

دليل تحديث مراكز العمليات الأمنية في المملكة

Saudi SOC Modernization Playbook

LogRhythm® exabeam™ سايبر كاست

الفهرس

	نبذة عن هذا الدليل	3
01	رسالة إلى مدير الأمن السيبراني (CISO)	4
02	مشهد مراكز عمليات الأمن السيبراني في المملكة عام 2026	7
03	ست قوى تعيد تشكيل مركز عمليات الأمن السيبراني السعودي	11
04	نهج المسارين لتحديث مراكز العمليات الأمنية في المملكة	26
05	كيف تسدّ Exabeam الفجوات	34
06	قياس ما يستحق القياس: مؤشرات أداء يثق بها مجلس الإدارة	38
07	خارطة طريق التسعين يوماً لتحديث مركز عمليات الأمن السيبراني	42
	المساهمون	47

نبذة عن هذا الدليل

يقدّم «دليل تحديث مراكز العمليات الأمنية في المملكة» لمديري مراكز عمليات الأمن السيبراني وقادة الأمن في المملكة العربية السعودية، الساعين إلى تعزيز عملياتهم الأمنية في ظل تطور التهديدات السيبرانية، وشح الكفاءات، وتنامي أحجام البيانات، وصرامة المتطلبات التنظيمية، قراءةً قائمة على الأدلة لهذه التحديات والخيارات المتاحة لمعالجتها، مستنداً إلى الأبحاث العالمية والإقليمية، والإحصاءات القطاعية، والأطر التنظيمية السعودية. ويستهل الدليل برؤية تنفيذية لتحديث المراكز، يليها عرض لمشهد مراكز عمليات الأمن السيبراني في المملكة عام 2026، والقوى الست التي تعيد تشكيل العمليات الأمنية فيها. ثم تتناول الأقسام اللاحقة خيارات النشر، ومنها النشر السيادي داخل مقار الجهات، والسحابة داخل المملكة، والنموذج الهجين، وتبيّن كيف تسهم المنصات الحديثة في سد الفجوات التشغيلية التي حددها الدليل. ويختتم الدليل بمؤشرات أداء قائمة على المحصلات، وخارطة طريق لتحديث المركز خلال تسعين يوماً، بما يمكّن القارئ من تقييم قدراته الحالية، وترتيب أولويات التحسين، وقياس التقدم المحرز.





01

رسالة إلى مدير الأمن السيبراني (CISO):

لماذا لم يعد تحديث مركز عمليات الأمن السيبراني يحتمل الانتظار؟

01

رسالة إلى مدير الأمن السيبراني (CISO):

لماذا لم يعد تحديث مركز عمليات الأمن السيبراني يحتمل الانتظار؟

عزيزي رئيس الإدارة المعنية بالأمن السيبراني،

إن كنت تقرأ هذه السطور، فالأرجح أن حديث التحديث قد بلغ مكتبك بالفعل؛ فلعل مجلس الإدارة طرح عليك سؤالاً لم تجد له جواباً وافياً، أو لعل تقييماً أو تدقيقاً أجرته الهيئة الوطنية للأمن السيبراني (NCA) كشف عن فجوة قائمة، أو ربما أخبرك أحد نظرائك في منشأة سعودية أخرى بما كلفتهم إياه حادثتهم الأخيرة. وأيّاً كان الدافع الذي قادك إلى هذه الرسالة، فإن توقيتها أبعد من أن يكون محض مصادفة؛ إذ ثمة ثلاثة ضغوط تتقاطع اليوم دفعة واحدة على مركز عمليات الأمن السيبراني في المملكة.

«يبدأ تحديث مركز العمليات بالكوادر البشرية والإجراءات والتقنية معاً، ليثمر اكتشافاً أسرع للتهديدات، وكلفة تشغيلية أدنى، والتزاماً يمكن إثباته.»

فمن جهة أولى، دفعت رؤية المملكة 2030 عجلة التحول الرقمي بوتيرة تفوق قدرة معظم فرق الأمن على مجاراتها، ومع كل نظام جديد يتسع سطح الهجوم. ومن جهة ثانية، استجابت الهيئة الوطنية للأمن السيبراني على ذلك بتشديد موقفها التنظيمي، لينتقل مفهوم وواقع الالتزام من كونه تمريناً تؤديه الجهات مرة واحدة في العام، ليكون واجباً مستمراً يقع على عاتق مركز العمليات لديك إثباته. ومن جهة ثالثة، باتت الكفاءات القادرة على إدارة هذه المنظومة كلها نادرة ومتزايدة الكلفة، إذ قفزت رواتب كبار المحللين بنسبة تتراوح بين 30% و40% خلال عام واحد.

