

SOC окуяларга мониторинг жүргүзүү боюнча кызматтарды көрсөтүү үчүн
(кызмат келишиминин негизинде)

ТЕХНИКАЛЫК ТАПШЫРМА

№	Негизги маалыматтар жана талаптар тизмеси	Негизги маалыматтар жана талаптар
1	Кызмат көрсөтүүчү жер	Бишкек шаары, Ибраимов көчөсү, 24.
2	Буйрутмачы	Маалымат коопсуздугу бөлүмү.
3	Кызматтык милдеттер	• Маалыматтык коопсуздук окуяларын (SIEM, SOAR, XDR, AV, FW, IPS/IDS, DLP ж. б.) коргонуу каражаттары аркылуу мониторингдөө жана талдоо; • Маалымат коопсуздугу боюнча инциденттерди каттоо жана иликтөө; • Инциденттерди жогорку деңгээлдеги линияларга эскалациялоо; • SOC борборунун 24/7 режиминде иштешин камсыз кылуу үчүн нөөмөттүк иш графиги; • Коопсуздук системаларында инциденттерди аныктоонун жаңы сценарийлерин иштеп чыгуу; • Маалыматтык коопсуздук инциденттерине жооп кайтаруу пландарын (playbook) иштеп чыгуу жана аларды автоматташтыруу; • Маалыматтык коопсуздуктун типтүү инциденттеринин базасын жүргүзүү жана актуалдуулугун камсыз кылуу; • Жалган ишке кирүүлөрдү аныктоо жана аларды жок кылуу боюнча сунуштарды берүү; • Коопсуздук системаларынын абалын көзөмөлдөө
4	Аткаруучуга коюлган квалификациялык талаптар	Тилдерди билүү: • Орус тилинде – эркин сүйлөшүү керек; • Кыргыз тилинде – эркин сүйлөшүү керек; • Англис тилинде - ортодон жогору (Upper Intermediate) же жогорку деңгээл (Advanced).: • Маалымат коопсуздугунун негиздерин билүү; • Windows жана Unix системаларынын иштөө принциптерин базалык деңгээлде түшүнүү; • Тармактык протоколдордун иштөө логикасын түшүнүү (OSI модели жана/же TCP/IP) • Active Directory системасынын негизги принциптерин түшүнүү (аутентификация механизмдери, чабуулдар);

		• <i>MITRE ATT&CK</i> жана <i>Cyber Kill Chain</i> сыяктуу ыкмалар аркылуу чабуулчулардын негизги тактикасын жана техникасын билүү жана түшүнүү.
5	Жеке сапаттар	• Майда-баратка көңүл буруу. • Жоопкерчилик; • Коммуникабелдүүлүк жана командада иштей билүү жөндөмү; • Стресске туруктуулук жана көп тапшырма шарттарында иштей билүү; • Аналитикалык ой жүгүртүү, жыйынтыкка багытталуу; • Жогорку деңгээлдеги өзүн-өзү уюштуруу жана өз алдынча чечим кабыл алуу жөндөмү; • Өзгөрүп жаткан шарттарга ийкемдүүлүк жана ыңгайлашуу жөндөмү.
6	Көзөмөл жана отчеттуулук	Иш тапшыруучу аткарылган иштер жөнүндө үзгүлтүксүз отчет берүүгө милдеттүү, анын ичинде: • Сменанын аягында маалымат коопсуздугу боюнча окуялар жөнүндө толук отчет; • Аткарылган иштер тууралуу ай сайын отчет.
7	Иш шарттары	• График: 1x2 (<i>экиден бир күн</i>); • 1 нөөмөт: 15 саат; • Кеңсе: Бишкек шаары, Ибраимова 24.