CROWDSTRIKE

MAGAZINE

ATT&CK v20.1 · FALCON



15 TAKTİK × FALCON

MITRE ATT&CK Tehdit Görünümü: CrowdStrike Falcon Modülleriyle Taktik Bazlı Eşleme

ATT&CK v20.1'in 15 Enterprise taktiğini, CrowdStrike 2026 Global Threat Report'taki tehdit eğilimleri ve resmi Falcon modülleriyle eşleyen bir CISO rehberi. Her eşlemenin resmi kaynağa mı dayandığı yoksa çıkarım mı olduğu ayrıca belirtildi.

Yapay zekâ görseli · Ressam

Hazırlayan: Selim ÖZİŞ

BU SAYIDA

İçindekiler

01	ATT&CK Enterprise: güncel çerçeve	3
02	Tehdit görünümü: 2025'te neler kötüye kullanıldı	4
03	Türkiye ve META bağlamı	6
04	15 taktik × Falcon modülleri eşleme tablosu	7
05	Kapsama ısı haritası	9
06	Falcon Guardian: AI ajanları için AIDR	10
07	Kesişen katman: SOC, otomasyon ve yönetilen hizmet	11
08	Yol haritası: satın almalar ve gelecek modül geliştirmeleri	12
09	MITRE ATT&CK Evaluations sonuçları	14
10	Türk CISO'ları için pratik çıkarımlar	15
–	Özel Ek	16
–	Kaynaklar	29
–	Kolofon	31

EDİTÖRDEN

ATT&CK v20.1'in 15 Enterprise taktiğini, CrowdStrike 2026 Global Threat Report'taki tehdit eğilimleri ve resmi Falcon modülleriyle eşleyen bir CISO rehberi. Her eşlemenin resmi kaynağa mı dayandığı yoksa çıkarım mı olduğu ayrıca belirtildi.

Hazırlayan: Selim ÖZİŞ

01 · ÇERÇEVE

ATT&CK Enterprise: güncel çerçeve

Önemli güncelleme: artık 14 değil, 15 taktik var.

ATT&CK v19 (Nisan 2026), Defense Evasion taktiğini ikiye böldü: Stealth (TA0005, eski ID'yi devraldı) ve Defense Impairment (TA0112, yeni). Güncel sürüm 13 Ekim 2026'da yayımlanan v20.1. T1562 Impair Defenses iptal edildi, yerini T1685 Disable or Modify Tools aldı.

GÜNCEL SÜRÜM	ATT&CK v20.1 (13 Ekim 2026'dan beri)
ENTERPRISE KAPSAMI	15 taktik, 227 teknik, 479 alt teknik, 178 grup
V19 YAPISAL DEĞİŞİKLİK	Defense Evasion → Stealth (TA0005) + Defense Impairment (TA0112)
V20 YENİLİKLERİ	Direct ve Indirect Prompt Injection, AI-Enabled Exfiltration, Anti-Automation Evasion (CAPTCHA) gibi yapay zekâ odaklı teknikler

Taktik saldırganın amacını ("neden"), teknik ise yöntemini ("nasıl") anlatır. Stealth, savunmalar çalışırken saldırganın normal davranışın içinde kaybolmasıdır; Defense Impairment ise EDR'ı, log hattını veya güven kontrollerini doğrudan bozmasıdır. Bu ayrım, SOC'taki tespit kurallarının ve kapsama raporlarının yeniden eşlenmesini gerektirir.

15 taktik

Reconnaissance 01 TA0043 RESMİ KAYNAK	**Resource Development** 02 TA0042 RESMİ KAYNAK	**Initial Access** 03 TA0001 RESMİ KAYNAK
Execution 04 TA0002 RESMİ KAYNAK	**Persistence** 05 TA0003 KISMEN ÇIKARIM	**Privilege Escalation** 06 TA0004 RESMİ KAYNAK
Stealth 07 TA0005 RESMİ KAYNAK	**Defense Impairment** 08 TA0112 KISMEN ÇIKARIM	**Credential Access** 09 TA0006 RESMİ KAYNAK
Discovery 10 TA0007 KISMEN ÇIKARIM	**Lateral Movement** 11 TA0008 RESMİ KAYNAK	**Collection** 12 TA0009 KISMEN ÇIKARIM
Command and Control 13 TA0011 RESMİ KAYNAK	**Exfiltration** 14 TA0010 RESMİ KAYNAK	**Impact** 15 TA0040 RESMİ KAYNAK

Defense Evasion → Stealth (TA0005) + Defense Impairment (TA0112)

Tehdit görünümü: 2025'te neler kötüye kullanıldı



Yapay zekâ görseli · Ressam

CrowdStrike 2026 Global Threat Report'a göre 2025 "kaçamak saldırganın yılı" oldu: saldırganlar geçerli kimlik bilgileri, güvenilen kimlik akışları ve onaylı SaaS entegrasyonlarıyla ilerledi.

29 dk

Ortalama eCrime breakout süresi

2024'e göre %65 daha hızlı

27 sn

Gözlenen en hızlı breakout

%82

Malware-free tespit oranı

2020'de %51

%89

AI destekli saldırganların saldırı artışı

%37

Cloud-conscious saldırı artışı

Devlet bağlantılılarda %266

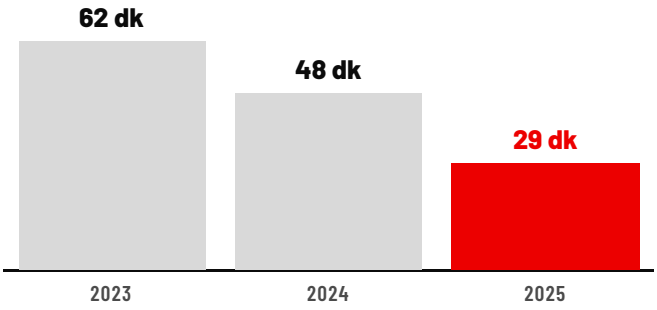
%35

Bulut olaylarında valid account kötüye kullanımı

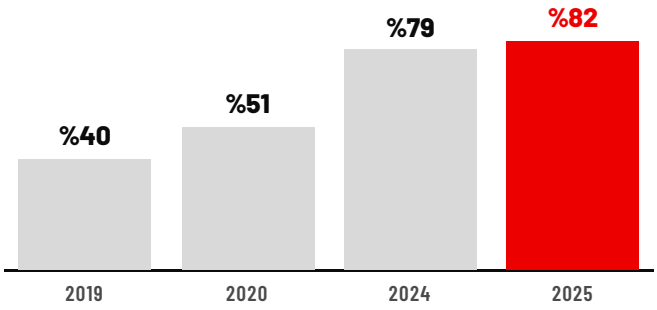
%42

Kamuya açıklanmadan istismar edilen zero-day artışı

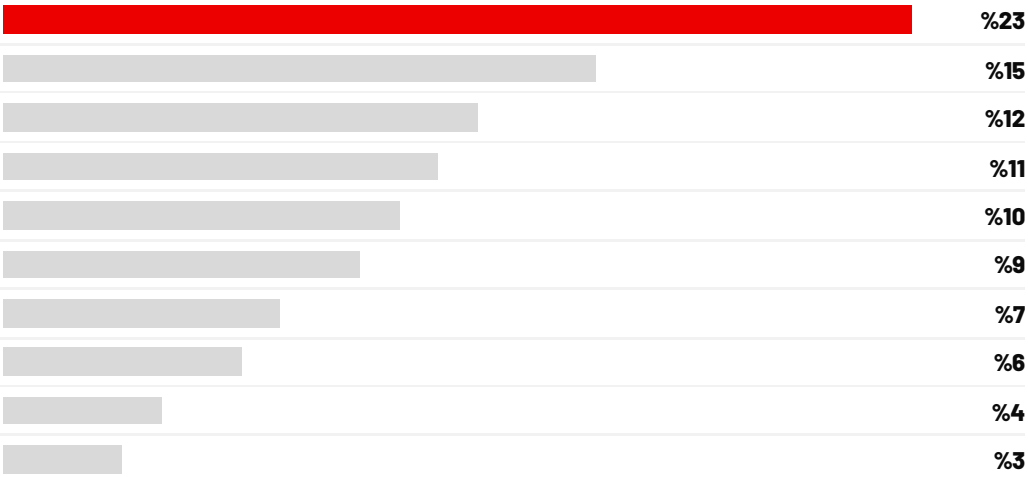
ORTALAMA BREAKOUT SÜRESİ (DAKİKA)



MALWARE-FREE TESPİT PAYI



INTERACTIVE INTRUSION HEDEFİNDEKİ İLK 10 SEKTÖR (2025)



KİMLİK

Vishing ve help desk sosyal mühendisliği

SCATTERED SPIDER vishing ve SSO kötüye kullanımını tercih etti; 2025 raporunda vishing H1→H2 2024 arasında %442 artmıştı. Eşlenen teknikler: T1566, T1078, T1621.

KULLANICI

Sahte CAPTCHA tuzaklarında %563 artış

Kullanıcıya komut kopyalatıp çalıştırma (T1204 User Execution), spam e-postada %141 artış.

UÇ CİHAZ

Edge cihaz ve zero-day istismarı

China-nexus aktörlerin istismar ettiği açıkların %67'si doğrudan sistem erişimi verdi, %40'ı edge cihazları hedefledi (T1190).

TEDARİK ZİNCİRİ

Güvenilen kanaldan giriş

PRESSURE CHOLLIMA'nın tedarik zinciri üzerinden 1,46 milyar USD kripto varlık hırsızlığı (T1195, T1657).

YAPAY ZEKÂ

Prompt'lar yeni malware

90'dan fazla kuruluşta meşru GenAI araçlarına zararlı prompt enjekte edildi; ATT&CK v20 bu davranışları yeni tekniklerle kataloğa ekledi.

HIZ

Dört dakikada exfiltration

CHATTY SPIDER vishing → RMM kurulumu → WinSCP ile veri sızdırma zincirini dakikalar içinde tamamladı (T1219, T1567).

03 · BÖLGE

Türkiye ve META bağlamı

ADLANDIRMA

Türkiye bağlantılı aktörler WOLF olarak izleniyor

CrowdStrike adlandırma şemasında WOLF Türkiye'yi, KITTEN İran'ı, SPHINX Mısır'ı, HAWK Suriye'yi temsil ediyor. Bölge kendi devlet bağlantılı tehdit kümelerine sahip.

İRAN

IMPERIAL KITTEN ilk kez bulut kimliklerini hedefledi

Kasım 2025'te EvilGinx2 AiTM kitiyle İsrail'deki Microsoft 365 kullanıcılarını hedef aldı, ardından M365 hesaplarında keşif yaptı (T1566, T1539, T1087).

BULUT KİMLİĞİ

Entra ID akışlarının kötüye kullanımı

COZY BEAR, MURKY PANDA ve BLOCKADE SPIDER Entra ID güven ilişkilerini ve kimlik doğrulama akışlarını hedef aldı. Microsoft 365 ağırlıklı Türk kurumları için doğrudan ilgili.

> *"Falcon Adversary Intelligence Recon+ filtered out the noise and surfaced real supplier breaches. Paired with identity protection, we caught credential risks early and acted before they became our problem."*
>
> **— Jaifar Al Mamari, CISO, Vodafone Oman (crowdstrike.com, Digital Risk Protection sayfası)**

Raporda Orta Doğu'ya ait ayrı bir yüzde net okunamadığı için bölgesel oran verilmedi; Türkiye'ye özgü olay istatistiği de raporda yer almıyor.

