مشروع شراء برامج حماية وكشف واستجابة موسعه XDR

وإنشاء منصة كشف واستجابة موسعة (XDR) موحدة للجامعات

مقدمة

في ظل التوسع المتسارع في الاعتماد على الأنظمة الرقمية داخل مؤسسات التعليم العالي، تبرز أهمية استكمال تأمين البنية التحتية التكنولوجية للجامعات كأحد المرتكزات الأساسية لضمان استمرارية العملية التعليمية وحماية البيانات الأكاديمية والإدارية والبحثية، وخاصة أجهزة الحاسب الآلي المستخدمة من قِبل أعضاء هيئة التدريس والعاملين والطلاب بالجامعات.

ويهدف هذا المشروع إلى توريد وتركيب برامج حماية وكشف واستجابة موسعة(XDR) ، بما يضمن توفير أعلى مستويات الحماية السيبرانية، وتهيئة بيئة عمل آمنة خالية من المخاطر السيبرانية، مع ضمان استمرارية تقديم الخدمات الإلكترونية بكفاءة واعتمادية عالية.

كما يأتي المشروع في إطار استراتيجية وزارة التعليم العالي للتحول الرقمي، ودعم التوجه نحو إنشاء مركز عمليات أمن سيبراني موحّد(SOC) ، حيث يُعد توفير حلول الحماية والكشف والاستجابة الموسعة (XDR)لبنة أساسية في بناء منظومة متكاملة للرصد والتحليل والاستجابة الأمنية على مستوى الجامعات.

الوضع الحالي:

- لا توجد بالجامعات حالياً تطبيقات حماية من الفيروسات أو حلول EDR أو XDR على الأجهزة الثابتة أو المتحركة الخاصة بكل من:
  - الطلاب
  - أعضاء هيئة التدريس
  - الأنظمة الإدارية والمالية
- مما يؤدي إلى:
  - احتمالية إصابة هذه الأجهزة ببرمجيات خبيثة تهدد أمن شبكات الجامعة.
  - إمكانية استغلال هذه الأجهزة كمنصات لشن هجمات على شبكات خارجية (مثل هجمات حجب الخدمة الموزعة DDoS).
  - ارتفاع مخاطر الاختراق وتعطل الأنظمة والخدمات الإلكترونية.

- يتم حصر أعداد الأجهزة وموديلاتها وأنظمة التشغيل الخاصة بها من خلال استبيان يتم تعميمه على الجامعات.

- **أهداف المشروع**

إطلاق مشروع **"منصة كشف واستجابة موسعة (XDR) موحدة للجامعات"**، بهدف ربط جميع طبقات الحماية (Firewall – Endpoints – Email – Identity – Servers) ضمن منصة

تحليل مركزية متكاملة، تدعم إنشاء مركز عمليات أمن سيبراني موحد(SOC) ، وذلك من خلال توفير حلول حماية وكشف واستجابة موسعة (XDR) متقدمة للحماية من الفيروسات والتهديدات السيبرانية.
مما ينعكس على تحقيق الآتي:

- توفير حماية شاملة ومتقدمة للشبكات والأنظمة الجامعية.
- الامتثال لمعايير ومتطلبات الأمن السيبراني الوطني.
- تقليل مخاطر الاختراق وفقدان البيانات.
- دعم استقرار واستمرارية الخدمات التعليمية الرقمية.
- توفير رؤية شاملة ومتكاملة لمنظومة الأمن السيبراني بالجامعات.
- رفع كفاءة الرصد والتحليل الأمني على مستوى الجامعات.
- تقليل مخاطر الهجمات الإلكترونية المتقدمة وتحسين سرعة الاستجابة للحوادث.
- إنشاء منظومة أمن سيبراني موحدة ومستدامة.

كما يمكن التوسع في نطاق المشروع بإضافة الأجهزة المحمولة الخاصة بأعضاء هيئة التدريس والطلاب، وذلك من خلال إضافة رخص تأمين إضافية، بما يعزز من مستوى الحماية الشاملة للبيئة الرقمية الجامعية.

- **نطاق العمل(Scope of Work)**

يشمل المشروع ما يلي:

- توفير حلول حماية وكشف واستجابة موسعة (XDR) للحماية من الفيروسات والتهديدات السيبرانية لأجهزة الحاسب الآلي الثابتة بالجامعات لمدة سنة واحدة، أو ثلاث سنوات (وفقًا لسياسة كل جامعة).

