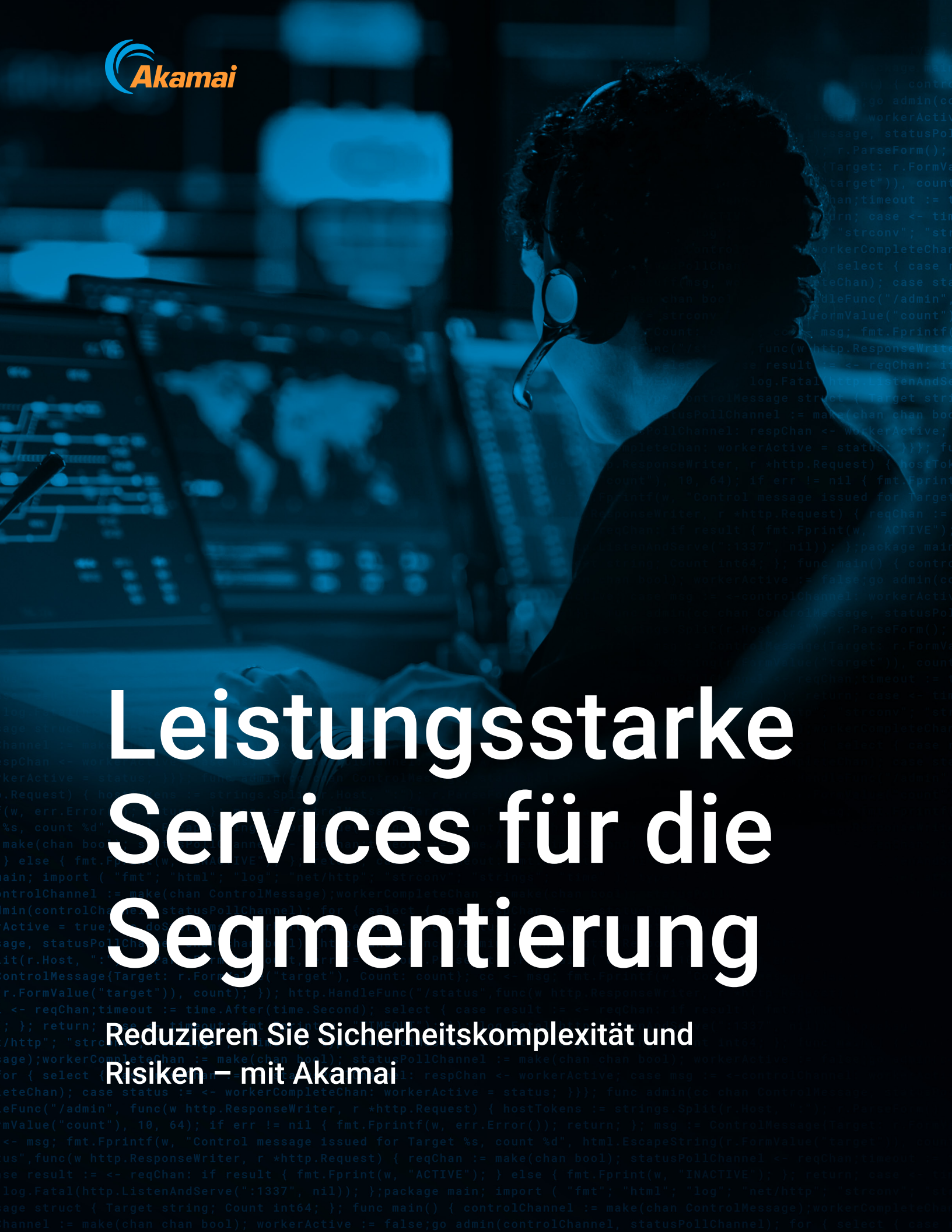


Leistungsstarke Services für die Segmentierung

Reduzieren Sie Sicherheitskomplexität und Risiken – mit Akamai

Einführung

Der Schutz wichtiger Ressourcen in Rechenzentren vor Ort und öffentlichen Cloudumgebungen ist wichtiger denn je. Dies erfordert zunehmend spezialisiertes Fachwissen, um mit neuen Bereitstellungsmodellen für Anwendungen in einer sich schnell entwickelnden Bedrohungslandschaft Schritt zu halten. Unsere Service-Experten sind stets bemüht, Ihre Investitionen in unser Sicherheitsportfolio in greifbare, geschäftsorientierte Ergebnisse umzusetzen.

