БАТЛАВ. "Боловсролын мэдээллийн технологийн төв"
УТҮГ-ын Захирлын үүрэг гүйцэтгэгч

.....
Д.Бат-Эрдэнэ

БАРААНЫ ТЕХНИКИЙН ТОДОРХОЙЛОЛТ

№	Техникийн үзүүлэлт
1	Мэдээллийн аюулгүй байдлын лог удирдлага, хяналтын систем болон автомат хариу үйлдэл үзүүлэх систем SIEM\SOAR
3	Санал болгож буй шийдэл нь Gartner magic Quadrant тайланд тухайн чиглэлээрээ Leader ангилалд багтсан NextGne SIEM байна.
4	Үндсэн мэдээллийн аюулгүй байдлын лог удирдлага, хяналтын систем буюу SIEM/SOAR нь Perpertual лицензтэй байх.
5	Систем нь 500MPS хэмжээтэй лог дээр ажиллах боломжтой байх.
6	Шийдэл нь ON-PREMISE хэлбэрээр байгууллагын өөрийн сервер, дотоод дата төвд суурилуулж ашиглах боломжтой байх.
7	SIEM системийн үндсэн доорх модулиуд агуулагдсан байх. Үүнд: • Логийн удирдлага, хяналтын функцууд: All sources of network security information, e.g., servers, operating systems, firewalls, antivirus software and intrusion prevention systems are configured to feed event data into a SIEM tool. • Логийн шинжилгээний функцууд: (User and Entity Behavior Analytics, AI Engine) • Логийн мэдээллийн нэгдсэн сангийн модулиуд: (Threat Intelligence Service, Knowledge Base) • Кибер эрсдэлийн шинжилгээний функцууд: (Risk Based Threat Prioritization) • Нийцлийн тайлангууд: (Compliance Reports) • Дашбоардын модулиуд: (Centralized Dashboards and Visualization), • Бүтэцтэй болон бүтэцгүй хайлтын (Unstructured and Structured Search) системийн модулиудтай байх.
8	Кибер эрсдэл, аюул заналын эсрэг хариу арга хэмжээний автомат функц SOAR (Аюулгүй байдлын автоматжуулсан хариу үйлдэл) болох SmartResponse and Automation заавал агуулагдсан агуулагдсан байх ба доорх чадамжтай байна. Үүнд: a) Төхөөрөмжийг тусгаарлах (Endpoint quarantine): Сэжигтэй төхөөрөмж холбогдсон сүлжээний портыг тодорхойлж, тухайн порт эсвэл төхөөрөмжийн холболтыг идэвхгүй болгох замаар тусгаарлах. b) Хэрэглэгчийн эрхийг түр түдгэлзүүлэх (Suspend users): Хэрэглэгчийн бүртгэл халдлагад өртсөн гэж үзвэл SOC-ийн баг тухайн хэрэглэгчийг ямар төхөөрөмж ашиглаж байгаагаас үл хамааран системд хандах эрхийг нь зогсоох. c) Төхөөрөмжийн өгөгдөл цуглуулах (Collect machine data): Хортой программ хангамжийн шинжилгээний явцад сэжигтэй төхөөрөмжөөс шүүх шинжилгээний (forensic) өгөгдлийг цуглуулах. d) Сүлжээний хандалтыг зогсоох (Suspend network access): Мэдээлэл гадагш алдагдаж буй тохиолдолд галт ханын (firewall) хандалтын хяналтын жагсаалтыг (ACL) шуурхай шинэчлэх замаар сүлжээний холболтыг хаах.

	e) Процессыг зогсоох (Kill processes): Чухал төхөөрөмжүүд дээр ажиллаж буй үл мэдэгдэх эсвэл хар жагсаалтад орсон процессыг автомат хариу үйлдлээр шууд зогсоох.
9	Аюулгүй байдлын шинжилгээний гол модулиудыг (Case Management, Case Playbooks, Case Metrics, Contextualization) агуулагдсан байх.
10	Санал болгож буй SIEM шийдэл нь стандарт протокол, API болон agent-based механизмаар дамжуулан олон төрлийн гуравдагч системүүдтэй өргөтгөх боломжтойгоор интеграци хийх чадамжтай байх. SIEM шийдэл нь дараах интеграцийн механизмуудыг **native** (системд суурилагдсан хэлбэр) **байдлаар** дэмждэг байх: • **Syslog (TCP/UDP, RFC 5424/3164)** • **RESTful API (JSON/XML)** • **Agent-based лог цуглуулалт** • **File-based болон database connector** • **SNMP Trap / Polling (шаардлагатай тохиолдолд)**
11	Standard Maintenance and Support Services (Арчилгаа үйлчилгээ болон техникийн дэмжлэгийн стандарт нөхцөл) нь 1 жил байх ба доорх хугацаанд нийлүүлсэн SIEM программ хангамжийн системүүдэд стандарт 11x5 нөхцөлөөр үйлдвэрлэгчийн зүгээс техникийн туслалцаа үзүүлэх багц үйлчилгээтэй байх. SIEM систем дээр үүссэн асуудлууд болон программын шинэчлэлтүүд багтсан байх.
12	Санал болгож буй үйлдвэрлэгчийн албан ёсны сертификаттай цахим сургалтад Захиалагчийн 2 мэргэжилтнийг тендерийн төсөвт өртөгт багтсан зардлаар хамруулах.
13	Нийлүүлэгч байгууллагын инженер, техникийн ажилчдын хувь Certified Ethical Hacker /3 хүн/ сертификаттай байх ба нийт инженерийн хувьд 4 болон түүнээс дээш тооны мэргэжилтэнтэй байна. /сертификатыг нотариатаар баталгаажуулан ирүүлнэ/.
19	Монгол улс дах албан ёсны борлуулагч байх.

