Tech Data
Advanced Solutions

SECURITY SALES GUIDE

So positionieren Sie IBM Resilient erfolgreich bei Ihren Kunden - als Lösung oder Service.

Resilienz beschreibt die Fähigkeit, Störungen und Schocks zu absorbieren, um in Krisen möglichst unbeschadet weiter funktionieren zu können.

Resilienz verkörpert Prozesse, die während oder nach dem IT-Angriff im Unternehmen greifen – als Reaktion auf die immer größer werdenden Herausforderungen im Hinblick auf komplexe, unkontrollierbare und bedrohungsanfällige Strukturen moderner IT-Landschaften.

Resilienz ist ein Prozess, der tief im Unternehmen verankert sein muss und selbst in extremen Ausnahmesituationen noch funktionieren muss. Er wird in guten Zeiten geplant und aufgesetzt, um in Krisensituationen die richtigen Notfallmaßnahmen effizient und schnell durchführen zu können.

Damit ist Resilienz das wichtigste Bindeglied eines IT-Security-Konzepts für Unternehmen und Managed Service Provider.

Schnelles, effizientes und zielgerichtetes Handeln mit einem fein orchestrierten schlagkräftigen Plan ist seit Jahrtausenden die Basis erfolgreicher Verteidigung des eigenen Hab und Guts.

So kommen Sie sicher durch den Kundentermin

FRAGEN FÜR DEN GESPRÄCHSEINSTIEG:

- Wissen Sie, wer bei einem IT-Angriff die Steuerung übernimmt und kennen Sie seine Strategie?
- Haben Sie einen Incident Response Plan für Ihr Unternehmen?
- Nutzen Sie zurzeit ein System zum Incident Response Management?

Einsatzfelder für IBM Resilient und Playbooks

Playbooks sind der Schlüssel zum Überstehen brenzliger Situationen. In der Verkehrsfliegerei werden Checklisten für Problemsituationen schon seit ewigen Zeiten benutzt, um Fehler bei der komplexen Lösung von Gefahrensituationen zu vermeiden. IT-Landschaften haben sich in den letzten 20 Jahren zu genau so einem komplexen Gebilde entwickelt. Daher bedarf es der richtigen Maßnahme zur richtigen Zeit – von der Person mit den besten Qualifikationen, um bedrohlichen Situationen schnell Herr zu werden. Hier helfen Playbooks.

RESILIENT SECURITY MODUL | RESILIENT ACTION MODUL | RESILIENT PRIVACY MODUL

RESILIENT SECURITY MODUL:

- Weiß Ihr Team, wer im Falle eines Cyber-Angriffes involviert werden muss und wer im Unternehmen welche Kompetenzen hat?
- Kennen Ihre Mitarbeiter nötige Arbeitsroutinen, um die Bedrohung einzugrenzen?

SCHNELLER REAGIEREN

Das Resilient Security Modul formuliert sofort umfassende, anpassbare und dynamische Aktionspläne für jeden Ereignistyp. Dies stellt sicher, dass die Incident Response Pläne konsistent, wiederholbar und stets aktuell sind. Wenn mehr Informationen über einen aktuellen Vorfall aufgedeckt werden, entwickeln sich die Incident Response Pläne automatisch weiter.

Darüber hinaus bietet das Resilient Security Modul schnelle und einfache Vorfallsimulationen und Tabletop-Übungen. Sie ermöglichen es dem Team, Reaktionen zu üben und sicherzustellen, dass es bereit ist, sich Sicherheitsbedrohungen schnell und effektiv zu stellen.

BESSER KOORDINIEREN

Die **Dynamic Playbooks** erleichtern es Incident Response Managern, Prioritäten zu setzen und sich auf die wirklich kritischen Ereignisse zu konzentrieren. Sie helfen auch, andere Abteilungen im gesamten Unternehmen zu koordinieren und zu informieren, bevor ein Vorfall sich zu einer Krise entwickelt.

Die Benutzeroberfläche des Resilient Security Moduls ist einfach, intuitiv und Aktionspläne enthalten alle relevanten Zusammenhänge und Anweisungen, sodass auch nicht-technische Mitarbeiter effektive Helfer sein können. Damit kann das gesamte Unternehmen - einschließlich der Rechts-, Marketing- und Personalabteilung - in den Verteidigungsprozess integriert werden.

