Техникийн тодорхойлолт

Барааны нэр: Эцсийн цэгийн хамгаалалтын систем (тоо ширхэг:300)

№	***Захиалагчийн техникийн тодорхойлолт*** *(Тухайн барааны үзүүлэлт тус бүрийг дор жагсааж бичих ба хэрвээ чанарын баталгаат хугацаа шаардах бол бичнэ үү.)*	***Санал болгож буй техникийн тодорхойлолт*** *(захиалагчийн техникийн тодорхойлолтыг хуулахгүй байхыг анхаарна уу. Зөвхөн санал болгож буй барааны техникийн тодорхойлолтыг бичнэ үү.)*	***Тайлбар*** *(дээрх үзүүлэлтийг нотлох баримт бичиг болон танилцуулгыг хавсаргана)*
1	Хамгаалалтын систем нь дараах үйлдлийн системүүдийг дэмжин ажилладаг байна **Windows Workstation** – 11, 10, 8, and 7 **Windows Server** – 2022, 2019, 2016, 2012, and 2008 **MacOS** –Sonoma (14), Ventura (13), Monterey (12), Big Sur (11), Catalina (10) **Linux** – Ubuntu (22.04.03, 22.04, 20.04, 18.04, 16.04), Amazon (2), CentOS (7.8-8.5), Debian (9.12- 11.7), OpenSUSE (15.3, 42.3), SUSE (12 SP5, 15 SP3), Oracle (7.9-8.7), RHEL (7.8-8.7, 9.0-9.2) **VDI & Terminal Server** – VMware, Citrix, Terminal Server Servers – SQL, Web Servers, DHCP Servers, Share Point (2010, 2016, 2013), Active Directory, Exchange, HyperV, DNS.		
2	Халдагад хариу үйлдэл үзүүлэх дараах чадамжуудыг агуулсан байна **Threat Intelligence** – ThreatCloud and IOC Management **Access Control** - Firewall, Application Control, Endpoint Compliance, Remote Access (VPN) **Threat Prevention** - Anti-Ransomware (Including Intel TDT), Anti-Malware, Anti-Bot, Anti-Exploit, Behavioral Guard, and Port Protection **Browser Security** – Zero Phishing, URL Filtering, Corporate password Reuse, Safe Search **EDR** – Forensics collection & automated reports, MITRE Mapping, and Threat Hunting **Sandboxing & CDR** – Threat Emulation and Threat Extraction & Sanitization **Data Protection** – Full Disk Encryption and Removable Media Encryption		
3	Автоматаар системийн шинэчлэлтийг хийж, аливаа программ хангамжийн аюулгүй байдлын цоорхойг зассан шинэчлэлт хийгдсэн эсэхийг баталгаажуулдаг байх		
4	Автоматаар системийн шинэчлэлтийг хийж, аливаа программ хангамжийн аюулгүй байдлын		

	цоорхойг зассан шинэчлэлт хийгдсэн эсэхийг баталгаажуулдаг байх		
5	Дэлгэрэнгүй тайлан гаргах болон системийн үйлдэл бүртгэх, сэрэмжлүүлэг илгээх чадвартай байх		
6	Бусад аюулгүй байдлыг хангах болон дэмжих программ хангамжтай харилцан холбогдож ажиллах чадвартай байх		
7	Программ хангамж нь төгсгөлийн цэгийн төхөөрөмжийн системийн нөөц болох CPU, санах ой, хадгалах диск дээр хамгийн бага ачаалал үзүүлдэг байх		
8	Гэрээний хугацаанд системийн шинэчлэлт болон техникийн туслалцаа тогтмол үзүүлэх		
9	Лицензийн ашиглалтын хугацаа 1 жил ба түүнээс дээш		

Барааны нэр: Сүлжээний галт хана төхөөрөмж (тоо ширхэг:1)