ХЯНАСАН:
"ЭРДЭМНЭТ" СҮЛЖЭЭНИЙ ХЭЛТСИЙН ДАРГА — Ж.ГОМБОДОРЖ

БОЛОВСРУУЛСАН:
"ЭРДЭМНЭТ" СҮЛЖЭЭНИЙ ХЭЛТСИЙН МАБ-ЫН МЭРГЭЖИЛТЭН — Б.СУГАР-ЭРДЭНЭ

БАТЛАВ. "Боловсролын мэдээллийн технологийн төв"
УТҮГ-ын Захирлын үүрэг гүйцэтгэгч

.....
Д.Бат-Эрдэнэ

	БАРААНЫ ТЕХНИКИЙН ТОДОРХОЙЛОЛТ
№	Техникийн үзүүлэлт
1	**Хэрэглэгчийн хандах эрхийн удирдлагын систем - CyberArk PAM system-тэй дүйцэх**
1	Нийт лицензийн тоо: 10 хэрэглэгчийнх байх ба хандах төхөөрөмж, датабааз, серверийн хувьд хязгааргүй байх Лицензийн хугацаа: 1 жил
2	Санал болгож буй шийдэл нь Gartner судалгааны байгууллагын үнэлгээг тасралтгүй 7 ба түүнээс дээш жил Тэргүүлэгч ангилалд багтдаг байх, нотлох зураг, эсвэл линкийг хавсаргах
3	Санал болгож буй систем нь on-premise суурилуулах боломжтой байх
4	Тавигдах ерөнхий шаардлага: - Санал болгож буй шийдэл нь системийн болон аппликейшний эрх бүхий нууц үг болон сессийг үр дүнтэй хамгаалж, удирдах боломжтой байх - Нууц үгийн удирдлага болон сессийн бүртгэлийн хувьд, санал болгож буй удирдлагатай төхөөрөмжийн тоонд үндэслэн нууц үгийн объектод хязгааргүй дэмжлэг үзүүлнэ. - Санал болгож буй шийдэл нь системийн хэвийн байдлыг тогтмол хянах healtcheck хяналтын чадвартай байх ёстой. Энэ нь нийт системийн гүйцэтгэл, хэвийн байдал болон тусдаа бүрэлдэхүүн хэсгүүдийн нарийвчилсан мэдээлэл үзэх боломжтой хянах самбар дээр харагдах ёстой. - Шийдэл нь шууд ашиглах боломжтой нэгдсэн SSO болон дасан зохицох MFA хяналтууд, дотоод хэрэглэгчдэд зориулсан аюулгүй алсын хандалт, сул холбогдсон төхөөрөмжүүдийг (LCD) удирдах чадвар, бизнесийн хэрэглэгчдэд зориулсан нууц үг удирдах чадвар, аюул заналын дүн шинжилгээний чадвар, хадгалагдсан эрхүүд эсвэл шууд эрхгүй (ZSP) ашиглан дэд бүтцийн аюулгүй хандалт болон байгууллагын аюулгүй хөтөч хэрэгслийг нэмэлт төлбөргүйгээр хангасан байх ёстой - Санал болгож буй шийдэл нь хэрэглэгчийн эрхүүдийг удирдах, байгууллагын нөөцөд хандах эрхийг удирдах, хандалтын эрхүүдийг автоматаар эргүүлэх, хандалтын сессүүдийг бүртгэх, хэрэглэгчийн үйл ажиллагааг хянах чадвартай нэгдсэн нэг платформ дээр бүтээгдсэн байх ёстой. - Санал болгож буй шийдэл нь эрх бүхий хэрэглэгчид HTTPS протоколоор зорилтот машинуудтай холбогдох үед VPN бус, агентгүй аргыг ашигладаг аюулгүй алсын хандалтын чадварыг ашиглах ёстой
5	**Санал болгож буй шийдлийн дэмжин ажиллах платформ, үйлдлийн системийн хувьд доорх байна.** - Windows (local and domain) - Linux - Solaris

	- Databases (Session management and recording through preferred database client. please indicate the supported clients) - Network Devices via SSH and Telnet - Virtual Servers (e.g. VMware, Oracle VM, etc) - Client Server Based Applications i.e. SAP, Checkpoint Smart Dashboard etc. - Support any SSH devices - Support any ODBC devices - Support AWS console access keys credentials for its AWS IAM accounts - Support loosely connected devices (roaming Windows machines)
6	Санал болгож буй шийдэл нь Active Directory, Linux/Unix орчинд болон SSH түлхүүрүүдийг энгийн бөгөөд ойлгомжтой вэб суурьтай визардыг ашиглан автоматаар илрүүлж, үр дүнг хянасны дараа эдгээр аккаунтуудыг нууц үг удирдах зорилгоор автоматаар тохируулах боломжийг олгоно.
7	Санал болгож буй шийдэл нь шинээр илэрсэн аккаунтуудыг шууд автоматаар бүртгэхийн тулд урьдчилан тодорхойлсон аккаунт бүртгэх дүрмийг үүсгэх, удирдах боломжийг олгоно.
8	Санал болгож буй шийдэл нь бодлого болон нууц үгийн аюулгүй хадгалах сангуудаар зохион байгуулагдсан зорилтот дансуудыг дэмжих ёстой
	Санал болгож буй шийдлийн систем архитектур хувьд: - Санал болгож буй шийдэл нь өгөгдлийн сан болон програм нь тусдаа байх олон давхаргат архитектурыг хангана. - Санал болгож буй шийдэл нь техник хангамжаар хязгаарлагдахгүй өргөтгөх боломжийг хангана. Мөн шийдэл нь хүчин чадлын төлөвлөлт болон өргөтгөх боломжийн хэмжигдэхүүнийг модулчлагдсан загвараар хангана. - Санал болгож буй шийдэл нь өөр өөр сүлжээний сегментүүд эсвэл байршилд байрлуулсан ч өндөр нөөцлөлт эсвэл гамшгийн сэргээх архитектурыг дэмжин ажилладаг байна. - Өөр өөр сүлжээний сегментүүдийн хооронд өгөгдөл хуулбарлах нь гадны шийдэл эсвэл дэд бүтцийн хэрэгцээгүйгээр шууд гүйцэтгэгдэнэ
9	**Санал болгож буй шийдлийн Disaster recovery хувьд:** - Санал болгож буй шийдэл нь өөр өөр Дата төвийн байршилд байрлах алслагдсан гамшгийн сэргээх байгууламжуудад multiple mirror системүүдийг дэмжих чадвартай байна. - Санал болгож буй шийдэл нь ямар нэгэн эвдрэл гарсан тохиолдолд хялбар сэргээх боломжтой байх ба гамшгийн сэргээлтийг өдөр тутмын үйл ажиллагаанд хамгийн бага саад учруулан аль болох жигд гүйцэтгэнэ.
10	**Санал болгож буй шийдлийн сүлжээний архитектур хувьд:** - Санал болгож буй шийдэл нь төвлөрсөн нууц үг удирдах шийдэлтэй холбоо тасрах тохиолдолд автоматаар зохицуулна. - Санал болгож буй шийдэл нь бүх давуу эрхтэй сессийг шийдлээр хянахын тулд сүлжээний топологийн өөрчлөлт шаардахгүй байх ёстой. - Төрөл бүрийн сегментүүдийг төвлөрсөн байршлаас дэмжих шаардлагатай тархсан сүлжээний архитектурыг дэмжин ажиллах боломжтой байх ёстой.
11	**Санал болгож буй шийдлийн сүлжээний архитектур хувьд:** - Санал болгож буй шийдэл нь бүх өгөгдөл шифрлэлтэд зориулж FIPS 140-2 баталгаажсан суурилуулсан криптографийг ашиглах ёстой.