Das Mikrosegmentierungsservice-Team von Akamai besteht aus intensiv geschulten Sicherheitsexperten mit umfangreicher Erfahrung aus der Praxis sowohl im privaten Sektor als auch in militärischen Geheimdiensten. Unsere flexiblen Serviceangebote bieten Ihnen Zugang zu diesem Fachwissen als Erweiterung Ihrer internen IT- und Sicherheitsteams, damit Sie die Möglichkeit erhalten, erstklassige Sicherheit vom Rechenzentrum bis zur Cloud zu implementieren.

Customer Journey

Eine typische Customer Journey beginnt mit der Bereitstellung und Konfiguration über unsere Professional Services Delivery: Wir richten Ihre Umgebung ein, definieren Assets und Kategorien und implementieren die Richtlinie für die ersten Anwendungsfälle.

Anschließend bieten wir einigen Teammitgliedern, die die Lösung verwenden, Verwaltungs- und Engineering-Schulungen an.

Darüber hinaus können Day-2-Betriebsservices zum Einsatz kommen, um die ursprüngliche Bereitstellung fortzuführen und zu verbessern (Definition weiterer Assets und Kategorien sowie Implementierung von Richtlinien für zusätzliche Anwendungsfälle), Sicherheitsvorfälle zu handhaben und die Sicherheitslage zu verbessern, erforderliche Kontrollen und Berichte für Prüfungen bereitzustellen und individuelle Entwicklung anzubieten, um die Integration in die Infrastruktur des Kunden zu verbessern.

Während des gesamten Lebenszyklus der Lösung helfen umfangreiche Supportservices, Probleme zu lösen, und unser Customer Success Team wird sicherstellen, dass Sie den maximalen Nutzen aus unserem Produkt ziehen.

Kundengeschichte mit Akamai-Mikrosegmentierungsservices

Customer Success
Sicherstellen, dass Kunden maximalen Nutzen aus unserem Produkt ziehen

Professional Services Delivery

Implementierung des Produktes; Implementierung erster Anwendungsfälle

Schulung

Umfassende Schulungs- und Zertifizierungsprogramme

Day-2-Betriebsservices

Durchgängige Wartung und Erweiterung von Assets/Kategorien/Richtlinien

Sicherheitskontrolle und IR, Audit-Vorbereitung, individuelle Entwicklung und Integration

Technical Account Manager/Resident Engineer

Kundensupport-Services
Technische Supportservices: Rund um die Uhr, fest zugeordneter Techniker

Professional Services Delivery

Ein umfangreiches Team aus Sicherheitsarchitekten, Projektmanagern und Entwicklern arbeitet mit Ihrem Team zusammen, um die Plattform Akamai Guardicore Segmentation zu implementieren. Je nach Ihren Anforderungen bietet Akamai entweder ein Leistungspaket oder einen Implementierungstechniker für einen konkreten Zeitraum an. Unabhängig davon, für welches Paket Sie sich entscheiden – unsere Serviceangebote sind auf den Schutz Ihrer kritischen Ressourcen zugeschnitten.

Jumpstart

Jumpstart wurde für Kunden entwickelt, die die Umsetzung von Akamai Guardicore Segmentation beschleunigen möchten, aber daran anschließende Richtlinien unter Anleitung unserer Experten selbst implementieren und verwalten möchten. Ganz gleich, ob Sie Ihre Netzwerkumgebung segmentieren, Anwendungen per Ringfencing abgrenzen oder den Zugriff auf Server einschränken möchten, unsere Techniker entwerfen und implementieren ein erstes Richtlinienziel für Sie, wobei sie Ihnen eine Einweisung zukommen lassen und bei der Implementierung nachfolgender Richtlinien Hilfestellung geben.

