

# 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

و راهکارهای **Guardicore** و **Cloud-Native**، نحوه

تحلیل معماری موجود، کشف وابستگی‌های برنامه‌ها، طراحی **Policy**های مبتنی بر **Least Privilege**، پیاده‌سازی کنترل‌ها و **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



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 **Spine-Leaf Overlay** و **Underlay Networks**

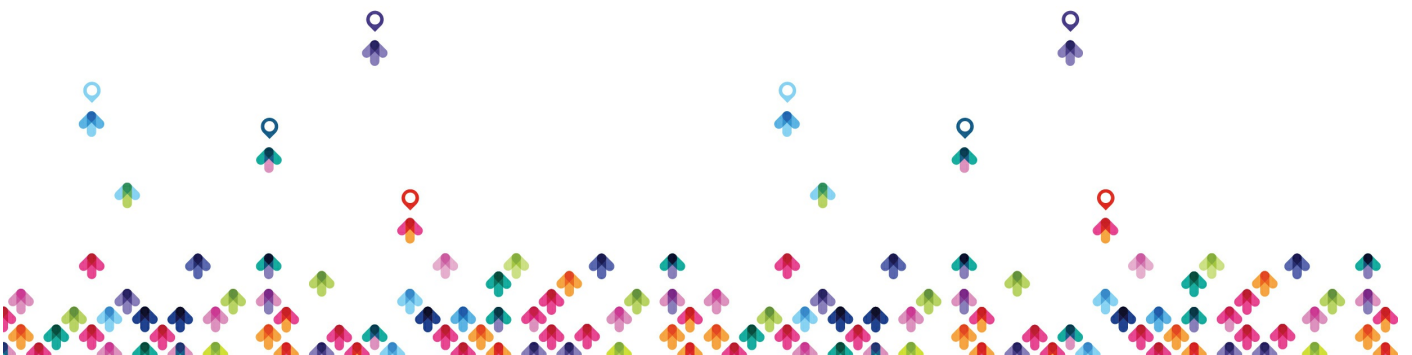
مدل‌های سنتی امنیتی ارزیابی امنیت مراکز داده

### جلسه دوم: تهدیدات نوین سایبری

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

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

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



### 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**

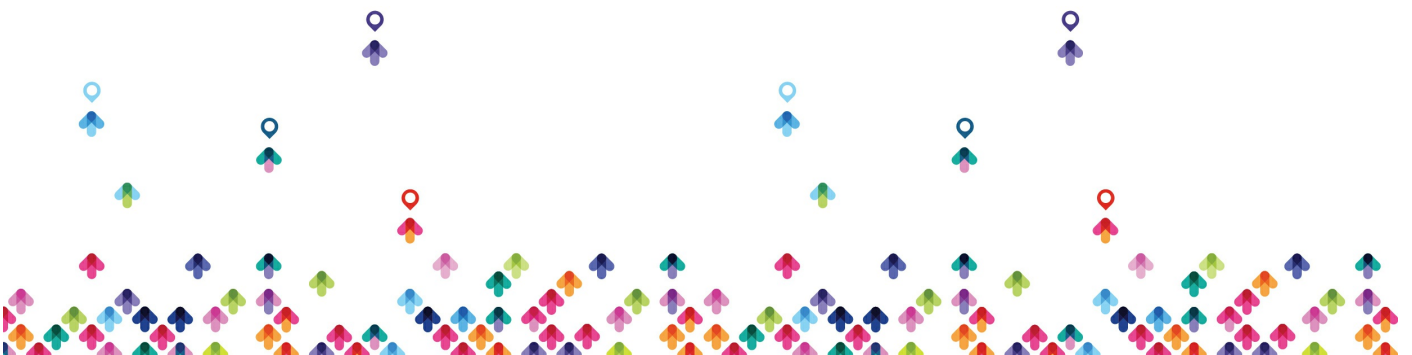
جمع‌آوری و تحلیل **Flow**ها **Dependency Mapping**  
طبقه‌بندی ترافیک شناسایی ارتباطات پرریسک  
طراحی **Baseline**

### 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



### 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

مهندسين شبکه (Network Engineers)

مهندسين امنيت (Security Engineers) مهندسين مراکز داده (Data Center)

(Engineers)

معماران امنيت (Security Architects) معماران زیرساخت (Infrastructure Architects)

مهندسين Cloud کارشناسان SOC

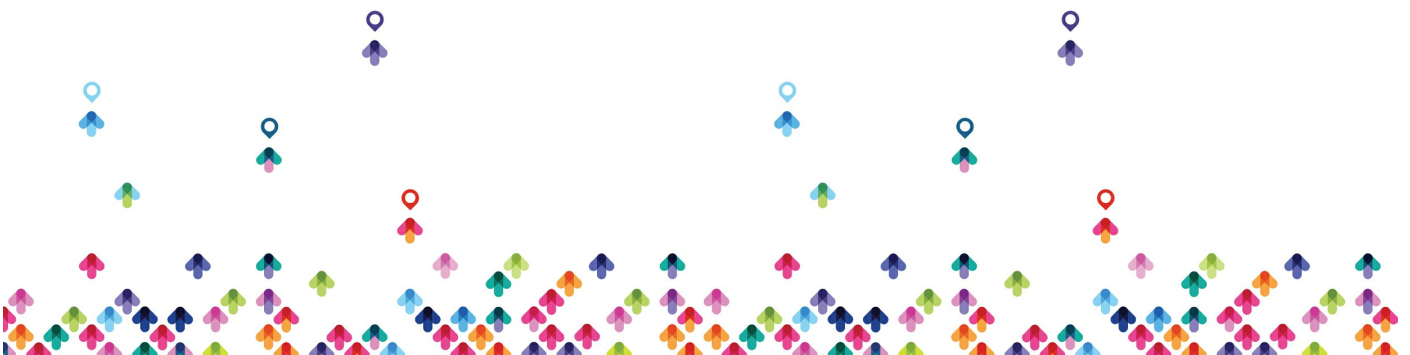
مدیران فناوری اطلاعات (IT Managers) مدیران امنیت اطلاعات

مشاوران امنیت و مراکز داده

پیش نیازها

آشنایی با مفاهیم TCP/IP و شبکه‌های Enterprise

آشنایی با Routing، Switching، VLAN و ACL



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