	- Санал болгож буй шийдэл нь хамгийн багадаа Common Criteria Evaluation Assurance Level EAL 2+ байх ёстой. - Системийн бүрэлдэхүүн хэсгүүдийн хоорондын харилцаа, түүний дотор нэг сервер дээр байрлах бүрэлдэхүүн хэсгүүд шифрлэгдсэн байх ёстой - Санал болгож буй шийдэл нь нөөц түлхүүрүүд системийг өөрөө удирдаж, аюулгүй хадгалах бүрэн шифрлэгдсэн нөөцлөлтийг хангана. - Аюулгүй платформ - үндсэн нууц үг хадгалах сан нь өндөр аюулгүй байх ёстой - Аудитын бүртгэл, бодлого, эрх, давуу эрхтэй итгэмжлэл, бичлэг гэх мэт зүйлсийг аюулгүй, өөрчлөлтөөс хамгаалсан байдлаар хадгалах ёстой. - Шийдэл дэх нууц үгийн аюулгүй санд хадгалагдсан нууц үгийн сав болон нууц үгийн объект бүр өвөрмөц шифрлэлтийн түлхүүрээр шифрлэгдсэн байх ёстой - Нийтлэг итгэмжлэлийн хулгайг бууруулахын тулд хэрэглэгчид болон администраторуудын нэвтрэлтийн бүрэн бүтэн байдлыг хангахын тулд олон хүчин зүйлийн баталгаажуулалтыг ашиглана. - Хэрэглэгчийг үүргээр салгах нь - Администратор хэрэглэгч болон бусад баг/ажлын бүлгүүдийн (UNIX, Oracle гэх мэт) хяналтанд байдаг өгөгдлийг (нууц үг) үзэх боломжгүй болгон үүргэр хуваарилах - Хэрэв гадны танигдах сангууд ашиглагдаж байгаа бол санал болгож буй шийдэл нь синхрончлолыг хангахын тулд тохируулга хийх ёстой. Жишээлбэл, хэрэглэгчийг лавлахаас нэмэх/хасах үед энэ нь автоматаар шийдэлд тохируулагдана/тохируулагдахгүй.
12	**Санал болгож буй шийдлийн PRIVILEGED ACCOUNT MANAGEMENT хувьд:** - Санал болгож буй шийдэл нь давуу эрхтэй аккаунтууд хаана байгааг илрүүлэх, давуу эрхтэй аккаунтуудын эрсдэлийг шалгах, бүх давуу эрхтэй нууц үг/SSH түлхүүр/нууц үгийн хаш, мөн AWS дахь Cloud хэрэглэгчид/инстанцын түлхүүрүүдийг тодорхойлох хэрэгслийг санал болгох нь зүйтэй. - Санал болгож буй шийдэл нь бодлогын удирдлагын хялбар байдлыг хангана, үүнд: ▪ а) Бүх систем, програм болон төхөөрөмжүүдэд нэг суурь аюулгүй байдлын бодлогыг зөвшөөрөх (жишээ нь, суурь бодлогыг хэрэгжүүлэхийн тулд нэг шинэчлэлт хийх). ▪ б) Сонгогдсон систем, програм болон төхөөрөмжүүдэд онцгой бодлого үүсгэх чадвар. - Санал болгож буй шийдэл нь параметрээр удирдагддаг нууц үг өөрчлөх сонголтуудыг гүйцэтгэнэ: ▪ а) Нэг мастер бодлогыг ашиглан өдөр, сар, жил бүр нууц үгийн сонголтууд болон нийцлийн сонголтуудыг тохируулах чадвар. ▪ б) Тодорхой шалгуурын дагуу нэг, бүлэг болон бүх системийн нууц үгийг нэг дор өөрчлөх чадвар. ▪ с) Бүтээгдэхүүн нь нэг мастер бодлогоор дамжуулан нууц үг эсвэл нууц үгийн бүлгийг өөрчлөхийг дэмжих ёстой: i) Бодлогын дагуу, ii) Хэрэглэгч гараар, iii) Нууц үг синхрончлогдоогүй үед автоматаар ▪ d) Санал болгож буй шийдэл нь зорилтот аккаунтуудын нууц үгийг санамсаргүй утгад тохируулах ёстой. i) Администратор

хэзээ ч зорилтот аккаунтуудын нууц үгийг гараар өөрчлөх чадвар. ii) Тодорхой хугацааны дараа автоматаар "гарах" болон тодорхой хугацаанд "орох" чадвар.