04 · EŞLEME

15 taktik × Falcon modülleri eşleme tablosu

TÜMÜ 15 | RESMİ KAYNAK 11 | KISMEN ÇIKARIM 4

Resmi kaynak / Kısmen çıkarım

"Resmi kaynak" satırları crowdstrike.com ürün sayfalarına, CrowdStrike'ın MITRE 2025 blog yazısına veya evals.mitre.org sonuçlarına dayanıyor. "Kısmen çıkarım" satırlarında ürün yeteneği resmi olarak tanımlı, ancak o taktiğe özgü eşleme editoryal yorumdur. Teknik ID'ler attack.mitre.org v20.1 üzerinde doğrulandı.

TAKTİK	TEMSİLİ TEKNİKLER	FALCON MODÜLLERİ	DAYANAK	KANIT NOTU
01 **Reconnaissance** (TA0043)	T1595 Active Scanning · T1593 Search Open Websites/Domains · T1598 Phishing for Information	Falcon Exposure Management (EASM) · Falcon Adversary Intelligence (dijital risk, Recon+)	RESMİ KAYNAK	Resmi: EASM ve otomatik keşif ürün sayfalarında; Recon taktiği ilk kez MITRE 2025'te test edildi
02 **Resource Development** (TA0042)	T1583 Acquire Infrastructure · T1585 Establish Accounts · T1588 Obtain Capabilities	Falcon Adversary Intelligence (sahte domain takedown, sahte hesap ve dark web izleme)	RESMİ KAYNAK	Resmi: Digital Risk Protection sayfası sahte domain ve sahte hesap takibini tanımlıyor
03 **Initial Access** (TA0001)	T1566 Phishing · T1078 Valid Accounts · T1190 Exploit Public-Facing Application · T1195 Supply Chain Compromise	Falcon Prevent · Falcon Next-Gen Identity Security · Falcon Exposure Management · Falcon Shield · Falcon Seraphic Enterprise Browser · Falcon Guardian (AI supply chain)	RESMİ KAYNAK	Resmi: Prevent'te paket indirme anında tedarik zinciri engelleme; girişte phishing-resistant MFA; MITRE 2025 Test 1 Protected. Seraphic ve Guardian'ın (zararlı MCP sunucusu/skill tespiti → T1195) bu taktiğe eşlenmesi çıkarım
04 **Execution** (TA0002)	T1059 Command and Scripting Interpreter · T1204 User Execution (sahte CAPTCHA) · T1047 WMI · T1699 Direct Prompt Injection · T1698 Indirect Prompt Injection	Falcon Prevent (IOA, davranış analizi, bellek tarama) · Falcon Insight XDR · Falcon Guardian (prompt injection, ajan runtime kontrolü)	RESMİ KAYNAK	Resmi: Prevent ürün sayfası; MITRE 2025 Test 4 Protected. Guardian prompt injection tespitini resmi olarak tanımlıyor; T1699/T1698 ATT&CK v20'de Execution taktiğinde
05 **Persistence** (TA0003)	T1547 Boot or Logon Autostart · T1053 Scheduled Task/Job · T1098 Account Manipulation · T1136 Create Account	Falcon Insight XDR · Falcon Cloud Security · Falcon Next-Gen Identity Security	KISMEN ÇIKARIM	Bulut tarafı resmi (MITRE 2025'te ayrıcalıklı backdoor tespiti); uç nokta ve kimlik kalıcılığı eşlemesi çıkarım
06 **Privilege Escalation** (TA0004)	T1068 Exploitation for Privilege Escalation · T1548 Abuse Elevation Control · T1078 Valid Accounts	Falcon Prevent (exploit mitigation) · Falcon Next-Gen Identity Security (standing privilege kaldırma) · Falcon Cloud Security (CIEM)	RESMİ KAYNAK	Resmi: ürün sayfaları; MITRE 2025 bulut koruma testinde yönetici IAM rolü kurulumu durduruldu

TAKTİK		TEMSİLİ TEKNİKLER	FALCON MODÜLLERİ	DAYANAK	KANIT NOTU
Stealth (TA0005)	07	T1036 Masquerading · T1027 Obfuscated Files · T1218 System Binary Proxy Execution · T1070 Indicator Removal · T1684 Social Engineering	Falcon Insight XDR · Falcon Prevent · Falcon Adversary Intelligence (sandbox) · Falcon Fusion SOAR	RESMİ KAYNAK	Resmi: MITRE 2025 blogu LOLbin ve çift kullanımlı araç tespiti ile MUSTANG PANDA kodlanmış shellcode analizini anlatıyor
Defense Impairment (TA0112)	08	T1685 Disable or Modify Tools · T1686 Disable or Modify System Firewall · T1556 Modify Authentication Process · T1484 Domain or Tenant Policy Modification	Falcon Firewall Management · Falcon Cloud Security · Falcon Next-Gen Identity Security · Falcon Next-Gen SIEM	KISMEN ÇIKARIM	Resmi: MITRE 2025'te bulut firewall kurcalama girişimi tespit edildi; kimlik ve GPO eşlemesi çıkarım
Credential Access (TA0006)	09	T1003 OS Credential Dumping · T1110 Brute Force · T1621 MFA Request Generation · T1539 Steal Web Session Cookie	Falcon Next-Gen Identity Security · Falcon Insight XDR · Falcon Adversary Intelligence · Falcon Adversary OverWatch · Falcon Guardian	RESMİ KAYNAK	Resmi: otomatik MFA veya parola sıfırlama, dark web kimlik bilgisi izleme; MITRE 2025 Test 1 Protected. Guardian eşlemesi çıkarım: GTR 2026'da GenAI araçlarına kimlik bilgisi çaldıran prompt'lar enjekte edildi
Discovery (TA0007)	10	T1087 Account Discovery · T1069 Permission Groups Discovery · T1046 Network Service Discovery	Falcon Insight XDR · Falcon Cloud Security · Falcon Next-Gen Identity Security	KISMEN ÇIKARIM	Resmi: MITRE 2025'te AWS IAM ve S3 haritalama tespit edildi; AD keşif eşlemesi çıkarım
Lateral Movement (TA0008)	11	T1021 Remote Services · T1550 Use Alternate Authentication Material · T1570 Lateral Tool Transfer	Falcon Next-Gen Identity Security · Falcon Insight XDR	RESMİ KAYNAK	Resmi: yönetilmeyen hosttan erişim engellendi; MITRE 2025 Test 3 ve Test 5 Protected
Collection (TA0009)	12	T1560 Archive Collected Data · T1005 Data from Local System · T1114 Email Collection · T1530 Data from Cloud Storage	Falcon Data Security · Falcon Shield · Falcon Cloud Security · Falcon Guardian	KISMEN ÇIKARIM	Ürün sayfaları veri hareketini, SaaS verisini ve ajanların hassas dosya erişimini kapsıyor; taktik bazlı eşleme çıkarım
Command and Control (TA0011)	13	T1071 Application Layer Protocol · T1219 Remote Access Tools (RMM) · T1572 Protocol Tunneling	Falcon Insight XDR · Falcon Adversary Intelligence · Falcon Next-Gen SIEM · Falcon Guardian (AI Gateway, Endpoint Network Inspection)	RESMİ KAYNAK	Resmi: MITRE 2025'te RMM kötüye kullanımı tespit edildi; sandbox C2 davranışını ortaya çıkarıyor. Guardian'ın AI/MCP trafiği denetiminin C2'ye eşlenmesi çıkarım
Exfiltration (TA0010)	14	T1567 Exfiltration Over Web Service · T1041 Exfiltration Over C2 Channel · T1537 Transfer Data to Cloud Account · T1700 AI-Enabled Exfiltration	Falcon Data Security · Falcon Device Control · Falcon Cloud Security · Falcon Guardian	RESMİ KAYNAK	Resmi: egress kanalı takibi ve USB sızıntı tespiti; MITRE 2025'te S3'e yönlendirilen veri akışı tespit edildi. Guardian prompt'larda hassas veri/PII korumasını resmi olarak tanımlıyor; T1700 eşlemesi çıkarım
Impact (TA0040)	15	T1486 Data Encrypted for Impact · T1490 Inhibit System Recovery · T1489 Service Stop · T1657 Financial Theft	Falcon Prevent · Falcon Insight XDR · Falcon Complete	RESMİ KAYNAK	Resmi: fidye yazılımı koruma sayfası, SE Labs EDR Ransomware Test (dört yıl üst üste %100)

05 · ISI HARİTASI

Kapsama ısı haritası

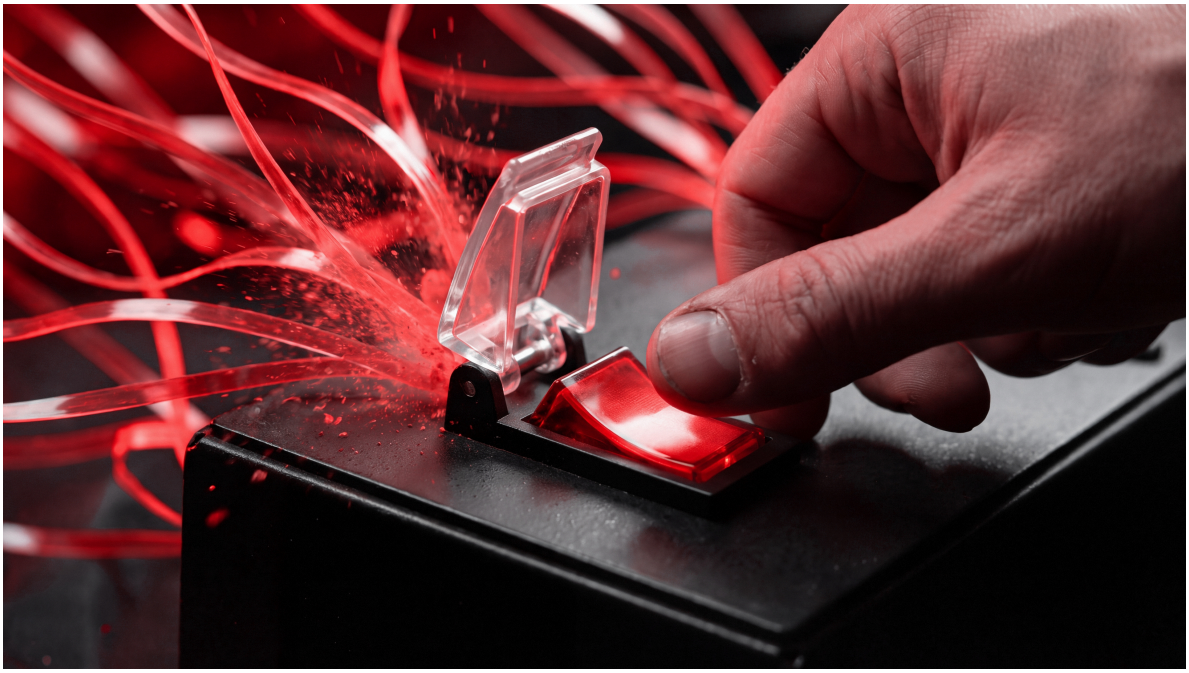
Endpoint katmanı orta zincirin omurgası olmaya devam ediyor. Ancak saldırı zincirinin başı (keşif, kaynak geliştirme) ve sonu (toplama, sızdırma) intel, exposure, SaaS ve veri katmanlarına kayıyor. Malware-free oranının %82 olması bu kaymanın nedenini açıklıyor.

