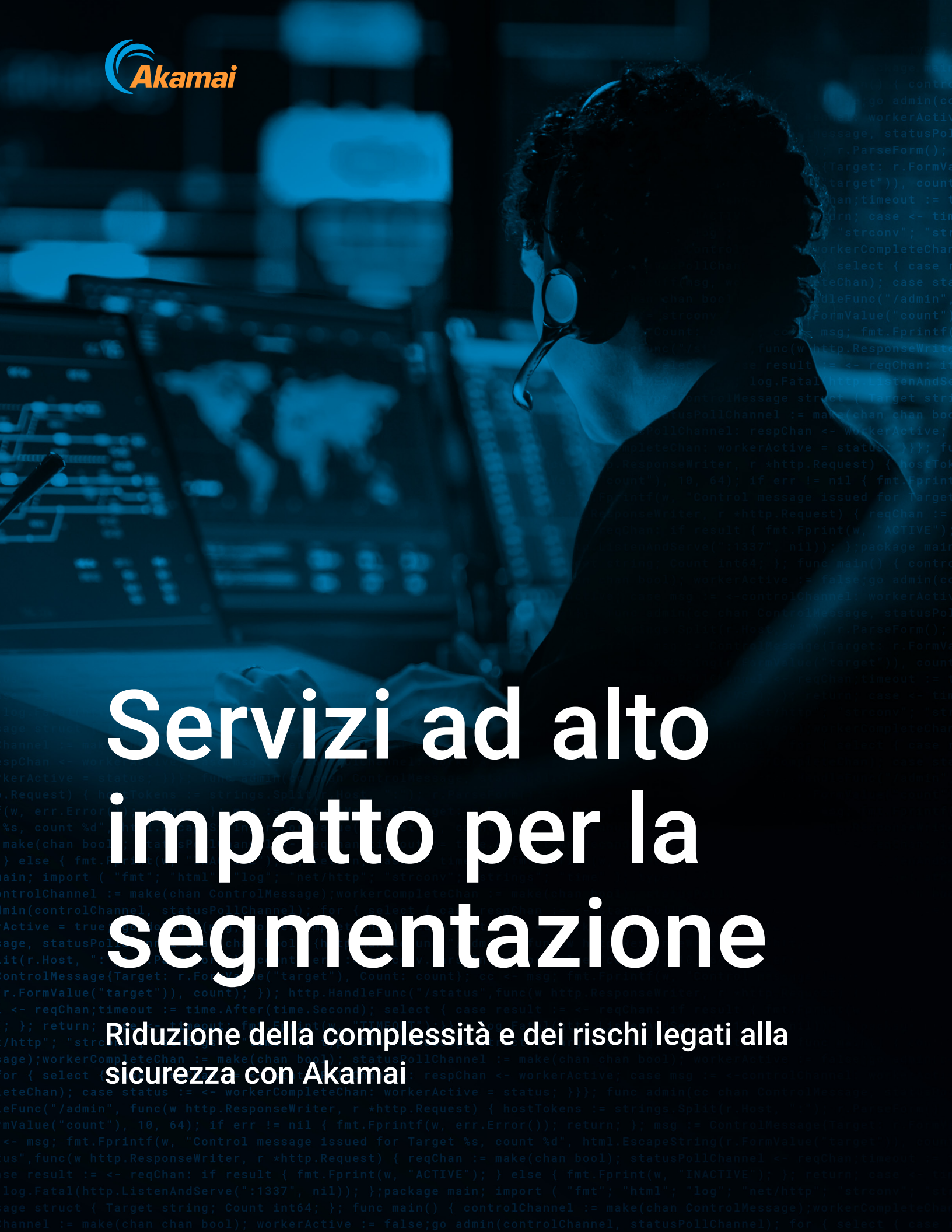


Servizi ad alto impatto per la segmentazione

Riduzione della complessità e dei rischi legati alla sicurezza con Akamai

Introduzione

La protezione delle risorse critiche nei data center on-premise e negli ambienti cloud pubblici è più importante che mai. Ciò richiede sempre più competenze specializzate per stare al passo con i nuovi modelli di distribuzione delle applicazioni in un panorama delle minacce in rapida evoluzione. I nostri esperti di servizi si concentrano sulla trasformazione del vostro investimento nel nostro portafoglio di sicurezza in risultati tangibili e orientati al business.