- Санал болгож буй шийдэл нь нууц үгийн баталгаажуулалтыг дэмжинэ
    - а) Нууц үгийн уттыг зорилтот системтэй нь автоматаар баталгаажуулах.
    - б) "Синхрончлогдоогүй" нууц үгэнд автоматаар мэдэгдэх
    - в) Бүх "синхрончлогдоогүй" нууц үгийн талаар тайлагнах.
- Санал болгож буй шийдэл нь нууц үгийн тохируулгыг дэмжинэ.
    - а) Гадны сэргээх хэрэгслүүдийг ашиглахгүйгээр "синхрончлогдоогүй" эсвэл алдагдсан гэж илэрсэн нууц үгийг автоматаар тохируулах.
    - б) Сонгогдсон, олон эсвэл бүх систем дээр нууц үгийг тохируулах чадвар.
    - в) Сонгогдсон, олон эсвэл бүх систем дээр нууц үгийг тохируулах чадвар.
- Санал болгож буй шийдэл нь нууц үгийн бодлогыг дэмжинэ.
    - а) Бүх системийн супер хэрэглэгчийн аккаунтуудад нэг мастер бодлогоор нууц үгийн хамгийн бага урт болон нарийн төвөгтэй байдлыг тохируулах чадвар.
    - б) Нууц үгийн түүхийг хадгалах чадвар, жишээлбэл, сүүлийн гурван нууц үг эсвэл хугацаагаар болон бүтээгдэхүүний вэб интерфэйсээр дамжуулан тэдэнд хялбар хандах боломжийг олгоно.
    - в) Аккаунтуудыг гараар өөрчлөх үед болон систем санамсаргүйгээр нууц үгийг өөрчлөх үед нууц үгийн бодлогыг хэрэгжүүлэх чадвар
    - г) Сүүлийн х өвөрмөц нууц үгийг хэрэгжүүлэх чадвар (өөрөөр хэлбэл, сүүлийн х нууц үгийг давтахгүй).
- Санал болгож буй шийдэл нь дараах нууц үг шалгах процессыг агуулна.
    - а) Нэг удаагийн нууц үгийг нэмэлт ажлын урсгал болгон үүсгэх чадвар.
    - б) Аливаа үйл ажиллагаагаар өдөөгдсөн имэйл эсвэл бусад хүргэх аргаар мэдэгдэл илгээх чадвар.
    - в) Тодорхой хугацааны турш нууц үгийг шалгах чадвар, жишээлбэл, цаг ба/эсвэл өдөр.
    - г) Нууц үг хүссэн хэрэглэгчид шалгалт дуусан тухай имэйлээр мэдэгдэл илгээх чадвар.
- Санал болгож буй шийдэл нь зорилтот системүүдтэй холбогдох боломжтой байна.
    - а) Холболтын нэг хэсэг болгон нууц үгийг харахгүй эсвэл бичихгүйгээр зорилтот төхөөрөмжтэй ил тод холболтыг дэмжинэ.
    - б) Windows удирддаг төхөөрөмжүүдтэй шууд холболтыг дэмжих чадварыг хангана.
    - в) Unix/Linux удирддаг төхөөрөмжүүдтэй (SSH) шууд холболтыг дэмжих чадварыг хангана.
    - г) Шууд дэмжигдээгүй нэмэлт зорилтот системүүдэд зориулсан динамик дэмжлэг.

	- Санал болгож буй шийдэл нь IPv6-аар тохируулагдсан Windows, UNIX болон өгөгдлийн сангууд дээрх давуу эрхтэй аккаунтуудын удирдлагыг дэмжинэ. - Санал болгож буй шийдэл нь UNIX/Linux хэрэглэгчдэд баталгаажуулалт болон тохируулга хийх, мөн эдгээр системүүдэд хандалтыг төвлөрсөн байдлаар хянахын тулд Active Directory (AD) Bridge чадварыг дэмжинэ. - AD Bridge чадварын дэмжлэг нь агентгүй байх ёстой. - Санал болгож буй шийдэл нь вэбтэй холбоотой программ холбогдох боломжийг олгохын тулд вэб плагинуудыг тохируулах уян хатан байдлыг хангах боломжтой байх ёстой.
13	**Санал болгож буй шийдэл нь PRIVILEGED ACTIVITY MONITOR & RECORDING тухайд** - Санал болгож буй шийдэл нь 2.0 ПЛАТФОРМ/ЗОРИЛТОТ СИСТЕМИЙН ДЭМЖЛЭГ/ҮЙЛДЛИЙН СИСТЕМ хэсэгт заасан давуу эрхтэй сессийг шууд бичих боломжтой байх ёстой. - Санал болгож буй шийдэл нь давуу эрхтэй нэг удаагийн нэвтрэлтийг хянах болон идэвхжүүлэх вэб програмуудыг оруулан аливаа програм эсвэл төхөөрөмжийн холболтыг дэмжихээр өргөжүүлэх боломжтой байна. - Санал болгож буй шийдэл нь бүх платформууд дээр бичлэгийн хайлтын чадварыг зөвшөөрөхийн тулд зорилтот системүүд дээр ямар нэгэн төрлийн агент байрлуулах шаардлагагүй. - Санал болгож буй шийдэл нь бүх платформууд дээр шууд бичээд хайхад олох боломжтой бичлэгийн чадвартай байна. - Санал болгож буй шийдэл нь түлхүүр үг, цаг, хэрэглэгчид болон зорилтот хаягаар текст болон Windows дээр суурилсан бичлэгийг хоёуланг нь хайх чадвартай байна. - Санал болгож буй шийдэл нь бичлэгийн эхнээс эхлэн тоглуулахын оронд текст болон Windows дээр суурилсан бичлэгийн хувьд хайсан түлхүүр үгийн цаг хугацааны цэгээс бичлэгийг хянах боломжийг олгоно. - Санал болгож буй шийдэл нь сессийг шууд хянах, шаардлагатай үед сессийг гараар зогсоох боломжийг хангана. - Санал болгож буй шийдэл нь зорилтот системд суулгасан агент шаардлагагүйгээр SSH сессүүдэд SSH командыг цагаан болон хар жагсаалтад оруулах боломжийг олгоно. - Санал болгож буй шийдэл нь RDP холболтод тодорхой командуудыг гүйцэтгэх боломжийг олгоно (жишээ нь, desktop эсвэл бусад гүйцэтгэх файлуудыг ил гаргахгүйгээр зорилтот машинд зориулалтын програм ажиллуулж холболтыг эхлүүлэх). - Байгуулагдсан сесс нь шууд дамжуулалтаар/шууд хяналтын нөхцөлд алсаас харах функцтэй байна. - Аудитор/сесс хянагчид байгуулагдсан сессийг алсаас терминал хийх чадвартай байна.