2 1 0 Editoryal değerlendirme: 2 = birincil kontrol katmanı, 1 = destekleyici, 0 = doğrudan rol yok.

	Endpoint	Identity	Cloud	SaaS ve Veri	Intel ve Exposure	AI ajanları
Reconnaissance	0	0	0	0	2	0
Resource Development	0	0	0	0	2	0
Initial Access	2	2	1	1	1	1
Execution	2	0	1	0	1	2
Persistence	2	1	2	1	0	0
Privilege Escalation	2	2	2	0	0	0
Stealth	2	0	1	0	1	0
Defense Impairment	2	1	1	0	0	0
Credential Access	2	2	1	1	1	1
Discovery	2	1	2	0	0	0
Lateral Movement	2	2	1	0	0	0
Collection	1	0	1	2	0	1
Command and Control	2	0	0	0	1	1
Exfiltration	1	0	2	2	0	2
Impact	2	0	1	0	0	0

06 · FALCON GUARDIAN

Falcon Guardian: AI ajanları için AIDR



Yapay zekâ görseli · Ressam

CrowdStrike Falcon Guardian, 1 Eylül 2026'da Fal.Con'da tanıtılan ve Eylül 2026'dan beri genel kullanımda olan AI Detection and Response (AIDR) çözümü. CrowdStrike'a göre Falcon AIDR'ın evrimi. Çalışan ve uykudaki AI ajanlarını keşfediyor, prompt'tan runtime davranışına kadar zinciri Falcon sensörüyle izliyor ve yetkisiz ajanları engelliyor. Kapsamı endpoint, SaaS ve cloud.

RESMİ ADI	CrowdStrike Falcon Guardian (ürün sayfası: Falcon AIDR)
KATEGORİ	AI Detection and Response (AIDR)
ÜÇ KONTROL KATMANI	OS seviyesinde runtime görünürlüğü (Falcon sensörü), Endpoint Network Inspection, agent-level hooks; CrowdStrike Agent Graph bunları birbirine bağlıyor
DESTEKLENEN AJANLAR (HOOKS)	Claude Code, OpenAI Codex, GitHub Copilot, Microsoft 365 Copilot, OpenCode, Cursor
TESPİT	SafeMind modelleri ve adversary intelligence ile prompt injection, zararlı talimat ve PII tespiti
ENTEGRASYON	Ajan verisi Falcon Next-Gen SIEM'e first-party veri olarak akıyor; Falcon Complete ve Falcon Adversary OverWatch Guardian kapsamını içeriyor

T1699 · T1698 · T1700

ATT&CK v20, Direct ve Indirect Prompt Injection'ı (T1699, T1698) Execution, AI-Enabled Exfiltration'ı (T1700) Exfiltration taktiğine ekledi. Guardian bu yeni tekniklere en doğrudan karşılık gelen Falcon modülü. Tablodaki taktik eşlemelerinin bir kısmı çıkarımdır ve satır notlarında belirtilmiştir.

07 · KESİŞEN KATMAN

Kesişen katman: SOC, otomasyon ve yönetilen hizmet

SIEM	**Falcon Next-Gen SIEM** Birinci ve üçüncü taraf verileri birleştirir, çoklu ajan soruşturmalarını yürütür; Falcon Onum veri hattı ve federated search içerir. Her taktikte korelasyon katmanı.
SOAR	**Falcon Fusion SOAR ve Charlotte Agentic SOAR** No-code iş akışları ve yerleşik case management sağlar. MITRE 2025'te intel çıktısı analist müdahalesi olmadan tespit ve korumaya dönüştürüldü.
AI	**Charlotte AI** Agentic detection triage ile alanlar arası bağlamı birleştirir ve yönetişimli yanıt aksiyonlarını orkestre eder.
HUNTING	**Falcon Adversary OverWatch** Endpoint, kimlik, bulut, AI ve 325'ten fazla NG-SIEM veri kaynağında 7/24 intel odaklı tehdit avı sunar; kimlik tarafında MFA challenge tetikler.
MDR	**Falcon Complete** Agentic MDR: 7/24 tespit, soruşturma ve uçtan uca iyileştirme sağlar; Falcon Shield ile SaaS kapsamını da içerir.
IT HİJYENİ	**Falcon for IT** Risk tabanlı yama, yapılandırma sapmasını giderme ve uç noktalardaki gölge AI keşfi sunar. Initial Access ve Impact öncesi saldırı yüzeyini küçültür.
AI	**Falcon Guardian** AI ajanları için AIDR: keşif, runtime görünürlüğü, AI Gateway, AI Kill Switch. Execution ve Exfiltration'daki yeni AI tekniklerine karşı.
TARAYICI	**Falcon Seraphic Enterprise Browser** Yönetilen ve yönetilmeyen cihazlarda tarayıcı içi kullanıcı, veri ve AI etkileşimi koruması; olaylar Falcon Next-Gen SIEM'e akar.
OT/IOT	**Falcon for XIoT** IT ve XIoT/OT varlık görünürlüğü ve koruması. ICS ATT&CK matrisi kapsamında olduğundan Enterprise tablosunda yer almadı.

08 · YOL HARİTASI

Yol haritası: satın almalar ve gelecek modül geliştirmeleri



Yapay zekâ görseli · Ressam

DUYURU	ŞİRKET	NE YAPIYOR	FALCON'A KATKISI (CROWDSTRIKE İFADESİYLE)	İLGİLİ TAKTİKLER (ÇIKARIM)
27 AĞUSTOS 2025	**Onum**	Gerçek zamanlı telemetri pipeline yönetimi	Falcon Next-Gen SIEM'in veri temeli; pipeline içinde tespit. Bugün Falcon Onum olarak sitede yer alıyor	**Tüm taktiklerde korelasyon (SOC katmanı)**
16 EYLÜL 2025	**Pangea**	AI prompt katmanı güvenliği	İlk tam AIDR; direct/indirect prompt injection engelleme. Falcon Guardian, Falcon AIDR'ın evrimi	**Execution, Exfiltration**
8 OCAK 2026	**SGNL**	Continuous Identity, dinamik yetkilendirme	Next-Gen Identity Security; insan, NHI ve AI kimlikleri için gerçek zamanlı riske göre erişim verme ve geri alma	**Privilege Escalation, Lateral Movement, Persistence**
13 OCAK 2026	**Seraphic Security**	Tarayıcı runtime güvenliği	Herhangi bir tarayıcıyı güvenli kurumsal tarayıcıya çevirmek. Bugün Falcon Seraphic Enterprise Browser	**Initial Access, Credential Access, Exfiltration**

16 TEMMUZ 2026

XM Cyber (yalnızca fikri mülkiyet)

NE YAPIYOR	FALCON'A KATKISI (CROWDSTRIKE İFADESİYLE)	İLGİLİ TAKTİKLER (ÇIKARIM)
Attack path görselleştirme ve ofansif simülasyon	Falcon platformunda exposure management. Kapanış FY27'nin ikinci yarısında bekleniyor	Reconnaissance, Lateral Movement, Privilege Escalation

3 KASIM 2026

Dreadnode

NE YAPIYOR	FALCON'A KATKISI (CROWDSTRIKE İFADESİYLE)	İLGİLİ TAKTİKLER (ÇIKARIM)
Otomatik AI güvenlik testi	Modeller, ajanlar ve MCP sunucularında 100'den fazla saldırı stratejisi. Bulgular MITRE ATLAS ve OWASP ile eşleniyor, Falcon Guardian'a politika önerisi olarak gidiyor. GA Q4 FY27	Execution (prompt injection), Initial Access (AI supply chain)

3 KASIM 2026

Fiddler AI

NE YAPIYOR	FALCON'A KATKISI (CROWDSTRIKE İFADESİYLE)	İLGİLİ TAKTİKLER (ÇIKARIM)
AI ajan gözlemlenebilirliği ve açıklanabilirlik	Falcon Observe adıyla satılacak: ajanların dağıtım öncesi değerlendirmesi, davranış sapması ve karar izlenebilirliği. GA Q4 FY27	Execution, Exfiltration, Impact

Duyurulmuş ve kullanılabilir

Falcon Guardian
Eylül 2026'dan beri GA

AI Gateway
GA ve Guardian'a dahil; prompt ve yanıt denetimi, MCP dahil

AI Kill Switch (gateway üzerinde)
Yetkisiz ajanları gerçek zamanlı sonlandırır

Agent-level hooks, SafeMind tespiti, AI Supply Chain Protection
3 Kasım 2026'da "Available Today" olarak duyuruldu

Endpoint Network Inspection
Windows'ta GA, Mac'te early access

Falcon Onum, Falcon Seraphic Enterprise Browser
crowdstrike.com'da ürün sayfaları yayında

Beklenen ve ileriye dönük

AI Kill Switch endpoint'te
"Soon" olarak duyuruldu

Agentic Identity
Ajanların neye erişebileceğini yetkilendiren kimlik farkındalıklı kontroller

Guardian bulut genişlemesi
Cloud workload, Linux, Kubernetes, yönetilen AI platformları, AWS AgentCore

NG-SIEM ajan davranış baseline'ı
Kullanıcı ve ajanlar için sapma tespiti, "coming soon"

Falcon Observe (Fiddler), Automated AI Security Testing (Dreadnode)
İkisinin de GA hedefi Q4 FY27; satın almaların kapanışı bekleniyor

XM Cyber IP
Kapanış FY27'nin ikinci yarısında bekleniyor

FY27

FY27, CrowdStrike'ın 31 Ocak 2027'de biten mali yılıdır. Son sütundaki taktik eşlemeleri editoryal çıkarımdır; satın alma duyuruları ATT&CK taktiği belirtmiyor. Dreadnode'un MITRE ATLAS ile eşlemesi ise resmi ifadedir.

MITRE ATT&CK Evaluations sonuçları

Enterprise 2025 (ER7), programın ilk bulut kontrol düzlemi emülasyonu oldu: SCATTERED SPIDER (eCrime, hibrit kimlik ve AWS) ile MUSTANG PANDA (Çin bağlantılı, uzun süreli casusluk). Reconnaissance taktiği de ilk kez değerlendirildi.

CROWDSTRIKE'IN AÇIKLADIĞI SONUÇLAR

%100	%100	%100	Sıfır
Detection	Protection	Technique-level detail	False positive

Not: Tespit sonuçları configuration run'a aittir

EVALS.MITRE.ORG KORUMA TESTLERİ (CROWDSTRIKE)

TEST	SONUÇ
1 · Credential Theft	PROTECTED
2 · Identity Providers	MITRE tüm katılımcılar için iptal etti
3 · Unmanaged to Managed Devices	PROTECTED
4 · Initial Access Malware Execution	PROTECTED
5 · Malware Execution & Lateral Movement	PROTECTED
6 · False Positives (noise testi)	NOT REPORTED (BEKLENEN)
7 · AWS Compromise	PROTECTED

Sıradaki tur: Enterprise 2026 (ER8).

MITRE, sonuçların Aralık 2026'da yayımlanacağını, 9–20 Kasım 2026'nın taslak sonuç inceleme penceresi olduğunu açıklıyor. Yeni Total Evaluation Score (TES) 0–2,0 ölçeğinde. CrowdStrike sekizinci kez katılıyor. Teknik kapsam ATT&CK v18.1'e (Defense Evasion dahil) göre tanımlı ve MITRE bireysel sonuçların gizli kalabileceğini not ediyor. Bu sayfada ER8 skoru yok.