Unser Team kooperiert auch mit Ihnen, soweit es um die Planung der Sicherheitsarchitektur und alle Überlegungen zum Anwendungsdesign geht. Dies umfasst Definieren und Dokumentieren der Kategorisierungsstrategie, das Kategorisieren Ihrer Assets auf der Plattform und die formelle Erstellung und Feinabstimmung der Richtlinien zur Unterstützung Ihrer Anwendungsfälle.

Nachdem Akamai die erste Richtlinienimplementierung abgeschlossen hat, unterstützen unsere Techniker Ihr Team weiterhin direkt bei zukünftigen Richtlinienimplementierungen und bleiben Teil Ihres erweiterten Teams, bis Ihre Bereitstellungsziele erreicht sind.

Extended Jumpstart

Für Unternehmen mit mehreren Segmentierungszielen ist Extended Jumpstart ideal. Die Experten von Akamai arbeiten mit Ihren Teams zusammen, um mehrere Segmentierungsrichtlinien umzusetzen und so den Schutz Ihrer kritischen und wertvollsten Ressourcen zu verbessern.

Unser Team kooperiert auch mit Ihnen, soweit es um die Planung der Sicherheitsarchitektur und alle Überlegungen zum Anwendungsdesign geht. Dies umfasst Definieren und Dokumentieren der Kategorisierungsstrategie, das Kategorisieren Ihrer Assets auf der Plattform und die formelle Erstellung und Feinabstimmung der Richtlinien zur Unterstützung mehrerer Sicherheitsinitiativen.

Typische umzusetzende Richtlinienziele

Egal, ob Sie Ihre Netzwerkumgebung segmentieren, Anwendungen per Ringfencing abgrenzen oder den Zugriff auf Server einschränken möchten – unsere Techniker gehen mit Ihnen jeden Schritt des Weges, um sicherzustellen, dass Ihre Ressourcen geschützt sind.

Im Rahmen dieses Angebots können Sie mehrere Richtlinienziele auswählen oder sich auf ein bestimmtes Ziel mit hoher Priorität konzentrieren. Unsere Ingenieure implementieren die erforderlichen Kategorisierungen und Regeln, aus denen sich unsere Richtlinien zusammensetzen, bis Ihre Assets gemäß Ihren vorab festgelegten Zielen gesichert sind.

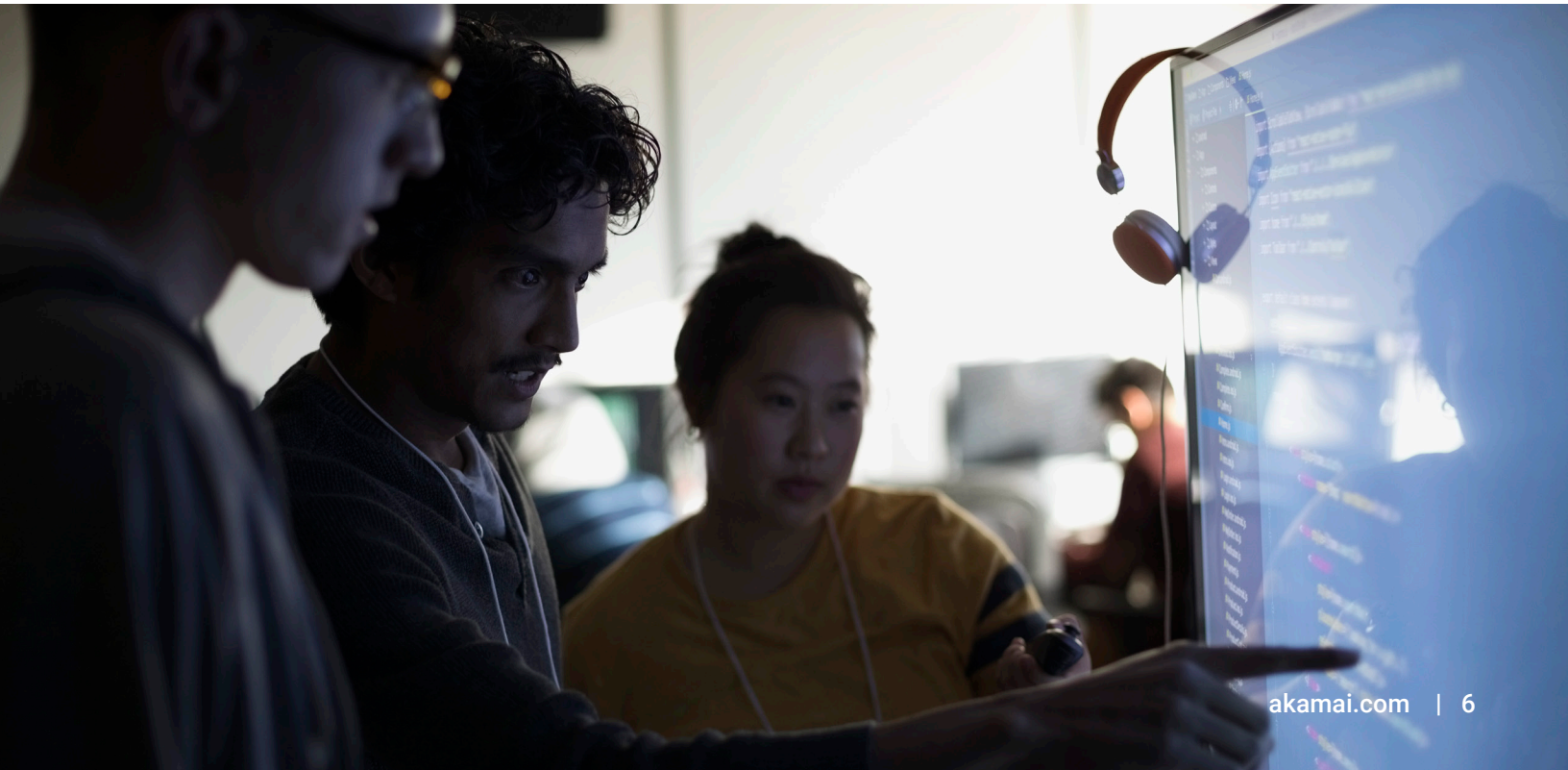
Beispiele:

