БАТЛАВ
УС СУВГИЙН УЛИРДАХ ГАЗРЫН ЕРӨНХИЙ ИНЖЕНЕР Ж.ДАГВАСҮРЭН

2024 оны 01 дүгээр сарын 31

ТЕХНИКИЙН ТОДОРХОЙЛОЛТ

2024 оны 01 дүгээр сарын 31 Улаанбаатар хот

Төслийн нэр хүчин чадал /бараа материал худалдан авах, ажил, үйлчилгээ, биет бус хөрөнгө, зөвлөх үйлчилгээ/	Цахим халдлагаас хамгаалах лиценз – 1
Төсөл хэрэгжих алба хэлтэс	Мэдээллийн технологи, автоматжуулалтын нэгж
Төсөл хэрэгжих хугацаа	2024 оны 2-р улиралд
Үндсэн хөрөнгийн код	
Байршил	УСУГ-ын серверийн өрөө
Хөрөнгийн ангилал /бараа материал худалдан авалт, техник технологийн шинэчлэл, их ба урсгал засвар/	
Огноо	2024-01-31

1.Зорилго Цахим халдлагаас хамгаалах лиценз шинээр худалдан авч тоноглосоноор мэдээллийн аюулгүй байдлын хэвийн найдвартай ажиллагааг хангахад зориулагдана.

2.Бүрдэл

- Халдлагаас хамгаалах лиценз – 1
- Лицензүүдийн техникийн үзүүлэлт, баримт бичиг
- Гарын авлагын хамт

3.Техникийн үзүүлэлт

- Халдлагаас хамгаалах лиценз Unified Security Platform Full solution - Hybrid On Premise - 3 жилийн лицензтэй байх
- System assemble based on Premise.
- Kubernetes based Native WAF 3.0 system with 3-year support.
- Layer 7 Ddos mitigation system with 3-year support
- Load Balancer system with 3-year support.
- Unified Security Platform installation shall be supportable on Kubernetes architect system.
- Should be automatically integrates with a containerized approach to scale security natively and elastically.
- Secures your website against hacking.
- Protecting your Brand against Breaches.
- Machine learning that detects and blocks threats while minimizing false positives.
- Advanced Bot Mitigation effectively protect web assets without imposing friction on legitimate users.
- Dynamic profiling learns protected applications and user behaviour, thus automatically applying a positive security model.
- Flexible deployment to support hybrid environments (on-premises and cloud).
- Updates web defences with research-driven intelligence on current threats.
- Visual analytics tools for advanced threat insights.
- Fully PCI compliant simplified event investigation with Attack Analytics.
- Correlates security violations to detect sophisticated, multi-stage attacks.
- Automated Virtual Patching.
- • Performs seamless migration of workloads from cloud to on premise or visa versa

- Secures applications proactively by end customers, by applying False positive manually.
- High performance, transparent, drop-in deployment .
- Defending your web apps against sophisticated denial of service attacks.
- Support able below systems assembled in platform.
- Kubernetes WAF
- Public Cloud WAF
- WAF as a Service
- Layer 7 DDoS Protection
- API Security
- OWASP TOP 10 Protection
- Bot Protection
- Runtime Application Security
- AI Firewall
- Virtual Patching

Supported Features

- OWASP top 10
- SANS top 25
- Free ssl certificate
- Zero day vulnerability protection
- IP reputations and blacklist and whitelist
- Geo-location based blacklist and whitelist
- URL whitelisting and blacklisting
- Rate limiting
- Advanced- ip based rate limiting
- Inbuilt vulnerability scanner
- Virtual patching based on vuln scans
- Bot Mitigation
- Layer 7 ddos protection
- Behavioural rules
- Self-learning rule engine
- Custom rules
- Machine fingerprinting
- Automated report generations from Dashboard
- Near Zero False positives
- Hotlinking protection
- ML & AI based threat insights
- Secure cdn
- Application profiling
- Automatic static caching
- Centralized Management
- Multi-tenant dashboard
- SIEM integrations
- Managed services
- Role Based Access Control
- 24/7 support
- Deployments
- Hybrid Cloud
- Multi-cloud deployment
- On-premise deployment
- Native kubernetes WAF(On-prem)
- Redirection of Brute Force Traffic
- Virtual Platform Independent of the Hardware
- Caching Compression & SSL Acceleration

- ATO and Credential Stuffing
- Resize of WAF, Horizontally and Vertically
- JIT Blacklisting/Whitelisting of IPs
- JIT custom rules propagation
- Supports 24/7 Blocking Mode
- RBAC Controls
- Fully Customizable/ Unlimited Integrations
- Browser Fingerprinting/UEBA
- Threat Intels Independent
- Customizable False Positives
- AI DDoS Protection
- Anti Automation Protection
- Rolling Updates
- Failover Protection
- Auto Scaling
- Security Assessment
- Server Health Check
- Auto OWASP / SANS Rules Configuration
- Auto Configuration/ Auto Tuning
- Dynamic Virtual Patching
- Advance API Protection

4.Чанарын шалгуур:

- Баталгаат хугацаа 3 жил ба түүнээс дээш байх.
- Лиценз нь УСУГ нэр дээр байх.
- Дээр дурдагдсан лицензүүдийг нийлүүлэх, тохируулах ажлын явцад цаг үеийн байдлаас шалтгаалсан нэмэлт тоног төхөөрөмж суурилуулах болон бусад нэмэлт ажил гарсан тохиолдолд гүйцэтгэгч компани өөрийн зардлаар тухайн ажлыг бүрэн гүйцэд хийж гүйцэтгэнэ.
- Шалгарсан байгууллага нь техникийн тодорхойлолтын дагуу багц лицензүүдийг шинээр худалдан авч суурилуулалт, тохируулга, хийж гүйцэтгэх.
- Олон улсын сертификаттай албан ёсны борлуулагчаас авах.
- Лицензийн хугацаа, техникийн үзүүлэлтүүдийг хавсаргах

Фото зураг:

5.Бусад:

Нийлүүлсэн аж ахуй нэгж нь техникийн үзүүлэлт, баталгааны хуудсыг хавсаргах.

ХЯНАСАН:

ИНЖЕНЕРИЙН БОДЛОГЫН ХЭЛТСИЙН ДАРГА Н.ОДХҮҮ

ИНЖЕНЕРИЙН БОДЛОГЫН ХЭЛТСИЙН ЦАХИЛГААН АВТОМАТИКИЙН ИНЖЕНЕР Ж.БАТЖАРГАЛ

МЭДЭЭЛЛИЙН ТЕХНОЛОГИ, АВТОМАТЖУУЛАЛТЫН НЭГЖИЙН МЕНЕЖЕР Б.АМГАЛАН

БОЛОВСРУУЛСАН:

МЭДЭЭЛЛИЙН ТЕХНОЛОГИ, АВТОМАТЖУУЛАЛТЫН НЭГЖИЙН СЕРВЕРИЙН СИСТЕМ ХАРИУЦСАН ИНЖЕНЕР Н.АРИУНБОЛД