INTELLIGENTER REAGIEREN

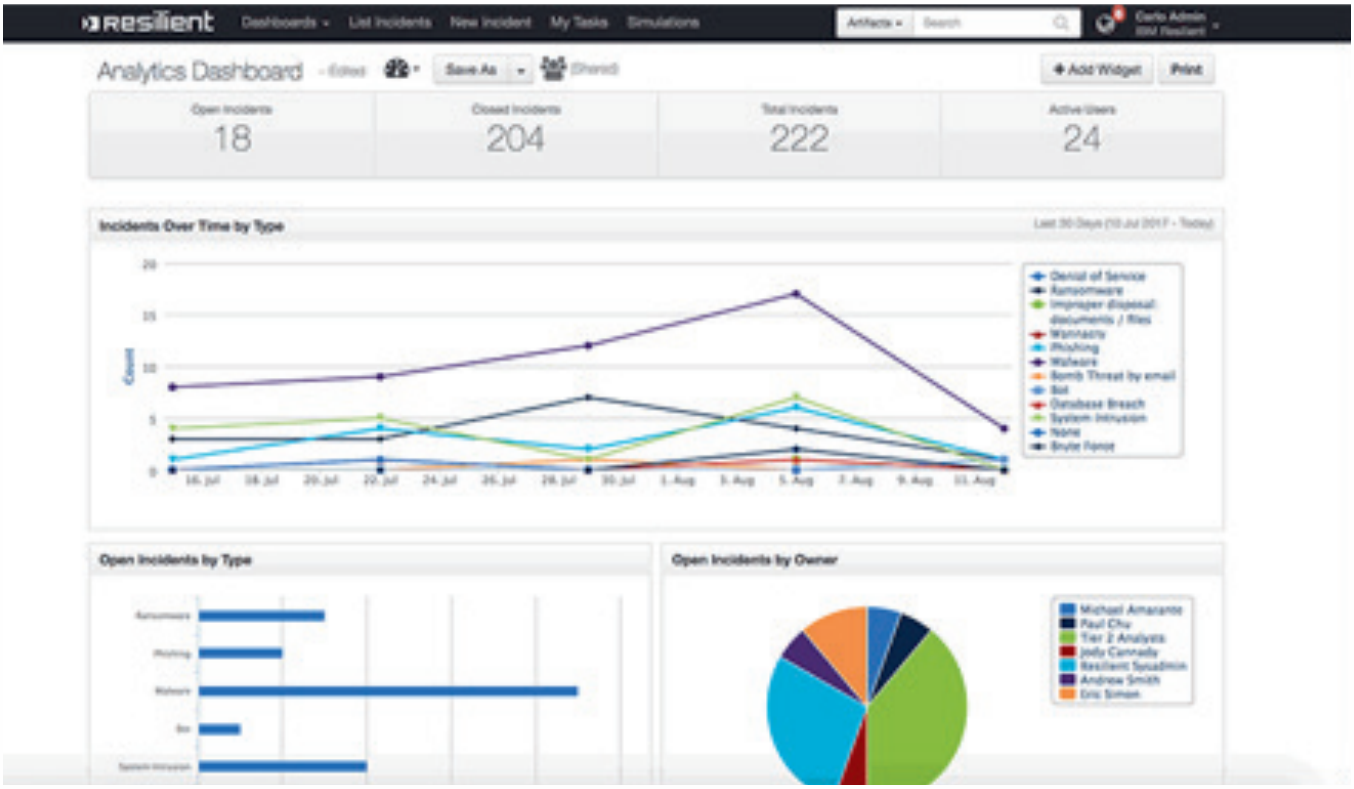
Das Resilient Security Modul beinhaltet viele Echtzeit-Intelligenz-Feeds, die den Incident Response Teams die wichtigen Zusammenhänge liefern, um die entscheidenden Antwort geben zu können.

Die umfassenden Berichts- und Analysefunktionen machen aus den Vorfalldaten umsetzbare Erkenntnisse, die eine Verbesserung der Incident Response Infrastruktur ermöglichen.

Beispiele

- Die Timeline-Funktion bietet eine ausgefeilte, flexible und anpassbare Sicht auf anstehende und abgeschlossene Aufgaben - ein wertvoller Einblick in den Status und die Verantwortlichkeit.
- Benutzerdefinierte Dashboard Widgets bieten eine grafische Möglichkeit, auf die wichtigsten Informationen zuzugreifen und diese zu visualisieren.
- Das Analyse-Dashboard zeigt Vorfall-Metriken in der gesamten Organisation, einschließlich Vorfallstufen nach Kategorie, Schweregrad und Dauer.