- **Umgebungssegmentierung** – Server aus verschiedenen Umgebungen dürfen nicht kommunizieren, mit Ausnahme ausdrücklich zugelassener Kommunikation.
- **Anwendungs-Ringfencing** – Kritische Anwendungen sollten nur mit ausdrücklich zugelassenen Parteien kommunizieren. Interne Anwendungskommunikation ist gestattet.
- **Mikrosegmentierung bei Anwendungen** – Interner und externer Traffic kritischer Anwendungen ist nur zulässig, wenn dies ausdrücklich genehmigt wurde (Zero Trust).
- **Endpoint-Segmentierung „außerhalb des Unternehmens“** – Die Angriffsfläche eines Endpoints außerhalb des Schutzes eines Unternehmensnetzwerks wird begrenzt. Akamai Guardicore Segmentation ermöglicht verschiedene Regelsätze für die Bereiche innerhalb und außerhalb Ihres Unternehmensnetzwerks.
- **Zugriffsberechtigungen auf Server** – Richtlinien zur Serverzugriffskontrolle können implementiert werden, um beispielsweise Verwaltungsportale auf Jumpboxen zu beschränken oder den Zugriff auf bestimmte Server basierend auf der Nutzeridentität der Quelle zu blockieren.
- **Durchsetzung von Best Practices für die Sicherheit** – Es werden Regeln für die Blockliste implementiert, um Best Practices für die Netzwerksicherheit durchzusetzen.

Implementierungstechniker

Wenn ein Unternehmen eine erhebliche Anzahl von Richtlinienzielen benötigt, ist es oft ratsam, für einen bestimmten Zeitraum mit einem zugewiesenen Techniker zusammenzuarbeiten, wobei die Anzahl der Richtlinien, die unser Techniker für Sie erstellen kann, unbegrenzt ist; dies gestattet eine erfolgreiche Implementierung. Wenn Ihr Netzwerk zum Erreichen Ihrer Sicherheitsziele eine vollständige End-to-End-Segmentierung benötigt, ist es ideal, die Implementierung durch Akamai unterstützen zu lassen.

