1. **LAN quyidagi qaysi asosiy tarkibiy va funktsional elementlardan iborat?**

**A. ishchi stantsiyalar, serverlar,tarmoqlararo aloqa tugunlari,aloqa kanallari**

B. shlyuzlar, routerlar, serverlar, tarmoq kartalari

C. ishchi stantsiyalar, serverlar, tarmoq kartalari

D. aloqa kanallari, serverlar, shlyuzlar, firewall

1. **… - tarmoqlarning foydaluvchanligi eng maqbul tarkibiy qismlari hisoblanadi va ular orqali ruxsatsiz xatti-harakatlarni amalga oshirish uchun eng ko'p urinishlar amalga oshirilishi mumkin.**

**A. Ishchi stantsiyalar**

B. video monitorlar

C. Serverlar va aloqa uskunalari

D. Aloqa kanallari

1. **…- maxsus himoyaga muhtoj, chunki ular tajovuzkorlar nuqtai nazari bo'yicha eng jozibalidir.**

**A. Serverlar va aloqa uskunalari**

B. video monitorlar

C. Ishchi stantsiyalar

D. Aloqa kanallari

1. **…. - nazoratsiz yoki kam nazorat qilinadigan hudud orqali katta bo'shliqqa qarab, imkoniyatni taqdim etadi.**

**A. Aloqa kanallari**

B. video monitorlar

C. Ishchi stantsiyalar

D. Serverlar va aloqa uskunalari

1. **Tashkilotda zaifliklarni to'g'ri boshqarishni ta'minlashning nechta bosqichi taklif etiladi?**

**A. 5**

B. 4

C. 3

D. 2

1. **Tashkilotda zaifliklarni to'g'ri boshqarishni ta'minlashning 1-bosqichi qanday ataladi?**

**A. Boshlovchi**

B. Takrorlanuvchi

C. O’rnatilgan

D. Optimallashtirish

1. **Tashkilotda zaifliklarni to'g'ri boshqarishni ta'minlashning 2-bosqichi qanday ataladi?**

**A. Takrorlanuvchi**

B. Boshlovchi

C. O’rnatilgan

D. Optimallashtirish

1. **Tashkilotda zaifliklarni to'g'ri boshqarishni ta'minlashning 3-bosqichi qanday ataladi?**

**A. O’rnatilgan**

B. Boshlovchi

C. Takrorlanuvchi

D. Optimallashtirish

1. **Tashkilotda zaifliklarni to'g'ri boshqarishni ta'minlashning 4-bosqichi qanday ataladi?**

**A. Boshqariluvchi**

B. Boshlovchi

C. Takrorlanuvchi

D. Optimallashtirish

1. **Tashkilotda zaifliklarni to'g'ri boshqarishni ta'minlashning 5-bosqichi qanday ataladi?**

**A. Optimallashtirish**

B. Boshlovchi

C. Takrorlanuvchi

D. O’rnatilgan

1. **Tarmoq xavfsizligini baholashning nechta asosiy bosqichi mavjud?**

**A. 4**

B. 3

C. 2

D. 5

1. **Tarmoq xavfsizligini baholash jarayonining ma'lumotlarni yig'ish bosqichida...**

**A. ….Internet Control Message Protocol (ICMP) yoki TCP protokollari yordamida real vaqt rejimida skanerlash orqali tarmoq qurilmalarini qidirish amalga oshiriladi.**

B. …xizmat yoki dastur ishlaydigan maxsus mashina aniqlanadi va potensial zaif joylar baholanadi.

C. …tizimga imtiyozli kirish uchun bir yoki bir nechta zaifliklardan foydalaniladi, so'ngra ushbu kompyuterda yoki butun tarmoq yoki domenda vakolatlar kengaytiriladi.

D. …berilgan ma'lumotlarga bo'lgan munosabatini qabul qilish va qayd etish bajariladi.

1. **Tarmoq xavfsizligini baholash jarayonining bog'lash va baholash bosqichlarida...**

**A. ….** **xizmat yoki dastur ishlaydigan maxsus mashina aniqlanadi va potensial zaif joylar baholanadi.**

B. …Internet Control Message Protocol (ICMP) yoki TCP protokollari yordamida real vaqt rejimida skanerlash orqali tarmoq qurilmalarini qidirish amalga oshiriladi.

C. …tizimga imtiyozli kirish uchun bir yoki bir nechta zaifliklardan foydalaniladi, so'ngra ushbu kompyuterda yoki butun tarmoq yoki domenda vakolatlar kengaytiriladi.

D. …berilgan ma'lumotlarga bo'lgan munosabatini qabul qilish va qayd etish bajariladi.

1. **Tarmoq xavfsizligini baholash jarayonining kirishish bosqichida...**

**A. ….** **tizimga imtiyozli kirish uchun bir yoki bir nechta zaifliklardan foydalaniladi, so'ngra ushbu kompyuterda yoki butun tarmoq yoki domenda vakolatlar kengaytiriladi.**

B. …Internet Control Message Protocol (ICMP) yoki TCP protokollari yordamida real vaqt rejimida skanerlash orqali tarmoq qurilmalarini qidirish amalga oshiriladi.

C. …xizmat yoki dastur ishlaydigan maxsus mashina aniqlanadi va potensial zaif joylar baholanadi.

D. …berilgan ma'lumotlarga bo'lgan munosabatini qabul qilish va qayd etish bajariladi.

1. **Zararli kodni qidirish texnologiyalari komponentalarini belgilang.**

**A. Texnik va analitik**

B. Passiv va faol

C. 1-darajali va 2-darajali

D. evristik va signaturali

1. **.... - tahlil qilish uchun ma'lumotlarning analitik komponentini ta'minlovchi dasturiy funktsiyalar va algoritmlar to'plamidir.**

A. **Texnik komponent**

B. Analitik komponent

C. Passiv komponent

D. Faol komponent

1. **.... - bu uning ixtiyorida mavjud bo'lgan ma'lumotlarni tahlil qiladigan va ular haqida bir xil qaror chiqaradigan algoritmdir.**

