KoçSistem iz. | SOC

2025 Q2

Sayı 05

SİBER GÜVENLİK BÜLTENİ

MITRE ATT&CK NEDİR?

GÜVENLİ YAPAY ZEKA

BT SERTİFİKASYONLARI

Güvende Kal

Editörün Mesajı

Değerli Okuyucularımız;

2025 yılının ilk yarısını geride bıraktık. Yılın ilk çeyreğinde araladığımız kapıyı tekrar çalıyoruz. Yepyeni içeriklerle ikinci sayımızı sizlerle buluşturmak bizim için büyük bir mutluluk kaynağı.

Bu sayımızda, Mitre ATT&CK çerçevesinin derinliklerinden, Windows sistem analizi detaylarına, yapay zekanın güvenli kullanımından güvenlik odaklı sertifikasyonlara pek çok keyifli içeriği konu olan makalelerimizi okuyacaksınız.

Mitre ATT&CK çerçevesini ele aldığımız makalemizde, çerçevenin temel amaçları ve KoçSistem SOC'deki yerine dair detayları sunduk.

Windows sistem analizi odaklı makalemizde kritik komutlara dair hap bilgiler paylaştık.

Ayrıca, güvenlik sertifikasyonlarını konu aldığımız detaylı bilgilendirme içeriğinde başucu kaynağı olacak bir yol haritası çıkardık.

Bu sayımızın, siz değerli okuyucularımız için faydalı ve bilgilendirici olmasını diliyor, soğuk kahvenize eşlik etmeyi sabırsızlıkla bekliyoruz!

Keyifli okumalar..

Aybala Sevinç

SOC SİBER SAVUNMA YTL

BİR BİLENE SOR - MITRE ATT&CK

Yazar: M. Hakan Yavuzyiğit

MITRE ATT&CK Nedir?

MITRE, 1958 yılında ABD'de kurulmuş, kâr amacı gütmeyen bağımsız bir araştırma ve geliştirme kuruluşudur. Savunma, siber güvenlik, sağlık, ulaştırma ve yapay zekâ gibi kritik alanlarda kamu yararına projeler yürütürken aynı zamanda MITRE ATT&CK, D3FEND gibi güvenlik topluluğuna açık kaynaklı çerçeveler de geliştirerek, tehdit modelleme ve savunma stratejileri konusunda dünya genelinde referans kabul edilen bir otorite haline gelmiştir.

Siber tehdit modellemeleri üzerine çalışmaları sonucu ortaya koyduğu ATT&CK Framework, dünya çapında güvenlik profesyonelleri tarafından benimsenmiştir. MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge), gerçek dünyada gözlemlenmiş siber saldırgan davranışlarını sistematik şekilde belgeleyen bir bilgi tabanıdır. Amacı, saldırganların sistemlere nasıl sızdığını, içeride nasıl hareket ettiğini ve hedeflerine nasıl ulaştığını detaylı şekilde sınıflandırmaktır.

MITRE ATT&CK Framework, saldırı tekniklerini sınıflandırmanın ötesinde; güvenlik operasyonları, tehdit istihbaratı, ürün değerlendirme ve denetim süreçlerinde aktif olarak kullanılan kapsamlı bir referans sistemidir.

MITRE ATT&CK Framework'u kimler kullanır?

1.SOC Ekipleri için Alarm Analizi ve Korelasyon

Güvenlik Operasyon Merkezleri (SOC), kurumdaki olaylara hızlı ve etkili müdahale etmekle sorumludur. Bu süreçte, çok sayıda güvenlik logunu anlamlandırmak ve şüpheli aktiviteleri önceliklendirmek için MITRE ATT&CK büyük kolaylık sağlar. SIEM sistemleri (QRadar, Sentinel), saldırgan davranışlarını MITRE taktik ve tekniklerine göre eşleştirecek şekilde yapılandırıldığında, olaylar daha doğru kategorize edilebilir.

MITRE'nin sunduğu bu yapı sayesinde SOC analistleri, örneğin sistemde komut satırı üzerinden çalışan şüpheli bir PowerShell işlemini "Execution" taktiği altında değerlendirebilir ve bu olayın saldırı zincirinin hangi aşamasına denk geldiğini hızlıca belirleyebilir. Bu sınıflandırma, alarmın ciddiyetini daha iyi kavramayı ve olay müdahale süresini kısaltmayı sağlar.

Ayrıca MITRE, uyumlu SIEM kuralları sayesinde farklı log kaynaklarından gelen olaylar ortak bir saldırı tekniği altında ilişkilendirilebilir; bu sayede saldırının bütünsel olarak değerlendirilmesi mümkün olur, alarm yükü daha verimli yönetilir, kritik tehditler önceliklendirilir ve müdahale süreçleri daha hızlı ve odaklı şekilde yürütülebilir.

2.Threat Hunting ve Davranış Analizi

Threat Hunting (Tehdit Avcılığı), bir sistemde aktif olarak herhangi bir alarm tetiklenmeden önce gizli kalmış tehditleri arama sürecidir. Bu yaklaşım, sadece imza ya da IOC (Indicator of Compromise) temelli değil, saldırgan davranışlarını temel alarak yapılır. İşte bu noktada MITRE ATT&CK büyük avantaj sağlar. MITRE ATT&CK, saldırganların sistemde hangi davranışları gösterebileceğini teknik seviyede tanımladığı için, tehdit avcıları bu davranışlara odaklanarak olası saldırıları tespit edebilir. Örneğin: "Credential Access" taktiği altında yer alan "LSASS process memory dump" tekniği, saldırganın şifre bilgilerini çıkarmaya çalıştığını gösterebilir. Threat hunter, sistem loglarında LSASS.exe'ye erişim ve bellek dökümü (dump) işlemlerini araştırarak bu davranışı yakalayabilir.

Davranış temelli bu analiz yaklaşımı sayesinde, daha önce bilinmeyen (zero-day) saldırıların tespiti mümkün hale gelirken, saldırganın sistem içerisinde izlediği adımlar geriye dönük olarak analiz edilebilir ve belirli davranış örüntülerine odaklanıldığı için yanlış alarm (false positive) oranı önemli ölçüde azaltılabilir.

3.Red Team ve Blue Team İşbirliği (Purple Teaming)

MITRE ATT&CK, saldırı ve savunma ekipleri arasında ortak bir dil oluşturur. Bu sayede Red Team'in gerçekleştirdiği saldırı senaryoları ile Blue Team'in savunma ve algılama mekanizmaları birbirine doğrudan bağlanabilir. Bu yaklaşım "Purple Teaming" olarak adlandırılır ve hem sızma testinin kalitesini hem de savunma sistemlerinin gerçek tehditlere karşı duyarlılığını artırır.

Red Team, test ettiği tüm saldırı adımlarını MITRE ATT&CK tekniklerine göre dokümante eder. Örneğin kullanılan e-posta eki saldırısı T1566.001 (Phishing: Attachment) olarak işaretlenir. Daha sonra sistemde yürütülen zararlı komut T1059.001 (PowerShell) ile tanımlanır. Bu yaklaşım sayesinde yapılan saldırıların kapsamı netleşir ve farklı testler arasında karşılaştırma yapılabilir.