Il team dei servizi di microsegmentazione di Akamai è composto da esperti di sicurezza con formazione approfondita ed esperienza reale sia nel settore privato che nelle organizzazioni di intelligence militare. La nostra serie flessibile di offerte di servizi fornisce l'accesso a queste competenze specializzate come integrazione ai team IT e di sicurezza interni per implementare la migliore strategia di sicurezza dal data center al cloud.

Percorso del cliente

Un tipico percorso del cliente inizia con l'implementazione e la configurazione tramite la nostra fornitura di servizi professionali: configuriamo il vostro ambiente, definiamo risorse ed etichette e implementiamo la policy per i primi casi di utilizzo.

Quindi, forniamo formazione amministrativa e tecnica ad alcuni membri del team che utilizzano la soluzione.

Inoltre, i servizi operativi del secondo giorno possono essere utilizzati per continuare e migliorare l'implementazione (definendo più risorse ed etichette, nonché implementando policy per casi di utilizzo aggiuntivi), gestire gli incidenti di sicurezza e migliorare il livello di sicurezza, fornire i controlli e i rapporti necessari per le verifiche e garantire uno sviluppo personalizzato per migliorare l'integrazione con l'infrastruttura del cliente.

Durante tutto il ciclo di vita della soluzione, i servizi di supporto estesi aiuteranno a risolvere qualsiasi problema che potrebbe verificarsi e il nostro team Customer Success si assicurerà che otteniate il massimo valore dal nostro prodotto.

Percorso del cliente con i servizi di microsegmentazione Akamai

Successo dei clienti
Garantire che i clienti massimizzino il valore del nostro prodotto

Fornitura di servizi professionali

Distribuzione del prodotto, implementazione dei primi casi di utilizzo

Formazione

Programmi di formazione e certificazione approfonditi

Servizi operativi dal secondo giorno

Manutenzione ed espansione delle risorse, le etichette e le policy esistenti

Analisi dell'approccio alla sicurezza e dell'IR, preparazione alle verifiche, sviluppo personalizzato e integrazione

Technical Account Manager/Resident Engineer

Servizi di assistenza ai clienti
Servizi di assistenza tecnica: supporto 24 ore su 24, 7 giorni su 7, con tecnico dedicato

Fornitura di servizi professionali

Un team completo composto da architetti della sicurezza, project manager e sviluppatori collaborerà con il vostro team per implementare la piattaforma di segmentazione Akamai Guardicore. A seconda delle vostre esigenze, Akamai offre un insieme di prodotti preconfezionati o un tecnico dell'implementazione a tempo determinato. Indipendentemente dal pacchetto scelto, le nostre offerte di servizi sono personalizzate per garantire la protezione delle vostre risorse critiche.

Jumpstart

Jumpstart è progettato per i clienti che necessitano di accelerare l'implementazione di Akamai Guardicore Segmentation ma preferiscono implementare e gestire autonomamente le policy successive con la guida dei nostri esperti. Sia che desideriate segmentare il vostro ambiente di rete, delimitare le applicazioni o limitare l'accesso ai server, i nostri ingegneri progetteranno e implementeranno il vostro primo obiettivo di policy, formandovi lungo il percorso e fornendovi indicazioni mentre implementate autonomamente le policy successive.

Il nostro team lavorerà inoltre assieme a voi per pianificare l'architettura di sicurezza e comprendere eventuali complessità relative alla progettazione dell'applicazione. Ciò include la definizione e la documentazione della strategia di etichettatura, l'etichettatura delle risorse nella piattaforma e la creazione e l'ottimizzazione formale delle politiche per supportare i casi d'uso.

Dopo che Akamai avrà completato la prima implementazione delle policy, i nostri ingegneri continueranno a fornire al vostro team assistenza diretta per eventuali future implementazioni delle policy e rimarranno parte del vostro team esteso fino al raggiungimento degli obiettivi di implementazione.

Extended Jumpstart

Per le aziende con molteplici obiettivi di segmentazione da raggiungere, Extended Jumpstart è l'ideale. Gli esperti Akamai collaboreranno con i vostri team per implementare molteplici policy di segmentazione, aumentando la protezione delle vostre risorse critiche e di punta.