**A. Analitik komponent**

B. Texnik komponent

C. Passiv komponent

D. Faol component

1. **….. - bu ma'lum operatsiyalarni avtomatik ravishda bajarish uchun mo'ljallangan dasturlar.**

**A. Botlar**

B. Ransomware

C. Rootkitlar

D. Troyanlar

1. **... - uchinchi tomonga kompyuterga masofadan kirish va boshqarish imkonini beradi.**

**A. Rootkitlar**

B. Botlar

C. Ransomware

D. Troyanlar

1. **... - kompyuteringizga zarar yetkazadi, so'ngra shaxsiy hujjatlar yoki fotosuratlar kabi nozik ma'lumotlarni shifrlaydi va ularni parolini ochish uchun to'lov talab qiladi.**

**A. Ransomware**

B. Troyanlar

C. Botlar

D. Rootkitlar

1. **Texnogen tahdidlarning ichki manbalari berilgan qatorni belgilang.**

**A.** **sertifikatlanmagan va litsenziyalanmagan dasturiy ta'minot, monitoring imkoniyatlari zaif bo'lgan axborot tarmoqlari faoliyatini monitoring qilish vositalari**

B. ulanish kanallari, muhandislik-texnik tarmoqlar

C. Internet provayderlari va bulutli texnologiya provayderlari

D. noto'g'ri yoki past sifatli uskunalar, muhandislik-texnik tarmoqlar

1. **Texnogen tahdidlarning tashqi manbalari berilgan qatorni belgilang.**

**A. Internet provayderlari va bulutli texnologiya provayderlari, ulanish kanallari, muhandislik-texnik tarmoqlar**

B. binolar va xodimlarni nazorat qilishning sifatsiz vositalari;

C. sertifikatlanmagan va litsenziyalanmagan dasturiy ta'minot, monitoring imkoniyatlari zaif bo'lgan axborot tarmoqlari faoliyatini monitoring qilish vositalari

D. noto'g'ri yoki past sifatli uskunalar, muhandislik-texnik tarmoqlar

1. **SOC (Security Operations Center) tahliliy imkoniyatlarini belgilang.**

**A. Prognozlash, Aniqlash, Oldini olish, Reaksiya**

B. dasturlar va axborot tizimlarini boshqarish

C. texnik jihozlardan foydalanish

D. tayyor dasturiy ta'minotni yuklash, texnik jihozlardan foydalanish

1. **Tahdidlarni tahlil qilish uchun asosiy SOC elementi, ya’ni bilimlarni boshqarish bu - …**

**A. SOCl mutahassislari tobora murakkablashib borayotgan hujumlarning oldini olish va ularga samarali javob berish uchun raqamli sud ekspertizasi, zararli dasturlarni tahlil qilish**

B. Ichki tahdidlar to'g'risidagi ma'lumotlar, ommaviy axborot manbalaridan olingan tahlillar

C. An'anaviy himoya vositalari (xavfsizlik devorlari, hujumlarni aniqlash va oldini olish tizimlari, SIEM va boshqalar) bilan aniqlab bo'lmaydigan zararli harakatlar haqida oldindan bilib olishga imkon beradi

D. To'g'ri qurilgan hodisaga javob berish jarayoni, bu zararni cheklash va oqibatlarini bartaraf etish xarajatlarini kamaytirish imkonini beradi

1. **Tahdidlarni tahlil qilish uchun asosiy SOC elementi, ya’ni yig'ilgan materiallar asosida tahdid tahlili bu - …**

**A. Ichki tahdidlar to'g'risidagi ma'lumotlar, ommaviy axborot manbalaridan olingan tahlillar**

B. SOCl mutahassislari tobora murakkablashib borayotgan hujumlarning oldini olish va ularga samarali javob berish uchun raqamli sud ekspertizasi, zararli dasturlarni tahlil qilish

C. An'anaviy himoya vositalari (xavfsizlik devorlari, hujumlarni aniqlash va oldini olish tizimlari, SIEM va boshqalar) bilan aniqlab bo'lmaydigan zararli harakatlar haqida oldindan bilib olishga imkon beradi

D. To'g'ri qurilgan hodisaga javob berish jarayoni, bu zararni cheklash va oqibatlarini bartaraf etish xarajatlarini kamaytirish imkonini beradi

1. **Tahdidlarni tahlil qilish uchun asosiy SOC elementi, ya’ni tahdidlarni faol qidirish bu - …**

**A. An'anaviy himoya vositalari (xavfsizlik devorlari, hujumlarni aniqlash va oldini olish tizimlari, SIEM va boshqalar) bilan aniqlab bo'lmaydigan zararli harakatlar haqida oldindan bilib olishga imkon beradi**

B. SOCl mutahassislari tobora murakkablashib borayotgan hujumlarning oldini olish va ularga samarali javob berish uchun raqamli sud ekspertizasi, zararli dasturlarni tahlil qilish

C.Ichki tahdidlar to'g'risidagi ma'lumotlar, ommaviy axborot manbalaridan olingan tahlillar

D. To'g'ri qurilgan hodisaga javob berish jarayoni, bu zararni cheklash va oqibatlarini bartaraf etish xarajatlarini kamaytirish imkonini beradi

1. **Tahdidlarni tahlil qilish uchun asosiy SOC elementi, ya’ni to’gri tuzilgan jarayon bu - …**

**A. To'g'ri qurilgan hodisaga javob berish jarayoni, bu zararni cheklash va oqibatlarini bartaraf etish xarajatlarini kamaytirish imkonini beradi**

B. SOC mutahassislari tobora murakkablashib borayotgan hujumlarning oldini olish va ularga samarali javob berish uchun raqamli sud ekspertizasi, zararli dasturlarni tahlil qilish

C.Ichki tahdidlar to'g'risidagi ma'lumotlar, ommaviy axborot manbalaridan olingan tahlillar

D. An'anaviy himoya vositalari (xavfsizlik devorlari, hujumlarni aniqlash va oldini olish tizimlari, SIEM va boshqalar) bilan aniqlab bo'lmaydigan zararli harakatlar haqida oldindan bilib olishga imkon beradi

1. **Tahdidli ma’lumotlar oqimlaridagi ma'lumotlarni tematik guruhlaridan biri - IP va URL manzillar…**

**A. Zararli va fishing saytlarining tarmoq identifikatorlari, shuningdek, botnet C&C serverlari (jumladan, mobil qurilmalar uchun) mavjud.**

B. Tegishli ma'lumotlar eng xavfli va keng tarqalgan zararli dasturlarni, shu jumladan mobil operatsion tizimlar uchun infektsiyalarni qamrab oladi.

