**BTEC Assignment Brief**

|  |  |
| --- | --- |
| **Qualification** | Pearson BTEC Higher Nationals in Digital Technologies |
| **Unit number and title** | Unit 3: Cyber Security |
| **Learning aim(s)** | Ushbu birjaning oxiriga kelib talabalar:  **LO1** Kiberjinoyatchilik va kiber tahdid aktyorlarining mohiyatini o'rganing  **LO2** Kiber xavfsizlik tahdidlari va xavf-xatarlarini o'rganib chiqish  **LO3** ICT infratuzilmasiga qo'llaniladigan axborotni kafolatlash konsepsiyalarining samaradorligini o'rganib chiqish  **LO4** Kiber xavfsizlik tahdidlariga hodisalarga javob berish usullarini o'rganib chiqish |
| **Assignment title** | Kiber xavfsizlik |
| **Assessor** | Khoshimov A |
| **Issue date** | May 01,2025 |
| **Hand in deadline** |  |

|  |  |
| --- | --- |
| **Ssenariy yoki kontekst** | Siz kiber xavfsizlik bo'yicha etakchi maslahat firmasida kiber xavfsizlik bo'yicha tahlilchisiz. Yaqinda sizning firmangizni moliya, sog'liqni saqlash va texnologiyalar sohasida faol bo'lgan yirik xalqaro korporatsiya yolladi. Korporatsiyaning muhim raqamli mavjudligi va uning ma'lumotlarining sezgirligini hisobga olsak, u ko'plab kiber tahdidlarga duch kelmoqda. Topshiriq: Tanlangan tashkilot uchun kiberxavfsizlik strategiyasini ishlab chiqing va quyidagi jihatlarni keng qamrovli hisobotda taqdim eting:   1. **Kiberjinoyatlar va xatarli aktyorlar tahlili:**    * Tashkilotga tahdid solishi mumkin bo‘lgan kiberjinoyat turlarini (masalan, phishing, ransomware, DDoS) va ularning xususiyatlarini tasvirlang.    * Tashkilotning qaysi resurslari (masalan, mijozlar ma’lumotlari, moliyaviy tizimlar, infratuzilma) potentsial nishon ekanligini aniqlang va nima uchun nishonga olinishini tushuntiring.    * Raqamli tizimlarning “nishon” va “vosita” sifatidagi rolini haqiqiy hayot misollari (masalan, IoT qurilmalari yoki bulutli serverlar) bilan tahlil qiling.    * Kiberxatarli faoliyat turlarini baholang va xatarli aktyorlarni zararsizlantirish uchun choralar (masalan, qonuniy, texnologik yoki xodimlar malakasini oshirish) taklif qiling. 2. **Kiberxavfsizlik xatarlari va mudofaa usullari:**    * Tashkilotning tizimi, xizmati yoki jarayonlariga tahdid soluvchi xavf va xatarlarni (masalan, zaif autentifikatsiya, tarmoq xavfsizligi muammolari) aniqlang.    * Tashkilotga qarshi qo‘llanilishi mumkin bo‘lgan umumiy hujum texnikalarini (masalan, SQL injection, social engineering) tadqiq qiling va ularga qarshi mudofaa usullarini (masalan, shifrlash, ko‘p faktorli autentifikatsiya) tavsiya qiling.    * Ushbu hujumlarga qarshi mudofaa qilishda xavf-xatar razvedkasining (threat intelligence) rolini misollar (masalan, SIEM tizimlari yoki real vaqtda monitoring) bilan baholang. 3. **Axborot xavfsizligi konsepsiyalarining qo‘llanilishi:**    * Tashkilotning AKT infratuzilmasidagi xatar va zaifliklarni kamaytirishda axborot xavfsizligi konsepsiyalarini (masalan, risklarni boshqarish, ma’lumotlarni shifrlash) qanday qo‘llash mumkinligini misollar bilan tushuntiring.    * Axborot xavfsizligi konsepsiyalari tashkilotning kiberxavfsizlik barqarorligini qanday oshirishi mumkinligini (masalan, ISO 27001 standartlari yoki NIST ramkasi) baholang.    * Turli tashkilotlar tomonidan kiberxavfsizlik xatarlariga qarshi qo‘llanilgan javob choralarini (masalan, incidentlarga tayyorgarlik, ma’lumotlar tiklash) taqqoslang va ularning samaradorligini baholang. 4. **Incidentlarga javob berish usullari:**    * Tashkilot faoliyat yuritadigan sohada (masalan, moliya, sog‘liqni saqlash) amaldagi xavfsizlik standartlari va qoidalarini tasvirlang va ularning oqibatlarini tahlil qiling.    * Kiberxavfsizlik xatarlariga qarshi qo‘llanilgan javob turlarini (masalan, incidentlarni boshqarish, ma’lumotlar tiklash) ko‘rib chiqing.    * Jinoyat va boshqa qonunlarning kiberjinoyatlarni oldini olishdagi rolini tahlil qiling. |