وهنا تتجلى الحجة الداعية إلى التحرك الآن؛ فتحديث مركز عمليات الأمن السيبراني ليس ترقية تقنية لذاتها، فهو تغيير يطال الركائز الثلاث التي تقوم عليها أي منظومة عمليات أمنية: الكوادر البشرية التي تديرها، والإجراءات التي تتبعها، والتقنية التي تسندها. فإذا انتظمت هذه الركائز في عمل متناغم، أثمر التحديث أربعة مكاسب تُعنى بها الأعمال حقاً: اكتشافاً للتهديدات واستجابة أسرع، وكلفة تشغيلية أدنى لكل حادثة، ووضع التزام يمكن إثباته، وتقارير تصلح لعرضها أمام مجلس الإدارة.

ومتى تم تنفيذ هذا التحديث بالطريقة المثلى، تحول مركز العمليات لديك من مركز تكلفة تضطر إلى تبرير وجوده مرة بعد أخرى، إلى وظيفة تخفض المخاطر على نحو ملموس.

على أنك لست مطالباً بالتسليم بذلك تسليماً أعمى، ولكن بطرح الأسئلة الصائبة. فقبل دورة الموازنة المقبلة، لا بأس بأن تجلس إلى مدير مركز عمليات الأمن السيبراني لديك، وتطرح عليه الأسئلة الخمسة الآتية:

1. كم من الوقت يستغرق منا التحقيق في حادثة مصدرها بيانات هويات الدخول، من بدايتها إلى نهايتها؟
2. ما نسبة التنبيهات الخاطئة من إجمالي تنبيهاتنا، وكم تكلفنا أسبوعياً من ساعات عمل المحللين؟
3. أين يجري تخزين بيانات سجلات الأحداث لدينا فعلياً، وهل بوسعنا اليوم إثبات ذلك أمام مدقق من الهيئة الوطنية للأمن السيبراني؟
4. لو غادرنا غداً أحد كبار المحللين، فكم يمضي من الوقت قبل أن تتراجع قدرتنا على اكتشاف التهديدات؟
5. ما هي ملامح خارطة طريق التحديث لدينا على مدى الاثني عشر شهراً المقبلة، وكيف تتواءم مع التزاماتنا بموجب الضوابط الأساسية للأمن السيبراني (ECC) وضوابط الأمن السيبراني للأنظمة التشغيلية (OTCC)؟

فإن جاءت الإجابات مبهمة، فاعلم أن التحديث قد فات موعده؛ ذلك أن مركز عمليات لا يقوى على قياس هذه الأمور لا يقوى على إثبات قيمته، ومركز عمليات لا يقاس أداؤه إنما هو خطر تحمله من دون أن تدرك حجمه.

أما بقية هذا الدليل العملي فهي مكتوبة لمن سيتولى ترجمة تلك الإجابات إلى أفعال، أي مدير مركز عمليات الأمن السيبراني لديك؛ إذ تتطرق إلى القوى التي تعيد تشكيل عمليات الأمن في المملكة، وما تتطلبه معمارية مركز عمليات حديث، مع خطة مدتها تسعون يوماً لبلوغ ذلك. ولست ملزماً بقراءتها كلها، غير أن عليك أن تستوثق من أن أحداً في فريقك سيفعل.



سلطان العنزي

المدير الإقليمي لمكتب
المملكة العربية السعودية

LogRhythm - Exabeam



02

مشهد مراكز عمليات الأمن السيبراني في المملكة عام 2026

02

مشهد مراكز عمليات الأمن السيبراني في المملكة عام 2026

تعمل مراكز عمليات الأمن السيبراني (SOC) في المملكة ضمن مشهد لا تستوعبه الإرشادات العامة لعمليات الأمن استيعاباً كاملاً؛ فإن كنت مديراً لأحد هذه المراكز في المملكة العربية السعودية، فأنت تعمل في بيئة تنظيمية ناضجة تفصيلية الأحكام، وتستقطب كوادرك من سوق مواهب سيبرانية شديدة التنافس، وتسعى إلى مجاراة أجندة تحول وطنية توسّع سطح الهجوم الرقمي بوتيرة تفوق ما صُمّمت نماذج المراكز التقليدية لاستيعابه.

