Batuhan YAZICI



Senior Cyber Security Specialist

Finansal hizmetler / Altyapı ve siber güvenlik

ahmet@batuhanyazici.com batuhanyazici.com LinkedIn / batuhanyazici
İstanbul, Türkiye

Profesyonel profil

Finansal hizmetler ve elektronik ödeme sektöründe, kurumsal BT altyapılarının tasarımı, işletimi ve güvenliğinde 7 yılı aşkın deneyime sahip Senior Cyber Security Specialist. Siber güvenlik operasyonları, altyapı ve ağ güvenliği, güvenlik mimarisi ve düzenleyici uyum alanlarında çalışıyorum. Fortinet ve SIEM başta olmak üzere güvenlik platformlarını yönetiyor; risk değerlendirmesi, olay müdahalesi ve sürekli iyileştirme ile kritik hizmetlerin güvenliğini ve sürekliliğini destekliyorum. Sistem yönetimi geçmişim, güvenlik kontrollerini uygulama ve altyapı bağımlılıklarıyla birlikte değerlendirmemi sağlıyor.

Odak alanları Güvenlik operasyonları · Olay müdahalesi ve tehdit avcılığı · Zafiyet yönetimi · Fortinet · SIEM · DLP / WAF / VPN · Active Directory · Windows / Linux · VMware vSphere · PCI DSS / ISO 27001

Profesyonel deneyim

BPN Ödeme & E-Para Hizmetleri

Haziran 2019 - Devam ediyor | İstanbul

Senior Cyber Security Specialist

Ağustos 2026 - Devam ediyor

- **Güvenlik mimarisi ve ürün yaşam döngüsü:** Güvenlik çözümlerinin planlanması, kurulumu, entegrasyonu ve politika yönetimi; PoC değerlendirmeleri, üretici koordinasyonu ve mimari dokümantasyon.
- **Fortinet ve ağ güvenliği:** FortiGate, FortiAnalyzer ve FortiLogger yönetimi; HA, SD-WAN, statik/dinamik yönlendirme, NAT/VIP, IPS/IDS, SSL Inspection, Application Control, Web Filter ve DNS Security.
- **Güvenli bağlantı ve erişim:** Finans kuruluşları ve üçüncü taraflarla IPSec VPN; uzak kullanıcılar için SSL VPN, kullanıcı yetkilendirmesi ve erişim politikaları. Cisco, Aruba ve HP ağlarında VLAN, ACL ve NAC kontrolleri.
- **SIEM ve tehdit izleme:** Merkezi günlük toplama, korelasyon kuralları ve alarm mekanizmalarının geliştirilmesi; FortiAnalyzer, FortiLogger ve SIEM üzerinden anomali analizi, izleme ve raporlama.
- **Incident Response ve Threat Hunting:** Olay korelasyonu, IOC değerlendirmesi, kök neden analizi (RCA), zararlı yazılım ve bulaşma senaryolarının incelenmesi; siber güvenlik olaylarına L3 teknik destek.
- **Veri kaybı önleme:** DLP ve veri sınıflandırma politikaları; USB, yazıcı, e-posta, web yüklemeleri, dosya transferi ve pano kanallarındaki veri hareketlerinin kontrolü.
- **Uç nokta ve veri tabanı güvenliği:** Trellix/McAfee ePO, Endpoint Security, SIEM, DLP ve Database Security yönetimi; Application/Device Control ile SQL Server ve PostgreSQL güvenlik politikaları.
- **Uygulama güvenliği ve erişilebilirlik:** F5 üzerinde Node, Pool, yük dengeleme ve Health Monitoring; Cloudflare DNS/WAF yönetimi, güvenli uygulama yayını ve güvenlik politikalarının işletilmesi.
- **Vulnerability Management:** Nessus bulgularının analizi, risk önceliklendirmesi ve düzeltme takibi; sızma testi koordinasyonu, kritik CVE etkilerinin değerlendirilmesi ve yama yönetimi.
- **Kimlik güvenliği ve Hardening:** Active Directory, GPO, parola ve PAM politikaları; ayrıcalıklı hesap güvenliği, Windows/Linux sunucuları ve ağ cihazlarında güvenlik sıkılaştırma.
- **SSL/TLS yaşam döngüsü:** CSR ve wildcard sertifika işlemleri; yenileme, üretim sistemlerine dağıtım, süre takibi ve güvenli servis sürekliliğinin yönetimi.
- **Teknik uyum ve risk yönetimi:** TCMB, KVKK, PCI DSS ve ISO/IEC 27001 kontrolleri; iç/dış denetim desteği, bulgu kapatma, teknik aksiyon planları ve güvenlik farkındalık eğitimleri.