Türk CISO'ları için pratik çıkarımlar

1

Kapsama haritanızı ATT&CK v19/v20'ye taşıyın

Defense Evasion referanslarını Stealth ve Defense Impairment'a ayırın; T1562 geçen tüm kural, istisna ve raporları T1685 ve yeni ID'lere göre güncelleyin.

2

Kimliği birincil saldırı yüzeyi olarak yönetin

Phishing-resistant MFA, help desk parola sıfırlamada güçlü doğrulama, hibrit AD/Entra ID için gerçek zamanlı ITDR. Bulut olaylarının %35'i valid account ile başlıyor.

3

29 dakikalık breakout'a göre yanıt tasarlayın

Gece ve hafta sonu kapsamını 7/24 hunting/MDR ile kapatın; containment adımlarını SOAR playbook'larıyla otomatikleştirin.

4

Edge cihaz ve dış yüzey envanterini sürekli tutun

VPN, firewall ve gateway'ler China-nexus istismarının %40'ını oluşturuyor. EASM ve risk tabanlı yama ile önceliklendirin.

5

SaaS ve GenAI'ı veri kaybı zincirine dahil edin

OAuth token ve SaaS entegrasyon izleme, GenAI'a giden hassas veri kontrolü; Collection ve Exfiltration artık uç noktanın dışında gerçekleşiyor.

6

MITRE sonuçlarını doğru okuyun

Configuration run ile varsayılan ayarları ayırın, technique-level detail ve false positive davranışına bakın; ER8 TES skorlarını Aralık 2026'da kendi senaryonuzla karşılaştırın.



Yapay zekâ görseli · Ressam

ÖZEL EK · CROWDSTRIKE MAGAZINE

Özel Ek: ARTEX

Saldırganın Elindeki Otonom AI Pentest Ajanı

Özel Ek — FBI FLASH-20261113-001: ARTEX Otonom Penetrasyon Testi Framework'ü

https://www.ic3.gov/CSA/2026/261113.pdf (TLP:CLEAR)

Spot: FBI, 13 Kasım 2026'da LLM tabanlı ajan framework'ü ARTEX'in saldırganlar tarafından keşiften veri sızdırmaya kadar tüm zinciri "makine hızında" otomatikleştirmek için kullanıldığını duyurdu. Bu ek, FLASH'taki her ATT&CK tekniğini CrowdStrike Falcon modülleriyle tek tek eşliyor.

Hazırlayan: Selim ÖZİŞ

1. Bülten künyesi

ALAN	BİLGİ
Başlık	*Threat Overview of ARTEX Autonomous Penetration Testing Framework*
Tür / numara	FBI FLASH, **FLASH-20261113-001**, TLP:CLEAR
Tarih	13 Kasım 2026
Yayımlayan	Federal Bureau of Investigation (FBI). Belgede başka bir ortak kurum imzası yok; ic3.gov'un `CSA` dizininde yayımlanmış olsa da belge kendini **FLASH** olarak tanımlıyor.
Konu	ARTEX: Go ile yazılmış, açık kaynaklı, çoklu ajanlı, LLM güdümlü otonom penetrasyon testi platformu
Aktörler	Tek bir aktör değil: "çeşitli kötü niyetli siber aktörler". Bültende anılan kampanyalar: Güney Kore finans kampanyası (CrowdStrike kaynaklı), ConnectWise Cloud Backup tedarik zinciri saldırısı (Microsoft kaynaklı), Microsoft'un **Storm-3358** olarak izlediği finans sektörü kampanyası
Hedef sektörler	Finansal hizmetler, kamu, teknoloji, savunma, yarı iletken, enerji, sağlık, imalat, telekomünikasyon, hukuk
Coğrafya	Küresel; Güney Kore özellikle anılıyor
Kullanılan LLM'ler	Frontier modeller (Anthropic Claude, OpenAI GPT) ve açık kaynak / Çin kökenli modeller (DeepSeek, GLM, Grok, Kimi). Saldırgan kontrolündeki örneklerde en yaygın olanlar Çin modelleri, özellikle DeepSeek Flash ailesi

Öne çıkan bulgular (FLASH'tan)

- Bazı saldırılar ilk hedeflemeden ayrıcalıklı erişime **3 saatten kısa** sürede ulaştı.
- Güney Kore finans kurumlarına yönelik kampanyada yaklaşık **67.000 kişinin** kişisel verisi sızdırıldı.
- ConnectWise Cloud Backup tedarik zinciri saldırısı **2.250'den fazla downstream tenant'a** erişim sağladı.
- Kasım 2026 başında internete açık **1.600'den fazla ARTEX konsolu** tespit edildi.
- Orijinal repo kaldırılmış olsa da fork'lar, yerelleştirilmiş sürümler, arşivler ve ticari **ARTEX PRO** sürümüyle yayılım sürüyor.
- ARTEX ağırlıklı olarak **çevresel yüzeyleri** hedefliyor: partner/tedarikçi portalları, mobil backend'ler, çalışan uygulamaları, satış destek sistemleri, legacy servisler, üçüncü taraf entegrasyonlar.

Zaman çizelgesi

TARİH (2026)	OLAY	KAYNAK
Temmuz	ARTEX, "Autumn-27" adlı geliştirici tarafından GitHub'da yayımlandı (10 haftada tahmini 1.500–2.000 yıldız)	FLASH
Ağustos (en geç)	Kötü niyetli kullanım başladı	FLASH
Eylül sonu – Ekim başı	Güney Kore finans kurumlarına kampanya	CrowdStrike blogu, 7 Ekim
7 Ekim	CrowdStrike Intelligence: *Unknown Threat Actor Uses AI-Driven ARTEX to Target South Korean Finance*	crowdstrike.com
8 Ekim	Geliştirici repoyu erişime kapattı	FLASH

TARİH (2026)	OLAY	KAYNAK
15–16 Ekim	ConnectWise kampanyasında Graph API erişimi için kullanılan geçici VPN IP'lerinin ilgili olduğu dönem	FLASH
17 Ekim	VAPOR PANDA'nın ARTEX kampanyası başladı (11 günde 14+ ülkede 200+ kurum)	CrowdStrike blogu, 29 Ekim
21 Ekim	Microsoft: ARTEX ile ConnectWise tedarik zinciri raporu	FLASH dipnotu
29 Ekim	CrowdStrike: *VAPOR PANDA Uses AI-Driven ARTEX to Scale a Global Espionage Campaign*	crowdstrike.com
6 Kasım	Storm-3358 altyapısı hâlâ aktif	FLASH
13 Kasım	FBI FLASH-20261113-001 yayımlandı	ic3.gov

2. CrowdStrike bu aktörleri izliyor mu?

Evet, iki ayrı raporla:

1. **Güney Kore finans kampanyası (7 Ekim 2026):** CrowdStrike Intelligence faaliyeti adı verilmiş bir adversary'ye **atfetmedi**. Aktörün orta güvenle Çince konuşan ve finansal motivasyonlu olduğunu değerlendiriyor. FLASH'taki `38.244.50[.]120` (ARTEX host'u), dokuz proxy IP'si ve `xcai[.]pro` (LLM API reseller) göstergelerinin kaynağı CrowdStrike'tır. Raporun ATT&CK tablosu: T1583.003, T1588.007, T1090.
2. **VAPOR PANDA (29 Ekim 2026): CrowdStrike OverWatch** kampanyayı tespit etti; CrowdStrike Intelligence ARTEX kontrolcüsünü VAPOR PANDA altyapısına bağladı. VAPOR PANDA, Çin merkezli, devlet destekli, istihbarat ve fikri mülkiyet hırsızlığı odaklı bir targeted intrusion adversary'sidir. İlk kez Şubat 2021'de ProxyLogon istismarıyla tespit edildi. Topluluk tanımlayıcısı: Earth Estries (crowdstrike.com adversary sayfası).
    - Falcon telemetrisi, kamuya açık ARTEX raporlarında olmayan **BLOODALCHEMY** backdoor'unu ve C2 altyapısını ortaya çıkardı.
    - Operatör ajanlara Çince olarak *"domainde Falcon kurulu olmayan Windows makinelerini tasklist ve klasör listelerinden bul"* talimatı verdi ("猎鹰", Falcon sensörü için PRC red-team argosu).
    - CrowdStrike, bu kampanyanın sektörde **Storm-0940** adıyla raporlanan ARTEX faaliyetinden ayrı olduğunu belirtiyor.

Not: *FLASH, Microsoft kaynaklı Storm-3358 kampanyasını anıyor; CrowdStrike blogu ise Storm-0940'tan bahsediyor. Bu iki Microsoft tanımlayıcısının ilişkisi kaynaklarda açıklanmıyor.*

3. Teknik bazlı eşleme: FLASH ATT&CK tablosu → Falcon

Dayanak sütununun anlamı:

RESMİ: Teknik, CrowdStrike'ın kendi ARTEX raporlarında (VAPOR PANDA veya Güney Kore blogu) OverWatch, Intelligence ya da Falcon telemetrisiyle gözlenmiş ve ATT&CK tablosunda listelenmiş. Bu, CrowdStrike'ın bu aktörün bu davranışını gördüğünü gösterir; ilgili modülün o tekniği her ortamda **önlediği** anlamına gelmez.

KISMEN/ÇIKARIM: İlgili Falcon modülünün yeteneği crowdstrike.com ürün sayfalarında tanımlı, ancak bu aktör ve teknik için açık bir CrowdStrike beyanı yok. Eşleme editoryal değerlendirmedir.

Teknik ID ve adları FLASH'ta yazıldığı gibidir; v20.1 farkları bir sonraki bölümdedir. Satırlar FLASH'taki faz sırasını izler. FLASH'ta birden fazla fazda geçen T1606.002, T1190 ve T1059 bir kez sayıldı; toplam **43 benzersiz teknik** var.