Mit diesen Reporting- und Analysefunktionen kann jeder – vom Vorstand über den CSO bis hin zu den IR-Teammitgliedern – die benötigten Informationen in einem personalisierten Format erhalten und interpretieren.



Quelle: https://www.ibm.com/us-en/marketplace/resilient-incident-response-platform

RESILIENT ACTION MODUL:

- Bekommen Sie im Falle eines Angriffs Informationen über den aktuellen Status?
- Sind Ihre Kommunikationswege nachhaltig miteinander vernetzt, sodass keine Informationen verloren gehen?
- Sind Ihre Verteidigungsprozesse bereits automatisiert?

Das Resilient Action Modul ermöglicht die bi-direktionale Integration mit allen Systemen, einschließlich SIEM, Ticketing-Systemen, Datenbanken, Proxies oder Mail Services. Damit können automatisierte Aktionen gestartet werden, wie zum Beispiel das Erstellen von IT-Tickets, das Sammeln von Informationen und forensischen Daten, die Quarantäne oder sogar das erneute Aufsetzen infizierter Computer.

Das Incident Response Team kann so Sicherheitsvorfälle schneller und effizienter verwalten. Anstatt ständig kleine Brände zu löschen, kann es sich auf größere Brände konzentrieren und den Schaden für das Unternehmen begrenzen.

Anwendungsbeispiele:

DATENANREICHERUNG UND ESKALATION

Durch die Integration mit SIEM kann das Resilient Action Modul eine automatische methodische Reaktion auf Vorfälle starten. Es kann Daten zu einen Vorfall aus dem SIEM abrufen und so dem Security-Team tiefere Einblicke in den Vorfall liefern.

ÖFFNEN UND AKTUALISIEREN VON TICKETS

Benutzer können mit Tickets ein Ablaufprotokoll in Resilient auslösen und Teams Aktionen zuweisen.

MALWARE INVESTIGATION UND REMEDIATION

Benutzer können kompromittierte Konten deaktivieren, Quarantäne-Prozesse automatisieren oder sogar infizierte Rechner neu aufsetzen.

AKTUALISIERUNG VON IDS UND IPS-REGELN

Wenn Security-Teams bösartige IPs aufdecken, können sofort neue IDS/IPS-Regeln über das Resilient Action Modul generiert und ausgerollt werden.

NUTZUNG UND AKTUALISIERUNG VON ASSET-DATENBANKEN

Zu Beginn eines Vorfalls können kritische Informationen aus Asset-Datenbanken abgerufen werden. Dazu gehören auch historische Informationen über relevante Mitarbeiter oder Maschinen oder ob es sich um personenbezogene Daten handelt.

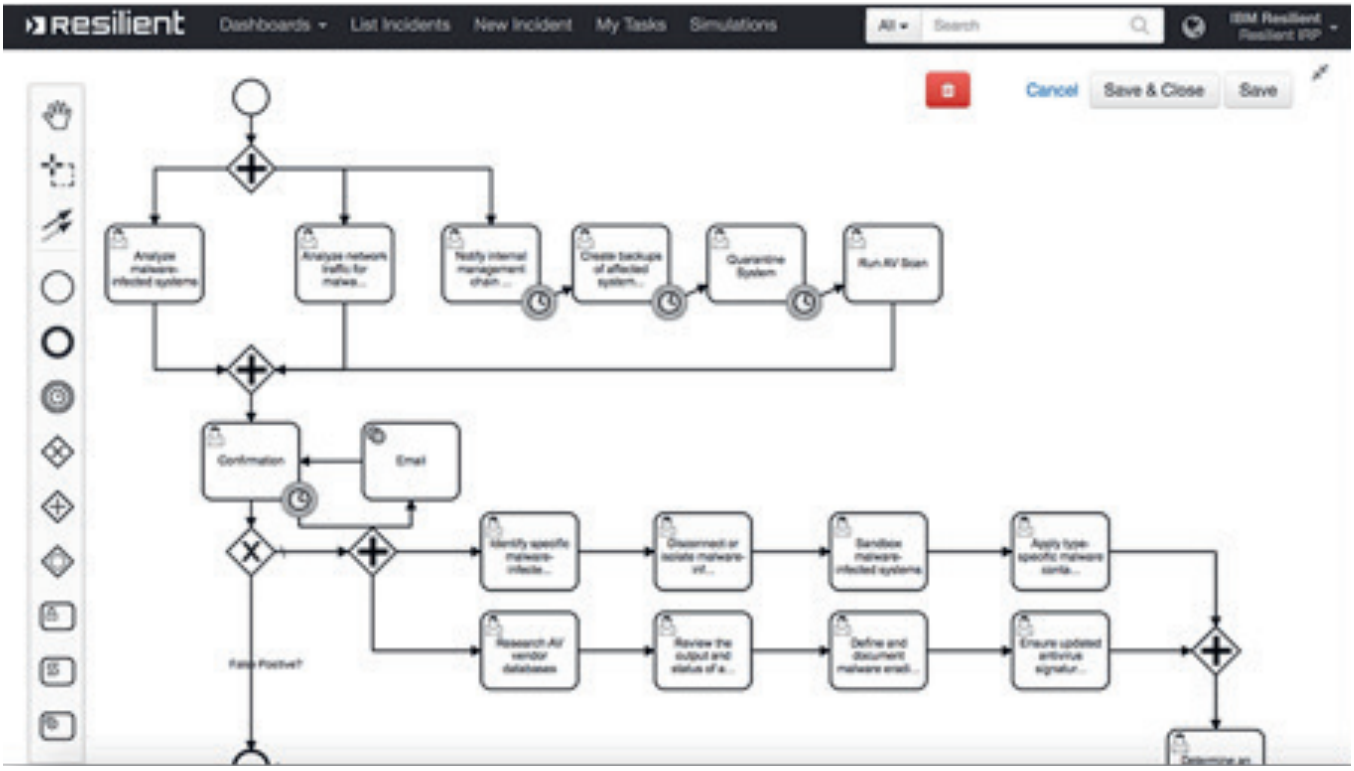
RESILIENT PRIVACY MODUL:

- Kennt Ihr Team alle regulatorischen und vertraglichen Pflichten im Falle eines Datenverlustes und handelt immer regelkonform?
- Als internationaler Konzern müssen Sie im Falle eines Datenverlustes nationale Gesetze befolgen. Haben Sie dafür eine Lösung, um keine Fehler zu begehen?

Aktionspläne und Incident Management

Wechselnde gesetzliche und unternehmerische Vorschriften können die internen Reaktionsprozesse in kritischen Situationen verlangsamen. Das Resilient Privacy Modul nimmt die Ungewissheit und erhöht die Effizienz:

- Es analysiert automatisch die Datenschutzbestimmungen der Industrie und der unternehmensspezifischen Verpflichtungen für jeden Vorfall. Es versorgt Security-Teams mit sofortigen Best-Practice Aktionsplänen, Dynamic Playbooks und Benachrichtigungsvorlagen.
- Eine kollaborative und agile Plattform hilft Security Teams, den GDPR Anforderungen gerecht zu werden. Damit können sie sich in Echtzeit bei der Entwicklung von Ereignissen auf die wichtigen Schritte fokussieren, bevor diese zu echten Krisen werden.
- Es bietet eine zentrale Drehscheibe für die Verwaltung von „Reaktionen“ und ermöglicht es Datenschutzbeauftragten, Marketing, HR oder die Rechtsabteilung einzubeziehen.



Quelle: https://www.ibm.com/us-en/marketplace/resilient-incident-response-platform

Mit dem Resilient Privacy Modul können Datenschutz- und Sicherheitsvorfälle innerhalb kürzester Zeit erledigt werden. Hinzu kommt die Gewissheit, dass das Unternehmen vollständig konform mit Vorschriften handelt.

Das Resilient Privacy Modul wird von der weltweit größten Wissensdatenbank unterstützt. Ein Team von Rechtsanwälten und zertifizierten Datenschutzexperten verwaltet die Wissensdatenbank von Resilient.

SCHNELLE, EFFEKTIVE SIMULATIONEN UND ÜBUNGEN

Übung macht den Meister. Mit den Simulationen und Tabletop-Übungen des Resilient Privacy Moduls können Datenschutzteams Antwortszenarien üben, die Leistung des Teams messen und anwenden. Damit werden Reaktionspläne optimiert.

GDPR PREPARATORY GUIDE

Der Resilient GDPR Preparatory Guide ist ein interaktives Tool, das Kunden Schritt für Schritt auf GDPR vorbereitet. Das Tool erlaubt etwa Aufgaben zu verteilen und Workflows zu managen, sodass im Ernstfall eine lückenlose Dokumentation sichergestellt ist.