Il nostro team lavorerà assieme a voi per pianificare l'architettura di sicurezza e comprendere eventuali complessità relative alla progettazione dell'applicazione. Ciò include la definizione e la documentazione della strategia di etichettatura, l'etichettatura delle risorse nella piattaforma e la creazione e l'ottimizzazione formale delle policy per supportare molteplici iniziative di sicurezza.

Obiettivi di policy tipici da implementare

Sia che desideriate segmentare il vostro ambiente di rete, delimitare le applicazioni o limitare l'accesso ai server, i nostri ingegneri lavoreranno con voi in ogni fase del percorso per garantire la protezione delle vostre risorse.

Nell'ambito di questa offerta potete selezionare più obiettivi di policy o concentrarvi su un obiettivo specifico ad alta priorità. I nostri ingegneri implementeranno le etichette e le regole richieste che formano le nostre policy fino a quando le vostre risorse non potranno avvalersi di una protezione in linea con i vostri obiettivi pre-identificati.

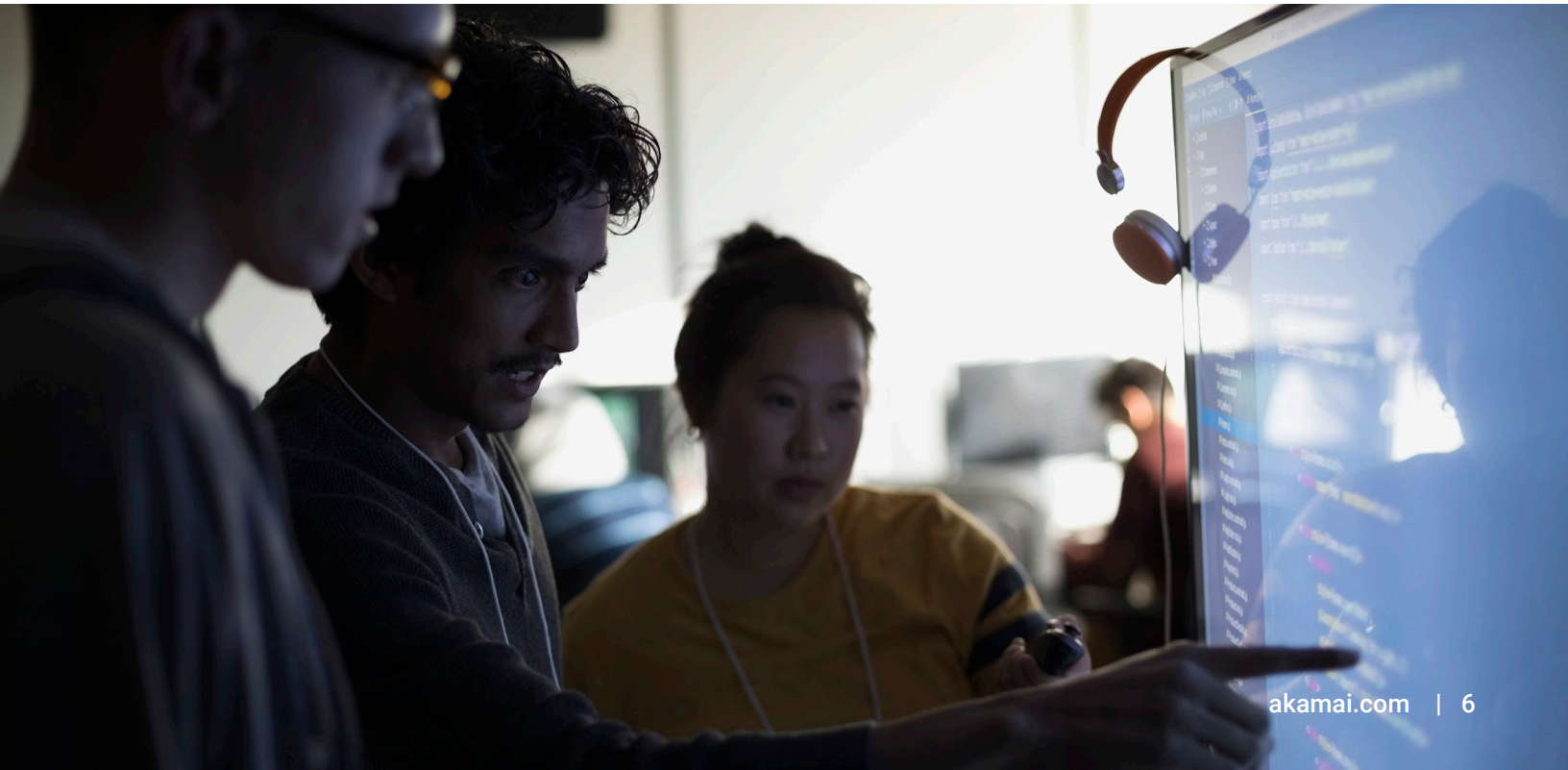
Alcuni esempi includono

- **Segmentazione dell'ambiente**: ai server di ambienti diversi non sarà consentito comunicare, ad eccezione delle comunicazioni esplicitamente consentite.
- **Isolamento delle applicazioni**: le applicazioni critiche devono comunicare solo con le parti esplicitamente autorizzate. Saranno consentite le comunicazioni delle applicazioni interne.
- **Microsegmentazione delle applicazioni**: il traffico interno ed esterno delle applicazioni critiche sarà consentito solo se esplicitamente approvato (Zero Trust).
- **Segmentazione degli endpoint "al di fuori dell'azienda"**: la superficie di attacco di un endpoint esterno alla protezione di una rete aziendale sarà limitata. Akamai Guardicore Segmentation abilita diversi set di regole all'interno e all'esterno della rete aziendale.
- **Accesso ai server basato sui privilegi**: è possibile implementare policy di controllo dell'accesso ai server, ad esempio, per limitare le porte di gestione solo ai jumpbox o per impedire l'accesso a server specifici in base all'identità dell'utente dell'origine.
- **Applicazione di best practice per la sicurezza**: le regole dell'elenco di blocco verranno implementate per applicare le migliori pratiche di sicurezza della rete.

Tecnico dell'implementazione