Blue Team, MITRE'ye göre etiketlenmiş bu adımlara karşı sistemlerinin nasıl tepki verdiğini analiz eder. Hangi adımlar loglandı? Hangileri tespit edildi ancak alarm üretilmedi? Hangi teknikler tamamen gözden kaçtı? Bu analiz sonucunda hem algılama kuralları geliştirilir hem de olay müdahale süreçleri iyileştirilir. Purple Team çalışmaları sayesinde, saldırıların teknik haritası detaylı şekilde çıkarılır, güvenlik ürünlerinin MITRE üzerindeki kapsama düzeyi test edilir ve savunma ekipleri gerçek dünyada karşılaşılan taktik ve tekniklere karşı daha hazırlıklı hale gelir.

BİR BİLENE SOR - MITRE ATT&CK

Yazar: M. Hakan Yavuzyiğit

4.Threat Intelligence Ekipleri için Haritalama

Tehdit istihbaratı ekipleri, saldırgan grupların geçmişte kullandığı taktik, teknik ve prosedürleri (TTP) analiz ederek kurumun güvenlik duruşunu proaktif şekilde güçlendirmeyi amaçlar. MITRE ATT&CK Framework, bu sürece sistematik bir yapı kazandırır. Saldırgan grupların davranışları MITRE matrisi üzerinde teknik bazda haritalandığında, istihbarat bilgileri soyut olmaktan çıkar ve doğrudan kullanılabilir hale gelir. Örneğin, APT29 gibi bilinen bir tehdit aktörünün MITRE'da tanımlanmış teknikleri analiz edilerek kurum içerisinde bu tekniklerin izlerine rastlanıp rastlanmadığı araştırılabilir. Bu yaklaşım, tehdit istihbaratını olay sonrası değerlendirme aracı olmaktan çıkarıp aktif bir savunma bileşeni haline getirir. Kurumlar, bu tekniklere karşı log toplama seviyelerini, alarm üretme kabiliyetlerini ve tespit mekanizmalarını analiz ederek olası saldırılara karşı hazırlık düzeyini ölçebilir. Böylece istihbarat raporları; SOC, SIEM ve güvenlik mühendisliği ekipleri tarafından doğrudan aksiyona dönüştürülebilir hale gelir.

MITRE ATT&CK tabanlı haritalama yöntemi, tehdit istihbaratını operasyonel hale getirerek siber güvenlik süreçlerinin merkezine taşır. Bu yapı sayesinde savunma ekipleri sadece "kim saldırabilir" sorusunu yanıtlamakla kalmaz, aynı zamanda "nasıl saldırabilir" ve "buna hazır mıyız" gibi kritik sorulara da sistematik yanıtlar üretebilir. Bu da hem tehdit farkındalığını hem de güvenlik olgunluğunu önemli ölçüde artırır.

5. Güvenlik Testi ve Değerlendirme Süreçleri

Günümüzde güvenlik kontrollerinin yalnızca var olup olmadığı değil, ne kadar etkili çalıştığı da önemli bir değerlendirme kriteridir. Bu kapsamda MITRE ATT&CK Framework, kurumların güvenlik testleri ve değerlendirme süreçlerinde referans olarak kullanılabilecek güçlü bir yapıdır. Sızma testlerinden ürün değerlendirmelerine kadar birçok senaryoda, test adımlarının MITRE teknikleriyle eşleştirilmesi hem testin kalitesini artırır hem de sonuçların daha objektif ve karşılaştırılabilir olmasını sağlar.

Örneğin, bir güvenlik çözümünün "Defense Evasion" tekniklerini tespit edip edemediğini test etmek isteyen bir ekip, MITRE'daki ilgili teknikleri temel alarak kontrollü saldırılar gerçekleştirebilir. Bu testlerde, ürünün tehditleri hangi aşamada yakaladığı, olaylara nasıl yanıt verdiği ve log düzeyinde hangi verileri ürettiği analiz edilir. Böylece test sadece "zararlı çalıştı mı" sorusuna değil, aynı zamanda "ne kadar etkin tespit edildi", "hangi teknik gözden kaçtı" gibi sorulara da yanıt verir. Bu analizlerin sonucunda, güvenlik ürünleri için MITRE tekniklerine göre kapsam haritası (coverage map) çıkarılabilir. Bu yaklaşım sayesinde kurumlar, güvenlik çözümlerinin güçlü ve zayıf yönlerini teknik düzeyde ölçebilir; aynı zamanda kendi sistemlerindeki görünürlük ve algılama kabiliyetlerini daha somut verilerle değerlendirebilir. MITRE tabanlı testler, ürün seçimi ve güvenlik yatırımı kararlarında nesnel dayanaklar sunar. Böylece hem ürün kalitesi hem de organizasyonun genel güvenlik olgunluğu sistematik biçimde geliştirilmiş olur.

MITRE ATT&CK Framework'ün Temel Bileşenleri Nelerdir

1. Matris (Matrix): MITRE, saldırıların aşamalarını ve yöntemlerini bir tablo şeklinde sunar. Yatayda saldırganın amacı (örneğin sisteme sızmak), dikeyde bu amacı gerçekleştirmek için kullanılan yollar yer alır. Bu tabloya "ATT&CK matrisi" denir.
2. Taktik (Tactic): Saldırganın her adımda neyi başarmaya çalıştığını gösterir. Örneğin, sisteme giriş yapmak, kalıcılık sağlamak ya da bilgi çalmak gibi amaçlar birer taktiktir.
3. Teknik (Technique): Taktiklerin nasıl uygulandığını, yani saldırganın hangi yöntemi kullandığını açıklar. Örneğin, bir dosya göndererek kimlik bilgilerini çalma veya uzaktan komut çalıştırma bu yöntemlerdendir.
4. Veri Kaynakları (Data Sources): Saldırıları anlayabilmek için sistemden toplanan loglardır. Örneğin bir kullanıcının sisteme ne zaman giriş yaptığı ya da hangi işlemi başlattığı bu veri kaynaklarıyla takip edilir.
5. Önlemler (Mitigation): Her saldırı yöntemine karşı alınabilecek savunma önlemlerini açıklar. Bu öneriler sayesinde kurumlar riskleri azaltabilir veya saldırganın işini zorlaştırabilir.
6. Saldırgan Gruplar (Groups): MITRE, bazı saldırgan grupların (örneğin APT29 gibi) hangi yöntemleri sıklıkla kullandığını örnekleriyle birlikte gösterir. Bu sayede kurumlar bu gruplara karşı daha bilinçli savunma yapabilir.
7. Yazılımlar (Software): Saldırganların kullandığı araçlar ve bu araçların ne işe yaradığı açıklanır. Örneğin parola çalan bir yazılım veya ağ taraması yapan bir araç burada tanımlanır.