	Jumpstart	Extended Jumpstart	Implementierungs-techniker
Installation	✔	✔	✔
Installation des Kategorisierungsschemas	✔ Eingeschränkt	✔ ✔ ✔	Umfassende Implementierungsressourcen für einen festgelegten Zeitraum ohne Einschränkung der Anwendungsfälle, um sicherzustellen, dass Ihre Erfolgsziele erreicht werden
Anleitung zur allgemeinen Sicherheit	✔ Eingeschränkt	✔ ✔ ✔	
Anleitung zur Richtlinienerstellung	✔ Eingeschränkt	✔ ✔ ✔	
Anwendungsfälle zur Richtlinien-Implementierung	**Einzelrichtlinie**	**Mehrere Richtlinien**	
Endnutzerschulung	✔	✔	✔
Typische Dauer	**6 Monate**	**12 Monate**	**6–18 Monate**
Wann welche Option ratsam ist	Kunden oder Partner bevorzugen die Implementierung überwiegend intern; Akamai implementiert nur den ersten Anwendungsfall	Akamai implementiert mehrere Anwendungsfälle, mehrere Richtlinien und bietet umfassende Anleitungen	Der Kunde oder Partner wünscht eine vollständige Implementierung (mehrere Anwendungsfälle) und untersucht und definiert während des gesamten Zeitraums lieber genau, was wie zu erfolgen hat



Akamai-Schulungen

Die Zertifizierungsschulung für Mikrosegmentierung von Akamai vermittelt Administratoren (GCSA) und Betriebstechnikern (GCSE) die erforderlichen Fähigkeiten und Informationen, um ihre jeweiligen Wartungs- und Verwaltungsaufgaben erfüllen zu können.

Die Schulungsmethoden sind vielseitig, um den Bedürfnissen von Kunden und Partnern gerecht zu werden: Von einfachen Online-Schulungen über Zertifizierungsschulungen mit Ausbildern bis hin zu privaten, dedizierten (virtuellen oder persönlichen) Schulungen.

Guardicore Certified Segmentation Administrator (GCSA)

Unser Programm vermittelt Nutzern der Akamai Guardicore Segmentation Plattform an fünf halben Arbeitstagen das nötige Fachwissen, um alle Aspekte der Plattform erfolgreich betreiben zu können. GCSA-Absolventen wird das Vertrauen vermittelt, die Plattform eigenständig nutzen zu können, um die Sicherheitsanforderungen ihres Unternehmens zu implementieren und aufrechtzuerhalten.

Der Kurs behandelt die Kernfunktionen von Akamai Guardicore Segmentation: Sichtbarkeit, Kategorisierung, Mikrosegmentierung und Erkennung von Angriffen. Der Schwerpunkt liegt in erster Linie auf dem Verhalten von Funktionen und ihrer Nutzung. Der Kurs führt die Teilnehmer von der anfänglichen Konfiguration der Akamai Guardicore Segmentation hin zum üblichen Alltagsbetrieb.

Guardicore Certified Segmentation Engineer (GCSE)

Unser Programm vermittelt den Betreibern des Systems an drei halben Arbeitstagen die Fähigkeiten und Kenntnisse, die sie zur Durchführung plattformbezogener Verwaltungs- und Wartungsaufgaben benötigen.

GCSE-Absolventen können den gesamten Betrieb der Akamai Guardicore Segmentation-Umgebung verwalten. Der Kurs behandelt die folgenden Themen: Konfiguration von Plattformen und Komponenten, Integration mit Tools von Drittanbietern, Prüfung des Plattformzustands, Fehlerbehebung und allgemeine Wartungsaufgaben.

Beide Kurse werden von einer praktischen Laborumgebung unterstützt, die für alle Teilnehmer während des Kurses verfügbar ist. Am Ende jedes Kurses findet eine Zertifizierungsprüfung statt.

Enterprise Support und Customer Success

Unser Programm Enterprise Support ist darauf ausgelegt, alle erdenklichen Auswirkungen der Nutzung von Akamai Guardicore Segmentation in Ihrem Unternehmen zu unterstützen. Unsere Support-Organisation betreut Sie ganzjährig und rund um die Uhr, bearbeitet alle Supportanfragen und unterstützt Sie bei Upgrades und Fehlerbehebung.