3.1 Initial Recon

#	TEKNİK (FLASH)	AKTÖRÜN KULLANIMI (FLASH)	FALCON MODÜLLERİ	DAYANAK
1	T1595 – Active Scanning	WHOIS ile varlık haritalama, aktif zafiyet taraması, 500+ istekle web dizini fuzzing, `api.db-ip[.]com` ile kurban coğrafi konumu	Falcon Exposure Management (EASM), Falcon Adversary Intelligence	KISMEN/ÇIKARIM
2	T1580 – Cloud Infrastructure Discovery	Azure SAS token, Service Principal, Kudu, Storage Account key yetkilerini saniyenin altında kontrol; test blob yazma/silme; ARM deployment dry-run; IAM yetkilerini DryRun ile test	Falcon Cloud Security (CDR, Real-Time Cloud IOA)	KISMEN/ÇIKARIM
3	T1087.004 – Account Discovery: Cloud Account	Bulut kimlik bilgilerinin etkin yetkilerini haritalama	Falcon Cloud Security (CIEM), Falcon Next-Gen Identity Security	KISMEN/ÇIKARIM
4	T1069.003 – Permission Groups Discovery: Cloud Groups	Aynı	Falcon Cloud Security (CIEM)	KISMEN/ÇIKARIM
5	T1526 – Cloud Service Discovery	Aynı	Falcon Cloud Security	KISMEN/ÇIKARIM

3.2 Initial Access

#	TEKNİK (FLASH)	AKTÖRÜN KULLANIMI (FLASH)	FALCON MODÜLLERİ	DAYANAK
6	T1190 – Exploit Public-Facing Application	İmzasız SAML assertion, XXE, anonim dosya yükleme, SSRF, command injection ve SSTI ile RCE, SQL injection, IDOR, kimlik doğrulamasız Web API, authentication bypass	Falcon Exposure Management, Falcon Cloud Security, Falcon Insight XDR, Falcon Adversary OverWatch	RESMİ: VAPOR PANDA blogu, "Exploited SAML, XXE"
7	T1078 – Valid Accounts	Zayıf admin kimlik bilgileri, çalıntı VPN konfigürasyonları ve sızdırılmış kimlik bilgileri	Falcon Next-Gen Identity Security, Falcon Adversary Intelligence (dark web credential izleme), Falcon Adversary OverWatch	RESMİ: VAPOR PANDA blogu
8	T1133 – External Remote Services	VPN üzerinden iç ağa erişim	Falcon Next-Gen Identity Security, Falcon Next-Gen SIEM (VPN logları), Falcon Exposure Management	RESMİ: VAPOR PANDA blogu

#	TEKNİK (FLASH)	AKTÖRÜN KULLANIMI (FLASH)	FALCON MODÜLLERİ	DAYANAK
9	T1195 – **Supply Chain Compromise**	ConnectWise Cloud Backup müşterileri; açık bulut kimlik bilgileriyle iOS uygulama dağıtım altyapısının değiştirilmesi	Falcon Shield (üçüncü taraf SaaS uygulamaları, NHI), Falcon Cloud Security, Falcon Next-Gen SIEM	KISMEN/ÇIKARIM
10	T1199 – **Trusted Relationship**	Harici partner tenant'tan cross-account bulut güveni; ele geçirilmiş tedarikçi kimlik bilgileriyle B2B federasyon üzerinden pivot	Falcon Next-Gen Identity Security, Falcon Cloud Security, Falcon Shield	KISMEN/ÇIKARIM
11	T1606.002 – **Forge Web Credentials: SAML Tokens**	İmzasız SAML assertion (FLASH'ta Privilege Escalation fazında da geçiyor)	Falcon Next-Gen Identity Security, Falcon Next-Gen SIEM	RESMİ: VAPOR PANDA blogu
12	T1552.001 – **Unsecured Credentials: Credentials in Files**	SPA JavaScript bundle'larında hardcoded admin parolaları	Falcon Cloud Security (ASPM), Falcon Exposure Management	KISMEN/ÇIKARIM

3.3 Establish Foothold / Persistence

#	TEKNİK (FLASH)	AKTÖRÜN KULLANIMI (FLASH)	FALCON MODÜLLERİ	DAYANAK
13	T1505.003 – **Server Software Component: Web Shell**	JSP ve PHP web shell'leri, MySQL log poisoning dahil	Falcon Insight XDR, Falcon Prevent, Falcon Cloud Security (runtime), Falcon Adversary OverWatch	RESMİ: VAPOR PANDA blogu
14	T1078.004 – **Valid Accounts: Cloud Accounts**	Hesap ele geçirme (parola sıfırlama)	Falcon Cloud Security, Falcon Next-Gen Identity Security	KISMEN/ÇIKARIM
15	T1098.001 – **Account Manipulation: Additional Cloud Credentials**	Mevcut OAuth uygulamalarına kimlik bilgisi ekleme	Falcon Shield, Falcon Next-Gen Identity Security, Falcon Next-Gen SIEM	KISMEN/ÇIKARIM
16	T1574.001 – **Hijack Execution Flow: DLL**	FLASH'ta faz içinde listeli. CrowdStrike'a göre BLOODALCHEMY loader DLL'i, yeniden adlandırılmış meşru bir binary ile yüklendi	Falcon Insight XDR, Falcon Prevent, Falcon Adversary Intelligence	RESMİ: VAPOR PANDA blogu
17	T1036.005 – **Masquerading**	CrowdStrike'a göre meşru GameHook binary'si `svchost.exe` adıyla kullanıldı	Falcon Insight XDR, Falcon Prevent	RESMİ: VAPOR PANDA blogu
18	T1105 – **Ingress Tool Transfer**	Açık kaynak RAT'ler (WISP, vshell, AdaptixC2)	Falcon Insight XDR, Falcon Prevent, Falcon Next-Gen SIEM	KISMEN/ÇIKARIM
19	T1059 – **Command and Scripting Interpreter**	Kudu yönetim API'leriyle rastgele komut çalıştırma; iç Windows veritabanı sunucularında C2 (FLASH'ta Collection fazında da geçiyor)	Falcon Cloud Security, Falcon Insight XDR	KISMEN/ÇIKARIM

FLASH bu fazda SSH anahtar çifti oluşturma ve Elastic IP tahsisini de gözlem olarak sayıyor, ancak bunlara ayrı bir teknik ID vermiyor.

3.4 Privilege Escalation

#	TEKNİK (FLASH)	AKTÖRÜN KULLANIMI (FLASH)	FALCON MODÜLLERİ	DAYANAK
20	T1134.001 – **Access Token Manipulation**	Resource-based constrained delegation (RBCD) kötüye kullanımı	Falcon Next-Gen Identity Security, Falcon Insight XDR	RESMİ: VAPOR PANDA blogu

#	TEKNİK (FLASH)	AKTÖRÜN KULLANIMI (FLASH)	FALCON MODÜLLERİ	DAYANAK
21	T1098.003 – **Account Manipulation: Additional Cloud Roles**	Yüksek değerli IAM rolleriyle compute instance başlatma; `is_admin=true` bayrağıyla hesap oluşturma	Falcon Cloud Security (CIEM, CDR)	KISMEN/ÇIKARIM. Not: MITRE 2025 koruma testinde benzer bir senaryo (yönetici IAM rolü ve EC2 başlatma) Falcon Cloud Security tarafından durduruldu
22	T1552.005 – **Unsecured Credentials: Cloud Instance Metadata API**	XXE üzerinden bulut metadata servisi sorgusu	Falcon Cloud Security	RESMİ: VAPOR PANDA blogu
23	T1606 – **Forge Web Credentials**	Rotasyonu yapılmamış kimlik doğrulama anahtarlarıyla admin token sahteleme	Falcon Next-Gen Identity Security, Falcon Next-Gen SIEM	RESMİ: VAPOR PANDA blogu
24	T11558.003 – **Steal or Forge Kerberos Tickets: Kerberoasting (FLASH'taki yazım)**	Kerberoasting ile servis bileti toplama; DCSync ile domain krbtgt anahtarının çalınması; SQL injection ile veritabanı kimlik bilgilerinin dökülmesi	Falcon Next-Gen Identity Security, Falcon Insight XDR	KISMEN/ÇIKARIM

3.5 Internal Recon

#	TEKNİK (FLASH)	AKTÖRÜN KULLANIMI (FLASH)	FALCON MODÜLLERİ	DAYANAK
25	T1518.001 – **Software Discovery: Security Software Discovery**	**Falcon kurulu olmayan Windows makinelerini** bulmak için sensör kapsamını envanterleme	Falcon Exposure Management (CAASM, yönetilmeyen varlık keşfi), Falcon Insight XDR, Falcon Adversary OverWatch	RESMİ: VAPOR PANDA blogu
26	T1555 – **Credentials from Password Stores**	LAPS parolalarını okuma	Falcon Next-Gen Identity Security, Falcon Insight XDR	RESMİ: VAPOR PANDA blogu
27	T1087.002 – **Account Discovery: Domain Account**	110.000'den fazla Active Directory nesnesinin enumerasyonu	Falcon Next-Gen Identity Security, Falcon Insight XDR	KISMEN/ÇIKARIM
28	T1552.006 – **Group Policy Preferences**	(FLASH'ta faz içinde listeli)	Falcon Next-Gen Identity Security (ISPM)	KISMEN/ÇIKARIM
29	T1059.001 – **Command and Scripting Interpreter: PowerShell**	Domain Controller'lara karşı yinelemeli PowerShell enumerasyon script'leri	Falcon Insight XDR, Falcon Prevent, Falcon Next-Gen Identity Security	KISMEN/ÇIKARIM

3.6 Lateral Movement

#	TEKNİK (FLASH)	AKTÖRÜN KULLANIMI (FLASH)	FALCON MODÜLLERİ	DAYANAK
30	T1550.003 – **Use Alternate Authentication Material: Pass the Ticket**	Domain Controller'lara yanal hareket girişimi. FLASH'a göre bu girişimler endpoint koruması tarafından **engellendi**; ürün adı verilmiyor	Falcon Next-Gen Identity Security, Falcon Insight XDR	KISMEN/ÇIKARIM
31	T1550.002 – **Use Alternate Authentication Material: Pass the Hash**	Aynı	Falcon Next-Gen Identity Security, Falcon Insight XDR	KISMEN/ÇIKARIM

#	TEKNİK (FLASH)	AKTÖRÜN KULLANIMI (FLASH)	FALCON MODÜLLERİ	DAYANAK
32	T1021.006 – Remote Services: Windows Remote Management (WinRM)	Aynı	Falcon Insight XDR, Falcon Next-Gen Identity Security	KISMEN/ÇIKARIM
33	T1557.001 – Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay	Kerberos relay	Falcon Next-Gen Identity Security, Falcon Insight XDR	KISMEN/ÇIKARIM

3.7 Collection / Exfiltration Prep

#	TEKNİK (FLASH)	AKTÖRÜN KULLANIMI (FLASH)	FALCON MODÜLLERİ	DAYANAK
34	T1114.002 – Email Collection: Remote Email Collection	Ele geçirilmiş mail sunucusunda posta kutularını okuma	Falcon Next-Gen SIEM, Falcon Shield (M365), Falcon Next-Gen Identity Security	RESMİ: VAPOR PANDA blogu
35	T1555.006 – Cloud Secrets Management Stores	(FLASH'ta faz içinde listeli)	Falcon Cloud Security	KISMEN/ÇIKARIM
36	T1530 – Data from Cloud Storage	Toplu blob okuma	Falcon Cloud Security, Falcon Data Security	KISMEN/ÇIKARIM
37	T1005 – Data from Local System	Backend SQL veritabanlarının sorgulanması; EC2 üzerinden özel boot script'leriyle veri toplama	Falcon Insight XDR, Falcon Data Security	KISMEN/ÇIKARIM
38	T1074.001 – Data Staged: Local Data Staging	Komut çıktısını dönen `webhook.site` uç noktalarına gönderme	Falcon Insight XDR, Falcon Data Security	KISMEN/ÇIKARIM
39	T1074.002 – Data Staged: Remote Data Staging	Exfiltration hazırlığı için 100 GB'lık yeni volume'lar oluşturma	Falcon Cloud Security	KISMEN/ÇIKARIM

3.8 Command and Control

#	TEKNİK (FLASH)	AKTÖRÜN KULLANIMI (FLASH)	FALCON MODÜLLERİ	DAYANAK
40	T1090 – Proxy	Residential proxy servisleri	Falcon Adversary Intelligence (IOC), Falcon Next-Gen SIEM	RESMİ: Güney Kore blogu
41	T1090.003 – Proxy: Multi-hop Proxy	Tor, SOCKS proxy'leri, ele geçirilmiş relay'ler	Falcon Adversary Intelligence, Falcon Insight XDR, Falcon Next-Gen SIEM	RESMİ: VAPOR PANDA blogu
42	T1572 – Protocol Tunneling	Chisel ve SoftEther ile tünelleme	Falcon Insight XDR, Falcon Prevent, Falcon Next-Gen SIEM	RESMİ: VAPOR PANDA blogu
43	T1071.001 – Application Layer Protocol: Web Protocols	BLOODALCHEMY'nin C2 domain'leriyle iletişimi	Falcon Insight XDR, Falcon Adversary Intelligence, Falcon Next-Gen SIEM	KISMEN/ÇIKARIM. BLOODALCHEMY C2'si CrowdStrike tarafından Falcon telemetrisiyle belgelendi, ancak T1071.001 CrowdStrike'ın tablosunda yok

Özet: 43 benzersiz tekniğin **16'sı resmi**, **27'si kısmen/çıkarım**.