**O'quv natijalari va baholash mezonlari**

|  |  |  |
| --- | --- | --- |
| **Pass** | **Merit** | **Distinction** |
| **LO1** Kiberjinoyatchilik va kiber tahdid aktyorlarining mohiyatini o'rganing | |  |
| **P1** Zararli va/yoki jinoiy kiber faoliyat turlarini ko'rib chiqish.  **P2** Kiberjinoyatchilikning potentsial maqsadlarini oʻrganish. | **M1** Raqamli tizimlar tushunchasini kiber xavfsizlik bilan bog'liq bo'lgan "maqsadlar" va "vositalar" deb tahlil qiling, haqiqiy dunyo misollarini keltiring. | **LO1 and LO2**  **D1** Zararli kiber faoliyat turlarini va kiber tahdid aktyorlarini neytrallashtirish uchun amalga oshirilishi mumkin bo'lgan choralarni baholash. |
| **LO2** Kiber xavfsizlik tahdidlari va xavf-xatarlarini o'rganib chiqish | |  |
| **P3** Tizim yoki xizmat yoki jarayonga xavfsizlik tahdidi va xavf-xatarlarini tasvirlab bering.  **P4** Umumiy hujum usullarini o'rganib, ulardan himoya qilishni tavsiya eting. | **M2** Umumiy hujum usullaridan himoya qilishda tahdid razvedkasining rolini bahola. |  |
| **LO3** ICT infratuzilmasiga qo'llaniladigan axborotni kafolatlash konsepsiyalarining samaradorligini o'rganib chiqish | |  |
| **P5** Axborotni kafolatlash tushunchalari ICT infrastrukturasidagi tahdid va zaifliklarni qanday yengillashtirishi mumkinligini tushuntirib bering, misollar keltiring. | **M3** Axborotni kafolatlash ICT infratuzilmasining kiber o'zgaruvchanligini qanday oshirishi mumkinligini bahola. | **LO3 and LO4**  **D2** Javoban turli tashkilotlar tomonidan kiber xavfsizlik tahdidlariga amalga oshirilgan javoblarni baholash. |
|  | |
| **LO4** Kiber xavfsizlik tahdidlariga hodisalarga javob berish usullarini o'rganib chiqish. | |  |
| **P6** Xavfsizlik standartlari, qoidalari va ularning oqibatlarini kamida ikkita sektor bo'yicha tavsiflang. | **M4** Kiberjinoyatchilikni to'xtatishda jinoyat va boshqa qonunning rolini tahlil qilish. |  |
| **P7** Kiber xavfsizlik tahdidlariga javoban amalga oshirilgan javob turlarini tekshirish. |  |  |

|  |  |
| --- | --- |
| **Sources of information to support you with this Assignment** | Amoroso, E. and Amoroso, M. (2017) From CIA to APT: An Introduction to Cyber Security.  New York: Independently published.  Gillespie, A. A. (2015) Cybercrime. Oxon: Routledge.  Grabosky, G. (2015) Cybercrime (Keynotes Criminology Criminal Justice series).  New York: Oxford University Press.  Stevens, T. (2015) Cyber Security and the Politics of Time. Cambridge:  Cambridge University Press.  Sutton, D. (2017) Cyber Security: A practitioner’s guide. Swindon: BCS. |
| **Other assessment materials attached to this Assignment Brief** |  |