Unser Programm Customer Success hilft Ihnen dabei, kurz- und langfristigen Sicherheitsziele Ihres Unternehmens zu erreichen und gleichzeitig den Wert Ihrer Investition in unsere Plattform zu maximieren.

Elite Support

Das Programm Elite Support von Akamai bietet Ihrem Unternehmen bevorzugten Zugriff auf explizit zugewiesene, erfahrene, Eskalationsexperten erster Güte. Ein hochqualifizierter Spezialist, der mit Ihrem Rechenzentru m und internen Prozessen vertraut ist, wird Ihr konkreter Ansprechpartner und hilft Ihnen, die Reaktion auf Probleme und deren Lösung zu beschleunigen und den Nutzen Ihrer Investitionen in eine softwarebasierte Segmentierung zu maximieren.

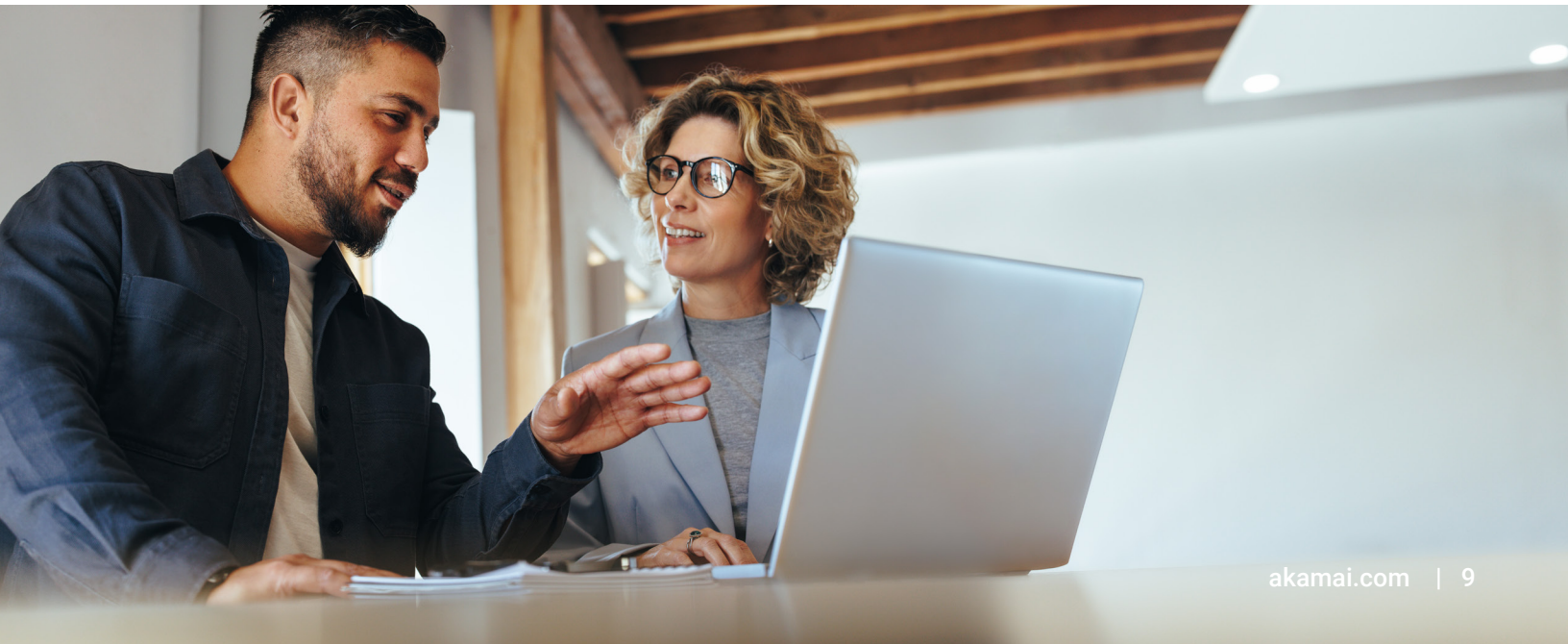
	Premium	Elite
Support-Verfügbarkeit	**Ganzjährig, rund um die Uhr**	**Ganzjährig, rund um die Uhr**
Unbegrenzte Fallzahl	✔	✔
Upgrades und Fehlerbehebungen	✔	✔
Telefon, E-Mail, Slack und Portal	✔	✔
Ursachenanalyse (nach Bedarf)	**Schweregrad 1**	**Schweregrad 1 und Schweregrad 2**
Bearbeitung von Fällen mit hoher Priorität durch einen zugewiesenen erfahrenen Techniker		✔ Zuständiger Techniker steht während der Geschäftszeiten zur Verfügung
Proaktive und kontinuierliche Überwachung des Systemzustands		✔
Personalisierte Optimierung		✔ Vierteljährliche Optimierungssitzung
Regelmäßige Problemberichte und Support-Bericht		✔ Wöchentliche Problemberichte; monatlicher Support-Bericht
Beratungstage		✔ 2, 4 oder 6 Beratungstage pro Jahr, je nach Größe (Artikelposition)
Wann welche Option ratsam ist	Kleinere Implementierung; benötigt hauptsächlich Support	Größere Implementierung; benötigt eine bessere Kontrolle laufender Probleme