3.9 CrowdStrike raporlarında olup FLASH tablosunda olmayan teknikler

TEKNİK	CROWDSTRIKE GÖZLEMİ	KAYNAK
T1588.007 – Obtain Capabilities: Artificial Intelligence	ARTEX ajan framework'ünün edinilmesi ve kullanılması	Her iki CrowdStrike blogu
T1583.003 – Acquire Infrastructure: Virtual Private Server	Birden çok IP'de C2 altyapısı	Güney Kore blogu
T1651 – Cloud Administration Command	Cloud systems manager üzerinden instance'lara komut gönderme	VAPOR PANDA blogu
T1110.003 – Brute Force: Password Spraying	Kamu, think tank ve kurumsal hesaplara password spraying	VAPOR PANDA blogu

4. ATT&CK v20.1 ile adlandırma ve ID farkları

FLASH'ta **T1562 (Impair Defenses) geçmiyor**; dolayısıyla T1562'den T1685'e geçiş bu bültende uygulanmıyor. Tespit edilen farklar şunlar:

FLASH'TAKİ YAZIM	V20.1 KARŞILIĞI	AÇIKLAMA
T11558.003 – Steal or Forge Kerberos Tickets: Kerberoasting	**T1558.003** – Steal or Forge Kerberos Tickets: Kerberoasting	FLASH'ta yazım hatası (fazladan "1")
T1134.001 – Access Token Manipulation	T1134.001 – Access Token Manipulation: **Token Impersonation/Theft**	FLASH yalnızca üst teknik adını yazmış
T1557.001 – Adversary-in-the-Middle: **LLMNR/NBT-NS Poisoning** and SMB Relay	T1557.001 – Adversary-in-the-Middle: **Name Resolution Poisoning** and SMB Relay	v19'da alt teknik yeniden adlandırıldı (major version değişikliği)
T1021.006 – Remote Services: Windows Remote Management **(WinRM)**	T1021.006 – Remote Services: Windows Remote Management	Parantez içi ek
T1552.006 – Group Policy Preferences	T1552.006 – **Unsecured Credentials:** Group Policy Preferences	Üst teknik adı yazılmamış
T1555.006 – Cloud Secrets Management Stores	T1555.006 – **Credentials from Password Stores:** Cloud Secrets Management Stores	Üst teknik adı yazılmamış
T1574.001, T1036.005 (CrowdStrike blogunda "Defense Evasion" altında)	v20.1'de **Stealth (TA0005)** altında (T1574.001 ayrıca Execution)	v19'daki Defense Evasion bölünmesi
T1580, T1087.004, T1069.003, T1526 ("Initial Recon" fazında)	v20.1'de **Discovery** taktiğinde	FLASH resmi taktik yerine kendi faz adlarını kullanıyor
T1555, T1552.006 ("Internal Recon" fazında)	v20.1'de **Credential Access**	Aynı sebep
T1505.003, T1078.004, T1098.001	v20.1'de Persistence (T1078.004 ve T1098.001 ayrıca Privilege Escalation)	Uyumlu

5. FLASH'taki mitigasyonların Falcon karşılıkları

FLASH ÖNERİSİ	FALCON YETENEĞİ	DAYANAK
Tüm internete açık uygulamaları envanterleyin (partner/tedarikçi portalları, mobil backend'ler, legacy servisler dahil)	Falcon Exposure Management: EASM ve CAASM	Ürün sayfası; eşleme çıkarım
Bulut yönetimi, Kudu/SCM, hypervisor ve backup arayüzlerini güvenilir ağlarla sınırlayın; public IP tahsisini yönetişime bağlayın	Falcon Cloud Security: CSPM ile misconfiguration tespiti, CIEM	Ürün sayfası; eşleme çıkarım
Basic publishing authentication'ı kapatın, deployment kimlik bilgilerini kısıtlayın	Falcon Cloud Security: CSPM	Çıkarım

FLASH ÖNERİSİ	FALCON YETENEĞİ	DAYANAK
Uygulamaları Zero Trust erişimin arkasına alın	Falcon Next-Gen Identity Security (Zero Trust), Falcon Seraphic Enterprise Browser	Ürün sayfaları; eşleme çıkarım
Multi-tenant uygulama izinlerinde ve consent grant'lerde en az yetki; kimlik bilgisi eklemelerini ve anormal app-only aktiviteyi izleyin	Falcon Shield (aşırı yetkili ve riskli NHI tespiti), Falcon Next-Gen Identity Security	Falcon Shield sayfası NHI ve aşırı yetkiyi açıkça anıyor; eşleme çıkarım
Entra audit kayıtlarını, service principal sign-in'lerini ve Graph aktivitesini inceleyin	Falcon Next-Gen SIEM (üçüncü taraf log ingest), Falcon Next-Gen Identity Security (Entra ID)	Identity sayfası Entra ID'yi anıyor; eşleme çıkarım
Sertifika kaydında CA onayı ve EPA; olağandışı sertifika kayıtlarını izleyin	Falcon Next-Gen Identity Security	Çıkarım; AD CS kapsamı bu çalışmada doğrulanmadı
İş API'lerinde rate limit ve hacim alarmları; portallarda sıralı sorgu tespiti	Falcon Next-Gen SIEM (korelasyon), Falcon Onum (pipeline içi tespit)	Çıkarım
Hata mesajlarında stack trace ve iç yolları göstermeyin	Doğrudan bir Falcon karşılığı yok (uygulama geliştirme pratiği)	—
Kod, IaC, CI/CD ve container image'larında gömülü secret taraması; ifşa olan kimlik bilgilerini döndürün	Falcon Cloud Security (ASPM, container security), Falcon Adversary Intelligence (sızdırılmış kimlik bilgisi izleme)	Kısmen; secret taraması bu çalışmada ürün sayfasında açıkça doğrulanmadı
Kanıtları koruyun (Entra, Purview, SIEM, Graph telemetrisi)	Falcon Next-Gen SIEM (retention), CrowdStrike Incident Response	Çıkarım
Doğrulanmış yetkisiz kimlik bilgilerini, grant'leri ve kimlikleri kaldırın	Falcon Fusion SOAR, Falcon Complete	Çıkarım

CrowdStrike'ın VAPOR PANDA blogundaki ek öneriler (resmi):

- Veri ifşası şüphesinde signing key, preauthentication key ve servis kimlik bilgilerini döndürün; tarihî yedekler ve dizin export'larındaki anahtarlar dahil.
- SAML imza doğrulamasını zorunlu kılın, **IMDSv2** kullanın, bulut rollerinin komut çalıştırma yetkisini minimum instance ile sınırlayın.
- ARTEX işaretlerini avlayın: `artx` / `artex` içeren komut satırı parametreleri, `artx` önekli bulut rolleri, `art18-` ile başlayan yönetim komutu yorumları, `C:\ProgramData\artx5v\` dizini.
- İnternete açık cihazları, özellikle uzun ömürlü Linux sunucuları yamalayın.
- Gerçek zamanlı EDR'ı (ör. Falcon sensörü) **internetten erişilemez sanılan sunucular dahil** tüm ortama yayın.

Editoryal vurgu: *Operatörün ajanlara açıkça "Falcon kurulu olmayan makineleri bul" demesi, sensör kapsamındaki boşlukların hedef listesine dönüştüğünü gösteriyor. Yönetilmeyen varlık keşfi (Falcon Exposure Management) ve %100 sensör kapsamı bu ekin en somut çıkarımıdır.*

6. Falcon Guardian ve AI katmanı

ARTEX saldırganın kendi altyapısında çalışıyor; yani kurbanın ortamında bir "AI ajanı" olarak bulunmuyor. Bu nedenle **Falcon Guardian**'ın ARTEX'e karşı doğrudan rolü sınırlıdır ve aşağıdaki eşlemeler çıkarımdır.

- FLASH'ın davranışsal göstergelerinden biri, `api.anthropic.com`, `api.deepseek.com`, `open.bigmodel.cn` ve `api.x.ai` gibi LLM API uç noktalarına beklenmeyen çağrılardır. Guardian'ın Endpoint Network Inspection ve AI Gateway yetenekleri kurum içinden yapılan bu tür çağrılara görünürlük sağlayabilir (**çıkarım**).
- Kurum içindeki AI ajanlarının ARTEX benzeri framework'lerle istismarına karşı prompt injection tespiti ve AI Kill Switch, Guardian'ın resmi olarak tanımlı yetenekleridir.

7. Türkiye ve Körfez (GCC) için önemi

- **Kaynaklı bilgi:** CrowdStrike'a göre VAPOR PANDA ARTEX kampanyasında **Orta Doğu'daki bir içişleri bakanlığını ele geçirdi** ve BLOODALCHEMY'yi burada konuşlandırdı. Ayrıca Orta Doğu dahil birçok bölgede dışişleri bakanlıklarını hedef aldı. Komşu coğrafyada bir **Yunan kamu kurumu** da hedefler arasındaydı.
- FLASH ve CrowdStrike raporları **Türkiye'yi veya belirli bir GCC ülkesini adıyla anmıyor**. Bu nedenle ülkeye özgü bir etki iddiasında bulunulmamıştır.
- Hedef sektör listesi (finans, kamu, telekom, enerji, savunma), bölgenin kritik sektörleriyle örtüşüyor. Bu bir değerlendirmedir, kaynaklı bulgu değildir.

8. IOC özeti

Uzun listeler burada tekrarlanmamıştır; aksiyon almadan önce IOC'leri **FLASH'ın kendisinden** doğrulayın. FBI da adreslerin dinamik olabileceği konusunda uyarıyor.

TÜR	ADET	BAĞLAM
IP adresi	24	1 ARTEX host/open directory ve 9 proxy (Güney Kore, kaynak CrowdStrike); 6 ConnectWise kampanyası (kaynak Microsoft); 3 WISP C2, 4 ARTEX sunucusu ve 1 C2 sunucusu (Storm-3358, kaynak Microsoft)
Domain	1	LLM API reseller (kaynak CrowdStrike)
Ağ ve davranış göstergesi	4 tür	LLM API çağrıları, yüksek frekanslı sıralı HTTP istekleri, yapılandırılmış veri transferleri, beklenmeyen yollardaki `.aspx` / `.jsp` dosyaları
CrowdStrike VAPOR PANDA blogu (FLASH dışı)	3 domain, 3 IP, 3 SHA256	BLOODALCHEMY C2 ve dosyaları

FBI, ARTEX olaylarının bildiriminde sekiz bilgi kategorisi talep ediyor: konsol ve konfigürasyon, kimlik doğrulama logları, API aktivitesi, LLM altyapısı, bulut ve container aktivitesi, istismar artefaktları, saldırı karakteristiği, kayıp bilgisi.