رؤية 2030 والبُعد السيبراني للتحول الرقمي

تشكل أجندة التحول الوطني ذاتها الخلفية الحاكمة لهذا المشهد؛ فقد وضعت رؤية المملكة 2030 التحول الرقمي في صميم التنمية الاقتصادية الوطنية، إذ تمضي الوزارات والمؤسسات المالية وشركات المرافق وجهات القطاع الخاص في رقمنة خدماتها وعملياتها ومنصاتها الموجهة إلى المواطنين على نطاق واسع.

ومع اتساع هذه المنظومة الرقمية، يتسع معها حجم الأنظمة والهويات والبيانات والخدمات المتصلة التي يُنتظر من المراكز السعودية مراقبتها وحمايتها. وقد استجابت الهيئة الوطنية للأمن السيبراني (NCA) لذلك بجعل حوكمة الأمن السيبراني أكثر تنظيماً واستمرارية وقابلية للإنفاذ، بما يعكس الدور الذي بات الأمن السيبراني يؤديه في الصمود الوطني.

الأطر التنظيمية السعودية

تمنح التنظيمات السيبرانية السعودية مراكز العمليات تفويضاً واضحاً ضمن أجندة الصمود السيبراني الوطني في المملكة. وبالنسبة إلى مديري هذه المراكز، ترسم هذه الأطر التوقعات المتعلقة بالمراقبة، وتسجيل الأحداث، والاستجابة للحوادث، وجمع الأدلة، والتعامل مع البيانات في مختلف القطاعات.

وثمة أربعة أطر تمسّ فرق مراكز العمليات على وجه الخصوص:

- تضع الضوابط الأساسية للأمن السيبراني (ECC) الصادرة عن الهيئة خط الأساس للجهات الحكومية والبنية التحتية الوطنية الحساسة.
- وتمد ضوابط الأمن السيبراني للأنظمة التشغيلية (OTCC) خط الأساس هذا إلى بيئات التقنية التشغيلية، حيث قد يعرض أي إخفاق أمني السلامة والعمليات المادية والأرواح البشرية للخطر.
- ويحكم إطار الأمن السيبراني الصادر عن البنك المركزي السعودي (SAMA) المؤسسات المالية، وينصّ صراحة على توقع مراقبة بمستوى أنظمة إدارة سجلات الأحداث ومراقبة الأمن السيبراني (SIEM).
- ويضيف نظام حماية البيانات الشخصية (PDPL) بعداً يتصل بالخصوصية يرتبط ارتباطاً مباشراً بكيفية تسجيل الجهات للبيانات الشخصية والاحتفاظ بها وضبط الوصول إليها.

ويبين الجدول أدناه الجهات التي يغطيها كل إطار، وما يطلبه من مركز العمليات.

الجدول 1: المنظومة التنظيمية السعودية في لمحة واحدة. أربعة أطر، والجهات الخاضعة لها، وما تطلبه من مركز العمليات، وثمن التقصير فيها.

