چک‌لیست ممیزی امنیت شبکه سازمانی

- **Perimeter Security مرز شبکه**

☐آیاRule های فایروال بر اساس deny all by default هستند؟

☐آیا فقط پورت‌های ضروری باز هستند؟

☐آیا VPN با MFA محافظت می‌شود؟

☐آیا WAF برای سرویس‌های وب فعال است؟

☐آیا IDS/IPS فعال و به‌روز است؟

☐آیا Geo-IP Filtering پیاده‌سازی شده؟

☐ آیا لاگ‌های فایروال مانیتور می‌شوند ؟

DMZ Security

☐آیا DMZ از شبکه داخلی کامل جدا شده؟

☐آیا دسترسی DMZ به داخل محدود شده؟

☐آیا Reverse Proxy استفاده شده؟

☐آیا سرورهای DMZ Hardening شده‌اند؟

☐ آیا لاگ‌گیری کامل فعال است؟

Core Layer Security

☐آیا Routing Protocol Authentication فعال است؟

☐آیا Control Plane Protection (CoPP) فعال است؟

☐آیا ICMP و Broadcast محدود شده‌اند؟

☐ آیا NetFlow یا مانیتورینگ ترافیک فعال است ؟

Distribution Layer (Segmentation)

☐آیاVLAN ها بر اساس Role طراحی شده‌اند؟

☐آیا ACL بینVLAN ها تعریف شده؟

☐آیا دسترسی بینVLAN ها محدود است؟

☐آیا DTP غیرفعال است؟

☐ آیا Private VLAN استفاده شده ؟

Access Layerکاربران

☐آیا 802.1 Xفعال است؟

☐آیا Port Security تنظیم شده؟

☐آیا DHCP Snooping فعال است؟

☐آیا Dynamic ARP Inspection فعال است؟

☐ آیا دستگاه‌های ناشناس بلاک می‌شوند؟

Endpoint Security

☐آیا EDR/XDR روی سیستم‌ها نصب است؟

☐آیا سیستم‌ها Patch به‌روز دارند؟

☐آیا آنتی‌ویروس فعال و آپدیت است؟

☐آیا USB و Device Control محدود شده؟

☐ آیا Firewall سیستم‌عامل فعال است؟

Data Center / Server Security

☐آیا سرورها Segmentation شده‌اند؟

☐آیا دسترسی Admin محدود شده؟

☐آیا Backup به‌صورت آفلاین نگهداری می‌شود؟

☐آیا Application Whitelisting وجود دارد؟

☐ آیا لاگ سرورها مانیتور می‌شود؟

Identity & Access Management

☐آیا MFA برای کاربران و Admin فعال است؟

☐آیا اصل Least Privilege رعایت شده؟

☐آیا حساب Admin جدا از User است؟

☐آیا Password Policy قوی است؟

☐آیا حساب‌های غیرفعال حذف شده‌اند؟

☐آیا WPA3 یا حداقل WPA2-Enterprise استفاده می‌شود؟

☐آیا VLAN مهمان جدا شده؟

☐آیا NAC پیاده‌سازی شده؟

☐ آیا Rogue AP Detection فعال است؟

Monitoring & Logging

☐آیا SIEM پیاده‌سازی شده؟

☐آیا لاگ‌ها متمرکز جمع‌آوری می‌شوند؟

☐آیاAlert های امنیتی تعریف شده؟

☐آیا Incident Response Plan وجود دارد؟

☐ آیا مانیتورینگ 7/24 انجام می‌شود؟

سیاست‌ها و فرآیندها (خیلی مهم در پروژه)

☐آیا Policy امنیتی مستند وجود دارد؟

☐آیا Backup Policy تعریف شده؟

☐آیا Disaster Recovery Plan وجود دارد؟

☐آیا آموزش امنیت برای کارکنان انجام شده؟

☐ آیا تست نفوذ دوره‌ای انجام می‌شود؟

🎯سطح امنیت:

80٪ تا 100٪ → □ خوب(Secure)

60٪ تا 80٪ → □ متوسط(Need Improvement)

کمتر از 60٪ → ● پرریسک (High Risk)