BİR BİLENE SOR - MITRE ATT&CK

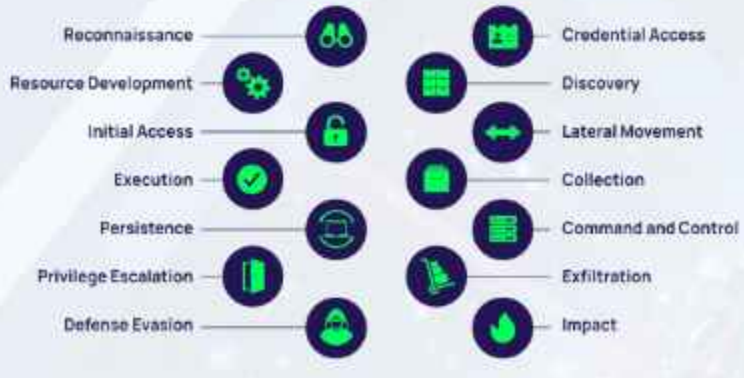
Yazar: M. Hakan Yavuzyiğit

MITRE ATT&CK Framework, siber güvenlik dünyasında yalnızca bir referans tablosu değil; kurumların tehditleri tanımlama, analiz etme ve savunma stratejilerini yapılandırma biçimini kökten değiştiren bir yaklaşımdır. Gerçek saldırı senaryolarına dayalı olarak oluşturulan bu yapı, saldırgan davranışlarını anlamaya yönelik sistematik bir yol sunar ve bu sayede teknik ekiplerin olaylara daha hızlı ve etkili yanıt vermesine yardımcı olur.

SOC analistlerinden threat hunter ekiplerine, red-blue team çalışmalarından ürün değerlendirmelerine kadar birçok alanda doğrudan uygulanabilir olan MITRE ATT&CK, güvenlik mimarisinin hem görünürlüğünü hem de olgunluğunu artırmak için kritik bir araçtır. Kurumlar, MITRE tabanlı değerlendirmeleri düzenli olarak uygulayarak, hem teknolojik yatırımlarını optimize edebilir hem de tehditlere karşı daha dirençli bir savunma yapısı oluşturabilir.

Bu çerçevede, MITRE ATT&CK Framework'ün benimsenmesi ve kurum geneline entegre edilmesi; güvenlik süreçlerinin daha etkin, tehdit yönetiminin daha bilinçli ve siber dayanıklılığın daha sürdürülebilir hale gelmesi açısından stratejik bir adımdır.

KoçSistem SOC'de SIEM ve EDR kurallarımızın tümü Mitre ATT&CK framework uyumludur. Kritik siber olayların tespiti adına geliştirdiğimiz 1000'e yakın senaryo ile %90 üzeri Mitre ATT&CK kapsamı elde edilmektedir.



Merhaba ben **Hakan Yavuzyiğit**. 3 yıldır KoçSistem'de çalışmaktayım. Bu süreçte edindiğim bilgiler, teknik becerilerimi ve siber güvenlik alanındaki stratejik bakış açımı geliştirmemi sağladı. Farklı araçlarla yaptığım analizler yorumlama yeteneğimi artırırken, çalışma arkadaşlarımın desteği ve paylaşımları sayesinde bu alanda kendimi geliştirmeye devam ediyorum.

HAKAN YAVUZYİĞİT
SOC TEHDİT İZLEME UZMANI

KoçSistem | SOC
GELECEĞİ KEŞFET

GELECEĞİ KEŞFET!

BİR BİLENE SOR - WINDOWS ARTIFACT

Yazar: İsmail Külah

Windows işletim sistemi, kullanıcı ve sistem aktivitelerini kaydetmek için birçok "artifact" (dijital iz) dosyası oluşturur. Bu dosyalar; bilgisayarınızda kimin ne yaptığını, hangi programların çalıştırıldığını, hangi dosyaların açıldığını ve daha fazlasını gösterir. Aşağıda Windows 10 ve 11 sistemleri için en güncel ve kapsamlı artifact dosyalarının listesi ve açıklamaları yer almaktadır.

1. Prefetch Dosyaları (Program Çalıştırma Kayıtları)

- Konum: C:\Windows\Prefetch

Ne İşe Yarar?

- Programların daha hızlı açılabilmesi için .exe dosyalarının çalıştırılma zamanı ve yolu kayıt altına alınır.
- Windows 10/11'de son 1024 uygulamanın bilgisi tutulur.
- Adli analizde hangi programın ne zaman açıldığını gösterir.

2. Event Logları (Olay Günlükleri)

- Konum: C:\Windows\System32\winevt\Logs

Ne İşe Yarar?

- Security.evtx: Oturum açma/kapama, yetkisiz erişim
- System.evtx: Donanım ve sistem olayları
- Application.evtx: Uygulama hataları
- PowerShell.evtx: PowerShell komut geçmişi
- TerminalServices.evtx: Uzak masaüstü oturumları

3. Registry (Kayıt Defteri) Artifactları

- USB Geçmişi: HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR
- Son Açılan Dosyalar (MRU): HKCU\...\Explorer\RecentDocs
- Çalıştır Komutu Geçmişi: HKCU\...\Explorer\RunMRU
- Ağ Profilleri: HKLM\...\NetworkList\Profiles
- Shellbags: HKCU\Software\Microsoft\Windows\Shell\Bags
- UserAssist (ROT13 şifreli): HKCU\...\Explorer\UserAssist
- Zaman Dilimi Bilgisi: HKLM\SYSTEM\...\TimeZoneInformation

4. Amcache.hve & ShimCache (AppCompatCache)

- Amcache.hve: C:\Windows\AppCompat\Programs\Amcache.hve
- .exe dosyalarının hash'i, yolu, çalışma zamanı
- ShimCache: SYSTEM hive içinde
- Uyumluluk verisi, silinen dosyaların da geçmişini içerir

5. Tarayıcı Geçmişleri

- Chrome/Edge: %LocalAppData%\...\History, Cookies, Downloads
- Firefox: %AppData%\Mozilla\...\places.sqlite

6. LNK (Kısayol) Dosyaları

- Konum: %AppData%\Microsoft\Windows\Recent
- İçerik: Açılan dosyaların yol bilgisi, zaman damgaları

BİR BİLENE SOR - WINDOWS ARTIFACT

Yazar: İsmail Külah

7. Thumbcache / Thumbs.db
- Konum: %LocalAppData%\Microsoft\Windows\Explorer\thumbcache_*.db
- Görüntülenen görsellerin küçük önizlemeleri. Silinen resimlerin izleri bulunabilir.

8. Hiberfil.sys & Pagefile.sys
- Konum: C:\
- RAM dump verisi içerir. Adli analizde parola ve oturum verileri bulunabilir.

9. SRUDB.dat & SRU.log
- Konum: C:\Windows\System32\sru\
- Uygulama ağ, CPU ve enerji kullanımı. Sistem kaynak geçmişi.

10. Jump Lists
- Konum: %AppData%\Microsoft\Windows\Recent\AutomaticDestinations
- Son kullanılan dosyalar listesi (Başlat menüsü vb.)

11. Clipboard Artifactları (Windows 10/11)
- Konum: %LocalAppData%\Microsoft\Windows\Clipboard
- Kopyalanan içerik geçmişi, veri sızıntısı analizinde önemlidir.

12. User Timeline (ActivitiesCache.db)

- Konum: %LocalAppData%\ConnectedDevicesPlatform\...\ActivitiesCache.db
- Hangi dosyaların açıldığı, uygulama aktiviteleri.