الإطار	الجهات الخاضعة له	الالتزامات الرئيسة الواقعة على مركز العمليات	تبعات التقصير
ECC الضوابط الأساسية للأمن السيبراني	الجهات الحكومية ومشغّلو البنية التحتية الوطنية الحساسة؛ ويجري التعامل معها على نطاق واسع بوصفها خط الأساس الوطني.	تسجيل مركزي للأحداث محميٌ من العبث مع الاحتفاظ به مدة لا تقل عن 12 شهراً؛ ومراقبة مستمرة؛ وآليات محددة للاكتشاف والاستجابة للحوادث. وتضم النسخة ECC-2:2024 أربعة مكونات أساسية و108 ضوابط أساسية.[1]	ملاحظات رقابية، ومعالجات إلزامية، وفقدان الأهلية للعمل في السياقات الخاضعة للتنظيم.
OTCC ضوابط الأمن السيبراني للأنظمة التشغيلية	بيئات التقنية التشغيلية وأنظمة التحكم الصناعي في القطاعات الحيوية، مثل الطاقة والمرافق والصناعة.	مراقبة متخصصة لأصول التقنية التشغيلية، وإشراف مستمر، ومعالجة الثغرات في وقتها، مع تقييم الاستجابة قياساً على الأثر التشغيلي.	انكشاف مضاعف: فالإخفاقات قد تحمل تبعات على الصحة والسلامة والبيئة إلى جانب العقوبات التنظيمية.
SAMA CSF إطار الأمن السيبراني للبنك المركزي السعودي	المصارف وشركات التأمين وسائر المؤسسات المالية الخاضعة لإشراف البنك المركزي السعودي.	ضوابط تفصيلية إلزامية تتوقع صراحة تجميع سجلات الأحداث وربطها التحليلي بمستوى أنظمة SIEM، ومراقبة على مدار الساعة طوال أيام الأسبوع.	إجراءات إشرافية من البنك المركزي؛ وتدقيق وثيق خلال التقييم.
PDPL نظام حماية البيانات الشخصية	أي جهة تعالج البيانات الشخصية للأفراد في المملكة؛ وهو نافذ منذ عام 2023.	سجلات تفصيلية للوصول إلى البيانات الشخصية ومعالجتها، مع ضوابط على الاحتفاظ بها ونقلها خارج الحدود.	عقوبات على سوء التعامل مع البيانات الشخصية؛ ويتقاطع مباشرة مع التزامات التعامل مع حوادث الاختراق.

نظام ترخيص مراكز عمليات الأمن السيبراني المُدارة

فوق هذه الأطر يقوم مستجد أحدث عهداً؛ إذ باتت الهيئة الوطنية للأمن السيبراني تشترط على مقدمي خدمات مركز عمليات الأمن السيبراني المُدار (MSOC) الحصول على ترخيص موزع على مستويين.

فالمستوى الأول يشمل مقدمي الخدمة للجهات الحكومية والبنية التحتية الوطنية الحساسة، ويشترط حداً أدنى لرأس المال قدره 50 مليون ريال سعودي، وأن يكون المحللون من المواطنين السعوديين.[2]

أما المستوى الثاني فيغطي مقدمي الخدمة للسوق التجارية الأوسع.

1 الهيئة الوطنية للأمن السيبراني، الضوابط الأساسية للأمن السيبراني ECC-2:2024.
https://nca.gov.sa/en/regulatory-documents/controls-list/ecc/

2 الهيئة الوطنية للأمن السيبراني، دليل المستثمر في قطاع الأمن السيبراني.
https://cdn.nca.gov.sa/api/files/public/upload/f7fb3d13-c23c-4aff-904a-dbb4b1fe6507_Investor-Guide-EN.pdf

وبالنسبة إلى الجهات التي تقيّم خدمات المراكز المدارة، غدت متطلبات الترخيص مصفاة تغربل قرارات الشراء قبل أن يبدأ التقييم الفني أصلاً؛ فمن دون بنية تحتية داخل المملكة وسجل التزام موثوق، تتضاءل باطراد حظوظ أي مورد في بلوغ القائمة المختصرة.

النشر الهجين لمراكز العمليات

يعكس مشهد البنية التحتية لمراكز العمليات في المملكة واقعاً عملياً: فالأنظمة المنشورة داخل مقار الجهات (On-premises) ما زالت مهيمنة، في حين باتت حلول التحليلات السحابية الأصيلة أعصى على التجاهل.

فحتى عام 2025، ظلت عمليات النشر داخل مقار الجهات تستأثر بأكثر من 70% من سوق الأمن السيبراني في المملكة، مدفوعة بأفضليات سيادة البيانات، وقواعد توطين أحمال العمل الحساسة، والاستثمارات الضخمة القائمة في المنصات ذاتية الاستضافة.[3]

وفي الوقت نفسه، يتصاعد الطلب على التحليلات السحابية الأصيلة بوتيرة متسارعة، إذ من المتوقع أن تتبنى 94% من الجهات السعودية الكبرى المراقبة المدعومة بالذكاء الاصطناعي بحلول عام 2026.[4] ولا تنتقي كثير من فرق عمليات الأمن أحد الخيارين دون الآخر، بل تشغلهما معاً وتدير مواضع الالتحام بينهما.

