Dokument im Folgenden aufgelistet. Dazu gehören sowohl die Kontaktdaten in Kapitel 3 als auch die Gegenüberstellung der einzelnen Leistungsmerkmale in Kapitel 5. Die Leistungsmerkmale, welche sowohl die Kriterien beinhalten als auch weitere individuelle Unterschiede der Dienstleister darstellen, werden zuvor in Kapitel 4 genauer beschrieben.

---

<sup>1</sup> [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Auswahlkriterien\\_APT-Response\\_Dienstleister.html](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Auswahlkriterien_APT-Response_Dienstleister.html)

## 2 Verfahren

Um den Betreibern Kritischer Infrastrukturen eine leichtere Übersicht über den Markt der APT-Response-Dienstleister zu bieten, wurde, basierend auf den Auswahlkriterien, ein Verfahren zur Identifizierung geeigneter Dienstleister durchgeführt.

Das Verfahren gliedert sich in die folgenden Schritte:

1. Überprüfung der vom Dienstleister bereitgestellten Dokumentation  
Der Dienstleister musste zunächst eine vollständige Dokumentation bereitstellen. Hierzu zählten sowohl Beschreibungen der Produkte und Dienstleistungen, als auch Erläuterungen in Bezug auf die Einhaltung der vom BSI aufgestellten Kriterien. Des Weiteren bestand die Möglichkeit, vorhandene Zertifizierungen von Rechenzentren oder dem Unternehmen selbst mitzuliefern.
2. Durchführung eines Fachinterviews  
In einem mehrstündigen Termin beim BSI musste der Dienstleister anhand fiktiver Szenarien zeigen, dass er in der Lage ist, die Situationen fach- und zielgerichtet zu bedienen. Dabei wurde sowohl auf das allgemeine Vorgehen des Dienstleisters, als auch auf gestellte Fragen und Verarbeitung der erhaltenen Informationen geachtet.

Weiteren interessierten Dienstleistern steht das Verfahren jederzeit offen, sie können sich für Informationen an das Funktionspostfach [qdl@bsi.bund.de](mailto:qdl@bsi.bund.de) wenden.

## 3 Qualifizierte APT-Response-Dienstleister

Im Folgenden werden die bisher identifizierten qualifizierten APT-Response-Dienstleister mit den entsprechenden Kontaktdaten in alphabetischer Reihenfolge aufgelistet.

### 3.1 @-yet GmbH

Homepage <https://www.at-yet.de>  
Kontakt-Telefonnummer +49 (0) 2175 1655 0  
Kontakt-E-Mail-Adresse [notfall@at-yet.de](mailto:notfall@at-yet.de)

### 3.2 Airbus Protect GmbH

Homepage <https://www.protect.airbus.com/cyber-incident-response/>  
Kontakt-Telefonnummer +49 16 03 21 61 84  
+33 9 72 30 13 99  
Kontakt-E-Mail-Adresse [acs-csirt-de@airbus.com](mailto:acs-csirt-de@airbus.com)

### 3.3 Antago GmbH

Homepage <https://antago.de/>  
Kontakt-Telefonnummer +49 (0) 6251 86158 0  
Kontakt-E-Mail-Adresse [incident@antago.de](mailto:incident@antago.de)

### 3.4 Arctic Wolf Networks Germany GmbH

Homepage <https://arcticwolf.com/de/solutions/incident-response/>  
Kontakt-Telefonnummer +49 (0) 30 16637144  
Kontakt-E-Mail-Adresse [newcase@arcticwolf.com](mailto:newcase@arcticwolf.com)

### 3.5 BDO Cyber Security GmbH

Homepage <https://www.bdosecurity.de>  
Kontakt-Telefonnummer +49 (0) 40 32890 6540  
Kontakt-E-Mail-Adresse [circc@bdosecurity.de](mailto:circc@bdosecurity.de)

### 3.6 Bechtle AG

Homepage <https://www.bechtle.com>  
Kontakt-Telefonnummer +49 (0) 7132 981 2783  
Kontakt-E-Mail-Adresse [help.sirt@bechtle.com](mailto:help.sirt@bechtle.com)