	- Санал болгож буй шийдэл нь хэрэглэгчид өөрсдийн уугуул SSH болон RDP клиентаар дамжуулан гарцаар дамжуулан зорилтот Unix болон Windows серверүүдэд нэвтрэх уугуул туршлагыг хангах өөр аргуудыг хангана. - Санал болгож буй шийдэл нь хэрэглэгчийн үйлдлийн системийн платформ эсвэл хөтөчөөс үүсч болох хязгаарлалтыг арилгахын тулд HTML 5 дээр суурилсан прокси гэх мэт өөр холболтын аргуудыг хангана. - Санал болгож буй шийдэл нь аудитор болон аюулгүй байдлын багуудаар давуу эрхтэй сессүүдийн хяналтыг эрсдэлд суурилсан тэргүүлэх чиглэлээр хийх боломжтой байх ёстой.
14	**Санал болгож буй шийдлийн СИСТЕМИЙН УДИРДЛАГА хувьд:** - Нэгдсэн багц доторх төвлөрсөн удирдлага (нэг хэрэглэгчийн интерфэйс, төвлөрсөн сан). - Санал болгож буй шийдэл нь хөтөч байхгүй тохиолдолд клиент дээр суурилсан болон хөтөч дээр суурилсан удирдлагыг хоёуланг нь дэмжинэ. - Хэрэв back-end өгөгдлийн сан ашиглаж байгаа бол шийдэл нь бүрэн өөрөө удирдагддаг байх ёстой бөгөөд үйлдвэрлэлийн байршуулалт, нөөцлөлт/сэргээлт эсвэл өгөгдлийн сангийн хатууруулалтад өгөгдлийн сангийн администратор (DBA) шаардлагагүй байх ёстой. - Санал болгож буй шийдэл нь шийдлийн администраторуудыг нууц үгэнд хандах эсвэл үзэх эсвэл нууц үгийн хүсэлтийг батлахаас хязгаарлах ёстой. - Үүрэгт суурилсан хандалтын хяналтад зориулж AD бүлгүүд эсвэл LDAP лавлах ашиглан ил тод бүлэг/үүргийн удирдлага. - Санал болгож буй шийдэл нь аккаунтууд дээр гүйцэтгэсэн бөөн үйлдлүүдийг дэмжих ёстой. - Logrhythm, IBM QRadar, Splunk зэрэг SIEM системүүдтэй нэгтгэх чадвартай байх ёстой байх
15	**Санал болгож буй шийдлийн СИСТЕМИЙН УДИРДЛАГА хувьд:** - Хос хяналтыг дэмжих чадвар - Систем нь нууц үг авахыг оролдох үед "4 нүдний зарчим" гэх мэт баталгаажуулалтын өөр тохиргоог автомат имэйл мэдэгдлийн дэмжлэгийг оруулан дэмжих ёстой. - Санал болгож буй шийдэл нь хэрэглэгчийн ирээдүйн өдөр/цагт зорилтот аккаунт ашиглах хүсэлтийг дэмжинэ. - Бүтээгдэхүүн эсвэл загварт үндэслэн олон түвшний батлагчдыг томилох уян хатан ажлын урсгалын баталгаажуулалтын процессыг дэмжинэ (өөрөөр хэлбэл, хандалт зөвшөөрөгдөхөөс өмнө 2 ба түүнээс дээш баталгаа шаардана). - Эцсийн баталгаа олгогдохоос өмнө батлагчид дараалаар байх шаардлагатай ажлын урсгалын баталгаажуулалтын процессыг дэмжинэ. - LDAP серверийн мэдээлэлд үндэслэн хүсэлт гаргагчийн шууд менежер л хүсэлтийг батлах боломжтой ажлын урсгалын баталгаажуулалтын процессыг дэмжинэ. - Ажлын урсгалын процессуудыг бүртгэх болон/эсвэл тайлагнах эсвэл аудит хийх чадвартай байх.

16	**Санал болгож буй шийдлийн ДАВУУ ЭРХТЭЙ АККАУНТЫН ЭРСДЛИЙН ШИНЖИЛГЭЭ хувьд** - Сэжигтэй болон хортой давуу эрхтэй хэрэглэгчийн зан үйлийг тодорхойлохын тулд оюун ухаанд суурилсан шинжилгээг хийх чадвартай байх. - Давуу эрхтэй аккаунтуудаас үүдэлтэй сэжигтэй үйл ажиллагааг илрүүлж, үргэлжилж буй халдлагуудад идэвхтэй хариу өгөх чадвартай байх. - Шийдэл нь санал болгож буй нууц үгийн удирдлагын шийдэл, удирддаг UNIX, Windows машинууд болон Oracle өгөгдлийн сангуудаас түүхий үйл явдлуудыг хүлээн авах боломжтой байх ёстой; аюулгүй байдлын үйл явдлыг бодит цагтай ойролцоо барьж, холбогдох анхааруулгуудтай хяналтын самбар дээр харуулах ёстой.
17	**Санал болгож буй шийдэл нь нэмэлтээр дараах чадвартай байх ёстой** - Зөвшөөрөгдсөн хэрэглэгчид болон удирддаг аккаунтууд дээрх аюулгүй байдлын үйл явдлуудыг илрүүлэх - Давамгай давуу эрхтэй хэрэглэгчийн үйл ажиллагаа / удирддаг давуу эрхтэй аккаунтууд дээрх аюулгүй байдлын үйл явдлуудыг илрүүлэх чадвартай байх. - Тэмдэглэгдсэн аюулгүй байдлын үйл явдлуудад хариу өгөх - Хурдан үйл явдлын сөрөг нөлөөг бууруулахад дэмжлэг үзүүлэх боломжтой ойлголтуудыг гаргах чадвартай байх. - Тэмдэглэгдсэн нийт аюулгүй байдлын үйл явдлуудад үндэслэн нийт эрсдэлийн оноог тодорхойлно - Үргэлжилж буй аюул эсвэл халдлагыг илтгэх системийн нийт аюулын индексийг тооцоолно. - Үргэлжилж буй давуу эрхтэй сессийн үеэр зөвшөөрөгдөөгүй командуудыг гүйцэтгэх үед аюулгүй байдлын үйл явдлуудад нэн даруй хариу өгөх чадвар. - Аудиторуудад эрсдэлийн онооны үнэлгээнд үндэслэн давуу эрхтэй сессийн видео бичлэгийг хянах тэргүүлэх чиглэлийг тогтооход туслах. - Санал болгож буй шийдэл нь өндөр эрсдэлтэй үйл ажиллагаанд хариу өгөхийг тодорхойлох боломжтой байх ёстой. Тохируулах үйл ажиллагаанууд нь: ▪ Итгэмжлэлийн хулгайн үйл явдлын хувьд ашигласан итгэмжлэлийг нэн даруй эргүүлэх замаар автоматаар засах. ▪ Эрсдэлтэй давуу эрхтэй сессийг зогсоох замаар автоматаар засах. ▪ Эрсдэлтэй давуу эрхтэй сессийг түр зогсоох замаар автоматаар засах. ▪ Тодорхой тодорхойлсон хүрээнд үндэслэн өндөр эрсдэлтэй командуудыг нарийвчилсан байдлаар томилохыг зөвшөөрөх.