C. Ular uchinchi tomon yechimlari va xizmatlari tomonidan foydalanish mumkin bo'lgan ishonchli fayllar xeshlarini o'z ichiga oladi.

D. xavfsizlik strategiyasini moslashtirish orqali himoya choralarini yaxshilash imkonini beradi

1. **Tahdidli ma’lumotlar oqimlaridagi ma'lumotlarni tematik guruhlaridan biri - Zararli ob'ektlar xeshlari …**

**A. Tegishli ma'lumotlar eng xavfli va keng tarqalgan zararli dasturlarni, shu jumladan mobil operatsion tizimlar uchun infektsiyalarni qamrab oladi.**

B.Zararli va fishing saytlarining tarmoq identifikatorlari, shuningdek, botnet C&C serverlari (jumladan, mobil qurilmalar uchun) mavjud.

C. Ular uchinchi tomon yechimlari va xizmatlari tomonidan foydalanish mumkin bo'lgan ishonchli fayllar xeshlarini o'z ichiga oladi.

D. xavfsizlik strategiyasini moslashtirish orqali himoya choralarini yaxshilash imkonini beradi

1. **Tahdidli ma’lumotlar oqimlaridagi ma'lumotlarni tematik guruhlaridan biri – Oq ro’yhatga olish …**

**A. Ular uchinchi tomon yechimlari va xizmatlari tomonidan foydalanish mumkin bo'lgan ishonchli fayllar xeshlarini o'z ichiga oladi.**

B.Zararli va fishing saytlarining tarmoq identifikatorlari, shuningdek, botnet C&C serverlari (jumladan, mobil qurilmalar uchun) mavjud.

C. Tegishli ma'lumotlar eng xavfli va keng tarqalgan zararli dasturlarni, shu jumladan mobil operatsion tizimlar uchun infektsiyalarni qamrab oladi.

D. xavfsizlik strategiyasini moslashtirish orqali himoya choralarini yaxshilash imkonini beradi

1. **… - tashqaridan foydalanish mumkin bo'lgan mamlakat veb-resurslarining xavfsizlik holatini aniqlash va tahlil qilish yo'li bilan tuziladi.**

A. **Tahdid vektorlari ro'yxati**

B. Zararli dasturlar va kiberhujumlarni tahlil qilish

C. Oldindan shartlarni aniqlash

D. Retrospektiv tahlil

1. **… - Kasperskiy laboratoriyasining noyob manbalaridan olingan ichki monitoring ma'lumotlari asosida ma'lum bir mamlakatga qaratilgan zararli dasturlar va kiberhujumlarni tahlil qilish.**

**A. Zararli dasturlar va kiberhujumlarni tahlil qilish**

B. Tahdid vektorlari ro'yxati

C. Oldindan shartlarni aniqlash

D. Retrospektiv tahlil

1. **… - muayyan mamlakatda ma'lumotlarning sizib chiqishi uchun zaruriy shartlarni aniqlash.**

**A. Oldindan shartlarni aniqlash**

B. Tahdid vektorlari ro'yxati

C. Zararli dasturlar va kiberhujumlarni tahlil qilish

D. Retrospektiv tahlil

1. **… - obuna davrida avval chiqarilgan barcha yopiq hisobotlarga kirish imkoniyati taqdim etiladi.**

**A. Retrospektiv tahlil**

B. Tahdid vektorlari ro'yxati

C. Zararli dasturlar va kiberhujumlarni tahlil qilish

D. Oldindan shartlarni aniqlash

1. **Threat Hunting nima?**

**A. Tahdidlarni ovlash**

B. Tahdid vektorlari ro'yxati

C. Tahdidlarni aniqlash

D. Tahdidlarni oldini olish

1. **Threat Hunting nechta bosqichdan iborat?**

**A. 2**

B. 3

C. 4

D. 5

1. **Threat Hunting bosqichlari nimadan iborat?**

**A. Gipotezani shakllantirish va gipotezani tekshirish**

B. Gipotezani tekshirish va gipotezani tasdiqlash

C. Gipotezani aniqlash va gipotezani tekshirish

D. Gipotezani tekshirish va gipotezani tugallash

1. **Ovchining yetuklik modeli ([HMM](https://medium.com/@sqrrldata/the-cyber-hunting-maturity-model-6d506faa8ad5) - Hunting Maturity Model) nechta darajadan iborat?**

**A. 5**

B. 4

C. 3

D. 2

1. **Hunting Maturity Model 1-darajasi qanday ataladi?**

**A. HMM0 - Boshlang'ich**

B. HMM1 - Minimal

C. HMM2 - Protsessual

D. HMM3 - Innovatsion

1. **Hunting Maturity Model 2-darajasi qanday ataladi?**

**A. HMM1 - Minimal**

B. HMM4 - Leading

C. HMM2 - Protsessual

D. HMM3 - Innovatsion

1. **Hunting Maturity Model 3-darajasi qanday ataladi?**

**A. HMM2 - Protsessual**

B. HMM4 - Leading

C. HMM1 - Minimal

D. HMM3 – Innovatsion

1. **Hunting Maturity Model 4-darajasi qanday ataladi?**

**A. HMM3 – Innovatsion**

B. HMM4 - Leading

C. HMM2 - Protsessual

D. HMM1 - Minimal

1. **Hunting Maturity Model 5-darajasi qanday ataladi?**

**A. HMM4 - Leading**

B. HMM1 - Minimal

C. HMM2 - Protsessual

D. HMM3 – Innovatsion

1. **Tahdid razvedkasi hayot siklining rejalashtirish va boshqaruv bosqichidagi asosiy vazifalarni belgilang?**