### 3.7 BFK edv-consulting GmbH

Homepage <https://www.bfk.de>  
Kontakt-Telefonnummer +49 (0) 721 962011  
Kontakt-E-Mail-Adresse [cfischer@bfk.de](mailto:cfischer@bfk.de)

### 3.8 BlackBerry Deutschland GmbH

Homepage <https://www.blackberry.com/de/de/services/blackberry-cybersecurity-consulting/overview>

Kontakt-Telefonnummer +49 (0) 800 2060 2065

Kontakt-E-Mail-Adresse [irretainer@blackberry.com](mailto:irretainer@blackberry.com)

### 3.9 CERTAINITY Holding GmbH

Homepage <https://certainty.com/en/>

Kontakt-Telefonnummer +49 (0) 800 2378246  
AUT: +43 664 88844686

Kontakt-E-Mail-Adresse [csirt@certainty.com](mailto:csirt@certainty.com)

### 3.10 Cirosec GmbH

Homepage <https://www.cirosec.de>

Kontakt-Telefonnummer +49 (0) 7131 59455 0

Kontakt-E-Mail-Adresse [info@cirosec.de](mailto:info@cirosec.de)

### 3.11 Cisco Talos Incident Response

Homepage [https://talosintelligence.com/incident\\_response](https://talosintelligence.com/incident_response)

Kontakt-Telefonnummer +44 808 234 6353

Kontakt-E-Mail-Adresse [IncidentResponse@cisco.com](mailto:IncidentResponse@cisco.com)

### 3.12 Code Blue GmbH

Homepage <https://codebluecyber.de/>

Kontakt-Telefonnummer +49 (0) 69 979 460-999

Kontakt-E-Mail-Adresse [notfall@codebluecyber.de](mailto:notfall@codebluecyber.de)

### 3.13 Corporate Trust Business Risk & Crisis Management GmbH

Homepage <https://www.corporate-trust.de>

Kontakt-Telefonnummer +49 (0) 89 599 88 75 80

Kontakt-E-Mail-Adresse [info@corporate-trust.de](mailto:info@corporate-trust.de)

### 3.14 CrowdStrike

Homepage <https://www.crowdstrike.de/gab-es-eine-sicherheitsverletzung/>

Kontakt-Telefonnummer +49 (0) 800 3252669

Kontakt-E-Mail-Adresse [services@crowdstrike.com](mailto:services@crowdstrike.com)

### 3.15 DCSO Deutsche Cyber-Sicherheitsorganisation GmbH

Homepage <https://dcso.de>  
Kontakt-Telefonnummer +49 (0) 30 726219 0  
Kontakt-E-Mail-Adresse [incident@dcso.de](mailto:incident@dcso.de)

### 3.16 Deloitte GmbH

Homepage <https://www2.deloitte.com/de/de/pages/risk/solutions/cyber-services.html>  
Kontakt-Telefonnummer +49 (0) 40 32080 4499 (englischsprachige Hotline)  
Kontakt-E-Mail-Adresse [csirt@deloitte.de](mailto:csirt@deloitte.de)

### 3.17 Deutsche Telekom Security GmbH

Ansprechpartner Malte Fiedler  
Homepage <https://geschaeftskunden.telekom.de/digitale-loesungen/cyber-security>  
Kontakt-Telefonnummer +49 (0) 170 3278537  
Kontakt-E-Mail-Adresse [Pentesting+IRS@t-systems.com](mailto:Pentesting+IRS@t-systems.com)

### 3.18 DigiFors GmbH

Homepage <https://digifors.de>  
Kontakt-Telefonnummer +49 (0) 0341 6567 3381  
Kontakt-E-Mail-Adresse [notfall@digifors.de](mailto:notfall@digifors.de)

### 3.19 Dr. Michael Gorski Consulting GmbH

Homepage <https://www.michaelgorski.net/>  
Kontakt-Telefonnummer +49 (0)2173 9998710  
Kontakt-E-Mail-Adresse [soc@michaelgorski.net](mailto:soc@michaelgorski.net)

### 3.20 ERNW Research GmbH

Homepage <https://www.ernw-research.de>  
Kontakt-Telefonnummer +49 (0) 6221 7569637  
Kontakt-E-Mail-Adresse [incident-response@ernw.de](mailto:incident-response@ernw.de)

