FACTSHEET

Unser Service - Ihr Mehrwert!

INCIDENT RESPONSE RETAINER

Antares-NetlogiX unterstützt Sie im Rahmen der IRGA mit dem **Incident Response Retainer** bei technischen und organisatorischen Maßnahmen, um IT-Bedrohungen schnell abzuwehren und einzudämmen. Dieser Retainer **vereinfacht die Abwicklung von Aufträgen und sorgt für Kostentransparenz** bei der Unterstützung zu unterschiedlichen Tageszeiten.

IHRE VORTEILE

IRGA Incident Response Retainer

- Optimierte Sicherheit: Verringern Sie die Auswirkungen und Kosten von Sicherheitsverletzungen durch den Einsatz eines Koordinators bei der Reaktion auf Vorfälle.
- Experten für die Reaktion auf Vorfälle stehen Ihnen rund um die Uhr zur Verfügung.
- Verkürzte Wiederherstellungszeiten: Vordefinierte Reaktionspläne und Kommunikationskanäle beschleunigen die Wiederherstellung nach Vorfällen.
- Wegfall der Einarbeitung: Die Notwendigkeit, Mitarbeiter und Technologien für Incident Response einzuarbeiten, entfällt.
- Flexiblität bei der Nutzung der Retainer-Stunden.
- Planbare Budgets und verbesserte Reaktionsfähigkeit ermöglichen eine effiziente Ressourcennutzung.

INCIDENT RESPONSE GROUP AUSTRIA

- Die Allianz

Die IRGA ist eine Allianz von vier etablierten, hochspezialisierten österreichischen Unternehmen, die das gesamte Leistungsspektrum des Incident Response Managements abdeckt.

Alle Mitglieder der IRGA Allianz verfügen über mehr als 20 Jahre Erfahrung im Bereich IT-Sicherheit und Verfügbarkeit.

Wir begleiten Sie von der proaktiven Planung über die Eindämmung von Ransomware-Angriffen bis hin zum Wiederanlauf Ihrer IT-Infrastruktur.

WWW.IRGA.AT

ANTARES NETLOGIX

CoreTec

IT/DESIGN software projects & consulting

SCHOELLER

DAS BIETEN WIR IHNEN

Der IRGA Incident Response Retainer umfasst die folgenden Bereiche:

1. JÄHRLICHER RETAINER

Beziehen Sie reaktive Leistungen im Rahmen des Incident Response Einsatzes sowie proaktive Leistungen.

Proaktive Leistungen umfassen zum Beispiel:

- Notfallhandbücher: Erstellung bzw. Review
- Technische Playbooks bei Ransomware Angriffen
- Pentests, Phishing Tests
- Incident Response Tests (Table Top Exercises, in weiterer Folge aktive Tests in der Infrastruktur)
- Awareness Schulungen
- Managed Awareness Training
- Darknet Monitoring
- Vulnerability Management Service
- Azure/O365 Audit
- AD Security Analyse, AD Passwort Analyse

- **NIS 2 Qualifizierungsaudits**
  Die CoreTEC GmbH ist qualifizierte Stelle für NIS2-Überprüfungen

IN DREI PAKETEN VERFÜGBAR

SMALL	MEDIUM	LARGE

2. INHALT DES INCIDENT RESPONSE SUPPORTS (BEISPIELE)

Prozess-Unterstützung:

- Unterstützung von einem erfahrenen Incident Response Koordinator (als rechte Hand Ihres internen IT-Notfallmanagers)
- Support bei der Koordination von technischen und forensischen Analysen
- Unterstützung bei der Beweissicherung in Zusammenhang mit Sicherheitsvorfällen
- Technische Best Practices für Eindämmung und Wiederanlauf
- Beratung für die Kommunikation mit Kunden und Partnern
- Analyse von Logs zur Nachvollziehbarkeit des Angriffsszenarios und zur Eingrenzung des betroffenen Scopes

Konfigurationsunterstützung im Zuge des Incident Response Supports unter anderem für:

- VMWare und Hyper-V
- VEEAM
- Firewalls: Fortigate, Checkpoint
- Netzwerk: LAN, WLAN
- Windows Server inkl. AD und PKI
- Linux Server

Zusatzoptionen

- Rollout einer EDR Lösung zur Unterstützung bei der forensischen Analyse und zur Isolation der betroffenen Systeme (sofern beim Kunden noch nicht umgesetzt)
- Temporäre Authentifizierungsplattform (bei komplett verschlüsseltem AD) für die IT-Partner
- E-Mail Continuity Service: ermöglicht den „Notbetrieb" beim Ausfall eines On-Premise-Mailservers.

IRGA

Wir bieten Ihnen eine zukunftssichere Notfallplanung

Im Notfall muss eine klare Rollenverteilung vorhanden sein, um rasch zu reagieren.
Federführend bei der Notfallbewältigung ist der interne IT-Notfallmanager. Er kennt das Unternehmen, Geschäftsprozesse, Infrastruktur und alle relevanten internen und externen Akteure.

Ein externer Incident Response Koordinator kann zusätzlich wertvolle Unterstützung bieten. Im Zuge des SLA wird der Incident Response Koordinator während des gesamten Incident Response Prozesses tatkräftig unterstützen.