Quando un'impresa richiede un numero significativo di obiettivi di policy, per garantire un'implementazione di successo, spesso è preferibile collaborare con un tecnico assegnato per un periodo prestabilito senza limiti al numero di policy che il nostro tecnico può creare. Consentire ad Akamai di fornire il supporto di implementazione necessario per raggiungere i vostri obiettivi è l'ideale quando la vostra rete necessita di una segmentazione end-to-end completa.

	Jumpstart	Extended Jumpstart	Tecnico dell'implementazione
Installazione	✔	✔	✔
Installazione dello schema di etichettatura	✔ Limitata	✔ ✔ ✔	Risorse di implementazione complete per un periodo stabilito, senza alcuna limitazione sui casi di utilizzo, garantendo il raggiungimento degli obiettivi
Guida all'approccio generale alla sicurezza	✔ Limitata	✔ ✔ ✔	
Guida alla creazione di policy	✔ Limitata	✔ ✔ ✔	
Implementazione di casi di utilizzo di policy	**Una policy**	**Più policy**	
Formazione per l'utente finale	✔	✔	✔
Durata tipica	**6 mesi**	**12 mesi**	**6 - 18 mesi**
Quando scegliere una determinata opzione	Il cliente o il partner preferisce implementare principalmente in sede; Akamai implementa solo il primo caso di utilizzo	Akamai implementa molteplici casi di utilizzo e diverse policy, fornendo un'assistenza estesa	Il cliente o il partner desidera un'implementazione completa (molteplici casi di utilizzo), preferisce esplorare e definire esattamente tutto durante l'intero periodo



Formazione Akamai

La formazione sulla certificazione Akamai per la microsegmentazione fornisce agli amministratori (GCSA) e agli ingegneri operativi (GCSE) le competenze e le informazioni necessarie per svolgere con successo le attività amministrative e di manutenzione correlate.

I metodi di formazione sono versatili per soddisfare le esigenze di clienti e partner: dalla formazione online di base alla formazione di certificazione con istruttore e persino alla formazione privata dedicata (virtuale o di persona).

GCSA (Guardicore Certified Segmentation Administrator)

Il nostro programma di cinque mezze giornate fornisce agli utenti della piattaforma Akamai Guardicore Segmentation le competenze necessarie per gestire con successo tutti gli aspetti della piattaforma. I diplomati GCSA acquisiranno la sicurezza necessaria per utilizzare autonomamente la piattaforma al fine di implementare e gestire le esigenze di sicurezza della propria organizzazione.