### 3.21 ETAS GmbH

Homepage <https://www.etas.com/de/portfolio/incident-response-as-a-service.php>  
Kontakt-Telefonnummer +49 (0) 234 43870-200  
Kontakt-E-Mail-Adresse [incident@escrypt.com](mailto:incident@escrypt.com)

## 3.22 EY GmbH & Co. KG Wirtschaftsprüfungsgesellschaft

Homepage [https://www.ey.com/de\\_de/assurance/privacy-cyber-response](https://www.ey.com/de_de/assurance/privacy-cyber-response)  
Kontakt-Telefonnummer +49 (0) 800 2323273  
Kontakt-E-Mail-Adresse [ir@de.ey.com](mailto:ir@de.ey.com)

## 3.23 Eye Security GmbH

Homepage <https://www.eye.security/de/>  
Kontakt-Telefonnummer +49 (0)203 6688 1900  
Kontakt-E-Mail-Adresse [cert@eye.security](mailto:cert@eye.security)

## 3.24 GDATA Advanced Analytics GmbH

Homepage <https://www.gdata-advancedanalytics.de>  
Kontakt-Telefonnummer +49 (0) 234 9762 800  
Kontakt-E-Mail-Adresse [info@gdata-adan.de](mailto:info@gdata-adan.de)

## 3.25 glueckkanja AG

Homepage <https://www.glueckkanja.com>  
Kontakt-Telefonnummer +49 (0) 1805009823  
Kontakt-E-Mail-Adresse [apt@glueckkanja.com](mailto:apt@glueckkanja.com)

## 3.26 Grant Thornton AG Wirtschaftsprüfungsgesellschaft

Homepage <https://www.grantthornton.de/services/cyber-security/>  
Kontakt-Telefonnummer +49 (0) 211 9524-3347  
Kontakt-E-Mail-Adresse [CIR@de.gt.com](mailto:CIR@de.gt.com)

## 3.27 HiSolutions AG

Homepage <https://www.hisolutions.com>  
Kontakt-Telefonnummer +49 (0) 30 533289 0  
Kontakt-E-Mail-Adresse [info@hisolutions.com](mailto:info@hisolutions.com)

## 3.28 HvS-Consulting GmbH

Homepage <https://www.hvs-consulting.de/de/incident-response/>  
Kontakt-Telefonnummer +49 (0) 89 890 636 261  
Kontakt-E-Mail-Adresse [incidentresponse@hvs-consulting.de](mailto:incidentresponse@hvs-consulting.de)

### 3.29 intersoft consulting services AG

Homepage	<a href="https://www.intersoft-consulting.de">https://www.intersoft-consulting.de</a>	
Kontakt-Telefonnummer	zu normalen Geschäftszeiten	+49 (0) 40 790 235 0
	24/7 Hotline	+49 (0) 180 622 124 6
Kontakt-E-Mail-Adresse	<a href="mailto:it-forensik@intersoft-consulting.de">it-forensik@intersoft-consulting.de</a>	

### 3.30 InfoGuard AG

Homepage	<a href="https://www.infoguard.de/incident-response">https://www.infoguard.de/incident-response</a>	
Kontakt-Telefonnummer	+49 (0) 896 282-5265	
Kontakt-E-Mail-Adresse	<a href="mailto:investigations@infoguard.de">investigations@infoguard.de</a>	

### 3.31 KPMG AG Wirtschaftsprüfungsgesellschaft

Homepage	<a href="https://home.kpmg/de/de/home/dienstleistungen/audit/forensic/cyber-incident-response-investigation.html">https://home.kpmg/de/de/home/dienstleistungen/audit/forensic/cyber-incident-response-investigation.html</a>	
Kontakt-Telefonnummer	innerhalb Deutschlands	+49 (0) 800 767 5764
	außerhalb Deutschlands	+49 202 251557146
Kontakt-E-Mail-Adresse	<a href="mailto:de-sos@kpmg.com">de-sos@kpmg.com</a>	