- **الفئات المستفيدة:**
  - الطلاب.
  - أعضاء هيئة التدريس.
  - الإدارات الإدارية والمالية.
  - مراكز البحث.
  - إدارات تكنولوجيا المعلومات(IT)

- **الفوائد المتوقعة من تنفيذ المشروع:**
  - رفع مستوى الأمن السيبراني داخل الجامعات.
  - حماية البيانات الأكاديمية والإدارية والبحثية الحساسة.
  - ضمان استمرارية الأنظمة التعليمية، مثل أنظمة إدارة التعلم(LMS) ، وبوابات التعليم الإلكتروني، ومنصات الامتحانات الإلكترونية.
  - تقليل مخاطر الهجمات الإلكترونية وتعطل الشبكات والأنظمة.
  - دعم جهود التحول الرقمي في قطاع التعليم العالي.
  - التهيئة لإنشاء مركز عمليات أمن سيبراني (SOC) موحد للجامعات.

- **مدة التنفيذ**

يتم تنفيذ المشروع على ثلاث مراحل تمتد لثلاث سنوات، وذلك بهدف توفير التمويل اللازم وضمان التطبيق التدريجي والآمن لمنصة الكشف والاستجابة الموسعة(XDR) .

واستنادًا إلى أهمية تحقيق تمثيل عادل ومتنوع للبنية التحتية الرقمية بمختلف الجامعات، يُقترح تنفيذ المشروع من خلال اختيار عدد من الكليات متوسطة الحجم بكل جامعة من الجامعات المستهدفة، بواقع من (2 إلى 5) كليات لكل جامعة، بما يتيح اختبار الحلول المقترحة في بيئات تشغيلية متنوعة قبل التوسع الكامل على مستوى الجامعة.

ويهدف هذا النموذج إلى:

- اختبار المنظومة في بيئات تشغيل متنوعة (الشبكات – الأجهزة – الأنظمة).
- قياس الجاهزية الفنية والإدارية بكل جامعة.
- تقييم فعالية التكامل مع أجهزة تأمين البيانات والبنية التحتية الحالية.
- تحليل مؤشرات الأداء الأمنية قبل التعميم الكامل على مستوى الجامعة.
- تقليل المخاطر التشغيلية المصاحبة للتطبيق الشامل.

وتشمل كل مرحلة تشغيل المنظومة على متوسط عدد أجهزة يتراوح بين (2000 – 3000) جهاز بكل جامعة، مع ربطها بمركز عمليات أمن سيبراني مركزي (SOC) لتحليل الأحداث الأمنية وإعداد تقارير تقييم تفصيلية لدعم اتخاذ القرار بشأن التوسع المرحلي.

مدة التنفيذ المتوقعة لكل مرحلة:

من 6 إلى 12 أشهر، وتشمل كافة الإجراءات ذات الصلة، بما في ذلك:

- إجراءات التعاقد مع الجامعات.
- التفاوض الفني والمالي مع الشركات.
- إعداد كراسات الشروط والمواصفات الفنية.
- تنفيذ عمليات الطرح والشراء والترسية.
- أعمال التنفيذ والتشغيل الفعلي.

- **المخاطر في حال عدم التنفيذ:**
  - زيادة احتمالية التعرض للاختراقات والهجمات السيبرانية.
  - فقدان أو تسريب البيانات الحساسة والمعلومات السرية.
  - تعطل أو توقف الخدمات التعليمية والإدارية الحيوية.
  - عدم الامتثال لمتطلبات وضوابط الأمن السيبراني القومية والتشريعات ذات الصلة.
- **التكلفة التقديرية:**
  - يتم حصر أعداد الأجهزة المطلوبة وتحديد عدد الرخص اللازمة، مع تحديد مدة الترخيص المناسبة.
  - إعداد دراسة تقديرية للتكلفة الإجمالية قبل بدء مرحلة التفاوض مع الشركات الموردة، لضمان دقة التخطيط المالي واتخاذ القرار المناسب.

- **الملخص التنفيذي (Executive Summary)**

المشروع: مشروع شراء برامج الحماية والكشف والاستجابة الموسعة (XDR) وإنشاء منصة موحدة للكشف والاستجابة الموسعة لخدمة الجامعات.

الهدف: استكمال وتعزيز منظومة حماية البنية الرقمية للجامعات، ورفع مستوى الجاهزية السيبرانية، من خلال توحيد أدوات المراقبة والتحليل والاستجابة للحوادث الأمنية.

المدة الزمنية: من 12 إلى 48 أسبوعًا من تاريخ بدء التنفيذ.

الأثر المتوقع:

- تعزيز مستوى الأمن السيبراني
- ضمان استقرار واستمرارية الخدمات التعليمية والإدارية
- تحقيق الامتثال لمتطلبات وضوابط الأمن السيبراني المعتمدة.

المخاطر في حال عدم التنفيذ:

- زيادة احتمالية التعرض للاختراقات والهجمات السيبرانية.
- توقف أو تعطل الأنظمة والخدمات الحيوية.
- فقدان أو تسريب البيانات الحساسة.