9. Savunma mimarisi, sınırlar ve SOC use-case'leri (Selim ÖZİŞ'in enablement notlarından)

Kaynak notu: Bu bölümdeki akış, matris, use-case kataloğu ve kontrol listesi, **Selim ÖZİŞ'in ARTEX enablement notlarından** aktarılmıştır. Ürün adları güncel resmi adlarla verilmiş, eski adlar parantez içinde takma ad olarak bırakılmıştır. Notlarda vurgulandığı gibi bu eşlemeler **mimari değerlendirmedir**; FBI'ın ürün bazında doğruladığı tespit testi sonuçları değildir. Lisans, veri kaynağı, desteklenen işletim sistemi ve sürüm farkları sonucu değiştirir. FLASH, CrowdStrike ürünlerinin her saldırıyı önlediğinin kanıtı değildir.

9.1 Savunma mimarisi akışı

DISCOVER → PRIORITIZE → PREVENT → DETECT → INVESTIGATE → CONTAIN → RECOVER

AŞAMA	FALCON KATMANI (SELİM'İN NOTLARINA GÖRE)
Discover	Falcon Exposure Management (EASM; eski adı Spotlight olan zafiyet yönetimi dahil) ile görünürlük
Prioritize	Falcon Cloud Security ve Falcon Next-Gen Identity Security (eski adı Identity Protection): yanlış yapılandırma ve kimlik riski değerlendirmesi
Prevent / Detect	Falcon Prevent ve Falcon Insight XDR (EPP/EDR), Falcon Data Security (eski adı Data Protection): uygun kapsamdaki endpoint etkinliklerini önleme ve algılama
Investigate	Falcon Next-Gen SIEM: üçüncü taraf SaaS, IAM, API, WAF, ağ ve bulut loglarını korele eder
Contain	Falcon Fusion SOAR ve Charlotte AI müdahaleyi hızlandırır
Recover	Falcon Complete (MDR), Falcon Adversary OverWatch ve CrowdStrike Services operasyonu destekler

9.2 FBI TTP → Falcon: savunma değeri ve sınır / bağımlılık

FBI TEKNİĞİ	İLGİLİ MODÜLLER	SAVUNMA DEĞERİ	SINIR / BAĞIMLILIK
Dış keşif, fuzzing, 500+ istek	Exposure Management (EASM, Spotlight); Next-Gen SIEM	Envanter ve zafiyet önceliği; WAF/API loglarında hız ve sıralı erişim anomalisi tespiti	WAF/API gateway rate limiting ve gerçek zamanlı HTTP engelleme için ayrı kontrol gerekir
SSRF, XXE, SQLi, IDOR, SAML bypass	Cloud Security, Exposure Management, Next-Gen SIEM, Falcon for IT	Yanlış yapılandırma ve zafiyet görünürlüğü, exploit sonrası davranış, uygulama log korelasyonu	EDR web uygulaması kod kusurlarını tek başına yamalamaz; WAF, güvenli kod ve uygulama testi gerekir
Azure SAS, AWS IAM, Kudu, metadata	Falcon Cloud Security (CSPM, CIEM, CWP), Next-Gen SIEM	IAM yetkileri, rol varsayımı, anomalik API ve Kudu/SCM erişimi	CloudTrail, Entra, Azure Activity, Kudu ve storage telemetrisi entegrasyonu doğrulanmalı
OAuth / service principal'a credential ekleme	Next-Gen Identity Security (Identity Protection); Cloud Security; Next-Gen SIEM	Entra audit, service principal sign-in, consent ve rol değişikliği korelasyonu	İnsan kimliği kapsamı ile workload identity kapsamı farklıdır; entegrasyon ve lisans doğrulanmalı
Web shell, RAT, PowerShell, DLL	Falcon Prevent, Insight XDR, Adversary OverWatch, Falcon Complete, Sandbox	İşlem ağacı, script, dosya ve C2 davranışını algılama; uygun policy ile blokaj ve izolasyon	Sensör bulunmayan web sunucusunda endpoint algılaması yoktur
Kerberoasting, DCSync, PtH/PtT, WinRM	Next-Gen Identity Security + Insight XDR + Next-Gen SIEM	AD ve kimlik saldırı sinyalleriyle uç nokta hareketinin korelasyonu	DC, AD ve kimlik sensörü kapsamı gerekir; blokaj yeteneği senaryo bazında test edilmeli
Tor, SOCKS, Chisel, SoftEther, C2	Insight XDR, Adversary Intelligence (Threat Intelligence), Next-Gen SIEM, Falcon Complete	DNS, proxy, firewall, endpoint bağlantısı ve threat intel korelasyonu	Endpoint dışı ağ trafiğinin görünmesi için ağ/proxy logları gerekir
Blob, mailbox, SQL toplu okuma ve exfil	Falcon Data Security (Data Protection), Cloud Security, Next-Gen SIEM	Endpoint veri hareketi ile cloud/SaaS erişim anomalisini araştırma	Her HTTPS/SaaS API sızdırmasını Falcon Data Security tek başına engellemez
Tedarik zinciri, CI/CD secret sızıntısı	Cloud Security, Exposure Management, Next-Gen SIEM, Adversary Intelligence	Cloud posture, workload, repo/CI-CD ve secret bulgularını ilişkilendirme	Dedicated SAST/DAST, secret scanning ve tedarikçi yönetişimi tamamlayıcıdır
AI ajanları, LLM API kullanımı	Falcon Guardian (AIDR, AI Gateway), Next-Gen SIEM	Kurumsal AI ajan ve model kullanımının uygun kapsamda yönetimi ve görünürlüğü	Saldırganın kendi altyapısındaki ARTEX ajanını uzaktan kapatmaz; Kill Switch kapsamı gateway ile sınırlıdır

Modül bazında sınırlar (Selim'in eğitim kataloğundan, özet):

MODÜL	KAPSAM	SINIR / BAĞIMLILIK
Falcon Prevent / Insight XDR	Endpoint prevention, EDR, process tree, RTR, host containment	Sensör kapsamı önkoşul
Falcon Complete / Adversary OverWatch	7/24 MDR ve threat hunting	Sözleşme kapsamı ve müdahale yetkisi kontrol edilir
Next-Gen Identity Security (Identity Protection, Workforce Security, SGNL)	AD ve kimlik saldırıları, yetki ilişkileri, sürekli yetkilendirme	Her SaaS ve service principal kapsamı varsayılmaz
Falcon Cloud Security	CSPM, CIEM, cloud workload, container/Kubernetes, cloud threat detection	API ve workload bağlantıları gerekir
Falcon Exposure Management (EASM, Spotlight, Discover)	İnternete açık yüzey, varlık envanteri, zafiyet ve risk önceliği	Keşif sağlar, exploit engellemez
Falcon Next-Gen SIEM (LogScale) / Falcon Onum	Entra, Graph, CloudTrail, Azure, WAF, proxy, SaaS ve uygulama logları; Onum ingest/route optimizasyonu	Log kaynaklarının bağlanması gerekir
Falcon Fusion SOAR / Charlotte AI	Triage, enrichment, playbook, otomatik müdahale	İnsan onayı ve rol tabanlı yetkiyle çalışır
Falcon Adversary Intelligence (Threat Intelligence, Falcon X, Sandbox)	IOC/TTP bağlamı, malware analizi, hunting	Tek başına önleme değildir
Falcon Data Security (Data Protection)	Desteklenen uç nokta veri akışlarında veri hareketi kontrolleri	Cloud API exfil için ayrıca log ve native kontroller gerekir
Falcon FileVantage	Kritik dosya değişim izleme (webroot, hassas konfigürasyon)	Uygun host kapsamı gerekir
Falcon for IT	Envanter, hijyen, operasyonel sorgular, remediation	Güvenlik kontrollerini destekler, onların yerini almaz
Falcon Guardian (AIDR, AI Gateway, Agent Graph)	Kurumsal AI uygulama ve ajan riskleri	Saldırganın dış LLM modelini durdurma vaadi verilmez
Falcon Shield (SaaS Security Posture)	SaaS konfigürasyon ve erişim görünürlüğü	Desteklenen SaaS kapsamına bağlı
Falcon Seraphic Enterprise Browser (Secure Browser)	Kurumsal tarayıcı oturumlarında politika	Sunucu tarafı web zafiyetlerini kapatmaz
Falcon Foundry / Custom IOA	Özel detection ve uygulama	Test, false-positive yönetimi ve bakım gerektirir
CrowdStrike Services (IR, Red Team) / Dreadnode / Fiddler	IR, adversary simulation, AI test ve observability	Entegrasyon, satın alma ve GA durumu teyit edilmeli; Dreadnode ve Fiddler için GA Q4 FY27 olarak duyuruldu

9.3 Örnek SOC detection use-case kataloğu

ID	HİPOTEZ	GEREKLİ TELEMETRİ	ÖNCELİK	YANIT
UC01	Service principal'a yeni credential + kısa sürede Graph bulk read	Entra audit + SP sign-in + Graph logları	Yüksek	Sahibi ve credential'ı doğrula; token revoke/rotate; kanıtı sakla
UC02	Kudu/SCM erişimi + webroot'ta yeni JSP/PHP/ASPX	Azure App Service + EDR/FileVantage + web logları	Kritik	SCM erişimini sınırla, host'u izole et, artefakt topla
UC03	AWS DryRun/PassRole artışı + yeni yüksek yetkili EC2	CloudTrail + CSPM/CIEM	Yüksek	Rolü ve instance profile'ı araştır; geçici credential'ı iptal et
UC04	AD enumeration + Kerberoasting + DC'ye WinRM	Identity + EDR + Windows security logları	Kritik	Hesabı sınırla, lateral hareketi kes, DC triage

ID	HİPOTEZ	GEREKLİ TELEMETRİ	ÖNCELİK	YANIT
UC05	Portalda sıralı IDOR + sıra dışı kayıt export'u	API gateway + WAF + app audit + Next-Gen SIEM	Yüksek	Rate limit, session revoke, authorization düzeltmesi
UC06	Yeni web shell + proxy tunnel + dışarı veri aktarımı	EDR + DNS/proxy + NDR + Next-Gen SIEM	Kritik	Host'u izole et, egress'i engelle, forensic capture
UC07	OAuth consent değişimi + anormal mailbox erişimi	Entra + M365/Purview + Graph + Next-Gen SIEM	Kritik	Grant revoke, credential rotate, mailbox kapsamını belirle
UC08	LLM API çıkışında beklenmedik artış	Egress/proxy + AI Gateway + Next-Gen SIEM	Orta	Meşru geliştirici trafiğinden ayır; model kullanımını araştır

9.4 Kontrol listesi ve dürüst konumlandırma

- [ ] FBI IOC'lerini tarihsel sinyal olarak ele alın; IP bloklamadan önce doğrulayın. (FLASH da göstergeleri aktivite penceresinde gözlenmiş altyapı olarak yorumlamayı öneriyor.)
- [ ] ConnectWise ile ilişkili tenant'larda kayıtları en az 1 Ekim 2026'dan itibaren inceleyin. (FLASH önerisi.)
- [ ] Uygulamaları application ID ile sorgulayın, yalnızca display name'e güvenmeyin. (FLASH önerisi.)
- [ ] SAML imza doğrulaması, OAuth least privilege, API authorization ve rate limit için uygulama sahibiyle çalışın.
- [ ] GA/roadmap durumunu, ürün SKU'sunu ve telemetri desteğini müşteri ortamında doğrulayın.

CrowdStrike, FBI raporunda araştırma kaynağı olarak geçiyor; FBI ürün onayı vermiyor.