### 3.32 LEITWERK AG

Homepage	<a href="https://www.leitwerk.de">https://www.leitwerk.de</a>	
Kontakt-Telefonnummer	+49 (0) 7805 918 112	
Kontakt-E-Mail-Adresse	<a href="mailto:support@leitwerk.de">support@leitwerk.de</a>	

### 3.33 Mandiant Deutschland GmbH

Homepage	<a href="https://www.mandiant.com">https://www.mandiant.com</a>	
Kontakt-Telefonnummer	+49 (0) 800 181 7231	
Kontakt-E-Mail-Adresse	<a href="mailto:investigations@mandiant.com">investigations@mandiant.com</a>	

### 3.34 Microsoft Deutschland GmbH

Homepage	<a href="https://www.microsoft.com/security">https://www.microsoft.com/security</a>	
Kontakt-Telefonnummer	+49 (0) 89 23 129 129	
Kontakt-E-Mail-Adresse	<a href="https://aka.ms/serviceshub">https://aka.ms/serviceshub</a>	

### 3.35 NCC Group GmbH

Homepage	<a href="https://www.nccgroup.com">https://www.nccgroup.com</a>	
Kontakt-Telefonnummer	24/7 Hotline	+49 (0) 89 2019 0489
	Telefon Zentrale	+49 (0) 89 599 762 0
Kontakt-E-Mail-Adresse	<a href="mailto:michiel.renzenbrink@nccgroup.com">michiel.renzenbrink@nccgroup.com</a>	

### 3.36 Northwave

Homepage <https://www.northwave-security.com>  
Kontakt-Telefonnummer + 31 85 043 7909  
Kontakt-E-Mail-Adresse [info@northwave-security.com](mailto:info@northwave-security.com)

### 3.37 NVISO GmbH

Homepage <https://www.nviso.eu/de>  
Kontakt-Telefonnummer +49 (0) 69 8088 3829  
Kontakt-E-Mail-Adresse [csirt@nviso.de](mailto:csirt@nviso.de)

### 3.38 Oneconsult Deutschland AG

Homepage <https://www.oneconsult.com/>  
Kontakt-Telefonnummer DE: +49 89 248 820 690  
CH: +41 43 377 22 90  
Kontakt-E-Mail-Adresse [csirt@oneconsult.com](mailto:csirt@oneconsult.com)

### 3.39 Orange Cyberdefense Germany GmbH

Homepage [www.orange cyberdefense.com](http://www.orange cyberdefense.com)  
Kontakt-Telefonnummer +49 (0) 821 808 30 470  
Kontakt-E-Mail-Adresse [CSIRT@orange cyberdefense.com](mailto:CSIRT@orange cyberdefense.com)

### 3.40 Palo Alto Networks

Homepage <https://unit42.paloaltonetworks.com/>  
Kontakt-Telefonnummer +31202993130  
Kontakt-E-Mail-Adresse [unit42-investigations@paloaltonetworks.com](mailto:unit42-investigations@paloaltonetworks.com)

### 3.41 pco GmbH & Co. KG.

Homepage <https://www.pco-online.de>  
Kontakt-Telefonnummer +49 (0) 541 605 1501  
Kontakt-E-Mail-Adresse [support@pco-online.de](mailto:support@pco-online.de)

### 3.42 PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft

Homepage <https://pwc.de>  
<https://www.pwc.de/de/im-fokus/cyber-security/cyber-incident-response.html>  
Kontakt-Telefonnummer +49 (0) 69 9585 9992  
Kontakt-E-Mail-Adresse [de\\_sir@pwc.com](mailto:de_sir@pwc.com)

### 3.43 QGroup GmbH

Homepage <https://www.qgroup.de>  
Kontakt-Telefonnummer +49 (0) 69 175363-047  
Kontakt-E-Mail-Adresse [emergency@qgroup.de](mailto:emergency@qgroup.de)

### 3.44 Rapid7 Germany GmbH

Homepage <https://www.rapid7.com/>  
Kontakt-Telefonnummer +1 844 727 4347  
Kontakt-E-Mail-Adresse [sales-dach@rapid7.com](mailto:sales-dach@rapid7.com)