Il corso comprende il set di funzionalità principali di Akamai Guardicore Segmentation: visibilità, etichettatura, microsegmentazione e rilevamento delle violazioni. L'attenzione si concentra principalmente sul comportamento e sull'utilizzo delle funzionalità e il corso guiderà gli studenti dalla configurazione iniziale di Akamai Guardicore Segmentation fino alle operazioni quotidiane più comuni.

GCSE (Guardicore Certified Segmentation Engineer)

Il nostro programma di tre mezze giornate fornisce ai proprietari operativi del sistema le competenze e le conoscenze necessarie per eseguire attività amministrative e di manutenzione relative alla piattaforma.

I diplomati del GCSE saranno in grado di gestire il funzionamento complessivo dell'ambiente Akamai Guardicore Segmentation. Il corso tratta i seguenti argomenti: configurazione della piattaforma e dei componenti, integrazione con strumenti di terze parti, controllo dell'integrità della piattaforma, risoluzione dei problemi e attività di manutenzione comuni.

Entrambi i corsi sono integrati da un laboratorio pratico online disponibile per tutti gli studenti per tutta la durata del corso. Alla fine di ogni corso è previsto un esame di certificazione.

Supporto aziendale e successo dei clienti

Il nostro programma di supporto aziendale è progettato per supportare tutte le possibili conseguenze dell'utilizzo della microsegmentazione Akamai Guardicore nella vostra organizzazione. Il nostro team di supporto sarà disponibile 24 ore su 24, 7 giorni su 7, 365 giorni all'anno, gestirà qualsiasi problema che riscontrate e vi assisterà con aggiornamenti e correzioni.

Il nostro programma Customer Success vi aiuta a raggiungere gli obiettivi di sicurezza a breve e lungo termine della vostra organizzazione, massimizzando al tempo stesso il valore dell'investimento effettuato nella nostra piattaforma.

Supporto Elite

Il supporto Elite di Akamai fornisce alla vostra organizzazione l'accesso prioritario a esperti di escalation designati, competenti e di alto livello. Uno specialista altamente qualificato, che conosca il vostro data center e i processi interni, sarà il vostro unico punto di contatto e vi aiuterà ad accelerare la risposta e la risoluzione di qualsiasi problema e a massimizzare l'investimento nella segmentazione basata su software.