FLASH'ın feragat notu bunu açıkça söylüyor: FBI hiçbir ticari kuruluşu, ürünü veya hizmeti onaylamaz. Raporda Falcon'un adı, saldırganın Falcon kurulu olmayan makineleri aradığı bir gözlemde geçiyor.

Kaynaklar

1. FBI, *Threat Overview of ARTEX Autonomous Penetration Testing Framework*, FLASH-20261113-001, 13 Kasım 2026. https://www.ic3.gov/CSA/2026/261113.pdf
2. CrowdStrike, *VAPOR PANDA Uses AI-Driven ARTEX to Scale a Global Espionage Campaign*, 29 Ekim 2026. https://www.crowdstrike.com/en-us/blog/vapor-panda-uses-artex-to-scale-global-campaign/
3. CrowdStrike, *Unknown Threat Actor Uses AI-Driven ARTEX to Target South Korean Finance*, 7 Ekim 2026. https://www.crowdstrike.com/en-us/blog/unknown-threat-actor-uses-artex-to-target-south-korean-finance/
4. CrowdStrike Adversary Universe, VAPOR PANDA. https://www.crowdstrike.com/en-us/adversaries/vapor-panda/
5. MITRE ATT&CK v20.1, Enterprise teknik sayfaları. https://attack.mitre.org/
6. Falcon ürün sayfaları (crowdstrike.com): Insight XDR, Prevent, Next-Gen Identity Security, Cloud Security, Exposure Management, Adversary Intelligence, Adversary OverWatch, Next-Gen SIEM, Falcon Shield, Data Security, Falcon Guardian, Falcon Seraphic Enterprise Browser.
7. Selim ÖZİŞ, *CrowdStrike ARTEX Defense Enablement* (iç eğitim notları, 2026); 9. bölümdeki akış, matris, use-case kataloğu ve kontrol listesi.

Kaynaklar

1 **ATT&CK Version History (v20.1 güncel)**
attack.mitre.org
https://attack.mitre.org/resources/versions/

2 **Enterprise Tactics (15 taktik)**
attack.mitre.org
https://attack.mitre.org/tactics/enterprise/

3 **Updates – April 2026 (v19, Defense Evasion split)**
attack.mitre.org
https://attack.mitre.org/resources/updates/updates-april-2026/

4 **ATT&CK Updates (v20)**
attack.mitre.org
https://attack.mitre.org/resources/updates/

5 **ATT&CK v19: The Defense Evasion Split**
MITRE ATT&CK blog (Medium)
https://medium.com/mitre-attack/att-ck-v19-the-defense-evasion-split-ics-sub-techniques-new-ai-social-engineering-coverage-ff329cb65d66

6 **CrowdStrike 2026 Global Threat Report bulguları**
crowdstrike.com · 24 Şubat 2026
https://www.crowdstrike.com/en-us/blog/crowdstrike-2026-global-threat-report-findings/

7 **2026 Global Threat Report (PDF)**
go.crowdstrike.com
https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrike-2026-Global-Threat-Report.pdf

8 **CrowdStrike 2025 Global Threat Report bulguları**
crowdstrike.com
https://www.crowdstrike.com/en-us/blog/crowdstrike-2025-global-threat-report-findings/

9 **CrowdStrike, 2025 MITRE ATT&CK Enterprise Evaluations'da %100**
crowdstrike.com · 10 Aralık 2025
https://www.crowdstrike.com/en-us/blog/crowdstrike-achieves-100-percent-2025-mitre-attack-enterprise-evaluation/

10 **Enterprise 2025 koruma sonuçları (cohort)**
evals.mitre.org
https://evals.mitre.org/results/enterprise?evaluation=er7&result_type=PROTECTION&scenarios=3%2C4%2C5%2C6%2C7%2C8%2C9&view=cohort

11 **ATT&CK Evaluations Enterprise 2026 (ER8)**
evals.mitre.org
https://evals.mitre.org/enterprise/er8/

12 **Falcon Insight XDR**
crowdstrike.com
https://www.crowdstrike.com/en-us/platform/endpoint-security/falcon-insight-xdr/

13 **Falcon Prevent**
crowdstrike.com
https://www.crowdstrike.com/en-us/platform/endpoint-security/falcon-prevent-ngav/

14 **Falcon Next-Gen Identity Security**
crowdstrike.com
https://www.crowdstrike.com/en-us/platform/next-gen-identity-security/

15 **Falcon Cloud Security**
crowdstrike.com
https://www.crowdstrike.com/en-us/platform/cloud-security/

16 **Falcon Exposure Management**
crowdstrike.com
https://www.crowdstrike.com/en-us/platform/exposure-management/

17 **Falcon Adversary Intelligence**
crowdstrike.com
https://www.crowdstrike.com/en-us/platform/threat-intelligence/adversary-intelligence/

18 **Digital Risk Protection**
crowdstrike.com
https://www.crowdstrike.com/en-us/platform/threat-intelligence/digital-risk/

19 **Falcon Adversary OverWatch**
crowdstrike.com
https://www.crowdstrike.com/en-us/platform/threat-intelligence/adversary-overwatch/

20 **Falcon Complete (Agentic MDR)**
crowdstrike.com
https://www.crowdstrike.com/en-us/services/falcon-complete-mdr/

21 **Falcon Next-Gen SIEM**
crowdstrike.com
https://www.crowdstrike.com/en-us/platform/next-gen-siem/

22 **Falcon Fusion**
crowdstrike.com
https://www.crowdstrike.com/en-us/platform/next-gen-siem/falcon-fusion/

Kaynaklar

23 Charlotte AI
crowdstrike.com
https://www.crowdstrike.com/en-us/platform/charlotte-ai/

24 Falcon Data Security
crowdstrike.com
https://www.crowdstrike.com/en-us/platform/data-security/

25 Falcon Shield
crowdstrike.com
https://www.crowdstrike.com/en-us/platform/falcon-shield/

26 Falcon for IT
crowdstrike.com
https://www.crowdstrike.com/en-us/platform/falcon-for-it/

27 Falcon Firewall Management
crowdstrike.com
https://www.crowdstrike.com/en-us/platform/endpoint-security/falcon-firewall-management/

28 Falcon Device Control
crowdstrike.com
https://www.crowdstrike.com/en-us/platform/endpoint-security/falcon-device-control/

29 Ransomware Protection
crowdstrike.com
https://www.crowdstrike.com/en-us/platform/endpoint-security/ransomware-protection/

30 Falcon Guardian (Falcon AIDR)
crowdstrike.com
https://www.crowdstrike.com/en-us/platform/falcon-guardian-aidr/

31 CrowdStrike Unveils Falcon Guardian
crowdstrike.com · 1 Eylül 2026
https://www.crowdstrike.com/en-us/press-releases/crowdstrike-unveils-falcon-guardian-ai-agent-security/

32 Falcon Guardian Defines the Next Generation of AI Security
crowdstrike.com · 1 Eylül 2026
https://www.crowdstrike.com/en-us/blog/falcon-guardian-defines-next-generation-of-ai-security/

33 CrowdStrike Delivers AI Security and Safety for the Enterprise (AI Kill Switch)
crowdstrike.com · 3 Kasım 2026
https://www.crowdstrike.com/en-us/press-releases/crowdstrike-delivers-ai-security-safety-for-the-enterprise/

34 Falcon Seraphic Enterprise Browser
crowdstrike.com
https://www.crowdstrike.com/en-us/platform/falcon-seraphic-enterprise-browser/

35 Falcon for XIoT
crowdstrike.com
https://www.crowdstrike.com/en-us/platform/falcon-for-xiot/

36 CrowdStrike to Acquire Onum
crowdstrike.com · 27 Ağustos 2025
https://www.crowdstrike.com/en-us/press-releases/crowdstrike-to-acquire-onum/

37 CrowdStrike to Acquire Pangea
crowdstrike.com · 16 Eylül 2025
https://www.crowdstrike.com/en-us/press-releases/crowdstrike-to-acquire-pangea-to-secure-every-layer-of-enterprise-ai/

38 CrowdStrike to Acquire SGNL
crowdstrike.com · 8 Ocak 2026
https://www.crowdstrike.com/en-us/press-releases/crowdstrike-to-acquire-sgnl-to-transform-identity-security-for-ai-era/

39 CrowdStrike to Acquire Seraphic
crowdstrike.com · 13 Ocak 2026
https://www.crowdstrike.com/en-us/press-releases/crowdstrike-to-acquire-seraphic-security/

40 CrowdStrike and Schwarz Digits (XM Cyber IP)
crowdstrike.com · 16 Temmuz 2026
https://www.crowdstrike.com/en-us/press-releases/crowdstrike-and-schwarz-digits-expand-strategic-partnership-to-deliver-sovereign-cybersecurity-across-europe/

41 CrowdStrike to Acquire Dreadnode
crowdstrike.com · 3 Kasım 2026
https://www.crowdstrike.com/en-us/press-releases/crowdstrike-to-acquire-dreadnode-advance-ai-trust/

42 CrowdStrike to Acquire Fiddler
crowdstrike.com · 3 Kasım 2026
https://www.crowdstrike.com/en-us/press-releases/crowdstrike-to-acquire-fiddler-to-deliver-agent-observability/

43 MITRE ATLAS
atlas.mitre.org
https://atlas.mitre.org/

KÜNYE

Kolofon

Hazırlayan: Selim ÖZİŞ

İÇERİK KAYNAĞI

"MITRE ATT&CK Tehdit Görünümü: CrowdStrike Falcon Modülleriyle Taktik Bazlı Eşleme" başlıklı makale. Rakamlar, eşlemeler ve "resmi kaynak / kısmen çıkarım" işaretleri makaleden aynen aktarılmıştır; kaynak listesi 11. bölümdedir.

İŞARETLER

RESMİ KAYNAK | KISMEN ÇIKARIM | ÇIKARIM

ÖZEL EK

"Özel Ek: ARTEX" metni ve tabloları, ek için hazırlanan metinden aynen dizilmiştir; ekin kaynakları kendi sonunda listelenmiştir. FBI/IC3 mührü veya amblemi kullanılmamıştır.

LOGO

CrowdStrike logosu, crowdstrike.com/en-us/about-us/brand/ sayfasındaki resmi logo paketinden (CS-Logos-SVG.zip, CrowdStrike_Logo_2023_Primary_White.svg) değiştirilmeden kullanılmıştır.

GÖRSELLER

- **kapak.jpg** — Yapay zekâ görseli · Ressam · Nano Banana Pro (Higgsfield) + Pillow renk notu
- **bolum-1.jpg** — Yapay zekâ görseli · Ressam · Nano Banana Pro (Higgsfield) + Pillow renk notu
- **bolum-2.jpg** — Yapay zekâ görseli · Ressam · Nano Banana Pro (Higgsfield) + Pillow renk notu
- **bolum-3.jpg** — Yapay zekâ görseli · Ressam · Nano Banana Pro (Higgsfield) + Pillow renk notu
- **ek-ic3.jpg** — Yapay zekâ görseli · Ressam · Cinema Studio Image 2.5 (Higgsfield) + Pillow renk notu

YAZI KARAKTERLERİ

Barlow ve Barlow Condensed (başlıklar), Inter (tablo ve bilgi metni), IBM Plex Serif (gövde), IBM Plex Mono (ID ve adresler), Noto Sans SC (Çince alıntı) — SIL Open Font License; PDF'e gömülü.

ÜRETİM

A4, HTML/CSS → headless Chrome PDF. Türkçe heceleme yumuşak tire ile.

CROWDSTRIKE

MAGAZINE

ATT&CK v20.1 · FALCON