Day-2-Betriebsservices

Kunden profitieren bereits nach der Implementierung der ersten Anwendungsfälle von Akamai Guardicore Segmentation. Es besteht jedoch fortlaufender Wartungs- und Aktualisierungsbedarf, um den Nutzen unseres Produkts zu maximieren:

- Die Bereitstellung (Assets, Kategorien, Richtlinien) muss aktualisiert werden, um Änderungen im Unternehmen umgehend zu berücksichtigen
- Zusätzliche Anwendungsfälle, die während der anfänglichen Bereitstellungsphase nicht bearbeitet wurden, müssen umgesetzt werden (neue Anwendungsfälle, die erst mit der Nutzung des Produkts ersichtlich werden, zusätzliche zu berücksichtigende Services und/oder Anwendungen, usw.)
- Akamai Guardicore Segmentation kann für weitere Bereiche Ihres Unternehmens umgesetzt werden, z. B. cloudbasierte Netzwerke und Anwendungen. (Entweder neu oder nur Verbleibendes für Phase 2)
- Bereitstellung auf zusätzlichen Endpoints, Geräten im Internet der Dinge, virtuellen Desktop-Infrastrukturumgebungen usw.
- Mit Akamai Guardicore Segmentation lassen sich Sicherheitsereignisse identifizieren und mindern (d. h. laterale Bewegungen in Ihrem Netzwerk können unterbunden werden). Sie können Ihre Umgebung mit dem Akamai Security Operations Command Center verbinden, für eine ganzjährige Rund-um-die-Uhr-Überwachung sowie für Echtzeitwarnungen und -abwehrmaßnahmen
- Profitieren Sie von verbesserter, proaktiver Sicherheit über Akamai Hunt, Akamai Edge DNS (für sicheres DNS und Schutz vor Distributed Denial of Service) und Akamai Enterprise Application Access (für Zugriffs- und Identitätsverwaltung)
- Nutzen Sie Akamai Guardicore Segmentation zur Unterstützung von Zertifizierungsprüfungen

Diese Services sollten von GcSP-zertifizierten Partnern erbracht werden



Technical Account Manager und Resident Engineers

Technical Account Manager und Resident Engineers sind leitende technische Berater für Unternehmen mit umfassenden und potenziell komplexen Segmentierungsanforderungen. Nachdem unsere Techniker in Ihr Unternehmen integriert sind, können sie schnell zu Experten bezüglich Ihrer Umgebung werden, sodass Sie über Akamai Guardicore Segmentation herausragende Erfolgserlebnisse realisieren können.

Der Ihrem Kundenkonto zugewiesene Resident Engineer* wird in Ihre Teams integriert und unterstützt proaktiv alle Ihre Vorgänge, um sicherzustellen, dass Sie jederzeit maximalen Nutzen aus Akamai Guardicore Segmentation ziehen können.

Der Resident Engineer kann Ihren Erfolg sicherstellen, indem er Sie bei Entscheidungen zu Richtlinien anleitet, Sie über die neuesten Funktionen unseres Produkts informiert, Upgrades plant (und bei der Umsetzung unterstützt) und Geschäftsprüfungen durchführt.