**A) Asosiy rollar va jarayonlar uchun ko'lam va maqsadlarni belgilash**

B) Ma'lumot yig'ish va qayta ishlash usullari va manbalarini kengaytirish

C) Dastlabki ma'lumotlarni mazmunli va tizimli (hodisalar va atributlarga) ko'rinishga keltirish

D) Biznes konteksti va muhitga asoslangan razvedkaning ahamiyatliligi va jiddiyligini baholash

**45. Tahdid razvedkasi hayot siklining to’plash bosqichidagi asosiy vazifalarni belgilang**

**A) Ma'lumot yig'ish va qayta ishlash usullari va manbalarini kengaytirish**

B) Asosiy rollar va jarayonlar uchun ko'lam va maqsadlarni belgilash

C) Dastlabki ma'lumotlarni mazmunli va tizimli (hodisalar va atributlarga) ko'rinishga keltirish

D) Biznes konteksti va muhitga asoslangan razvedkaning ahamiyatliligi va jiddiyligini baholash

**46. Tahdid razvedkasi hayot siklining tahlil bosqichidagi asosiy vazifalarni belgilang**

**A) Dastlabki ma'lumotlarni mazmunli va tizimli (hodisalar va atributlarga) ko'rinishga keltirish**

B) Asosiy rollar va jarayonlar uchun ko'lam va maqsadlarni belgilash

C) Ma'lumot yig'ish va qayta ishlash usullari va manbalarini kengaytirish

D) Biznes konteksti va muhitga asoslangan razvedkaning ahamiyatliligi va jiddiyligini baholash

**47. Tahdid razvedkasi hayot siklining ishlab chiqish bosqichidagi asosiy vazifalarni belgilang**

**A) Biznes konteksti va muhitga asoslangan razvedkaning ahamiyatliligi va jiddiyligini baholash**

B) Asosiy rollar va jarayonlar uchun ko'lam va maqsadlarni belgilash

C) Dastlabki ma'lumotlarni mazmunli va tizimli (hodisalar va atributlarga) ko'rinishga keltirish

D) Ma'lumot yig'ish va qayta ishlash usullari va manbalarini kengaytirish

**48. Tahdid razvedkasi hayot siklining tarqatish va teskari aloqa bosqichidagi asosiy vazifalarni belgilang**

**A) Tezkorlik va maxfiylikni hisobga olgan holda, tayyor ma'lumotlar to'g'risida hisobot berish**

B) Asosiy rollar va jarayonlar uchun ko'lam va maqsadlarni belgilash

C) Dastlabki ma'lumotlarni mazmunli va tizimli (hodisalar va atributlarga) ko'rinishga keltirish

D) Ma'lumot yig'ish va qayta ishlash usullari va manbalarini kengaytirish

**49. …. - ushbu bosqichda mutaxassislar tahdidlarni qayerdan qidirish kerakligi haqida taxminlar qiladilar. Gipotezani ilgari surish uchun ma'lumot manbai kompaniyaning ichki ma'lumotlari ham, tashqi ma'lumotlar ham bo'lishi mumkin.**

**A) Gipotezani shakllantirish**

B) Gipotezani tekshirish

C) Gipotezani tasdiqlash

D) Gipotezani tugallash

**50. … - ular yangi zararli dasturlar bilan bog'liq bo'lgan murosa ko'rsatkichlari uchun so'nggi nuqtalardan olingan ma'lumotlarni tahlil qiladilar.**

**A) Gipotezani tekshirish**

B) Gipotezani shakllantirish

C) Gipotezani tasdiqlash

D) Gipotezani tugallash

**51. Quyidagilardan qaysi biri bulutli muhitda odatiy muammolar bilan bog'liq umumiy holatlardan biri hisoblanadi?**

**A) Xavfsizlik jurnallari mavjud emas.**

C) Doimiy monitoring mavjud

C) Avtomatlashtirish oson

D) Saqlangan ma'lumotlarning hajmi juda katta.

**52. Quyidagilardan qaysi biri bulutli muhitda odatiy muammolar bilan bog'liq umumiy holatlardan biri hisoblanadi?**

**A) AX jurnallari qayerda saqlanganligi bilinmaydi yoki ularga kirish imkoni yo'q.**

B) Doimiy monitoring mavjud

C) Avtomatlashtirish oson

D) Saqlangan ma'lumotlarning hajmi juda katta.

**53. Quyidagilardan qaysi biri bulutli muhitda odatiy muammolar bilan bog'liq umumiy holatlardan biri hisoblanadi?**

**A) Barcha hodisalarni aniqlash uchun monitoringning yetarli emasligi**

B) Doimiy monitoring mavjud

C) Avtomatlashtirish oson

D) Saqlangan ma'lumotlarning hajmi juda katta.

**54. Quyidagilardan qaysi biri bulutli muhitda odatiy muammolar bilan bog'liq umumiy holatlardan biri hisoblanadi?**

**A) Jurnallar mavjud, lekin ularga kirishni avtomatlashtirish qiyin.**

B) Doimiy monitoring mavjud

C) Avtomatlashtirish oson

D) Saqlangan ma'lumotlarning hajmi juda katta.

**55. Bulutli xavfsizlik monitoringi hayotiy sikli bilan o'zingizning bulutli monitoring infratuzilmangizni yaratishingiz mumkin - ....**

**A) faqat IaaS/PaaS platformalari uchun.**

B) faqat SaaS/PaaS platformalari uchun.

C) faqat IaaS/SaaS platformalari uchun.

D) faqat SaaS / IaaS platformalari uchun.

**56. Bulutdagi axborot xavfsizligi monitoringi jarayonining asosiy komponentlarini belgilang.**

**A) Infratuzilmani tayyorlash, yig'ish, qayta ishlash, saqlash, tahlil qilish va hisobot berish.**

B) Infratuzilmani tayyorlash, yig'ish, uzatish, qayta ishlash, saqlash va tahlil qilish.

C) Axborotni tayyorlash, to'plash, qayta ishlash, saqlash va tahlil qilish.

D) Asosiy ko'rsatkichlarni tayyorlash, yig'ish, javob berish, qayta ishlash va saqlash.