### 3.45 r-tec IT Security GmbH

Homepage <https://www.r-tec.net/incident-response-service.html>  
Kontakt-Telefonnummer +49 (0) 202 31767-112  
Kontakt-E-Mail-Adresse [incident-response@r-tec.net](mailto:incident-response@r-tec.net)

### 3.46 SEC Consult Unternehmensberatung GmbH

Homepage <https://sec-consult.com/de/incident-response/sec-defence/>  
Kontakt-Telefonnummer +49 (0) 30 398 2027 77  
Kontakt-E-Mail-Adresse [secdefence@sec-consult.com](mailto:secdefence@sec-consult.com)

### 3.47 Sophos Technology GmbH

Homepage <https://www.sophos.de/rapid-response>  
Kontakt-Telefonnummer +49 (0) 611 7118 6766  
Kontakt-E-Mail-Adresse [RapidResponse@sophos.com](mailto:RapidResponse@sophos.com)

### 3.48 SVA System Vertrieb Alexander GmbH

Homepage <https://www.sva.de>  
Kontakt-Telefonnummer +49 (0) 6122 95092 92  
Kontakt-E-Mail-Adresse [incident-response@sva.de](mailto:incident-response@sva.de)

### 3.49 SySS GmbH

Homepage <https://www.syss.de>  
Kontakt-Telefonnummer +49 (0) 7071 407856 40  
Kontakt-E-Mail-Adresse [csrit@syss.de](mailto:csrit@syss.de)

### 3.50 Trend Micro Incident Response

Homepage <https://www.trendmicro.com/>  
Kontakt-Telefonnummer +49 (0) 89 54198959  
Kontakt-E-Mail-Adresse [incident\\_response@trendmicro.com](mailto:incident_response@trendmicro.com)

### 3.51 Verizon Deutschland GmbH

**Ansprechpartner**                    Stefan Englbrecht  
**Homepage**                            <https://www.verizon.com/business/de-de/products/security/>  
**Kontakt-Telefonnummer**        00 - 80085757575  
**Kontakt-E-Mail-Adresse**        [ir-hotline@verizon.com](mailto:ir-hotline@verizon.com)

### 3.52 Wipro

**Homepage**                            [www.wipro.com](http://www.wipro.com)  
**Kontakt-Telefonnummer**        Jeff Hamm: +49 (0) 162 2831672  
    Holger Wilken: +49 (0) 151 61 888 928  
**Kontakt-E-Mail-Adresse**        [jeff.hamm@wipro.com](mailto:jeff.hamm@wipro.com)  
    [holger.wilken@wipro.com](mailto:holger.wilken@wipro.com)

### 3.53 WithSecure GmbH

**Homepage**                            <https://www.withsecure.com/de/home>  
**Kontakt-Telefonnummer**        +49 (0) 891 2086 531  
**Kontakt-E-Mail-Adresse**        [mdr-dach@withsecure.com](mailto:mdr-dach@withsecure.com)

## 4 Leistungsmerkmale

### 4.1 24x7 Erreichbarkeit

Ist der APT-Response-Dienstleister rund um die Uhr bei Angriffen oder Problemen erreichbar? Dies kann insbesondere für erste Einschätzungen notwendig sein.

### 4.2 ISO27001-Zertifizierung der Institution

Besitzt der APT-Response-Dienstleister eine ISO27001 Zertifizierung für die Institution?

### 4.3 Hauptsitz des Dienstleisters in der EU

Befindet sich der Hauptsitz des Dienstleisters in einem Land der Europäischen Union?

### 4.4 Sichere Aufbewahrungsmöglichkeiten

Während der Bearbeitung des APT-Vorfalles fallen verschiedene Daten an. Dazu gehören zum Beispiel Dokumentationen, Log-Dateien oder Festplattenkopien. Diese können zum Teil vertrauliche Daten enthalten, welche auch beim Dienstleister entsprechend geschützt werden müssen.

### 4.5 APT-Dienstleistungen durch eigene Mitarbeitende

Bei der Aufarbeitung eines APT-Vorfalles werden viele verschiedene Kenntnisse benötigt, welche auch in den veröffentlichten Kriterien<sup>2</sup> aufgeführt sind. Teilweise greifen die Dienstleister dabei auch auf externe Unterstützung zurück, sodass keine eigenen Kenntnisse vorhanden sind.

