مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

# میکروسگمنتیشن برای مراکز داده مدرن (Microsegmentation for Modern Data Centers)

از امنیت سنتی تا حفاظت Zero Trust برای Workloadها

## مروری بر دوره

با گسترش مراکز داده مدرن، محیط‌های Hybrid Cloud، Multi-Cloud و افزایش تهدیدات سایبری مانند **Ransomware**، مدل‌های سنتی امنیت شبکه دیگر پاسخگوی نیاز سازمان‌ها نیستند. مهاجمان پس از نفوذ اولیه، از طریق ارتباطات داخلی و مسیرهای مورد اعتماد اقدام به حرکت جانبی (**Lateral Movement**) کرده و به سامانه‌های حیاتی دسترسی پیدا می‌کنند. میکروسگمنتیشن به عنوان یکی از مهم‌ترین ارکان معماری **Zero Trust**، امکان کنترل دقیق ارتباطات بین **Workload**ها و کاهش سطح حمله را فراهم می‌سازد.

این دوره تخصصی با رویکردی کاملاً عملی و مبتنی بر نیازهای واقعی سازمان‌های **Enterprise** طراحی شده است و شرکت‌کنندگان را با مفاهیم، معماری‌ها، فناوری‌ها و فرآیندهای پیاده‌سازی میکروسگمنتیشن در مراکز داده مدرن، محیط‌های ابری و زیرساخت‌های مجازی آشنا می‌کند.

در طول دوره، فراگیران ضمن آشنایی با راهکارهای مطرح جهانی نظیر Cisco Secure Workload، VMware NSX، Illumio، Akamai **Guardicore** و راهکارهای **Cloud-Native**، نحوه تحلیل معماری موجود، کشف وابستگی‌های برنامه‌ها، طراحی **Policy**های مبتنی بر **Least Privilege**، پیاده‌سازی کنترل‌های **Zero Trust** و مدیریت عملیاتی و حاکمیتی این راهکارها را فرا خواهند گرفت.

## آنچه در این دوره خواهید آموخت

تحلیل معماری مراکز داده و شناسایی نقاط ضعف امنیتی

خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ - ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

شناسایی و کنترل مسیرهای حرکت جانبی مهاجمان طراحی معماری **Zero Trust** برای **Workload**ها
ایجاد Application Dependency Map طراحی **Policy**های مبتنی بر **Least Privilege**
انتخاب فناوری مناسب میکروسگمنتیشن برای هر محیط پیاده‌سازی و استقرار تدریجی **Policy**ها
مدیریت عملیات و حاکمیت امنیتی میکروسگمنتیشن ارزیابی و کاهش **Blast Radius** حملات
تدوین نقشه راه سازمانی برای Zero Trust

## سرفصل ها

### جلسه اول: معماری امنیتی مراکز داده مدرن

تکامل مراکز داده **North-South** و **East-West Traffic**
معماری **Overlay** Spine-Leaf و **Underlay Networks**
مدل‌های سنتی امنیت ارزیابی امنیت مراکز داده

### جلسه دوم: تهدیدات نوین سایبری

چرخه حملات سایبری **Credential Theft**
Living Off The Land عملیات **Ransomware**
ریسک‌های Identity و Management Plane **Threat Modeling**

### جلسه سوم: حرکت جانبی مهاجمان (**Lateral Movement**)

Discovery و Scanning تهدیدات RDP، SMB و **SSH**
Credential Reuse **Privilege Escalation**
Blast Radius Analysis تکنیک‌های **Containment**

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

### جلسه چهارم: مبانی میکروسگمنتیشن

مفاهیم و معماری Microsegmentation **Workload-Centric Security**
Policy Enforcement Points **Allow-List Models**
Identity-Based Policies **Zero Trust Principles** و Tagging

### جلسه پنجم: دیدپذیری و **Application Dependency Mapping**

جمع‌آوری و تحلیل Flowها **Dependency Mapping**
طبقه‌بندی ترافیک شناسایی ارتباطات پرریسک
طراحی Baseline

### جلسه ششم: معماری‌ها و فناوری‌های میکروسگمنتیشن

**Agent-Based Enforcement**
Hypervisor-Based Security **Fabric Integration**
Cloud Security Controls **Kubernetes Security Policies**
مقایسه فناوری‌های مطرح بازار

### جلسه هفتم: طراحی و پیاده‌سازی Policy

ساختار **Policy**ها
Naming Standards **Tagging Strategy**
Ring-Based Rollout **Simulation & Test Mode**
Exception Handling

خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

### جلسه هشتم: عملیات، حاکمیت و انطباق

مدل عملیاتی

Change Management **Monitoring & Alerting**

Compliance & Audit **SOC Integration**

Governance Framework

### جلسه نهم: نقشه راه سازمانی و آینده میکروسگمنتیشن

**Adoption Strategy**

Maturity Models **Pilot Planning**

Enterprise Rollout **Cloud & Container Expansion**

Future Trends

## مخاطبان دوره

مهندسین شبکه (**Network Engineers**)

مهندسین امنیت (Security Engineers) مهندسین مراکز داده (**Data Center Engineers**)

معماران امنیت (Security Architects) معماران زیرساخت (**Infrastructure Architects**)

مهندسین Cloud کارشناسان **SOC**

مدیران فناوری اطلاعات (IT Managers) مدیران امنیت اطلاعات

مشاوران امنیت و مراکز داده

## پیش نیاز ها

آشنایی با مفاهیم **TCP/IP** و شبکه‌های **Enterprise**

آشنایی با VLAN، Switching، Routing و ACL

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

آشنایی با **Firewall**ها و مفاهیم امنیت شبکه

آشنایی اولیه با Virtualization و Cloud Computing

آشنایی با مفاهیم پایه امنیت اطلاعات و Incident Response

* نیاز به دانش قبلی در محصولات Microsegmentation وجود ندارد