Der für Sie zuständige Technical Account Manager oder Resident Engineer kann auch Ihre Day-2-Betriebsservices überwachen und ausführen.

**Der Resident Engineer befindet sich nicht zwingend vor Ort*

Akamai Hunt: Ein Managed Service zum Threat Hunting

Akamai Hunt, eine Erweiterung von Akamai Guardicore Segmentation, ist unser Managed Service zum Threat Hunting, mit dem Sie auch äußerst schwer zu fassenden Bedrohungen immer einen Schritt voraus sind und Ihr Unternehmen besser schützen können.

Das Team von Akamai Hunt spürt kontinuierlich anomales Angriffsverhalten und hoch entwickelte Bedrohungen auf, die selbst modernste Sicherheitslösungen regelmäßig umgehen. Mit Hunt werden Sie sofort über alle kritischen Vorfälle in Ihrem Netzwerk informiert, und unsere Experten arbeiten eng mit Ihrem Team zusammen, um betroffene Assets zu beseitigen und Probleme schnell zu beheben.

Ganz gleich, ob es um die Erkennung und Vermeidung von Ransomware-Angriffen, die Abwehr hochentwickelter persistenter Bedrohungen, den Schutz vor Zero-Day-Schwachstellen oder die Verbesserung Ihrer allgemeinen IT-Sicherheitshygiene geht – mit Akamai Hunt erzielen Sie den größtmöglichen Sicherheitsnutzen aus Ihrer Implementierung von Akamai Guardicore Segmentation, und das ohne zusätzliche Software, Agent-Rollouts oder Upgrades.

Akamai Hunt umfasst Folgendes:

Fachkundige menschliche Analyse rund um die Uhr – Unsere Cybersicherheitsprofis stammen aus verschiedenen Bereichen wie Sicherheitsforschung, offensive Sicherheit, militärische Aufklärung, Red Teams, Vorfallsreaktion und Data Science.

Benachrichtigung bei echten Bedrohungen – Um Abstumpfung auf Grund zu häufiger Warnmeldungen zu vermeiden, warnt das Hunt-Team Kunden nur vor echten Bedrohungen und vermeidet nach Möglichkeit False Positives.

Proprietäre Tools zum Threat Hunting – Die Hunt-Experten entwickeln routinemäßig fortschrittliche Algorithmen zur Bedrohungsbekämpfung wie Anomalien bei der Nutzer- und Netzwerkaktivität, ausführbare Analysen, Log-Analysen und mehr, um ein leistungsstarkes Toolset für eine schnelle Detektion und Reaktion aufzubauen. Akamai Guardicore Insight, ein leistungsstarkes Tool auf Betriebssystem-Query-Basis zur Abfrage von Endpoints und Servern in Echtzeit, ist ohne zusätzliche Kosten im Service inbegriffen.

Kontextbezogene Bedrohungsinformationen – Unsere Threat Hunter sammeln Indicators of Compromise, die von IPs und Domains bis hin zu Prozessen, Nutzern und Services reichen, indem sie Akamai Guardicore Segmentation und die umfassende globale Threat Intelligence von Akamai nutzen.

Transparenz von Netzwerken, Cloud und Endpoints – Die Kombination aus durch Akamai Guardicore Segmentation und globale Sensoren von Akamai generierten Daten – darunter über sieben Billionen DNS-Anfragen pro Tag an die Akamai DNS-Cloud – bietet unserem Team einen umfassenden Überblick über Ihre Umgebung.

Sofortige Benachrichtigung und proaktive Einblicke –

- E-Mail-Benachrichtigungen werden sofort gesendet, nachdem eine Bedrohung erkannt wurde
- Regelmäßige Berichte über Bedrohungen auf Führungsebene mit Analysen, Statistiken und Metriken, damit Ihre Führungskräfte oder Vorstandsmitglieder in Bezug auf maßgebliche Angriffe immer auf dem neuesten Stand sind
- Die Vorfallsverwaltung ist dank der Integration in die Akamai Guardicore Segmentation-Konsole denkbar einfach

Weitere Informationen zu Akamai Guardicore Segmentation Besuchen Sie akamai.com