جـــامعـــة
عبـــدالله الســـالـــم
Abdullah Al Salem
University

إدارة خدمات الرقمنة

محضر الاجتماع التمهيدي
للممارسة رقم (23-2025\2026) بشأن توريد وتركيب وتشغيل أجهزة حماية الشبكة الخارجية وأجهزة المستخدمين

البيانات :

- اليوم والتاريخ: يوم الخميس الموافق 25-9-2025
- الوقت: الساعة 12 ظهرا
- المكان: قاعة اجتماعات ادارة خدمات الرقمنة – مبنى 31خ
- الحضور:

ممثلي جامعة عبدالله السالم		
1	السيدة / آمنه الراشد	مهندس حاسب آلي
2	السيدة / منار المطيري	مهندس حاسب آلي
3	حضور ممثلي الشركات المفوضين	

وقائع الاجتماع

افتتحت السيدة/ آمنه الراشد الاجتماع بالترحيب بالحضور من ممثلي الشركات وقد تم اعطاء نبذة عن المشروع وتم تزويد الشركات بالبريد الالكتروني it.tender@aasu.edu.kw ونموذج Qr code لتعبئة الاستفسارات والاسئلة الفنية المتعلقة بالممارسة بحد أقصى يوم الاحد 28-9-2025 في الساعة 1 مساء وسيتم الرد على الاستفسارات خلال مدة 24-48 ساعة.

وعليه فقد شكرت السيدة/ آمنه الراشد الحضور, وانتهى الاجتماع في الساعة 12:30 مساء. نرفق لكم الاستفسارات والاجوبة.

والله ولي التوفيق

استفسارات
للممارسة رقم (23-2025\2026) بشأن توريد وتركيب وتشغيل أجهزة حماية الشبكة الخارجية وأجهزة المستخدمين

1. How should the solution installed and deployed in on - prem or cloud or hybrid ?
- The solution must have the capability to cover the full environment because we might need it as a hybrid deployment according to the University topology
2. Is it a must for the solution to have a relay server ?
- Yes to minimize the resource consumption on our endpoints
3. Is it a must for the solution to have Security Virtual Appliances SVA?
- Yes, because s a virtual machine that centralizes antimalware scanning in virtualized environments, offloading workloads from VMs to improve performance and scalability while maintaining strong protection
4. Is it important for the solution to have the capability to do full disk encryption when needed as add on?
- Yes we will use this feature in the future for our servers and the solution provider must have it as add-on feature
5. Is it must for the solution to provide user content control module with the below features:
   1 blocking internal access for specific clients or clients group
   2 blocking actions for certain applications
   3 blocking internet access for certain period of time
   4 block web pages that contain keywords or categories
   5 allow access to specific web pages specified by the administrators
- All the above are mandatory required for the solution to cover and manage
6. Is It must for the solution sandbox analyser to control the size of file that can be submitted smaller than and x larger than y KB?
- Yes, the solution should have the capability to manage the files that will be submitted to the sandbox under size control.
7. Please clarify the required support and license duration for perimeter firewall.
- 3 Years
8. Is there any required training according to incidents responder?
- Yes
9. Is there any update on the BOQ?
- No
10. No of years you are looking for Firewall
- 3 Years
11. No of years you are looking for EDR,
- 3 Years

12. Clarification Queries for EDR & XDR Proposal

Licensing & Scope

1. What licenses are currently available for students and for faculty/staff?
o Are both groups expected to be in scope for EDR/XDR coverage?
o If not, which user groups are to be prioritized?

- Please Refer to the RFP

2. Are you currently subscribed to any Microsoft 365 A3/A5 Education licenses? If yes, which SKUs and for how many users?

- Please Refer to the RFP

3. Do you require coverage for personally owned devices (BYOD) used by students, or only institution-owned endpoints and servers?

- Please Refer to the RFP

13. Current Security Posture

1. What is your current Antivirus/EDR/XDR solution (if any) across endpoints and servers?
o Are you looking for a complete replacement or coexistence with the existing solution?
2. Do you have an existing email security gateway (e.g., Proofpoint, FortiMail, Trend Micro)?
o Should Defender for Office 365 be considered as part of the XDR scope?
3. Do you have an Identity Threat Detection & Response (ITDR) solution for Active Directory/domain controllers today?
o If not, should Defender for Identity be included?
4. Do you have a CASB solution (Cloud Access Security Broker) in place?
o If not, would you like us to propose Defender for Cloud Apps?
5. What is your existing SIEM platform, if any?
o If you already have one, do you expect Microsoft XDR to integrate with it, or would Microsoft Sentinel become the primary SIEM/XDR platform?