**57. Turli bulutli xizmatlarda nechta HR (Human resources) xizmatlari mavjud?**

**A) 175 dona**

B) 200 dona

C) 50 dona

D) 120 dona

**58. Turli bulut xizmatlaridan nechtasi marketing bilan bog'liq?**

**A) 170 dona**

B) 52 dona

C) 90 dona

D) 224 dona

**59. Turli bulutli xizmatlardan nechtasi aloqa sohasi uchun mo’ljallangan?**

**A) 110 dona**

B) 72 dona

C) 200 dona

D) 430 dona

**60. Turli xil bulutli xizmatlar orasida, ularning qanchasi moliya va CRM (Customer Relationship  Management) uchun mo'ljallangan?**

**A) 76 dona**

B) 72 dona

C) 95 dona

D) 37 dona

**61. Turli bulut xizmatlarida Cisco kompaniyasining ulushi qanchani tashkil etadi?**

**A) 700 dona**

B) 400 dona

C) 50 dona

D) 200 dona

**62. Bulutli tarmoqlar xizmatlarida ANTI DDOS dan foydalanishda lokal himoya qilish uchun qanday jarayonlar amalga oshiriladi?**

**A) Identifikatsiya, filtrlash, tarmoqni aniqlash va himoya qilish.**

B) Identifikatsiya, autentifikatsiya, tarmoqni aniqlash va himoya qilish.

C) Identifikatsiya, autentifikatsiya, tekshirish va kashf qilish.

D) Tarmoqni filtrlash, aniqlash, tozalash va himoya qilish.

**63. Cloud Networks xizmatlarida ANTI DDOS-dan foydalanishda bulutga qarshi choralar qanday jarayonlardan iborat?**

**А) Aylanib o’tish, qamrab olish, yo‘nalishni o‘zgartirish va tozalash.**

B) Identifikatsiya, singdirish, yo‘nalishni o‘zgartirish va tozalash.

C) Identifikatsiya, autentifikatsiya, yo‘nalishni o‘zgartirish va tozalash.

D) Filtrlash, aniqlash, yo‘nalishni o‘zgartirish va tozalash.

**64. Hujumlarni aniqlash tizimi (IDS) qaysi vazifani bajaradi?**

**A) Intrusion Detection System (IDS) – trafikni skanerlovchi va tahdidlar haqida xabar beruvchi passiv tizim.**

B) Tizim ekspluatatsiyalarni aniqlash va oldini olish uchun tarmoq trafigini, oqimlarni tekshiradi.

C) Intrusion Detection System (IDS) - bu trafikni kuzatuvchi va muammoni hal qiluvchi faol tizim.

D) Ichki tahdidlar paydo bo'lganda tizim tarmoq trafigini bloklaydi.

**65. Hujumlarni oldini olish tizimi (IPS) qaysi vazifani bajaradi?**

**A) Tizim tarmoq trafigini, ekspluatatsiyalarni aniqlash va oldini olish uchun oqimlarni tekshiradi.**

B) Hujumlarni aniqlash tizimi - bu trafikni skanerlaydigan va tahdidlar haqida xabar beruvchi passiv tizim.

C) Hujumlarni aniqlash tizimi - bu harakatni kuzatuvchi va muammoni hal qiluvchi faol tizim.

D) Ichki tahdidlar paydo bo'lganda tizim tarmoq trafigini bloklaydi.

**66. Bulutdagi axborot xavfsizligi monitoringi jarayonining asosiy komponentlaridan biri infratuzilmani tayyorlash bu - …**

**A) axborot xavfsizligi uchun muhim bo'lgan hodisalarni yig'ish uchun zarur ilovalar va infratuzilmani aniqlash**

B) xavfsizlik hodisalari ularni qayta ishlash, saqlash va tahlil qilish uchun keyinchalik uzatish uchun turli manbalardan jamlanadi

C) siz hodisalarni aniqlash va ularga avtomatik yoki qo'l yechimida javob berish imkoniyatiga egasiz

D) yig'ilgan qayta ishlangan va "xom" ma'lumotlarni qisqa muddatli va uzoq muddatli saqlash uchun javobgardir

**67. Bulutdagi axborot xavfsizligi monitoringi jarayonining asosiy komponentlaridan biri - yig’ish bosqichida …**

**A) xavfsizlik hodisalari ularni qayta ishlash, saqlash va tahlil qilish uchun keyinchalik uzatish uchun turli manbalardan jamlanadi**

B) axborot xavfsizligi uchun muhim bo'lgan hodisalarni yig'ish uchun zarur ilovalar va infratuzilmani aniqlanadi

C) siz hodisalarni aniqlash va ularga avtomatik yoki qo'l yechimida javob berish imkoniyatiga egasiz

D) yig'ilgan qayta ishlangan va "xom" ma'lumotlarni qisqa muddatli va uzoq muddatli saqlash uchun javobgardir

**68. Bulutdagi axborot xavfsizligi monitoringi jarayonining asosiy komponentlaridan biri – qayta ishlash bosqichida …**

**A) ma'lumotlar keyingi tahlilini osonlashtirish uchun o'zgartiriladi va boyitiladi**

B) axborot xavfsizligi uchun muhim bo'lgan hodisalarni yig'ish uchun zarur ilovalar va infratuzilma aniqlanadi

C) siz hodisalarni aniqlash va ularga avtomatik yoki qo'l yechimida javob berish imkoniyatiga egasiz

D) yig'ilgan qayta ishlangan va "xom" ma'lumotlarni qisqa muddatli va uzoq muddatli saqlash uchun javobgardir

**69. Bulutdagi axborot xavfsizligi monitoringi jarayonining asosiy komponentlaridan biri saqlash bu - …**

**A) yig'ilgan qayta ishlangan va "xom" ma'lumotlarni qisqa muddatli va uzoq muddatli saqlash uchun javobgardir**

B) axborot xavfsizligi uchun muhim bo'lgan hodisalarni yig'ish uchun zarur ilovalar va infratuzilma aniqlanadi

C) siz hodisalarni aniqlash va ularga avtomatik yoki qo'l yechimida javob berish imkoniyatiga egasiz

D) ma'lumotlar keyingi tahlilini osonlashtirish uchun o'zgartiriladi va boyitiladi