Batuhan YAZICI

Senior Cyber Security Specialist

batuhanyazici.com

Sistem ve ağ yönetimi deneyimi

BPN Ödeme & E-Para Hizmetleri

Senior System and Network Administrator

Temmuz 2025 - Ağustos 2026

Kurumsal sistemlerin, sanallaştırma ve ağ altyapısının işletilmesi; kritik iş uygulamalarının sürekliliği, teknik sorunların çözümü ve güvenlik kontrollerinin altyapıya uygulanması.

- **VMware vSphere ve sanal sunucular:** Sanallaştırma altyapısının yönetimi; sanal sunucuların ve üzerlerinde çalışan uygulamaların sistem ve hizmet bazında izlenmesi, yönetimi ve denetimi.
- **Microsoft Active Directory:** Etki alanı yapısı, kullanıcı ve grup yönetimi; erişim yetkileri, parola ve Group Policy yapılandırmaları ile etki alanı kullanıcılarına teknik destek.
- **Windows Server hizmetleri:** DNS, DHCP, IIS ve WSUS rollerinin kurulumu ve yönetimi; ad çözümleme, adres dağıtımı, uygulama yayını ve güncelleme hizmetlerinin takibi.
- **Linux sunucu yönetimi:** Ubuntu, CentOS, Red Hat ve Rocky Linux üzerinde uygulama ve web sunucularının kurulumu, yapılandırılması, işletimi ve teknik sorunlarının giderilmesi.
- **LAN/WAN operasyonları:** Kurumsal ağ cihazlarının yönetimi ve izlenmesi; bağlantı, erişim ve iletişim sorunlarının sunucu ve uygulama bağımlılıklarıyla birlikte incelenmesi.
- **Yedekleme ve kurtarma hazırlığı:** Yedekleme prosedürlerinin hazırlanması, uygulanması ve düzenli doğrulanması; geri dönüş gereksinimlerinin ve kritik hizmet bağımlılıklarının değerlendirilmesi.
- **Kurumsal depolama:** Depolama sistemlerinin kurulumu ve yönetimi; sunucu ve uygulamaların depolama gereksinimleri, kapasite kullanımı ve erişim sorunlarının takibi.
- **Merkezi izleme:** İzleme sistemlerinin devreye alınması ve yönetimi; sunucu kaynakları, hizmet erişilebilirliği ve alarm takibi. Ubuntu, CentOS ve Windows sistemlerine izleme ajanlarının dağıtımı.
- **Güvenlik platformlarının işletimi:** Trellix/McAfee DLP, Database Security, ePO ve SIEM ürünlerinin yönetimi; sistem, ağ ve bilgi güvenliği bileşenleri arasındaki operasyonel koordinasyon.
- **Denetim ve teknik uyum:** Resmî düzenlemeler kapsamındaki denetimlere destek; PCI DSS ve ISO/IEC 27001 gereksinimlerine uygun güvenlik yapılandırmaları ve teknik kontroller.
- **Uygulama performansı ve sorun giderme:** Veri tabanı yöneticileriyle birlikte performansın izlenmesi; iş uygulamalarının sağlıklı çalışması için sistem, ağ ve veri tabanı katmanlarının birlikte değerlendirilmesi.
- **Teknik ekip desteği:** Sistem ve ağ destek ekibine idari ve teknik destek; karmaşık altyapı sorunlarının incelenmesi ve çözüm süreçlerinin ilgili ekiplerle yürütülmesi.

