Swiss IT Security Deutschland GmbH

Secure MultiCloud Workshop

https://sits.group/managedservices

SWISS IT SECURITY
PART OF SWISS IT SECURITY GROUP

Microsoft Solutions Partner
Modern Work

Microsoft Solutions Partner
Infrastructure
Azure

Specialist
Azure Virtual Desktop

Microsoft Solutions Partner
Security

Specialist
Identity and Access Management
Information Protection and Governance
Threat Protection

Der Schutz für Multi-Cloud und Hybrid-Workloads

Die Sicherheitsbedrohungen werden durch die Komplexität von Hybrid- und Multi-Cloud-Umgebungen verschärft. Da immer mehr unserer kritischsten Daten ausschließlich in der Cloud vorliegen und die Aufrechterhaltung konsistenter Zugriffskontrollen eine Herausforderung darstellt, steigt der Bedarf an integriertem Schutz für Ihre Multi-Cloud-Ressourcen, Apps und Daten.

Herausforderungen

Da sich Unternehmen weiterhin auf Hybrid- und Remote-Workflows einstellen, ist die Bewertung Ihrer aktuellen Sicherheitslage von entscheidender Bedeutung. Die Sichtbarkeit sowie die Bewertung der aktuellen Sicherheitslage wird durch Multi-Cloud sowie Hybrid-Workloads zunehmest schwieriger.

Die Lösung

Mit Microsoft Defender for Cloud können Sie Ihre Hybrid- und Multi-Cloud-Infrastruktur-Workloads bewerten und schützen, sodass Sie unabhängig von der Umgebung flexibel bleiben. In gemeinsamen Workshops helfen wir Ihnen die Vorteile und Features von Microsoft Defender for Cloud zu erkennen und für Ihr Unternehmen zu nutzen.

Ihr Vorteil

Wissen ist Macht. Um Ihre wichtigsten cloudbasierten Daten zu schützen und sich gegen potenzielle Bedrohungen zu verteidigen, benötigen Sie ein klares Bild Ihrer Hybrid- und Multi-Cloud-Sicherheit.

Der Secure Multi-Cloud Workshop hilft Ihnen dabei, Ihre aktuelle Sicherheitslage zu bewerten, den Umfang der geschützten Ressourcen zu erweitern und einen Aktionsplan zur Behebung zu entwickeln.

Swiss IT Security Deutschland GmbH

Secure MultiCloud Workshop

Ein definierter, personalisierter Plan für umsetzbare nächste Schritte, einschließlich eines Zeitplans für Abhilfemaßnahmen, basierend auf den spezifischen Sicherheitsanforderungen und -zielen Ihres Unternehmens.

Define scope & design

Analysieren Sie Anforderungen und Prioritäten für eine Hybrid- und Multi-Cloud-Sicherheitslagemanagement- und Bedrohungsschutzlösung.

Definieren Sie gemeinsam mit uns, Umfang und Design für zusätzliche Hybrid- und Multi-Cloud-Ressourcen, geschützt werden sollen.

Discover & Protect

Entdecken Sie Schwachstellen und Bedrohungen für Hybrid- und Multi-Cloud-Workloads und geben Sie Empfehlungen zu Risikominderungsstrategien.

Schützen Sie zusätzliche Hybrid- und Multi-Cloud-Ressourcen, indem Sie sie in Microsoft Defender for Cloud integrieren.

Guidance & Recommend

Wir helfen Ihnen Produkte wie Microsoft Defender for Cloud, Azure Arc, Disaster Recovery, Azure Policys etc. In Ihre Sicherheitsabläufe zu integrieren.

Wir geben Empfehlungen zur Verbesserung der Sicherheitslage und des Schutzes von Hybrid- und Multi-Cloud-Infrastruktur-Workloads ab und helfen Ihnen, diese selbstständig zu implementieren.

Security Build-In

Sicheres Management Ihrer hybriden Multi-Cloud Umgebung auf Basis des Zero-Trust-Prinzip mit Microsoft Defender for Cloud.

Protect (hybrid) multicloud resources

Microsoft Defender for Cloud stellt mit agentenlosen, API-basierten Methoden eine Verbindung zu Ihren Multicloud-Umgebungen her, um tiefe Security-Einblicke zu erhalten und die entsprechenden Schutzmaßnahmen ableiten. Sie können Azure Arc nutzen, um Ihre on-prem Workloads ebenfalls optimal einzubinden.