**70. Bulutdagi axborot xavfsizligi monitoringi jarayonining asosiy komponentlaridan biri – tahlil qilish bosqichida …**

**A) siz hodisalarni aniqlash va ularga avtomatik yoki qo'l yechimida javob berish imkoniyatiga ega bo’lasiz**

B) axborot xavfsizligi uchun muhim bo'lgan hodisalarni yig'ish uchun zarur ilovalar va infratuzilma aniqlanadi

C) yig'ilgan qayta ishlangan va "xom" ma'lumotlarni qisqa muddatli va uzoq muddatli saqlash uchun javobgardir

D) ma'lumotlar keyingi tahlilini osonlashtirish uchun o'zgartiriladi va boyitiladi

**71. Bulutdagi axborot xavfsizligi monitoringi jarayonining asosiy komponentlaridan biri hisobot berish bu- …**

**A) manfaatdor tomonlar (boshqaruv, auditorlar, bulutli provayder, mijozlar va boshqalar) uchun bizga ma'lum qarorlar qabul qilishda yordam beradigan asosiy ko'rsatkichlarni shakllantirishga yordam beradi**

B) axborot xavfsizligi uchun muhim bo'lgan hodisalarni yig'ish uchun zarur ilovalar va infratuzilma aniqlanadi

C) yig'ilgan qayta ishlangan va "xom" ma'lumotlarni qisqa muddatli va uzoq muddatli saqlash uchun javobgardir

D) ma'lumotlar keyingi tahlilini osonlashtirish uchun o'zgartiriladi va boyitiladi

**72. FortiDDoS bu - …**

**A) minglab parametrlarni boshqarish, ilovalar va trafikni boshqarishni hisobga olgan holda barcha** **DDoS hujumlaridan himoya qilishni o'z ichiga oladi**

B) keng doiradagi hujumlarni blokirovka qilish orqali nol kunlik DDoS himoyasi

C) trafik anomaliyalarini aniqlaydi va g'ayritabiiy paketlarni tekshiradi, tarmoq mavjudligi va biznesning uzluksizligini ta'minlaydi

D) web-ilovaning xavfsizlik devori, DDoS qoidalari mexanizmi va qonuniy trafikka ko'rinmaydigan qator progressiv muammolar orqali trafikni filtrlaydi

**73. Check Point DDoS Protector bu - …**

**A) keng doiradagi hujumlarni blokirovka qilish orqali nol kunlik DDoS himoyasi**

B) minglab parametrlarni boshqarish, ilovalar va trafikni boshqarishni hisobga olgan holda barcha DDoS hujumlaridan himoya qilishni o'z ichiga oladi

C) trafik anomaliyalarini aniqlaydi va g'ayritabiiy paketlarni tekshiradi, tarmoq mavjudligi va biznesning uzluksizligini ta'minlaydi

D) web-ilovaning xavfsizlik devori, DDoS qoidalari mexanizmi va qonuniy trafikka ko'rinmaydigan qator progressiv muammolar orqali trafikni filtrlaydi

**74. Cisco DDoS himoyasi bu - …**

**A) trafik anomaliyalarini aniqlaydi va g'ayritabiiy paketlarni tekshiradi, tarmoq mavjudligi va biznesning uzluksizligini ta'minlaydi**

B) minglab parametrlarni boshqarish, ilovalar va trafikni boshqarishni hisobga olgan holda barcha DDoS hujumlaridan himoya qilishni o'z ichiga oladi

C) keng doiradagi hujumlarni blokirovka qilish orqali nol kunlik DDoS himoyasi

D) web-ilovaning xavfsizlik devori, DDoS qoidalari mexanizmi va qonuniy trafikka ko'rinmaydigan qator progressiv muammolar orqali trafikni filtrlaydi

**75. Imperva Incapsula bu - …**

**A) web-ilovaning xavfsizlik devori, DDoS qoidalari mexanizmi va qonuniy trafikka ko'rinmaydigan qator progressiv muammolar orqali trafikni filtrlaydi**

B) minglab parametrlarni boshqarish, ilovalar va trafikni boshqarishni hisobga olgan holda barcha DDoS hujumlaridan himoya qilishni o'z ichiga oladi

C) keng doiradagi hujumlarni blokirovka qilish orqali nol kunlik DDoS himoyasi

D) trafik anomaliyalarini aniqlaydi va g'ayritabiiy paketlarni tekshiradi, tarmoq mavjudligi va biznesning uzluksizligini ta'minlaydi

**76. Threat Intelligence - bu**

**A) kiberxavfsizlik chora tadbirlarini mustaxkamlash va axborot xavfsizligi bo‘yicha ma’lum bir jamiyatning axborot xavfsizligi haqida xabardorligini oshirish maqsadida joriy kiber tahdidlar haqida ma’lumot olish va to‘plash uchun ma’lum ma’lumot manbalarini o‘rganish va tahlil qilish jarayoni**

B) foydalanuvchi parolni kiritish jarayonida yonida turib qarab turish orqali bilib olishni maqsad qiladi

C) biror narsaga egalik qilishga asoslangan autentifikatsiya usulidagi mavjud muammolarni oldini olishda samarali hisoblanadi

D) hujumlarni axborot resurslarining mavjudligiga ta’sir qiladi.