13. Windows Defender Logları
- Konum: C:\ProgramData\Microsoft\Windows Defender\Support
- Tehdit tespiti, tarama detayları, koruma aktiviteleri.

14. PowerShell & CMD Geçmişi
- PowerShell: %AppData%\...\ConsoleHost_history.txt
- CMD: Doskey /history

15. Geri Dönüşüm Kutusu ($RECYCLE.BIN)
- Silinmiş dosyaların bulunduğu klasör. Metadata analiziyle silinme zamanı belirlenebilir.

16. Windows Error Reporting (WER)
- Konum: C:\ProgramData\Microsoft\Windows\WER\ReportArchive
- Uygulama çökmeleri, hata raporları

17. Cloud Sync Artifactları (OneDrive, MSA)
- %LocalAppData%\Microsoft\OneDrive\logs
- %AppData%\Microsoft\IdentityCache

18. Terminal ve WSL Logları

- Windows Terminal: %LocalAppData%\Packages\Microsoft.WindowsTerminal_8wekyb3d8bbwe\LocalState\State.json
- WSL: %LocalAppData%\Packages\CanonicalGroupLimited*

19. Disk & NTFS Artifactları

- $MFT: Dosya metadata kayıtları
- $LogFile: NTFS günlüğü (dosya değişiklikleri)
- $UsnJrnl: Dosya oluşturma, silme, yeniden adlandırma kayıtları

Komutlarla Artifact Analizi

1.Registry (Kayıt Defteri) Analiz Komutları

RecentDocs - Son açılan belgeler: reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs /s
Run geçmişi: reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
Ağ bağlantı profilleri: reg query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles" /s

2. Sistem ve Kullanıcı Aktivite Komutları

Son 10 başarılı oturum açma: Get-WinEvent -LogName Security -MaxEvents 10 | Where-Object {$_.ID -eq 4624} | Format-Table TimeCreated,Message -AutoSize
Aktif zamanlanmış görevler: Get-ScheduledTask | Where-Object {$_.State -ne "Disabled"} | Format-Table TaskName,State
Açık bağlantılar: netstat -ano | findstr ESTABLISHED

3. Dosya Sistemi Analizi

Son 7 gün içinde değişen .exe ve .dll dosyaları: Get-ChildItem C:\ -Recurse -ErrorAction SilentlyContinue | Where-Object {($_.LastWriteTime -gt (Get-Date).AddDays(-7)) -and ($_.Extension -eq ".exe" -or $_.Extension -eq ".dll")} | Select-Object FullName,LastWriteTime
MFT analizi: fsutil usn readjournal C:

4. Güvenlik Odaklı Komutlar

Defender tehdit geçmişi: Get-MpThreatDetection | Format-Table DetectionTime,ThreatName,ProcessName
Defender tehdit geçmişi karantinaya alınanlar: Get-MpThreat | Format-Table Resources
BitLocker durumu: manage-bde -status
Şüpheli servisleri listeleme: Get-Service | Where-Object {$_.Status -eq "Running" -and $_.DisplayName -notlike "*Microsoft*"} | Format-Table ServiceName,DisplayName
Sisteme yüklenen yazılımların kurulum tarihleri - 64 bit uygulamalar:
Get-ItemProperty HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall* | Select-Object DisplayName, InstallDate, Publisher | Format-Table -AutoSize
Sisteme yüklenen yazılımların kurulum tarihleri - 32 bit uygulamalar:
Get-ItemProperty HKLM:\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall* | Select-Object DisplayName, InstallDate, Publisher | Format-Table -AutoSize