Die Definitionen der einzelnen Rollen und Themenbereiche sind in den veröffentlichten Kriterien<sup>2</sup> zu finden.

#### 4.5.1 Ermittlungsleitung

#### 4.5.2 Malware-Analyse

#### 4.5.3 Host-Forensik

#### 4.5.4 Netzwerkforensik

### 4.6 Weitere Dienstleistungsangebote

#### 4.6.1 Beratung durch Dienstleister-eigene Juristen

Da bei der Bearbeitung eines APT-Vorfalles auch zahlreiche juristische Fragen geklärt werden müssen, ist die Hilfe von Juristen in den meisten Fällen zwingend notwendig. Falls der qualifizierte Dienstleister eigene Juristen für solche Fälle beschäftigt, können diese hinzugezogen werden.

#### 4.6.2 Krisenkommunikation

Bei einem APT-Vorfall muss häufig eine Strategie für den öffentlichen Umgang entwickelt und umgesetzt werden. Dabei kann, falls möglich der qualifizierte Dienstleister unterstützen.

---

<sup>2</sup> [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Auswahlkriterien\\_APT-Response\\_Dienstleister.html](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Auswahlkriterien_APT-Response_Dienstleister.html)

### **4.6.3 Durchführung des Wiederaufbaus der Systeme**

Nachdem der APT-Vorfall abschließend untersucht wurde, müssen mindestens die betroffenen Systeme bereinigt und neu aufgesetzt werden. Dies kann möglicherweise durch den qualifizierten Dienstleister erfolgen, falls dieser die Dienstleistung ebenfalls anbietet.

## **4.7 Technische Ausstattung**

### **4.7.1 Fähigkeit zur Malware-Analyse**

Verfügt der Dienstleister über die notwendigen technischen Voraussetzungen zur Analyse von Malware?

Dazu gehört zum Beispiel ein Labor mit der Möglichkeit, Malware in einer geschützten Umgebung auszuführen (dynamische Analyse) sowie durch Reverse Engineering (Disassemblierung, statische Analyse) zu analysieren.

### **4.7.2 Mobil einsetzbare Ausstattung**

Verfügt der Dienstleister über die notwendigen technischen Voraussetzungen zur Durchführung von forensischen Untersuchungen bei dem Auftraggeber vor Ort?

Dazu gehört mindestens eine ausreichende mobile Ausstattung, um die Datenakquise vor Ort durchführen zu können.

### **4.7.3 Hostbasierte Suche**

Für die Suche in einem großen Netzwerk mit vielen Systemen sollte der Dienstleister über Fähigkeiten verfügen, hostbasierte Indikatoren suchen zu können. Idealerweise besitzt er bereits a priori vor dem APT-Vorfall einen großen Satz an generischen und gruppenspezifischen Indikatoren.

## 5 Gegenüberstellung der Leistungsmerkmale der einzelnen APT-Response-Dienstleister

	4.1 24x7 Erreichbarkeit	4.2 ISO27001-Zertifizierung der Institution	4.3 Hauptsitz des Dienstleisters in der EU	4.4 Sichere Aufbewahrungsmöglichkeiten	4.5 APT-Dienstleistungen durch eigene Mitarbeitende				4.6 Weitere Dienstleistungsangebote			4.7 Technische Ausstattung		
					4.5.1 Ermittlungsleitung	4.5.2 Malware-Analyse	4.5.3 Host-Forensik	4.5.4 Netzwerkforensik	4.6.1 Beratung durch Dienstleister-eigene Juristen	4.6.2 Krisenkommunikation	4.6.3 Durchführung des Wiederaufbaus der Systeme	4.7.1 Fähigkeit zur Malware-Analyse	4.7.2 Mobil einsetzbare Ausstattung	4.7.3 Hostbasierte Suche
@-yet GmbH	+ <sup>a</sup>	+	+	+	+	+	+	+	+	+	+	+	+	+
Airbus Protect GmbH	+	+	+	+	+	+	+	+	- <sup>b</sup>	+	+	+	+	+
Antago GmbH	-	+	+	+	+	+	+	+	- <sup>b</sup>	-	- <sup>c</sup>	+	+	+
Arctic Wolf Networks Germany GmbH	+	+	+	+	+	+	+	+	-	-	+ <sup>d</sup>	+	+	+
BDO Cyber Security GmbH	+	+	+	+	+	+	+	+	+ <sup>e</sup>	+	- <sup>f</sup>	+	+	+
Bechtle AG	+	+	+	+	+	+	+	+	-	+	+	+	+	+
BFK edv-consulting GmbH	+	-	+	+	+	+	+	+	- <sup>b</sup>	+	- <sup>c</sup>	+	+	+
BlackBerry Deutschland GmbH	+	+	+	+	+	+	+	+	+ <sup>b</sup>	- <sup>b</sup>	- <sup>c</sup>	+	+	+