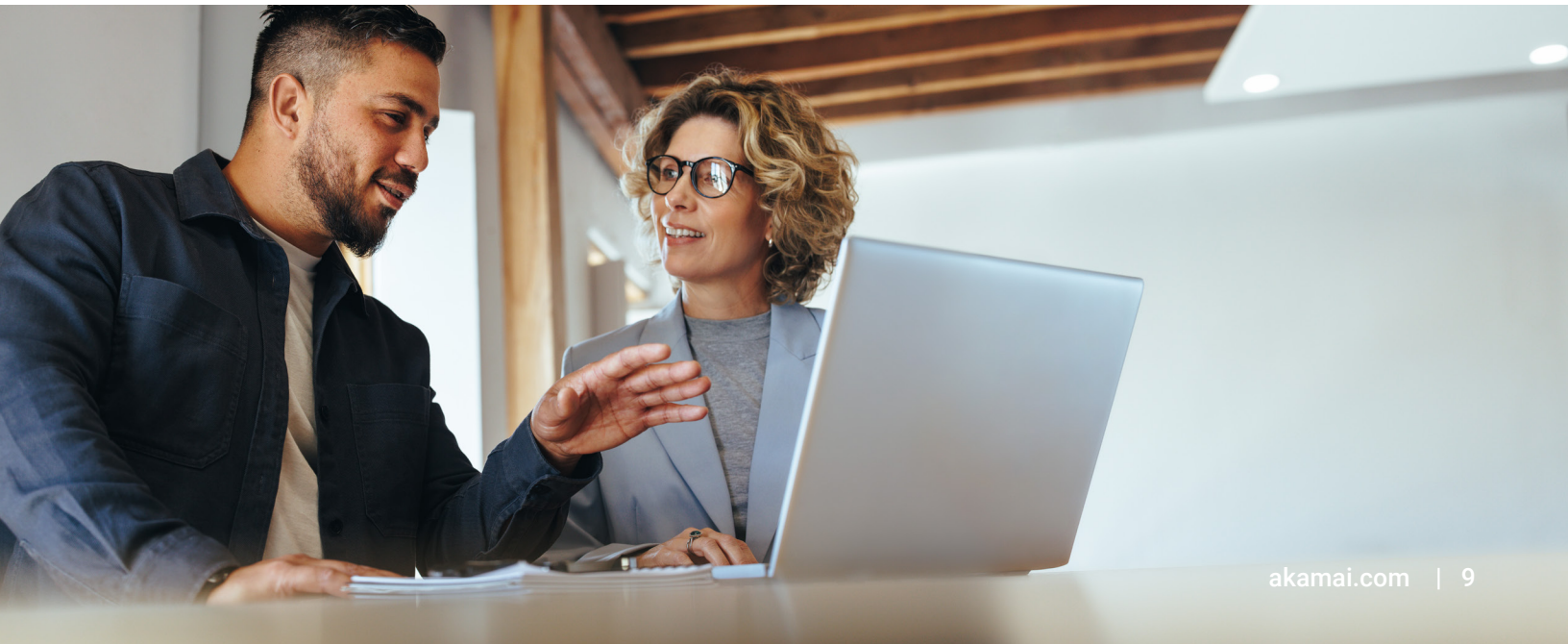
	Premium	Elite
Disponibilità del supporto	**24 ore su 24/7 giorni su 7/365 giorni all'anno**	**24 ore su 24/7 giorni su 7/365 giorni all'anno**
Casi illimitati	✔	✔
Aggiornamenti e correzioni	✔	✔
Telefono, e-mail, Slack e portale	✔	✔
Analisi delle cause principali (su richiesta)	**Gravità 1**	**Gravità 1 e Gravità 2**
Gestione degli interventi prioritari da parte di un esperto designato		✔ Ingegnere designato disponibile durante l'orario lavorativo
Monitoraggio dell'integrità del sistema proattivo e in tempo reale		✔
Ottimizzazione personalizzata		✔ Sessione di ottimizzazione trimestrale
Analisi dei problemi e rapporto di suppor to periodici		✔ Analisi dei problemi settimanale; rapporto di supporto mensile
Giorni di consulenza		✔ 2, 4 o 6 giorni di consulenza all'anno, a seconda delle dimensioni (SKU)
Quando scegliere una determinata opzione	Distribuzione più piccola; necessita quasi sempre di supporto	Distribuzione più grande; richiede un controllo più elevato dei problemi continui

Servizi operativi dal secondo giorno

Dopo aver implementato i primi casi di utilizzo, i clienti cominciano a sfruttare i vantaggi del prodotto Akamai Guardicore Segmentation. Tuttavia, sono necessari manutenzione e aggiornamenti continui per massimizzare il valore che si può ottenere dal nostro prodotto:

- Aggiornamento dell'implementazione (risorse, etichette, policy) per riflettere i cambiamenti dell'organizzazione non appena si verificano
- Implementazione di ulteriori casi di utilizzo che non sono stati gestiti durante la fase di implementazione iniziale (nuovi casi d'uso identificati ora che utilizzate il nostro prodotto, ulteriori servizi e/o applicazioni da gestire, ecc.)
- Implementazione di Akamai Guardicore Segmentation in altri reparti dell'organizzazione, ad esempio reti e applicazioni basate su cloud. (nuove o semplicemente quelle lasciate per la fase 2)
- Distribuzione su altri endpoint, dispositivi IoT (Internet of Things), ambienti di infrastruttura desktop virtuale, ecc.
- Utilizzo di Akamai Guardicore Segmentation per identificare e mitigare gli eventi di sicurezza (ad esempio, bloccare i movimenti laterali nella rete); potete collegare il vostro ambiente al SOCC (Security Operations Command Center) di Akamai e ottenere un monitoraggio 24/7/365 e avvisi e mitigazioni in tempo reale
- Raggiungimento di una sicurezza potenziata e proattiva tramite Akamai Hunt, Akamai Edge DNS (per un DNS sicuro e una protezione contro gli attacchi attacchi DDoS (Distributed Denial-of-Service) e Akamai Enterprise Application Access (per la gestione degli accessi e delle identità)
- Utilizzo di Akamai Guardicore Segmentation per assistervi nelle verifiche di certificazione

Questi servizi devono essere forniti da partner certificati GcSP



Technical Account Manager e Resident Engineer

I Technical Account Manager e i Resident Engineer di Akamai sono consulenti tecnici senior per le aziende con esigenze di segmentazione ampie e potenzialmente complesse. Una volta inseriti nella vostra organizzazione, i nostri ingegneri diventano rapidamente esperti del vostro ambiente, consentendovi di ottenere un successo superiore con Akamai Guardicore Segmentation.