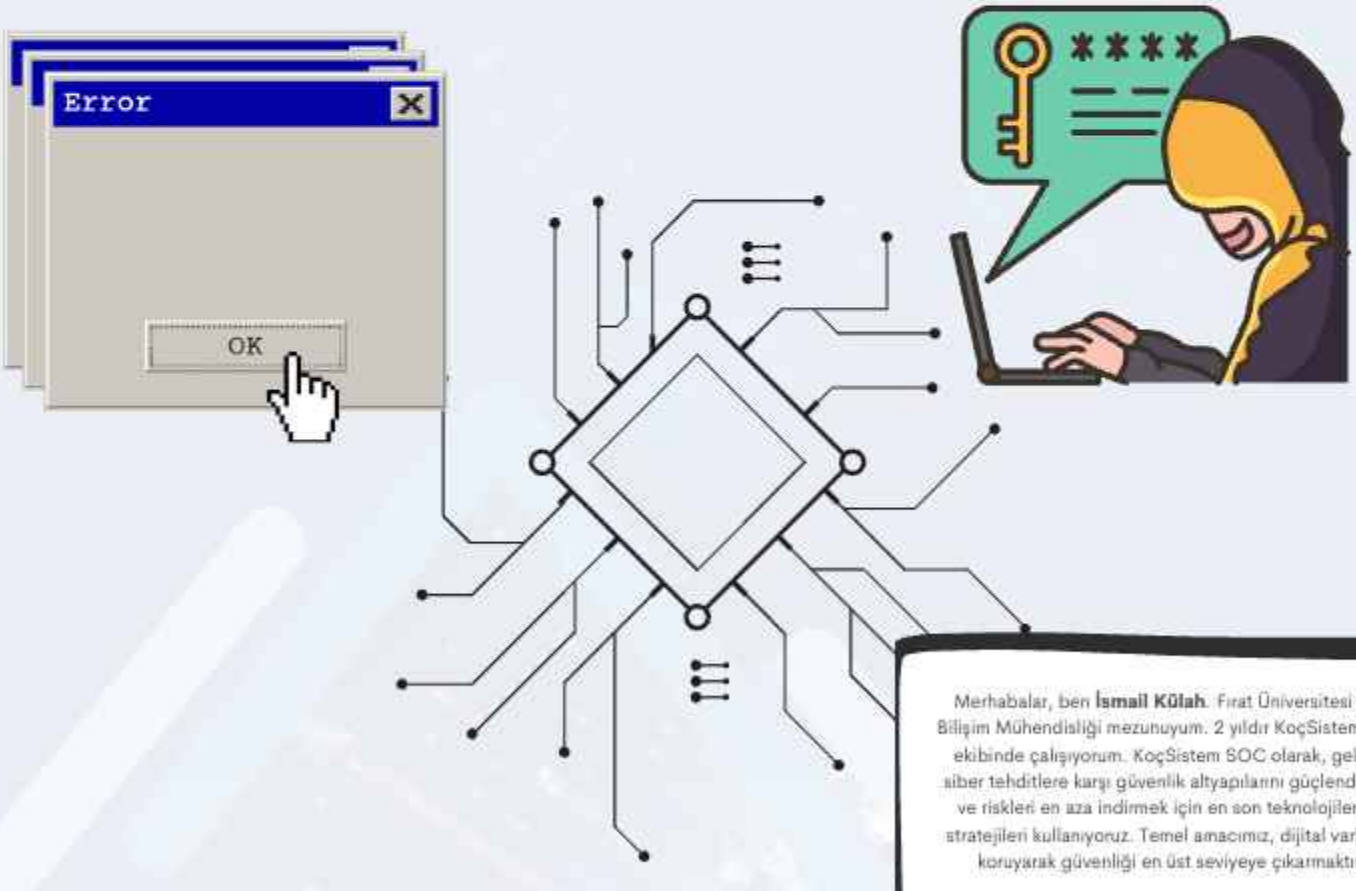
BİR BİLENE SOR - WINDOWS ARTIFACT

Yazar: İsmail Külah

5. Ağ (Network) Komutları
ARP tablosu: arp -a
DNS önbelleği: ipconfig /displaydns
Paylaşılan klasörler: net share

6.Zaman Çizelgesi Komutları
Prefetch-Son 24 saat:
Get-ChildItem C:\Windows\Prefetch*.pf | Where-Object {$_.CreationTime -gt (Get-Date).AddHours(-24)} | Select-Object Name,CreationTime
Jump List analizi: Get-ChildItem "$env:APPDATA\Microsoft\Windows\Recent\AutomaticDestinations" | Select-Object Name,LastWriteTime

7.Özel Analiz Komutları
Base64 encoded PowerShell komutlarını tespit etme:
Get-WinEvent -LogName "Microsoft-Windows-PowerShell/Operational" | Where-Object {$_.Message -like "*EncodedCommand*"} | Format-Table TimeCreated,Message -Wrap
Çalışan WSL örneklerini görme: wsl --list --running



Merhabalar, ben **İsmail Külah**. Fırat Üniversitesi Adli Bilişim Mühendisliği mezunuyum. 2 yıldır KoçSistem SOC ekibinde çalışıyorum. KoçSistem SOC olarak, gelişen siber tehditlere karşı güvenlik altyapılarını güçlendirmek ve riskleri en aza indirmek için en son teknolojileri ve stratejileri kullanıyoruz. Temel amacımız, dijital varlıkları koruyarak güvenliği en üst seviyeye çıkarmaktır.

İSMAİL KÜLAH
SOC TEHDİT İZLEME UZMANI

BİR BİLENE SOR - SERTİFİKASYON

Yazar: Kasım Gökhan Coşkun

Bilgi Güvenliği ile İlgili Alınabilecek Sertifikalar

Siber güvenlik alanında ilerlemek için yardımcı ve geçerli bir faktör olan Sertifikaları seçmek onları geçmek kadar değerlidir. Ülkemizde bilinen ve çokça tercih edilen sertifikalar ile birlikte Küresel çapta geçerliliği olan sertifikaları da inceleyebileceğiniz detaylı, güncel bir rehber hazırlamak istedim. Bu listeyi kullanarak kendinize bir yol belirleyebilir veya bu liste içindekiler ile bir araştırmaya girebilirsiniz.

	Organizasyon/Firma	Sertifika Adı	Düzey	Odak Alanı	Hedef Kitle	Geçerlilik
Küresel Standartlar & Yönetimsel Sertifikalar	ISC²	CC (Certified in Cybersecurity)	Temel	Giriş Seviyesi BT güvenliği, güvenlik operasyonları, erişim kontrolleri, network ve iş sürekliliği senaryoları.	Bilgi güvenliğinde kariyer yapmak isteyen ve yeni başlayanlar içindir.	Uluslararası
		SSCP (Systems Security Certified Practitioner)	Temel/Orta	Uygulamalı BT güvenliği, güvenlik operasyonları, erişim kontrolleri, risk tanımlama.	Güvenlik Yöneticileri, Ağ Güvenliği Mühendisleri, Güvenlik Analistleri (1+ yıl deneyim).	Uluslararası
		CISSP (Certified Information Systems Security Professional)	İleri/Yönetim	Kapsamlı bilgi güvenliği yönetimi ve stratejileri, risk yönetimi, güvenlik mimarisi, operasyonlar.	Güvenlik Yöneticileri, Danışmanlar, Mimarlar, Kıdemli Analistler (5+ yıl deneyim).	Uluslararası
		CCSP (Certified Cloud Security Professional)	Orta/İleri	Bulut güvenliği mimarisi, tasarımı, operasyonları, yasalara uygunluk. (CSA ile ortak).	Bulut Güvenliği Mimarları/Mühendisleri, Güvenlik Danışmanları, Bulut Yöneticileri.	Uluslararası
	ISACA	CISM (Certified Information Security Manager)	İleri/Yönetim	Bilgi güvenliği yönetişimi, program geliştirme ve yönetimi, olay yönetimi, risk yönetimi.	Bilgi Güvenliği Yöneticileri, Danışmanlar, Teftiş Görevlileri.	Uluslararası
		CISA (Certified Information Systems Auditor)	Orta/İleri	Bilgi sistemleri denetimi süreci, BT yönetişimi ve yönetimi, sistem edinim/geliştirme/bakım, bilgi varlıklarının korunması.	BT Denetçileri, Kontrol Uzmanları, Güvenlik Profesyonelleri.	Uluslararası
		CRISC (Certified in Risk and Information Systems Control)	Orta/İleri	Risk yönetimi, bilgi sistemleri kontrolü, risk tespiti, değerlendirme ve müdahale.	Risk Yöneticileri, Proje Yöneticileri, İş Analistleri, Kontrol Profesyonelleri.	Uluslararası
	ISO/IEC	ISO/IEC 27001	Orta/İleri	ISO 27001 standardı gereklilikleri, BGYS kurulumu, yönetimi ve denetimi. (Örn: Baş Denetçi, Baş Uygulayıcı)	Bilgi Güvenliği Yöneticileri, BGYS Sorumluları, İç Denetçiler, Danışmanlar.	Ulusal/Uluslararası (Standardın kendisi uluslararası)
	Cloud Security Alliance (CSA)	CCSK (Certificate of Cloud Security Knowledge)	Temel	Bulut bilişim güvenlik kavramları, bulut güvenlik riskleri, uyumluluk.	Bulut ortamlarında güvenlikten sorumlu IT profesyonelleri, Bulut Mimarları.	Uluslararası