					4.5 APT-Dienstleistungen durch eigene Mitarbeitende				4.6 Weitere Dienstleistungsangebote			4.7 Technische Ausstattung		
CERTAINTY Holding GmbH	+	- <sup>g</sup>	+	+	+	+	+	+	- <sup>b</sup>	- <sup>b</sup>	+	+	+	+
Cirosec GmbH	+ <sup>a</sup>	+	+	+	+	+	+	+	- <sup>b</sup>	- <sup>b</sup>	- <sup>c</sup>	+	+	+
Cisco Talos Incident Response	+	+	+	+	+	+	+	+	-	+	- <sup>c</sup>	+	+	+
Code Blue GmbH	+	-	+	+	+	+	+	+	- <sup>b</sup>	+	- <sup>i</sup>	+	+	+
Corporate Trust	+ <sup>a</sup>	-	+	+	+	+ <sup>h</sup>	+	+	- <sup>b</sup>	+	- <sup>c</sup>	+ <sup>h</sup>	+	+
CrowdStrike	+	+	+	+	+	+	+	+	-	- <sup>i</sup>	+	+	+	+
DCSO	+	+	+	+	+	+	+	+	-	-	- <sup>c</sup>	+	+	+
Deloitte GmbH	+ <sup>a</sup>	+	+	+	+	+	+	+	+	- <sup>b</sup>	+	+	+	+
DigiFors GmbH	+	+	+	+	+	+	+	+	- <sup>b</sup>	- <sup>b</sup>	- <sup>c</sup>	+	+	+
Dr. Michael Gorski Consulting GmbH	+	-	+	-	+	+	+	+	- <sup>b</sup>	+	- <sup>c</sup>	+	+	+
EY GmbH & Co. KG Wirtschaftsprüfungsgesellschaft	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ERNW Research GmbH	+	-	+	+	+	+	+	+	-	- <sup>b</sup>	+ <sup>j</sup>	+	+	+
ETAS GmbH	+ <sup>a</sup>	-	+	+	+	+	+	+	- <sup>b</sup>	- <sup>b</sup>	- <sup>c</sup>	+	+	+
Eye Security GmbH	+	+	+	+	+	+	+	+	- <sup>b</sup>	+	- <sup>i</sup>	+	+	+
GDATA Advanced Analytics	+	-	+	+	+	+	+	+	- <sup>b</sup>	- <sup>b</sup>	- <sup>c</sup>	+	+	+