№	***Захиалагчийн техникийн тодорхойлолт*** *(Тухайн барааны үзүүлэлт тус бүрийг дор жагсааж бичих ба хэрвээ чанарын баталгаат хугацаа шаардах бол бичнэ үү.)*	***Санал болгож буй техникийн тодорхойлолт*** ***(****захиалагчийн техникийн тодорхойлолтыг хуулахгүй байхыг анхаарна уу. Зөвхөн санал болгож буй барааны техникийн тодорхойлолтыг бичнэ үү.****)***	***Тайлбар*** *(дээрх үзүүлэлтийг нотлох баримт бичиг болон танилцуулгыг хавсаргана)*
1	Firewall Throughput: 9 Gbps		
2	Next Gen Firewall Throughput: 3.72 Gbps		
3	Threat Prevention Throughput: 1.8 Gbps		
4	IPS Throughput: 4.65 Gbps		
5	Concurrent Session: 8 million		
6	Memory: 16 GB		
7	CPU: 4 cores		
8	Local Storage: SSD 240GB		
9	AC power supply: 2 ширхэг 100 to 240V (50-60Hz) тэжээлийн блоктой байна.		
10	NG Firewall төхөөрөмж нь дараах функцуудын агуулсан лицензтэй байна. Active/Standby and Clustering: Дэмждэг • IPsec VPN : Дэмждэг		

	• SSL VPN: Дэмждэг • IPS • Mobile access • Identity Awareness • Application Control • URL Filtering • Anti-virus • Anti-Bot • Anti-Spam • DNS Security • Content Awareness • Threat emulation • Threat Extraction • Zero Phishing • TAC Support		
11	Cluster redundancy нь: 93.6 Gbps хүртэл хүчин чадлаар траффик дамжуулах боломжтой 50-аас дээш төхөөрөмжүүдийг нэгтгэх хүчин чадал боломжийг агуулсан Gateway mix clustering буюу өөр өөр загвар модел хүчин чадалтай төхөөрөмжүүдийг хооронд нь Cluster үүсгэх боломжтой		
12	Үйлдвэрээс шууд нийлүүлсэн, лацтай, шинэ, ашиглалтын хугацаа 0 байх Лицензийн ашиглалтын хугацаа 1 жил ба түүнээс дээш		

Барааны нэр: Сүлжээний халдлагыг илрүүлэх, хариу үйлдэл үзүүлэх систем (тоо ширхэг:1)

№	***Захиалагчийн техникийн тодорхойлолт*** *(Тухайн барааны үзүүлэлт тус бүрийг дор жагсааж бичих ба хэрвээ чанарын баталгаат хугацаа шаардах бол бичнэ үү.)*	***Санал болгож буй техникийн тодорхойлолт*** *(захиалагчийн техникийн тодорхойлолтыг хуулахгүй байхыг анхаарна уу. Зөвхөн санал болгож буй барааны техникийн тодорхойлолтыг бичнэ үү.)*	***Тайлбар*** *(дээрх үзүүлэлтийг нотлох баримт бичиг болон танилцуулгыг хавсаргана)*
1	Санал болгож буй шийдэл нь клаудад суурилсан		
2	Сүлжээний галт хана, эцсийн цэгийн хамгаалалт болон бусад гуравдагч мэдрэгчийг дэмждэг байх		
3	Цуглуулж буй лог бүртгэлийг бодит цаг хугацаанд дамжуулах боломжтой байх		
4	Цуглуулж буй логуудыг хамгийн багадаа 3 сар хадгалах боломжтой байх		

5	Цуглуулсан лог дээр шүүлт хийх боломжтой байх		
6	Сүлжээний халдлагыг бууруулах, хариу үйлдэл үзүүлэхээр хиймэл оюун ухааныг ашиглан автоматаар болон гараар хариу үйлдэл үзүүлэх боломжтой байх		
7	30 хүртэлх сүлжээний төхөөрөмжийг холбож ажиллах лицензийг агуулсан IOC		
8	Халдлагад өртсөн сүлжээний төхөөрөмжийг хост дээр суулган, хэвийн байдалд шилжтэл сүлжээнээс тусгаарлах Threat remediation хийдэг		
9	Сүлжээнд илэрсэн халдлагын топологи, үйл ажиллагааны зураглал, эмзэг байдлын сонар, зан үйлийн аналитик болон ач холбогдол бүхий аюул заналхийллийг ML-д суурилан тодорхойлно.		
10	Хиймэл оюун ухааныг ашиглан халдлагын талаарх мэдээлэлд нэвтэрч, сэжигтэй IP хаяг, хостуудын талаар мэдээлэл өгөхөд ашиглах боломжтой халдлагыг шуурхай, үнэн зөв илрүүлэх боломжтой		
11	MITER ATT&CK системд суурилсан халдлагын иж бүрэн дүн шинжилгээ, халдлагыг зогсоохын тулд хортой програмын мэдээллийг агуулсан тайлан репортыг гаргадаг		
12	Автоматаар хариу үйлдэл үзүүлэх SOAR-ын функцыг агуулсан		
13	Лицензийн ашиглалтын хугацаа 1 жил ба түүнээс дээш		