BİR BİLENE SOR - SERTİFİKASYON

Yazar: Kasım Gökhan Coşkun

	Organizasyon/Firma	Sertifika Adı	Düzey	Odak Alanı	Hedef Kitle	Geçerlilik
Siber Güvenlik Devleri	EC-Council	CEH (Certified Ethical Hacker)	Orta	Etik hacking teknikleri, penetrasyon testleri, zafiyet analizi, kötü amaçlı yazılım analizi.	Penetrasyon Test Uzmanları, Güvenlik Analistleri.	Uluslararası
		CHFI (Computer Hacking Forensic Investigator)	Orta/İleri	Dijital adli bilişim, olay müdahalesi, delil toplama ve analizi.	Adli Bilişim Uzmanları, Olay Müdahale Ekipleri, Güvenlik Analistleri.	Uluslararası
		CCISO (Certified Chief Information Security Officer)**	Yönetim	Bilgi güvenliği liderliği, strateji geliştirme, yönetişim, risk yönetimi.	CISO'lar, Bilgi Güvenliği Yöneticileri, Kıdemli Güvenlik Liderleri.	Uluslararası
		EH Practical**	Orta/İleri	Uygulamalı etik hacking becerileri, gerçek dünya senaryolarında sızma testi.	CEH sertifikasına sahip veya uygulamalı yetkinliğini kanıtlamak isteyen profesyoneller.	Uluslararası
	CompTIA	Security+	Temel	Temel bilgi güvenliği kavramları, ağ güvenliği, tehditler, zafiyetler, kriptografi, risk yönetimi.	BT Profesyonelleri, Ağ Yöneticileri, Güvenlik Analistleri (giriş seviyesi).	Uluslararası
		CySA+ (Cybersecurity Analyst+)	Orta	Siber tehdit analizi, zafiyet yönetimi, güvenlik operasyonları, güvenlik analizi.	SOC Analistleri, Siber Güvenlik Analistleri, Tehdit İstihbarat Analistleri.	Uluslararası
		PenTest+	Temel/Orta	Penetrasyon testi ve zafiyet değerlendirme metodolojileri, araçları, yasal ve uyumluluk konuları.	Penetrasyon Test Uzmanları, Güvenlik Danışmanları, Zafiyet Analistleri.	Uluslararası
		CASP+ (CompTIA Advanced Security Practitioner)	İleri	Kurumsal güvenlik mimarisi, risk yönetimi, araştırma ve geliştirme, entegrasyon.	Kıdemli Güvenlik Mühendisleri, Güvenlik Mimarları, Teknik Liderler.	Uluslararası
	InfoSec Institute	Certified Cyber Security Analyst (CCSA)	Orta	Siber güvenlik analizi, tehdit tespiti, zafiyet yönetimi, güvenlik operasyonları.	Güvenlik Analistleri, SOC Analistleri, Güvenlik Operasyon Uzmanları.	Uluslararası
		Certified Ethical Hacker (CEH) - EC-Council Ortaklığı	Orta	Etik hacking prensipleri ve metodolojileri.	Penetrasyon Test Uzmanları, Siber Güvenlik Profesyonelleri.	Uluslararası
	SANS Institute / GIAC	GSEC (GIAC Security Essentials Certification)	Temel	Ağ güvenliği, kriptografi, bulut güvenliği, güvenlik mimarisi, güvenlik operasyonları.	Temel güvenlik becerilerine sahip olmak isteyen IT Profesyonelleri.	Uluslararası
		GCIH (GIAC Certified Incident Handler)	Orta/İleri	Olay müdahalesi, adli bilişim, kötü amaçlı yazılım analizi, tehdit avcılığı.	Olay Müdahale Ekipleri, SOC Analistleri, Adli Bilişim Uzmanları.	Uluslararası
		GPEN (GIAC Penetration Tester)	İleri	Gelişmiş penetrasyon testi teknikleri, zafiyet keşfi ve sömürüsü, raporlama.	Penetrasyon Test Uzmanları, Kırmızı Takım Üyeleri, Güvenlik Araştırmacıları.	Uluslararası
		GCFA (GIAC Certified Forensic Analyst)	İleri	Bilgisayar adli bilişim, delil toplama, analiz ve raporlama, kötü amaçlı yazılım analizi.	Adli Bilişim Uzmanları, Güvenlik Analistleri, Olay Müdahale Ekipleri.	Uluslararası
		GCIA (GIAC Certified Intrusion Analyst)	İleri	Ağ tabanlı saldırı tespiti, IDS/IPS sistemleri, ağ trafiği analizi.	Ağ Güvenliği Analistleri, SOC Analistleri, Tehdit Avcıları.	Uluslararası
	OffSec	OSCP (Offensive Security Certified Professional)	Orta-İleri	Pratik penetrasyon testi becerileri (24 saatlik laboratuvar sınavı içerir).	Deneyimli pentester'lar.	Uluslararası
		OSCE (Offensive Security Certified Expert)	İleri	Gelişmiş saldırı teknikleri	Deneyimli pentesterlar	Uluslararası

BİR BİLENE SOR – SERTİFİKASYON

Yazar: Kasım Gökhan Coşkun

Özel Odaklı & Niş Programlar

Organizasyon/Firma	Sertifika Adı	Düzey	Odak Alanı	Hedef Kitle	Geçerlilik
INE Security	eCTHPv2 (Certified Threat Hunting Professional)	İleri	Siber tehdit avcılığı metodolojileri ve pratik uygulamalar.	SOC Analistleri, Tehdit Avcıları	Uluslararası
	eCIR (Certified Incident Responder)	İleri	Siber olay müdahale süreçleri ve teknikleri.	CSIRT Ekipleri, Güvenlik Uzmanları	Uluslararası
PICUS	MITRE ATT&CK - Data Encrypted for Impact	Orta	Ransomware ve veri şifreleme saldırılarının analizi.	SOC Analistleri, Incident Responder'lar	Uluslararası
	Fundamentals of SIEM Alert Rule Development	Temel	SIEM sistemlerinde kural yazma ve yönetimi.	Siber Güvenlik Yeni Başlayanlar, SOC Ekipleri	Uluslararası
MAD20	ATT&CK Purple Teaming Methodology Certification	Orta-İleri	MITRE ATT&CK tabanlı mor tim (purple team) egzersizleri.	Pentester'lar, Kırmızı/Mavi Tim Üyeleri	Uluslararası
	ATT&CK Detection Engineering Certification	İleri	ATT&CK matrisine dayalı tespit kuralları geliştirme.	SOC Mühendisleri, Threat Hunter'lar	Uluslararası
	ATT&CK Adversary Emulation Methodology Certification	İleri	Gerçek dünya saldırı senaryolarının simülasyonu.	Kırmızı Tim Üyeleri, Güvenlik Araştırmacıları	Uluslararası
TryHackMe	Jr Penetration Tester (JPT)	Başlangıç / Orta	Penetrasyon testi, temel saldırı teknikleri	Siber güvenliğe yeni başlayanlar, IT öğrencileri	Uluslararası
	Complete Beginner Path (rozeti)	Başlangıç	Temel siber güvenlik kavramları, Linux, ağ güvenliği	Yeni başlayanlar, öğrenciler	Uluslararası
	Pre-Security Path (rozeti)	Başlangıç	Bilgi güvenliği temelleri	IT'ye geçiş yapmak isteyenler, meraklılar	Uluslararası
	Offensive Pentesting Path	Orta/İleri	Pentest teknikleri, Red Teaming	Teknik bilgiye sahip kişiler	Uluslararası