توافر الكفاءات

تمثل سوق الكفاءات ملمحاً محورياً آخر في مشهد المراكز السعودية؛ فكبار محللي المستويين الثالث والرابع، القادرون على تفكيك التحقيق وإعادة تركيب ما جرى فعلاً، لا يزال المعروض منهم محدوداً، والسوق تعكس هذه الندرة، إذ قفزت رواتب هذه الأدوار المتخصصة في التحليل الجنائي الرقمي بنسبة تتراوح بين 30% و40% خلال عام واحد.[5]

وتزيد مستهدفات التوطين (السعودة)، واشتراط أن يكون محللو المراكز المُدارة من المواطنين السعوديين، من التأثير في وعاء التوظيف المتاح. وهذا ما يجعل التوسع في التوظيف، لدى معظم مديري المراكز، رافعة محدودة الأثر؛ فالقدرات الجديدة باتت مستمدة على نحو متزايد من رفع جودة سير العمل، وتحسين الأدوات، وحسن توظيف المحللين الموجودين أصلاً.

وبمجموع هذه الظروف تتحدد بيئة التشغيل للمراكز السعودية في عام 2026: توسع رقمي تقوده رؤية 2030، وتنظيم دقيق الأحكام، وترخيص إلزامي للمراكز المدارة، وبنية تحتية هجينة، ووصول مقيد إلى خبرات كبار المحللين. وينتقل القسم التالي بهذا المشهد إلى ست قوى تعيد تشكيل طريقة عمل هذه المراكز.

3 تقرير حصص سوق الأمن السيبراني في المملكة العربية السعودية، Research and Markets.
https://www.researchandmarkets.com/reports/5937858/saudi-arabia-cybersecurity-market-share

4 تقرير حصص سوق الأمن السيبراني في المملكة العربية السعودية، Research and Markets.
https://www.researchandmarkets.com/reports/5937858/saudi-arabia-cybersecurity-market-share

5 تقرير حصص سوق الأمن السيبراني في المملكة العربية السعودية، Research and Markets.
https://www.researchandmarkets.com/reports/5937858/saudi-arabia-cybersecurity-market-share