- Defend Amazon AWS resources
- Defend Google GCP resources
- Azure Arc
- Defender for Endpoint (Server)
- Zero Trust Infrastructure und Integrationen

Improve cloud security posture

Defender for Cloud überprüft Ihre Ressourcen, Subscriptions und Ihre Organisation kontinuierlich auf Sicherheitsprobleme.

- Security policies, initiatives, und Recommandations
- Secure Score
- Cloud Security Posture Management (CSPM)
- Identifizieren und analysieren Sie Risiken in (hybriden) Multi-Cloud-Umgebungen
- External attack surface management (EASM)
- Agentless scanning

Improve data security posture

Mit der Beschleunigung der digitalen Transformation verschieben Unternehmen Daten exponentiell in die Cloud und nutzen dabei mehrere Datenspeicher. Die dynamische und komplexe Natur der Cloud hat die Risiken für Daten erhöht. Dies stellt Sicherheitsteams vor große Herausforderungen im Hinblick auf die Datentransparenz und den Schutz des Cloud-Datenbestands.

- Data security in Defender CSPM
- Data security in Defender for Storage

Security Build-In

Sicheres Management Ihrer hybriden Multi-Cloud Umgebung auf Basis des Zero-Trust-Prinzip mit Microsoft Defender for Cloud.

Improve container security posture

Microsoft Defender für Container ist die cloudnative Lösung zur Verbesserung, Überwachung und Aufrechterhaltung der Sicherheit Ihrer Cluster, Container und ihrer Anwendungen.

- Defender for Container (Kubernetes)
- Agentless container posture (AKS)
- Container registry vulnerability assessment

Security recommandations

Empfehlungen in Defender für Cloud basieren auf dem Cloud-Sicherheitsbenchmark von Microsoft. Dieser weithin anerkannte Benchmark basiert auf den Controls des Center for Internet Security (CIS) und des National Institute of Standards and Technology (NIST) mit Schwerpunkt auf Cloud-zentrierter Sicherheit.

- Azure security recommandations
- AWS security recommandations
- GCP security recommandations
- Refernece list of attack paths and cloud security graph

Security alerts and incidents

Security-Alerts und Incidents sind die Benachrichtigungen, die von Defender for Cloud generiert werden, wenn Bedrohungen in Ihren Azure-, Hybrid- oder Multicloud-Umgebungen erkannt werden.

- Korrelation von Alerts in incidents
- Integrated threat intelligence
- Behavioral analytics
- Anomaly detection
- Response automation

Swiss IT Security Deutschland GmbH

Secure MultiCloud Workshop

Sicheres Management Ihrer hybriden Multi-Cloud Umgebung auf Basis des Zero-Trust-Prinzip mit Microsoft Defender for Cloud.

Wenn es um Sicherheit, Compliance und die Cloud-Transformation geht, brauchen Sie einen erfahrenen Partner.

Die digitale Transformation ist ein Erfolgsfaktor für jedes Unternehmen. Damit Sie die Chancen nutzen und Ihre Geschäftsziele erreichen können, bieten wir strategische und operative Beratung, damit Sie Risiken minimieren, Daten schützen und Compliance-Anforderungen einhalten können.

SWISS IT SECURITY
PART OF SWISS IT SECURITY GROUP

Microsoft Solutions Partner
Modern Work

Microsoft Solutions Partner
Infrastructure
Azure

Specialist
Azure Virtual Desktop

Microsoft Solutions Partner
Security

Specialist
Identity and Access Management
Information Protection and Governance
Threat Protection

Sprechen Sie uns für einen Beratungstermin zu einer Integration in Ihrer Umgebung an.

Rufen Sie uns an: **+49 611 9458810**

oder kontaktieren Sie uns per E-Mail: **info@sits-d.de**

SWISS IT SECURITY
PART OF SWISS IT SECURITY GROUP

Microsoft Solutions Partner
Modern Work

Microsoft Solutions Partner
Infrastructure
Azure

Specialist
Azure Virtual Desktop

Microsoft Solutions Partner
Security

Specialist
Identity and Access Management
Information Protection and Governance
Threat Protection