- the current security posture is out the scope of the pretender meeting

14. Endpoints & Servers

1. Approximate number of Windows, macOS, Linux endpoints (faculty, students, labs) in scope?

- it will be faculty, and the solution should support the three types od OS's so the number is 1000 whatever we will implement on.

2. Approximate number of Windows/Linux servers in scope?

- it will be faculty, and the solution should support the three types od OS's so the number is 1000 whatever we will implement on.

3. For policy updates and agent upgrades — Microsoft Defender can update via the cloud console (Intune/MDE service). Would this be acceptable, or do you prefer updates controlled internally?

- the update should be managed some Endpoint will be takes update direct through Cloud and other will be through a relay server because they will be in isolated network

4. For project delivery — should deployment and rollout be performed remotely, hybrid, or fully on-site?

- depend on the task but on-site is preferable

15. EDR Capabilities

1. Would you like automated remediation and rollback (to a known good state) to be enabled by default?

- if this feature have been applied it should cover all endpoint which have direct connection to cloud and endpoint through SVA and relay server which is isolated endpoints.

2. Do you require fileless attack prevention (via AMSI + .NET inspection) to be scoped in?

- the solution should prevents fileless attacks by combining exploit defense, memory protection, and behavior-based detection to block malicious activity that doesn't rely on traditional files.

3. For threat hunting queries:

o Do you expect to migrate existing hunting queries/use cases from your current solution?

o Or would you prefer we create a fresh set of new hunting rules and use cases aligned with MITRE ATT&CK?

- Threat hunting not required in this stage but the solution that you will provide must have it for future expansions.

4. Should tamper protection be enforced for all endpoint agents, including admin accounts?

- Tamper Protection is required for user, for administrators by requiring the solution console password to do a change.

16. XDR Capabilities

1. Which workloads do you specifically want to protect as part of XDR?

o Endpoints (Windows, Mac, Linux)

o Servers (on-prem / cloud-hosted)

o Microsoft 365 (Exchange, Teams, SharePoint, OneDrive)

o Identity (Active Directory, Entra ID)

o Cloud workloads (Azure, AWS, GCP)

o Mobile devices (iOS/Android)

o SaaS apps (Google Workspace, Atlassian Jira/Confluence/Bitbucket)

- The Network is the mandatory extended detection response we need but the solution should cover all the specs and the areas we asked for as add-ons for future expansion and future needs

2. For cloud workloads (AWS/GCP/Azure):

o Do you require a CSPM/CWPP solution (Defender for Cloud) or only alert/log monitoring?

o For AWS specifically, are services like Lambda, S3, CloudTrail, CloudWatch in scope for monitoring?

- The Network is the mandatory extended detection response we need but the solution should cover all the specs and the areas we asked for as add-ons for future expansion and future needs

3. For email detection and remediation:

o Do you require auto-remediation actions (delete emails, suspend accounts), or alert-only mode?

- Email detection is out of scope for this RFP but the system should support the integration if needed as add-ons

4. For identity protection:

o Should XDR include Kerberos attack detection (brute-force, replay, weak encryption)?

o Should account disabling and password resets be fully automated or manually approved?

- Identity Protection is out of scope for this RFP but the system should support the integration if needed as add-ons

5. For third-party apps like Atlassian:
o Do you want to integrate these directly into SIEM for monitoring or app-based activity monitoring?

- Third Party apps this out scope for this RFP but the system should support the integration if needed as add-ons

17. Operations & Strategic Direction
1. Do you already have a ticketing system (ServiceNow, Remedy, Jira) for incident management?
o Should incidents from Microsoft XDR integrate directly into it?

- SOC, SIEM, and Ticketing System is out of the Scope of this RFP but the system should support the integration if needed as add-ons.

2. How many SOC/security analysts will operate the solution?
o Do they require a single console (Microsoft 365 Defender portal) or are multiple views acceptable?

- all on one console is required.

3. Should incidents be correlated automatically into a single attack story (reduce alert fatigue), or do you prefer raw event-level alerts?

- the solution should correlated as the both option as been detected and we have the ability to deep dive in to raw event

4. For reporting — do you require executive-level dashboards (risk scoring, compliance summaries) in addition to SOC dashboards?

- this should be provided based on techniques

5. If you are looking at an ingestion-specific XDR model, would you be open to explore something like:
o Microsoft Sentinel + managed SOC service (full SIEM + 24/7 operations), or
o Microsoft XDR (Defender 365 + integrations) that provides continuous monitoring and automated correlation across Microsoft security products?
XDR is mentioned in the pricing table as XDR - Network
do you have an NDR solution, which is the existing solution or is it a typo you are looking XDR for the endpoints

- What we need is an EDR for Endpoint and an extended level of detection and response on the network Layer so it is EDR and XDR Network Sensor

18. Could you please clarify whether the warranty period is 1 year or 3 years ?
- Warranty on hardware is 3 years