ХЯНАСАН:

"ЭРДЭМНЭТ" СҮЛЖЭЭНИЙ ХЭЛТСИЙН ДАРГА — Ж.ГОМБОДОРЖ

БОЛОВСРУУЛСАН:
"ЭРДЭМНЭТ" СҮЛЖЭЭНИЙ ХЭЛТСИЙН МАБ-ЫН МЭРГЭЖИЛТЭН — Б.СУГАР-ЭРДЭНЭ

БАТЛАВ. "Боловсролын мэдээллийн технологийн төв"
УТҮГ-ын Захирлын үүрэг гүйцэтгэгч

.....
Д.Бат-Эрдэнэ

БАРААНЫ ТЕХНИКИЙН ТОДОРХОЙЛОЛТ

№	Техникийн үзүүлэлт
1	Нэр: Эмзэг байдлын шинжилгээний систем (Vulnerability Assessment System)
2	Нийлүүлэх систем нь байгууллагын мэдээллийн систем, сервер, сүлжээний төхөөрөмж болон программ хангамжид илэрч болзошгүй аюулгүй байдлын эмзэг байдлыг илрүүлэх, үнэлэх, тайлагнах зориулалттай Vulnerability Assessment (Эмзэг байдлын шинжилгээ) систем байна.
3	Санал болгож буй шийдэл нь Tenable Nessus Professional системтэй эсхүл түүнтэй дүйцэх буюу түүнээс дээш түвшний шийдэл байна.
4	Лицензийн нөхцөл: - Лицензийн төрөл: Professional - Лицензийн хугацаа: 1 жил - Шалгах боломжтой IP хаягийн тоо: хамгийн багадаа 256 IP хаяг
5	Санал болгож буй шийдэл нь Gartner Magic Quadrant тайланд Vulnerability Assessment (Эмзэг байдлын шинжилгээ) чиглэлээр Leader (Тэргүүлэгч) ангилалд багтсан үйлдвэрлэгчийн шийдэл байна.
6	Шийдэл нь байгууллагын дотоод сүлжээн болон дэд бүтцэд (on-premise) суурилуулах боломжтой байх.
7	Үндсэн функцийн шаардлага: - Санал болгож буй шийдэл нь дараах үндсэн боломжуудтай байна. - Сүлжээ, сервер, үйлдлийн систем, программ хангамжийн эмзэг байдлыг автоматаар илрүүлэх - CVE (Common Vulnerabilities and Exposures) /Түгээмэл эмзэг байдал болон өртөмтгий байдлын бүртгэл/ мэдээллийн санг ашиглан эмзэг байдлын шинжилгээ хийх - Эмзэг байдлын эрсдэлийг CVSS (Common Vulnerability Scoring System) /Эмзэг байдлыг үнэлэх нийтлэг систем/ стандартаар үнэлэх - Илэрсэн эмзэг байдлын тайлан, зөвлөмж гаргах - Шинжилгээний үр дүнг dashboard болон график тайлангаар харуулах
8	Санал болгож буй шийдэл нь дараах платформуудыг дэмжинэ. Үүнд: - Виндоус үйлдлийн систем - Линукс үйлдлийн систем - macOS - Виртуалчлалын орчин (VMware, Hyper-V гэх мэт) - Сүлжээний төхөөрөмжүүд (router, switch, firewall) - Өгөгдлийн сангийн системүүд (Oracle, MySQL, SQL Server гэх мэт) - Вэб програм хангамж (Web Application) серверүүд
9	Vulnerability Scanning боломж Шийдэл нь дараах хайлт буюу scan хийх боломжуудтай байна. Үүнд: - Network vulnerability scanning (Сүлжээний эмзэг байдлын илрүүлэлт)

	- Web application vulnerability scanning (Вэб программ хангамжийн эмзэг байдлын илрүүлэлт) - Configuration auditing (Тохиргооны аудит / хяналт) - Compliance auditing (Нийцлийн аудит / хяналт) - Credentialed scanning (Хэрэглэгчийн эрхтэйгээр хийх илрүүлэлт) - Agent-based scanning (Агент програмд суурилсан илрүүлэлт)
10	Санал болгож буй шийдэл нь Plugin (нэмэлт) ба мэдээллийн сангийн хувьд дараах боломжуудтай байна. Үүнд: - Эмзэг байдлын plugin (нэмэлт) мэдээллийн санг тогтмол шинэчлэх - Шинэ CVE (Түгээмэл эмзэг байдал болон өртөмтгий байдлын бүртгэл) эмзэг байдлыг хурдан илрүүлэх - Plugin update-ийг автоматаар татах (Нэмэлт өгөгдлийн сангийн (plugin) шинэчлэлтийг автоматаар татаж, суулгах)
11	Шийдэл нь дараах тайлан болон мониторингийн боломжуудтай байна. Үүнд: - Executive summary тайлан (Удирдлагын түвшний хураангуй тайлан) - Technical vulnerability тайлан (Техникийн эмзэг байдлын дэлгэрэнгүй тайлан) - Compliance тайлан (Стандарт, нийцлийн тайлан) - PDF, CSV, HTML форматаар тайлан гаргах - Эмзэг байдлын risk prioritization (Илэрсэн эмзэг байдлуудыг эрсдэлийн түвшнээр эрэмбэлэх (Risk prioritization)
12	Санал болгож буй шийдэл нь дараах системүүдтэй интеграци хийх боломжтой байна. - SIEM (Аюулгүй байдлын мэдээлэл болон үйл явдлын удирдлага) системүүд (Splunk, IBM QRadar, LogRhythm) - Гэмтэл, дуудлага бүртгэлийн системүүд (ServiceNow, Jira гэх мэт) - Хөрөнгийн бүртгэл, удирдлагын системүүд
13	Санал болгож буй шийдэл нь дараах аюулгүй байдлын шаардлагатай байна. Үүнд: - HTTPS протокол ашиглан шифрлэгдсэн холболт - Role-based access control (RBAC) (Дүрмийн санд суурилсан хандалтын хяналт) - Аудит лог бүртгэл - Хэрэглэгчийн эрхийн удирдлага
14	Системийн удирдлагын шийдэл нь: - Web-based management console (Вэб технологид суурилсан удирдлагын консол) - Scan хийх schedule тохируулах (Эмзэг байдлын илрүүлэлтийн хуваарь) - Олон төрлийн scan policy (Илрүүлэлтийн олон төрлийн бодлого) үүсгэх - Хайлт буюу шалгалтын үр дүнг төвлөрсөн удирдлага байдлаар удирдах.
15	Систем нь дараах тайлан гаргах боломжтой байна. Үүнд: - Эмзэг байдлын эрсдэлийн үнэлгээ - Аюулгүй байдлын аудитын тайлан - Compliance (Нийцлийн) стандартуудтай нийцэх