BPN bünyesindeki önceki pozisyonlar

System and Network Administrator — Ocak 2024 - Temmuz 2025

VMware vSphere ve sanal sunucular; Windows/Linux, Active Directory, DNS, DHCP, IIS ve WSUS; merkezi izleme, depolama, LAN/WAN yönetimi ve teknik sorun giderme.

Junior System and Network Administrator — Şubat 2023 - Ocak 2024

Sunucu ve izleme operasyonları; Ubuntu, CentOS ve Windows ortamlarında ajan dağıtımı.

System and Network Specialist — Haziran 2019 - Şubat 2023

Kurumsal sistem ve ağ altyapısının işletilmesi, izlenmesi ve teknik desteği.

Batuhan YAZICI

Senior Cyber Security Specialist

batuhanyazici.com

Diğer profesyonel deneyimler

Freelance Infrastructure Administrator

Hür Bilişim | Ağustos 2012 - Ekim 2025

- IPv6 altyapılarının planlanması ve ağ geçişleri; OpenVPN/WireGuard ile güvenli uzaktan erişim, sunucu taşıma ve veri merkezi geçiş süreçleri.
- Apache, Nginx ve LiteSpeed web sunucuları; cPanel, CyberPanel ve CWP yönetimi. Cloudflare, LiteSpeed Cache ve Redis ile web erişimi, önbellek ve performans yapılandırmaları.
- Bash, PHP ve Python ile sistem görevlerinin otomasyonu; Rsync/Rclone ile uzak yedekleme ve eşitleme; yedekleme prosedürleri ve hizmet sürekliliğinin takibi.
- Linux/Windows ve ağ cihazlarında zafiyet analizi ve güvenlik sıkılaştırma; Fail2Ban/CSF ile günlük analizi ve erişim kontrolleri. SSL sertifika kurulumu ve otomatik yenileme.
- İhtiyaca uygun altyapı çözümlerinin tasarlanması; proje koordinasyonu, teknik dokümantasyon, olay çözümü ve hizmet desteği.

IT Technician · Türkiye Finans Katılım Bankası · Mart 2018 - Temmuz 2018

IT Specialist · Tevafuk Elektronik · Şubat 2017 - Mart 2018

BT altyapısı, sistem ve kullanıcı desteği.

Teknik yetkinlikler

Ağ ve çevre güvenliği	FortiGate, FortiAnalyzer, FortiLogger; IPS/IDS, VPN, HA, SD-WAN, VLAN, ACL, NAT
Güvenlik operasyonları	SIEM, günlük yönetimi ve korelasyonu, olay müdahalesi, tehdit avcılığı, zafiyet ve yama yönetimi
Veri ve erişim güvenliği	Trellix/McAfee ePO, Endpoint Security, DLP, Database Security; Active Directory, GPO, PAM
Altyapı ve uygulama	VMware vSphere; Windows Server, Linux; DNS, DHCP, IIS, WSUS; F5, Cloudflare WAF, SSL/TLS
İzleme ve otomasyon	PRTG ve merkezi izleme; Bash, PHP, Python; Rsync, Rclone, yedekleme ve kurtarma süreçleri
Teknik uyum	PCI DSS, ISO/IEC 27001, risk değerlendirmesi, denetim bulguları ve güvenlik dokümantasyonu

Eğitim

İstanbul Üniversitesi | Yönetim Bilişim Sistemleri

Lisans | 2021 - Devam ediyor

Sertifikalar ve eğitimler

TÖDEB - Bilgi Sistemleri Tebliği Eğitimi, 2026 ve 2025. 2026 belgesi / 2025 belgesi

Paessler / KAVI - PRTG Network Monitor, webinar katılımı, Aralık 2025.

Cisco - CCNA, Temmuz 2018. **Microsoft** - MCSE, Ekim 2016.

Kariyer Mimarı Bilişim Teknolojileri Akademisi - Grafik ve Web Tasarım, Ağustos 2015.

T.C. Sağlık Bakanlığı - İlkyardımcı Belgesi, Mart 2025 - Mart 2028.

CCNA ve MCSE kayıtları sertifika geçmişidir; güncel geçerlilik iddiası taşımaz.