Il Resident Engineer* assegnato al vostro account si integrerà nei vostri team e supporterà in modo proattivo tutte le vostre operazioni per assicurarvi di ottenere sempre il massimo valore da Akamai Guardicore Segmentation.

Il Resident Engineer può garantivi il successo guidandovi nelle decisioni sulle policy, informandovi sulle ultime funzionalità in arrivo nel nostro prodotto, pianificando (e assistendo nell'esecuzione di) un aggiornamento ed eseguendo analisi aziendali di livello dirigenziale.

Il vostro Technical Account Manager o Resident Engineer può anche supervisionare ed eseguire i vostri servizi operativi dal secondo giorno.

**Il Resident Engineer può collaborare da remoto*

Akamai Hunt: un servizio gestito di rilevamento delle minacce

Akamai Hunt, un'estensione di Akamai Guardicore Segmentation, è il nostro servizio di rilevamento delle minacce gestito che può aiutarvi a stare al passo con le minacce più elusive e a proteggere meglio la vostra organizzazione.

Il team di Akamai Hunt cerca continuamente comportamenti di attacco anomali e minacce avanzate che aggirano costantemente anche le soluzioni di sicurezza più all'avanguardia. Con Hunt, ricevete immediatamente una notifica su qualsiasi incidente critico rilevato sulla vostra rete e i nostri esperti lavoreranno a stretto contatto con il vostro team per rimediare a qualsiasi risorsa compromessa con una risoluzione rapida.

Che siate concentrati sul rilevamento e sulla prevenzione del ransomware, sulla difesa da minacce persistenti avanzate, sulla protezione dalle vulnerabilità zero-day o sul miglioramento della sicurezza IT generale, Akamai Hunt vi consente di ottenere il massimo valore in termini di sicurezza dalla vostra implementazione di Akamai Guardicore Segmentation senza software aggiuntivo, implementazioni di agenti o aggiornamenti.

Akamai Hunt include:

Analisi di esperti 24 ore su 24, 7 giorni su 7: i nostri professionisti della sicurezza informatica provengono da una vasta gamma di campi, tra cui i settori di ricerca sulla sicurezza, sicurezza offensiva, intelligence militare, red team, risposta agli incidenti e data science.

Avvisi su minacce reali: per evitare i falsi allarmi, il team di Hunt avverte i propri clienti solo in caso di minacce reali, eliminando i falsi positivi.

Strumenti di rilevamento proprietari: gli esperti di Hunt sviluppano regolarmente algoritmi avanzati di ricerca delle minacce, come anomalie delle attività degli utenti e della rete, analisi eseguibili, analisi dei registri e molto altro, per creare un potente set di strumenti per un rilevamento e una risposta rapidi. Akamai Guardicore Insight, un potente strumento basato su OS query per eseguire query di endpoint e server in tempo reale, è incluso nel servizio senza costi aggiuntivi.

Intelligence sulle minacce completa di contesto: il nostro team di addetti alla sicurezza raccoglie indicatori di compromissione che vanno da IP e domini a processi, utenti e servizi, sfruttando Akamai Guardicore Segmentation e la notevole intelligence globale sulle minacce di Akamai.

Visibilità di rete, cloud ed endpoint : questa combinazione di dati generati dall'implementazione di Akamai Guardicore Segmentation e dai sensori globali di Akamai (inclusi più di 7 mila miliardi di richieste DNS al giorno) fornisce al nostro team la visibilità più completa del vostro ambiente.

Notifiche immediate e informazioni proattive:

- Invio immediato di e-mail di notifica dopo il rilevamento di una minaccia
- Rapporti sulle minacce a livello dirigenziale periodici con analisi, statistiche e metriche per tenere informati i dirigenti o il consiglio di amministrazione sulle campagne di attacco di alto profilo
- Gestione degli incidenti facilitata grazie all'integrazione della console di Akamai Guardicore Segmentation

Per ulteriori informazioni su Akamai Guardicore Segmentation, visitate la pagina akamai.com