					4.5 APT-Dienstleistungen durch eigene Mitarbeitende				4.6 Weitere Dienstleistungsangebote			4.7 Technische Ausstattung		
glueckkanja AG	+	+	+	+	+	+	+	+	- <sup>b</sup>	-	+	+	-	+
Grant Thornton AG	+	+	+	+	+	+ <sup>h</sup>	+	+	+	+	- <sup>c</sup>	+ <sup>h</sup>	+	-
HiSolutions AG	+ <sup>a</sup>	+	+	+	+	+	+	+	- <sup>b</sup>	+	- <sup>c</sup>	+	+	+
HvS-Consulting GmbH	+ <sup>a</sup>	-	+	+	+	+	+	+	- <sup>b</sup>	- <sup>b</sup>	- <sup>c</sup>	+	+	+
InfoGuard AG	+	+	-	+	+	+	+	+	+	+	+	+	+	+
intersoft consulting services AG	+	+	+	+	+	+	+	+	+	+	+ <sup>j</sup>	+	+	+
KPMG AG	+	+	+	+	+	+	+	+	+	+	- <sup>c</sup>	+	+	+
LEITWERK AG	+	+	+	+	+	+	+	+	-	+	+	+	+	+
Mandiant Deutschland GmbH	+	-	+	+	+	+	+	+	- <sup>b</sup>	+	- <sup>c</sup>	+	+	+
Microsoft Deutschland GmbH	+	+	-	+ <sup>a</sup>	+	+	+	+	-	+	+	+	+	+
NCC Group GmbH	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Northwave	+	+	+	+	+	+	+	+	-	- <sup>i</sup>	+	+	+	+
NVISO GmbH	+	+	+	+	+	+	+	+	-	- <sup>i</sup>	- <sup>c</sup>	+	+	+
Oneconsult Deutschland AG	+	+	+	+	+	+	+	+	+	- <sup>b</sup>	- <sup>i</sup>	+	+	+
Orange Cyberdefense Germany GmbH	+	+	+	+	+	+	+	+	-	+	-	+	+	+

					4.5 APT-Dienstleistungen durch eigene Mitarbeitende				4.6 Weitere Dienstleistungsangebote			4.7 Technische Ausstattung		
Palo Alto Networks	+	+	+	+	+	+	+	+	- <sup>b</sup>	- <sup>b</sup>	- <sup>c</sup>	+	+	+
pco GmbH & Co. KG	+ <sup>a</sup>	+	+	+	+	+	+	+	+	-	+	+	+	+
PricewaterhouseCoopers GmbH	+	+	+	+	+	+	+	+	+	+	- <sup>c</sup>	+	+	+
QGroup	+	- <sup>k</sup>	+	+	+	+	+	+	-	- <sup>i</sup>	- <sup>c</sup>	+	+	+
Rapid7 Germany GmbH	- <sup>a</sup>	+	+	+	+	+	+	+	-	+	- <sup>i</sup>	+	-	+
r-tec IT Security GmbH	+ <sup>a</sup>	+	+	+	+	+	+	+	- <sup>b</sup>	- <sup>b</sup>	+	+	+	+
SEC Consult	+	+	+	+	+	+	+	+	-	+	+	+	+	+
Sophos Technology GmbH	+	+	+	+	+	+	+	+	-	- <sup>i</sup>	- <sup>c</sup>	+	+	+
SVA	+ <sup>a</sup>	+	+	+	+	+	+	+	-	+	+	+	+	+
SySS GmbH	+	+	+	+	+	+	+	+	-	-	- <sup>c</sup>	+	+	+
Trend Micro Incident Response	+	+	+	+	+	+	+	+	-	-	- <sup>c</sup>	+	+	+
Telekom Security	+	+	+	+	+	+	+	+	-	+	+	+	+	+
Verizon Deutschland GmbH	+	+	+	+	+	+	+	+	- <sup>b</sup>	+	- <sup>i</sup>	+	+	+
Wipro	+	+	+	+	+	+	+	+	+	+	-	+	+	+
WithSecure GmbH	+	+	+	+	+	+	+	+	-	-	-	+	+	+

- 
- <sup>a</sup> Nach entsprechender Vereinbarung
  - <sup>b</sup> In Zusammenarbeit mit externen Partnerunternehmen
  - <sup>c</sup> Externes Systemhaus wird vom Dienstleister begleitet und beraten
  - <sup>d</sup> Ergänzend mit externen Partnerunternehmen
  - <sup>e</sup> In Zusammenarbeit mit internem Partnerunternehmen.
  - <sup>f</sup> Internes Partnerunternehmen wird beraten und unterstützt.
  - <sup>g</sup> Ist in Vorbereitung
  - <sup>h</sup> Bei umfangreichen Analysen in Zusammenarbeit mit einem externen Partnerunternehmen
  - <sup>i</sup> Unterstützung und fachliche Beratung wird angeboten
  - <sup>j</sup> Wiederaufbau erfolgt bei KMUs oder beim Thema Active Directory selbst, ansonsten wird externes Systemhaus vom Dienstleister begleitet und beraten
  - <sup>k</sup> In Erstellung