Mit der Funktion *Resilient GDPR Simulation* wird der Ernstfall trainiert: IT-Sicherheitsverantwortliche können notwendige Schritte und Maßnahmen durchspielen, die bei einer Datenpanne innerhalb der 72-Stunden-Frist ergriffen werden müssen.

Das Resilient GDPR-Enhanced Privacy Modul gibt Kunden Zugriff auf die weltweit umfangreichste Datenbank mit Richtlinien und Gesetzen zu GDPR.

Für welche Kunden ist IBM Resilient geeignet?

Zielkunden: ab 50 Mio. USD Umsatz; > 500 Mitarbeiter oder Service Provider.

Branchen: Banken, Chemie und Erdöl, Bildung, Energie und Versorgung, Finanzmärkte, Regierung, Gesundheitswesen und Biowissenschaften, Versicherungen, Einzelhandel, Reise und Transportwesen

Funktion: CIO, CISO, VP/Director - FP&A, Director of IT-Security, VP of IT, Security and Risk

KUNDENBEDÜRFNIS:

- Unternehmen kommen mit Email, XLS und SharePoint Lösungen an organisatorische Grenzen.
- Es herrscht Frust, weil das hauseigene Ticket-System nicht zielführend und leistungsorientiert arbeitet.
- Es gibt kein dediziertes Incident Response Personal oder Fähigkeiten im Unternehmen und das Unternehmen sucht Wege, um bestehende Fachkräfte im Krisenfall zusammenzuführen.
- Managed Service Kunden des Unternehmens erwarten eine Lösung bei Security-Vorfällen und müssen über Unternehmensgrenzen hinweg juristisch einwandfreie, nachvollziehbare Prozesse steuern und belegen können.

IBM Resilient – perfekt für die Bereitstellung eines Managed Services

IBM Resilent ist mit IBM QRadar, IBM BigFix und IBM MaaS360 das Rückgrat des IBM Immunsystems. Moderne Angriffe werden heute nicht mehr von einer einzigen Firewall abgewehrt. Es braucht ein fein abgestimmtes Orchester an Lösungen, die miteinander integriert sind. Nur die schnelle Weitergabe von Informationen zu Status und Bedrohung schafft heutzutage die nötige IT-Sicherheit.

Die Lösung kann von Ihnen auch als Managed Service betrieben werden. Denn jedes Unternehmen muss sich ernsthaft mit IT-Security auseinandersetzen und kann die Frage nach Sicherheit nicht mehr nur oberflächlich beleuchten. Bei der genaueren Betrachtung ihrer IT-Security-Anforderungen stoßen viele Unternehmen an Grenzen. Gutes Personal zu finden, das die Lücken schließen könnte, ist zeitaufwendig und sehr teuer. Was ihnen bleibt, ist die Expertise extern zu suchen und IT-Dienstleister zu beauftragen. Mit IBM Resilient haben Sie hervorragende Möglichkeiten, sich als Managed Service Provider bei Ihren Kunden zu positionieren.

So unterstützt Sie Tech Data im kompletten Vertriebsprozess

Unsere Experten widmen sich mit ihrer langjährigen Erfahrung und einem ausgereiften Portfolio aus branchenführenden und innovativen Lösungen der IT-Security in Ihrem Unternehmen. So können wir Sie im gesamten Vertriebsprozess unterstützen. Unsere technischen Teams erklären hierbei stets verständlich und bedarfsorientiert die Vorzüge der einzelnen Produkte und erarbeiten gemeinsam mit unseren Sales Mitarbeitern ein individuelles auf Sie abgestimmtes Konzept zur nachhaltigen Sicherung der Unternehmensdaten Ihrer Kunden.

Wir begleiten Sie von Ihrer Ausbildung, über die Lead-Generierung bis hin zum Proof-of-Concept. So können Sie sich voll und ganz auf die Anforderungen Ihrer Kunden konzentrieren.

Details für den Abschluss des Projekts

Die wichtigsten Kennzahlen:

Sales Cycle:	**Software Volumen:**	**Dienstleistungsanteil:**
9-15 Monate	50.000-1.500.000 € (plus S&S)	Sehr hoch, da Prozessintegration / Beratung der Schlüssel zum Erfolg ist. (ca. 50.000-80.000 Euro)

Tech Data
Advanced Solutions

Ihre Ansprechpartner

Patrick Olschewski
Business Development Manager
patrick.olschewski@techdata.com

Siegfried Markiefka
Business Development Manager
smarkiefka@techdata.de