Ağ Güvenliği Uzmanlığı Sertifikaları

Organizasyon/Firma	Sertifika Adı	Düzey	Odak Alanı	Hedef Kitle	Geçerlilik
Cisco	CCNA Security / CCNP Security	Orta/İleri	Ağ güvenliği, güvenlik duvarları, VPN, IPS/IDS, kimlik yönetimi, uç nokta güvenliği. (CCNA Security, CCNP Security içine entegre edildi)	Ağ Güvenliği Mühendisleri, Güvenlik Analistleri, Ağ Yöneticileri.	Uluslararası
	CyberOps Associate	Temel/Orta	Temel güvenlik operasyonları, tehdit tespiti, olay analizi, ağ izleme. (SOC odaklı başlangıç).	SOC Analistleri (giriş seviyesi), Güvenlik Teknisyenleri.	Uluslararası
Fortinet	NSE (Network Security Expert) Programı	Temel'den İleriye	Fortinet ürünlerinin (FortiGate, FortiAnalyzer, FortiSIEM vb.) kurulumu, yapılandırması, yönetimi ve güvenliği. (NSE 1-8 seviyeleri).	Ağ ve Güvenlik Mühendisleri, Güvenlik Uzmanları, Fortinet ürünlerini kullanan IT profesyonelleri.	Uluslararası (Ürün bazlı)
Palo Alto Networks	PCNSA (Palo Alto Networks Certified Network Security Administrator)	Orta	Palo Alto Networks güvenlik duvarlarının temel yapılandırması ve yönetimi.	Ağ Güvenliği Yöneticileri, Ağ Güvenliği Uzmanları.	Uluslararası (Ürün bazlı)
	PCNSE (Palo Alto Networks Certified Network Security Engineer)	İleri	Palo Alto Networks güvenlik çözümlerinin (Next-Gen Firewall, Panorama vb.) tasarımı, dağıtımı, yönetimi ve sorun giderme.	Güvenlik Mühendisleri, Güvenlik Mimarları, Kıdemli Ağ Güvenliği Uzmanları.	Uluslararası (Ürün bazlı)
	Palo Alto Networks Micro-Credential for Cortex XDR Consultant	Orta	Cortex XDR çözümlerinin danışmanlık ve entegrasyonu.	SIEM Uzmanları, Güvenlik Danışmanları	Uluslararası (Ürün bazlı)

Ulusal & Yerel Sertifikalar

Organizasyon/Firma	Sertifika Adı	Düzey	Odak Alanı	Hedef Kitle	Geçerlilik
TSE (Türk Standardları Enstitüsü)	ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Eğitimi ve Sertifikaları	Orta/İleri	ISO 27001 standardı gereklilikleri, BGYS kurulumu, yönetimi ve denetimi. (Örn: Baş Denetçi, Baş Uygulayıcı)	Bilgi Güvenliği Yöneticileri, BGYS Sorumluları, İç Denetçiler, Danışmanlar.	Ulusal/Uluslararası (Standardın kendisi uluslararası)
	TS 13638/T2 Sızma Testi Uzmanı	Orta/İleri	Etik hacking prensipleri ve metodolojileri.	Bilgi Teknolojileri – Güvenlik Teknikeri – Sızma testi yapan personel ve firmalar için şartlar	Ulusal

BİR BİLENE SOR – SERTİFİKASYON

Yazar: Kasım Gökhan Coşkun

	Organizasyon/Firma	Sertifika Adı	Düzey	Odak Alanı	Hedef Kitle	Geçerlilik
Ürün Bazlı Sertifikalar	IBM	IBM Certified Security Analyst - QRadar SIEM	Orta/İleri	IBM QRadar SIEM platformunun kurulumu, yapılandırması, olay tespiti, korelasyon kuralları oluşturma.	SOC Analistleri, Güvenlik Mühendisleri, SIEM Uzmanları.	Uluslararası (Ürün bazlı)
		IBM Certified Deployment Professional - Guardium	Orta/İleri	IBM Guardium veri tabanı güvenliği çözümünün kurulumu, yönetimi, izleme.	Veritabanı Yöneticileri, Veri Güvenliği Uzmanları.	Uluslararası (Ürün bazlı)
		IBM Security QRadar SIEM V7.5 Administration	Orta	IBM QRadar SIEM platformunun kurulumu, yapılandırması.	SOC Analistleri, Güvenlik Mühendisleri, SIEM Uzmanları.	Uluslararası (Ürün bazlı)
	Splunk	Splunk Core Certified User/Power User	Temel/Orta	Splunk arayüzünde arama yapma, rapor oluşturma, temel analiz.	Güvenlik Analistleri (Splunk kullanan), Veri Analistleri, IT Operasyonları.	Uluslararası (Ürün bazlı)
		Splunk Enterprise Certified Admin/Architect	Orta/İleri	Splunk Enterprise'ın kurulumu, yönetimi, mimarisi, performans optimizasyonu.	Splunk Yöneticileri, Mimarları, Sistem Mühendisleri.	Uluslararası (Ürün bazlı)
		Splunk Enterprise Security Certified Admin/Architect	Orta/İleri	Splunk Enterprise Security (ES) uygulamasının kurulumu, yönetimi, tehdit tespiti, uyumluluk.	SOC Yöneticileri, Güvenlik Mimarları, SIEM Uzmanları (Splunk ES kullanan).	Uluslararası (Ürün bazlı)
	Microsoft	Microsoft Certified: Azure Security Engineer Associate	Orta	Azure ortamlarında güvenlik kontrolleri uygulama, tehdit koruma, kimlik yönetimi.	Azure Güvenlik Mühendisleri, Bulut Güvenliği Uzmanları.	Uluslararası (Ürün bazlı)
		Microsoft Certified: Security Operations Analyst Associate	Orta	Microsoft 365 Defender, Azure Sentinel gibi araçlarla tehdit izleme, olay müdahalesi, güvenlik operasyonları. (SOC odaklı).	SOC Analistleri, Güvenlik Operasyon Uzmanları, Tehdit Avcıları.	Uluslararası (Ürün bazlı)
		Microsoft Certified: Identity and Access Administrator Associate	Orta	Microsoft kimlik ve erişim yönetimi çözümlerinin (Azure AD) uygulanması ve yönetimi.	Kimlik ve Erişim Yöneticileri, Güvenlik Yöneticileri.	Uluslararası (Ürün bazlı)
	AWS (Amazon Web Services)	AWS Certified Security – Specialty	İleri	AWS ortamlarında güvenlik çözümlerinin tasarımı, dağıtımı ve yönetimi, veri koruma, ağ güvenliği, olay yönetimi.	AWS Güvenlik Mühendisleri, Bulut Güvenliği Mimarları, Güvenlik Uzmanları.	Uluslararası (Ürün bazlı)
		AWS Certified Cloud Practitioner	Temel	Temel AWS bulut kavramları, hizmetleri ve güvenlik prensipleri.	Bulut bilişimde temel bilgi sahibi olmak isteyen herkes, Teknik olmayan rollerdeki profesyoneller.	Uluslararası (Ürün bazlı)

Özetle;

Bu rehber niteliğindeki listelenmiş tablolarla, siber güvenlik sertifikalarını organizasyon bazlı 6 ana kategoriye ayırarak analiz etmeye çalıştık;

- Küresel Standartlar & Yönetimsel Sertifikalar (CISSP, CISM gibi stratejik odaklılar).
- Siber Güvenlik Devleri (CEH, OSCP gibi teknik beceri ölçenler).
- Bulut & Ürün Bazlı Sertifikalar (AWS, Microsoft Azure gibi bulut uzmanlıkları).
- Ağ Güvenliği & Firewall Uzmanlıkları (Cisco, Palo Alto Networks sertifikaları).
- Özel Odaklı & Niş Programlar (Tehdit avcılığı, pentest gibi alanlar).
- Ulusal & Yerel Sertifikalar (TSE gibi yerel geçerliliği olanlar).