**77. Ochiq ma’lumot manbalari bu...**

**A) Google, Yandex, Bing va Shodan, Censys, nmap kabi boshqa maxsus vositalar yordamida topish mumkin bo‘lgan barcha manba**

B) ommaviy axborot vositalarida va Social Media Intelligence (SOCMINT) ijtimoiy platformalarida topiladigan barchasi

C) bo‘lajak kiber jinoyatlarning tafsilotlari muxokamasi qilinishi

D) biror narsaga egalik qilishga asoslangan autentifikatsiya usulidagi mavjud muammolarni oldini olishda samaraliligi

**78. Ommaviy axborot vositalari manbalari bu...**

**A) ommaviy axborot vositalarida va Social Media Intelligence (SOCMINT) ijtimoiy platformalarida topiladigan barchasi**

B) Google, Yandex, Bing va Shodan, Censys, nmap kabi boshqa maxsus vositalar yordamida topish mumkin bo‘lgan barcha manba

C) bo‘lajak kiber jinoyatlarning tafsilotlari muxokamasi qilinishi

D) biror narsaga egalik qilishga asoslangan autentifikatsiya usulidagi mavjud muammolarni oldini olishda samaraliligi

**79. Yopiq maydonlar va forumlar . . .**

**A) bo‘lajak kiber jinoyatlarning tafsilotlari muxokamasi qilinishi (deepweb, darknet)**

B) Google, Yandex, Bing va Shodan, Censys, nmap kabi boshqa maxsus vositalar yordamida topish mumkin bo‘lgan barcha manba

C) ommaviy axborot vositalarida va Social Media Intelligence (SOCMINT) ijtimoiy platformalarida topiladigan barchasi

D) biror narsaga egalik qilishga asoslangan autentifikatsiya usulidagi mavjud muammolarni oldini olishda samaraliligi

**80. Threat Intelligence platformasining asosiy elementi**

**A) kelishuv ko‘rsatkichlari sifatida tasvirlangan ma’lumotlar oqimlari hisoblanadi (Indicators of Compromise, IoC)**

B) ommaviy axborot vositalarida va Social Media Intelligence (SOCMINT) ijtimoiy platformalarida topiladigan barcha ma’lumot

C) biror narsaga egalik qilishga asoslangan autentifikatsiya usulidagi mavjud muammolarni oldini olishda samaraliligi

D) bo‘lajak kiber jinoyatlarning tafsilotlari muxokamasi qilinishi

**81. Fid lar– bu . . .**

**A) kelishuv ko‘rsatkichlarini o‘z ichiga olgan ma’lumotlar oqimlari, ya’ni potensial tahdidni aniqlash mumkin bo‘lgan belgilar**

B) kelishuv ko‘rsatkichlari sifatida tasvirlangan ma’lumotlar oqimlari hisoblanadi

C) bo‘lajak kiber jinoyatlarning tafsilotlari muxokamasi qilinishi

D) biror narsaga egalik qilishga asoslangan autentifikatsiya usulidagi mavjud muammolarni oldini olishda samaraliligi

**82. Kelishuv ko‘rsatkichlarini o‘z ichiga olgan ma’lumotlar oqimlari, ya’ni potensial tahdidni aniqlash mumkin bo‘lgan belgilar**

**A) fid lar**

B) xakerlar

C) tahdidlar

D) ma’lumot

**83. Fid larning kamchiligi nimadan iborat?**

**A) kontekstning yetishmasligi**

B) tahdid zaifliklari

C) yopiq manbalar

D) samaradorlik

**84. DDoS fid – tushunchasi.**

**A) taqsimlangan xizmatdan voz kechish hujumi**

B) xizmatdan voz kechish

C) xavfsiz axborot

D) zararli dastur

**85. Operatsion (texnik) tahdid razvedkasi – bu . . . .**

**A) raqobatbardosh ustunlikka erishish uchun texnik vositalardan foydalangan holda ma’lumot olishning maqsadi faoliyati**

B) razvedka shtati, tashkilot yoki strategiyani ishlab chiqishga ta’sir qiladigan razvedka

C) boshqa ijtimoiy hamjamiyatning strategik salohiyati va strategik ishlari to‘g‘risida ma’lumot olish maqsadidagi razvedka faoliyati

D)axborot texnologiyalari sohasida tahdidlar rivojlanishining tahdidga ta’siri

**86. Texnik razvedka o‘tkazish tamoyillarida “Tezkorlik” – bu. . .**

**A) razvedka idoralari o‘zlariga yuklangan vazifalarnit imkon qadar tezroq hal qilishlari kerak**

B) tadqiqotlar olib boriladigan sharoitlarning o‘zgarishi ishlab chiqarilgan ma’lumotlarning sifatiga ta’sir qilmasligi kerak

C) axborotni ajratib olish, oldindan ishlab chiqilgan razvedka dasturlariga muvofiq amalga oshiriladi

D) razvedkaning passiv texnik vositalaridan foydalanish, razvedka uskunalarini maskalash va birlashtirish, afsonaviylikni keng qo‘llash

**87. Texnik razvedka o‘tkazish tamoyillarida “Uzluksizlik” – bu . . .**

**A) tadqiqotlar olib boriladigan sharoitlarning o‘zgarishi ishlab chiqarilgan ma’lumotlarning sifatiga ta’sir qilmasligi kerak**

B) razvedka idoralari o‘zlariga yuklangan vazifalarnit imkon qadar tezroq hal qilishlari kerak

C) axborotni ajratib olish, oldindan ishlab chiqilgan razvedka dasturlariga muvofiq amalga oshiriladi

D) razvedkaning passiv texnik vositalaridan foydalanish, razvedka uskunalarini maskalash va birlashtirish, afsonaviylikni keng qo‘llash

**88. Texnik razvedka o‘tkazish tamoyillarida “Rejalashtirish” – bu . . .**

**A) axborotni ajratib olish, oldindan ishlab chiqilgan razvedka dasturlariga muvofiq amalga oshiriladi**

B) razvedka idoralari o‘zlariga yuklangan vazifalarnit imkon qadar tezroq hal qilishlari kerak

C) tadqiqotlar olib boriladigan sharoitlarning o‘zgarishi ishlab chiqarilgan ma’lumotlarning sifatiga ta’sir qilmasligi kerak

D) razvedkaning passiv texnik vositalaridan foydalanish, razvedka uskunalarini maskalash va birlashtirish, afsonaviylikni keng qo‘llash

**89. Texnik razvedka o‘tkazish tamoyillarida “Yashirinlik” – bu . . .**

**A) razvedkaning passiv texnik vositalaridan foydalanish, razvedka uskunalarini maskalash va birlashtirish, afsonaviylikni keng qo‘llash**

B) razvedka idoralari o‘zlariga yuklangan vazifalarnit imkon qadar tezroq hal qilishlari kerak

C) tadqiqotlar olib boriladigan sharoitlarning o‘zgarishi ishlab chiqarilgan ma’lumotlarning sifatiga ta’sir qilmasligi kerak