Хянасан: "Эрдэмнэт" сүлжээний хэлтсийн дарга Ж.ГОМБОДОРЖ

Боловсруулсан:
"Эрдэмнэт" сүлжээний
хэлтсийн МАБ-ын мэргэжилтэн Б.СУГАР-ЭРДЭНЭ

БАТЛАВ. "Боловсролын мэдээллийн технологийн төв"
УТҮГ-ын Захирлын үүрэг гүйцэтгэгч

.....
Д.Бат-Эрдэнэ

БАРААНЫ ТЕХНИКИЙН ТОДОРХОЙЛОЛТ
Техникийн үзүүлэлт
Өгөгдөл шинжилгээ, тайлан боловсруулах программ – Tableau систем эсхүл түүнтэй дүйцэх
Нийт лицензийн тоо: 5 Creator эрх 10 Viewer эрх байх. Лицензийн хугацаа: 1 жил
Байгууллагын өгөгдөлд дүн шинжилгээ хийх, тайлан дашбоард боловсруулах, түүнийг дотоод сүлжээнд (On-Premise) аюулгүйгээр байршуулж, хэрэглэгчдэд түгээх зориулалттай иж бүрэн программ хангамж.
Тавигдах ерөнхий шаардлага: - Программ хангамж нь Өгөгдөл боловсруулах (Desktop), Өгөгдөл бэлтгэх (Data Prep), Тайлан байршуулах төв сервер (Server) гэсэн хэсгүүдээс бүрдэнэ. - (Creator) эрх: 5 ширхэг. (Өгөгдөл холбох, анализ хийх, тайлан угсрах, серверт нийтлэх бүрэн эрхтэй хэрэглэгч) - (Viewer) эрх: 10 ширхэг. (Серверт нийтлэгдсэн бэлэн тайланг харах, шүүлтүүр ашиглах, өгөгдөл татаж авах хязгаарлагдмал эрхтэй хэрэглэгч) Шийдэл нь шууд ашиглах боломжтой нэгдсэн SSO (Нэгдсэн нэвтрэх систем) болон дасан зохицох MFA (Дасан зохицох олон шалтгаант баталгаажуулалт) хяналтууд, дотоод хэрэглэгчдэд зориулсан - Хамгийн сүүлийн үеийн албан ёсны хувилбар байх. **Өгөгдөлтэй холбогдох болон Нэгтгэх чадвар** - Систем нь байгууллагын олон төрлийн өгөгдлийн сангуудтай шууд болон шууд бусаар холбогдож ажиллах чадвартай байх шаардлагатай. - Өгөгдлийн сангууд: Уламжлалт (Microsoft SQL Server, Oracle, PostgreSQL, MySQL) болон орчин үеийн Cloud өгөгдлийн агуулахууд (Snowflake, Google BigQuery, Amazon Redshift)-тай шууд (Native) холбогдох. - Файлын формат: Excel, CSV, JSON, PDF болон текст файлуудаас өгөгдөл унших. - Шууд холболт ба Санах ой: Өгөгдлийг шууд (Live connection) татаж харуулахаас гадна, хурдтай ажиллах үүднээс өгөгдлийг системийн санах ойд (In-memory extract) татаж авах боломжтой байх. **Шинжилгээ ба Дүрслэл (Analytics & Visualization)** - Интерфэйс: Код бичих шаардлагагүйгээр (Drag-and-drop) чирч тавих үйлдлээр тайлан, дашборд угсрах боломжтой байх. - Дүрслэлийн төрлүүд: Бар, шугаман, пирог, дулааны зураглал (Heatmap), газарзүйн газрын зураг (Geospatial mapping), модны бүтэц зэрэг олон төрлийн график байгуулах. - Нарийвчилсан шинжилгээ: Тренд шугам (Trend lines), урьдчилсан таамаглал (Forecasting), кластер шинжилгээ (Clustering) болон хэрэглэгчийн тодорхойлсон томьёо (Calculated fields) оруулах боломжтой байх. **Архитектур ба Аюулгүй байдал (Architecture & Security)** - Байршуулалт: Байгууллагын өөрийн сервер дээр (On-Premise) эсвэл Үүлэн технологид (Cloud/SaaS) байршуулах сонголттой байх.

- Хандалтын удирдлага (SSO & AD): Active Directory эсвэл LDAP-тай холбогдож хэрэглэгчийн эрхийг удирдах, Single Sign-On (SAML, OpenID) дэмждэг байх.
- Өгөгдлийн нууцлал (Row-Level Security): Нэг дашбордыг олон хүн үзэхэд тухайн хүний эрх, албан тушаалаас хамаарч зөвхөн өөрт хамааралтай мөрийн өгөгдлийг харах хязгаарлалт хийх боломжтой байх.