Sonuç olarak;

BT dünyası dinamik, rekabetçi ve sürekli kendini yenileyen bir yapıya sahip. Güncel, sürekli doğru ve güçlü bir pozisyonda kalmak bu işin kazananlarının yöntemi. Sertifika da bunun temel göstergelerinden biri ama tabiki asıl olan bunları pratiğe nasıl döktüğünüz, becerileriniz ile nasıl farklar oluşturduğunuz.

Evet, bu yazımda da sizlere "Bilgi Güvenliği ile ilgili alınabilecek sertifikalar" hakkında bilgi paylaşımı yaptım. Bir sonraki yazımda yine bu tatta bir makale ile görüşmeyi umuyorum.

Okuduğunuz ve vakit ayırdığınız için teşekkürler.

Merhabalar. Ben **Kasım Gökhan Coşkun**. 4 yıldır Koç Sistem SOC ekibinde çalışıyorum. Gazi Üniversitesi Adli Bilişim Yüksek Lisans Eğitimim, "IBM Qradar SIEM Administrator" sertifikam ve "Linux /Os, Açık Kaynak Kod Projeler" özelinde vermiş olduğum eğitimlerim ve seminerlerim bulunmaktadır.
Doğa ve doğada olmak en büyük keyfim.

KASIM GÖKHAN COŞKUN
SOC SİSTEM YÖNETİMİ KD. ALAN UZMANI

Yapay Zeka Kullanımında

Siber Güvenlik

BİLGİNİ KORU, AV OLMA!

Günümüz dijital dünyasında yapay zeka, iş süreçlerini optimize etme ve yenilikçi çözümler geliştirme konusunda büyük fırsatlar sunmasıyla beraber ciddi siber güvenlik risklerini de gündeme getiriyor.

Yapay zeka sistemlerine kurumsal verilerin yüklenmesi, hassas bilgilerin yanlış ellere geçme riskini artırabilir, hassas verilerin kurum dışına çıkması şirketin itibarını zedeleyebilir ve finansal kayıplara neden olabilir.

Güvenliğin sağlanabilmesi için, kurumsal verilerin hiçbir şekilde yapay zeka ortamlarına yüklenmemesi önem taşımaktadır. Bu tür verilerin önce mutlaka kapsamlı bir risk analizi yapılmalı ve gerekli önlemler alınmalıdır. Unutulmamalıdır ki, bilginin korunması, dijital dönüşümün en kritik parçasıdır.

İstatistiklerle Riskler

Kontrolsüz yapay zeka kullanımı sebebiyle Dünya'da pek çok veri ihlali yaşanmaktadır.

Veri ihlalleri 2024 yılında **353.027.892** mağduru etkiledi ve olayların **%11'i** kurumsal verilerin yapay zeka botlarına yüklenmesi kaynaklı gerçekleşti.

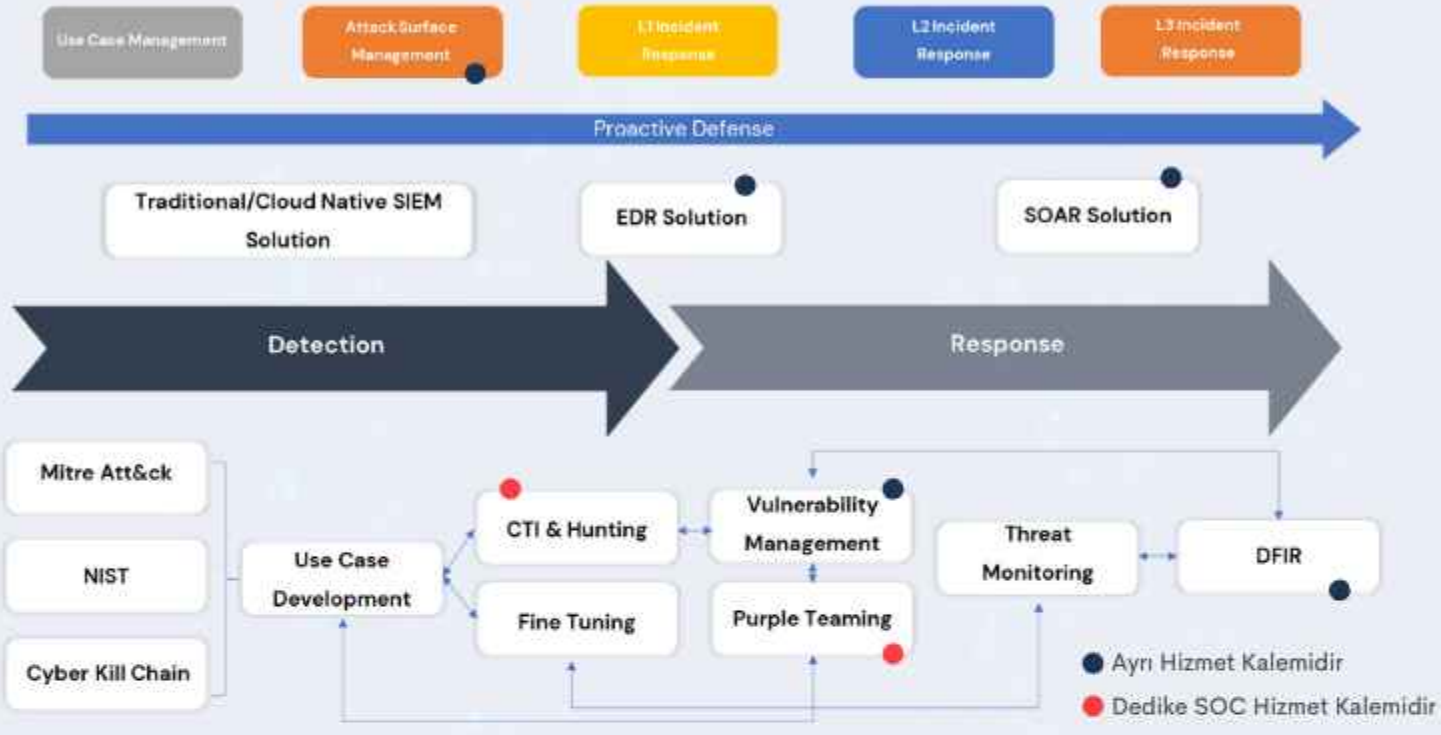
Yapay zeka kaynaklı veri ihlallerinin küresel maliyeti geçen yıl **ortalama 4,88 milyon dolardı.**

Siber güvenlik uzmanlarının **%75'i** geçen yıl yapay zeka kaynaklı veri ihlallerine yanıt vermek için stratejilerini değiştirmek zorunda kaldı.

KoçSistem | SOC
GELECEĞİ KEŞFET

GELECEĞİ KEŞFET!

Ürün ve Servislerimiz



Microsoft Defender

Microsoft Sentinel

BRANDEFENSE

PRODAFT

CROWDSTRIKE

CORTEX XDR

IBM QRadar

PICUS

CORTEX XSOAR
BY PALO ALTO NETWORKS

/ KocSistem