D) axborotni ajratib olish, oldindan ishlab chiqilgan razvedka dasturlariga muvofiq amalga oshiriladi

**90. Xujum shakli (Attack pattern) – bu**

**A) tajovuzkor o‘z nishonini buzish uchun ishlatgan yondashuvni (TTP) tasvirlaydi**

B) ma’lum vaqt davomida sodir bo‘ladigan zararli xulq-atvor belgilarining ketma-ketligini tavsiflaydi

C) hujumni oldini olish yoki unga qarshi turish uchun qilinadigan qadamlarni tavsiflaydi

D) zararli faoliyatni aniqlash uchun ishlatilishi mumkin bo‘lgan zararli texnik artefaktlar tasvirlaydi

**91. Zararli kampaniya (Campaign) –**

**A) ma’lum vaqt davomida sodir bo‘ladigan zararli xulq-atvor belgilarining ketma-ketligini tavsiflaydi**

B) tajovuzkor o‘z nishonini buzish uchun ishlatgan yondashuvni tasvirlaydi

C) hujumni oldini olish yoki unga qarshi turish uchun qilinadigan qadamlarni tavsiflaydi

D) zararli faoliyatni aniqlash uchun ishlatilishi mumkin bo‘lgan zararli texnik artefaktlar tasvirlaydi

**92. Harakat yo‘nalishi (Course of action) - . . .**

**A) hujumni oldini olish yoki unga qarshi turish uchun qilinadigan qadamlarni tavsiflaydi**

B) tajovuzkor o‘z nishonini buzish uchun ishlatgan yondashuvni tasvirlaydi

C) ma’lum vaqt davomida sodir bo‘ladigan zararli xulq-atvor belgilarining ketma-ketligini tavsiflaydi

D) zararli faoliyatni aniqlash uchun ishlatilishi mumkin bo‘lgan zararli texnik artefaktlar tasvirlaydi

**93. “Tahdid razvedkasining hayot sikli” – bu**

**A) firibgarlikka qarshi, jismoniy va kiberxavfsizlik dasturlarining asosiy poydevori**

B) ma’lumotlar texnik yoki insoniy vositalar yordamida turli yo‘llar bilan to‘planishi

C) tahdidlarni o‘rganish jamoaning operatsion samaradorligini oshishi

D) ajratib olingan intelekt iste’molchining axborot talablariga javob berish

**94. Teskari aloqa (Feedback)**

**A) ajratib olingan intelekt iste’molchining axborot talablariga javob berishi yoki yo‘qligini aniqlaydigan baho**

B) firibgarlikka qarshi, jismoniy va kiberxavfsizlik dasturlarining asosiy poydevori

C) ma’lumotlar texnik yoki insoniy vositalar yordamida turli yo‘llar bilan to‘planishi

D) tahdidlarni o‘rganish jamoaning operatsion samaradorligini oshishi

**95. Axborot xavfsizligi tamoyillaridan biri – “muvofiqlik prinsipi”da ....**

**A) xavfsizlikka tizimli ravishda yondashish kerak: xodimlarni tanlash va o'qitishdan tortib, ish yuritish qoidalarini yaratishgacha**

B) ma'lumotni hech narsaga ishonmang - ommaviy axborot vositalari, shifrlar, omborlar.

C) rahbardan tashqari, kompaniyada barcha ma'lumotlarga ega bo'lgan shaxs bo'lmasligi kerak

D) Ma'lumotni saqlang va uni turli kanallar orqali yuboring.

**96. Axborot xavfsizligi tamoyillaridan biri – “axborot shovqini prinsipi”da ....**

**A) ma'lumotni hech narsaga ishonmang - ommaviy axborot vositalari, shifrlar, omborlar**

B) xavfsizlikka tizimli ravishda yondashish kerak: xodimlarni tanlash va o'qitishdan tortib, ish yuritish qoidalarini yaratishgacha

C) rahbardan tashqari, kompaniyada barcha ma'lumotlarga ega bo'lgan shaxs bo'lmasligi kerak

D) ma'lumotni saqlang va uni turli kanallar orqali yuboring

**97. Axborot xavfsizligi tamoyillaridan biri – “Bo’lib ol va zabt et prinsipi”da ....**

**A) rahbardan tashqari, kompaniyada barcha ma'lumotlarga ega bo'lgan shaxs bo'lmasligi kerak**

B) xavfsizlikka tizimli ravishda yondashish kerak: xodimlarni tanlash va o'qitishdan tortib, ish yuritish qoidalarini yaratishgacha

C) ma'lumotni hech narsaga ishonmang - ommaviy axborot vositalari, shifrlar,omborlar

D) ma'lumotni saqlang va uni turli kanallar orqali yuboring

**98. Axborot xavfsizligi tamoyillaridan biri – “Turli savat prinsipi”da ....**

**A)** **ma'lumotni saqlang va uni turli kanallar orqali yuboring**

B) xavfsizlikka tizimli ravishda yondashish kerak: xodimlarni tanlash va o'qitishdan tortib, ish yuritish qoidalarini yaratishgacha

C) ma'lumotni hech narsaga ishonmang - ommaviy axborot vositalari, shifrlar,omborlar

D) rahbardan tashqari, kompaniyada barcha ma'lumotlarga ega bo'lgan shaxs bo'lmasligi kerak

**99. Axborot xavfsizligi tamoyillaridan biri – “Paranoya prinsipi”da ....**

**A)** **Har kimdan shubhalaning, yangi texnologiyalarning mutlaq imkoniyatlariga ishonmang**

B) xavfsizlikka tizimli ravishda yondashish kerak: xodimlarni tanlash va o'qitishdan tortib, ish yuritish qoidalarini yaratishgacha

C) ma'lumotni saqlang va uni turli kanallar orqali yuboring

D) rahbardan tashqari, kompaniyada barcha ma'lumotlarga ega bo'lgan shaxs bo'lmasligi kerak

**100. Tahdid ehtimolini baholash uchun mutaxassislar nechta darajadan iborat sifatli o'lchovdan foydalanadilar?**

**A) 3**

B) 4

C) 2

D) 5