Хянасан:

"Эрдэмнэт" сүлжээний хэлтсийн дарга — Ж.ГОМБОДОРЖ

Боловсруулсан:
"Эрдэмнэт" сүлжээний хэлтсийн сүлжээний инженер — Б.СУГАР-ЭРДЭНЭ

БАТЛАВ. "Боловсролын мэдээллийн технологийн төв"
УТҮГ-ын Захирлын үүрэг гүйцэтгэгч

.....
Д.Бат-Эрдэнэ

БАРААНЫ ТЕХНИКИЙН ТОДОРХОЙЛОЛТ

№	Техникийн үзүүлэлт
1	Дата өгөгдөлтэй ажиллах, статистик тайлан нэгтгэлийн систем (Data analysis& Statistic report)
2	Нийлүүлэх систем нь байгууллагын өгөгдлийг нэгтгэн боловсруулж, хүснэгтэн тайлангуулыг хялбар хөгжүүлэх, хөгжүүлэлтийн одоогийн ажиллагааг хялбарчилсан, хөгжүүлсэн тайлан нь хэрэглэгчид өөрийн хүссэн загвараар харах уян хатан нөхцөлтэй тайлангийн систем байна. Параметртэй тайлан, статистик шинжилгээ, HTML5 динамик график, компонент дахин ашиглалт зэрэг боломжуудаар дамжуулан өгөгдлийг бодит цагт шинжилж, ойлгомжтой байдлаар харуулах боломжийг олгодог байна.
3	Санал болгож буй шийдэл нь Байгууллагын мэдээллийн системүүдээс (Oracle 19c, MariaDB) өгөгдөл татан авч, стандарт болон удирдлагын тайланг автоматжуулсан байдлаар гаргах FineReport системийг нэвтрүүлэхэд оршино. Хамрах хүрээ: - Өдөр тутмын, сар, улирал, жилийн тайлан - Удирдлагын дүн шинжилгээний dashboard - Боловсролын яам, Үндэсний статистикийн хорооны тайлагналын формат - Олон эх үүсвэртэй тайлан боловсруулах FineReport 11.0.0 системтэй дүйцэхүйц буюу түүнээс дээш түвшний шийдэл байна.
4	Лицензийн нөхцөл: - Лицензийн төрөл: Perpetual - Лицензийн хугацаа: Хязгааргүй - Хэрэглэгчийн тоо: Хязгааргүй - Дэмжлэг үйлчилгээ: 1 жил
5	Шийдэл нь байгууллагын дотоод сүлжээнд (on-premise) суурилуулах боломжтой байх.
6	**Үндсэн функцийн шаардлага** • Нэгээс олон дата эх үүсвэрүүдтэй холбогдох боломжтой • Нэгээс олон sheet дизайн • Нэгээс олон Running орчин • Сайжруулсан статистик шинжилгээний функц • Параметр асуулгын интерфейс • Загварын эрхийн интеграц • Alpha нарийвчилсан алсын дизайн • Загвар илрүүлэх туслах • Компонент дахин ашиглалт • HTML5 динамик график / диаграм • JDBC холболт ашиглах • Stored Procedure, Function, • View дэмжих - Parameter-тэй тайлан • Master-Detail,

	• Pivot, Cross-tab - Dashboard, график, KPI - PDF, Excel, Word, CSV экспорт – • Email автоматаар илгээх – • Batch тайлан боловсруулах Нэмэлт функцийн шаардлага • Принт, экспорт хийх • Баазруу дата оруулах боломжтой • Эксел импорт хийх • Анализ хийх болон Шийдвэр гаргалтын платформтой байх
7	**Дэмжигдэх платформ** Санал болгож буй шийдэл нь дараах платформуудыг дэмжинэ. - Kubernetes k8s - Oracle 19c, - MariaDB
8	Vulnerability Scanning боломж Шийдэл нь дараах скан хийх боломжуудтай байна. - Network vulnerability scanning - Web application vulnerability scanning - Configuration auditing - Compliance auditing - Credentialed scanning - Agent-based scanning (шаардлагатай тохиолдолд)
9	**Plugin ба мэдээллийн сан** Санал болгож буй шийдэл нь: - - Өгөгдлийн сангийн холболт амжилттай - Тайлангийн зөв ажиллагаа - Экспорт хэвийн - - Хандалтын эрх зөв - Гүйцэтгэлийн тест амжилттай
10	**Интеграцийн боломж** Санал болгож буй шийдэл нь дараах системүүдтэй интеграц хийх боломжтой байна. - REST API холболт - ESIS / HEMIS / TVET системд embed хийх - Single Sign-On (SSO) дэмжих боломж - LDAP / Active Directory холбол
11	**Аюулгүй байдлын шаардлага** Санал болгож буй шийдэл нь: - HTTPS протокол ашиглан шифрлэгдсэн холболт - Role-based access control (RBAC) - Аудит лог бүртгэл - Хэрэглэгчийн эрхийн удирдлага - Нөөцлөлт ба сэргээх төлөвлөгөө - Нууц үг шифрлэлт
12	Системийн удирдлага Шийдэл нь: - Web-based management console - Суулгасан FineReport систем - 20–30 стандарт тайлан

	- Dashboard шийдэл - Техникийн баримт бичиг - Хэрэглэгчийн гарын авлага - 1 жилийн баталгаа - Хэрэглэгчийн тусламж Хэрэгжүүлэх төлөвлөгөө: - 1-р үе шат: Суулгалт, сервер тохиргоо - 2-р үе шат: Өгөгдлийн сан холболт - 3-р үе шат: Тайлан хөгжүүлэлт (20+ стандарт тайлан) - 4-р үе шат: Dashboard хөгжүүлэлт - 5-р үе шат: Ачааллын болон аюулгүй байдлын тест - 6-р үе шат: Сургалт ба Production нэвтрүүлэлт
13	**Тайлан ба аудит** Систем нь: - 2300+ зэрэг хэрэглэгч - Энгийн тайлан < 3 секунд - Нарийн тайлан < 10 секунд - Олон мөртэй өгөгдөл pagination ашиглах - Байгууллагын шаталсан бүтцээр тайлан гарах боломжтой байх - Executive summary тайлан - Technical vulnerability тайлан - Compliance тайлан - PDF, CSV, HTML, EXCEL форматаар тайлан гаргах

ХЯНАСАН:

СШТ ХЭЛТСИЙН АХЛАХ МЭРГЭЖИЛТЭН Б.АДЪЯАЦЭРЭН

БОЛОВСРУУЛСАН:

СШТ ХЭЛТСИЙН БИЗНЕСИЙН ШИНЖЭЭЧ Э.ДОЛГОРМАА