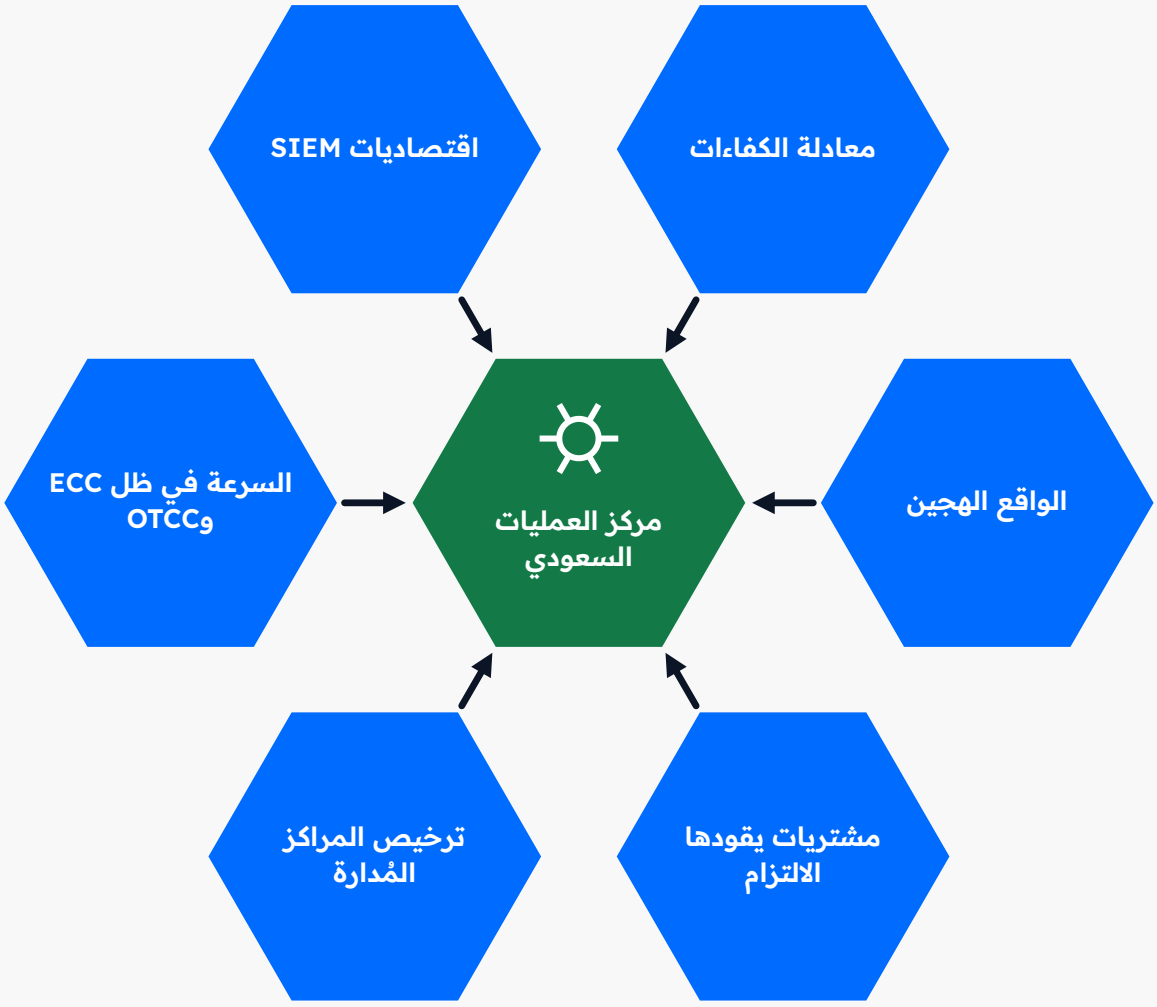
03

ست قوى تعيد تشكيل مركز عمليات الأمن السيبراني السعودي

03

ست قوى تعيد تشكيل مركز عمليات الأمن السيبراني السعودي

تلتقي الحقائق التي بسطها القسم السابق وتتقاطع داخل مركز عمليات الأمن السيبراني. ويتناول هذا القسم القوى الست الناشئة عن ذلك التقاطع، مبيناً لماذا يستلزم تحديث المراكز السعودية إجابة معمارية متماسكة.



الشكل 1: القوى الست التي تعيد تشكيل مركز عمليات الأمن السيبراني السعودي

1 معادلة الكفاءات:

جعل المحللين المبتدئين منتجين من يومهم الأول

لا تلوح في الأفق بوادر انفراج في نقص كبار المحللين الذي تشهده المملكة؛ فخبرات المستويين الثالث والرابع لا تزال شحيحة قياساً إلى الطلب عليها، ورواتب الأدوار المتخصصة في التحليل الجنائي الرقمي قفزت بنسبة تتراوح بين 30% و40% خلال عام واحد، فيما يزيد اشتراط أن يكون محللو المراكز المُدارة من المواطنين السعوديين من تضييق النطاق المتاح أمام مقدمي الخدمة المرخصين. وليس في هذه الظروف ما يتغير سريعاً.

وما يزيد الأمر صعوبة أن كثيراً من منصات إدارة سجلات الأحداث ومراقبة الأمن السيبراني (SIEM) التقليدية تفترض ضمناً أن فرق المراكز تملك فائضاً من المحللين المهرة؛ فلغات الاستعلام الخاصة بالمنصة، والربط التحليلي اليدوي عبر لوحات تحكم متعددة، ومنحنيات التعلم الطويلة، كلها تعني أن المتمرسين وحدهم قادرون على استخلاص القيمة الكاملة من هذه الأدوات.

ثم إن الخروج من هذه المعضلة بالتوظيف ليس خياراً متاحاً لمعظم مديري المراكز؛ فحتى لو توافرت الموازنة لدى جهاتهم، وكثير منها لا يملكها، فإن السوق ببساطة عاجزة عن توفير الخبرات التي تتطلبها تلك المنصات.

على أن الاستقطاب ليس إلا شطراً من المشكلة؛ فقد وجد استطلاع أجرته شركة Censuswide عام 2024 بتكليف من شركة Hack The Box أن 84% من المتخصصين في الأمن السيبراني وأمن المعلومات المشمولين بالاستطلاع في الولايات المتحدة والمملكة المتحدة كانوا يعانون ضغوطاً أو إرهاقاً أو احتراقاً وظيفياً مرتبطاً بالعمل.[1] والنتيجة عالمية الطابع لا سعودية الخصوصية، لكنها تجسد الإجهاد التشغيلي الذي ينشأ حين يُنتظر من فرق أمنية محدودة أن تستوعب أعباء متصاعدة من دون زيادة موازية في القدرات.

%84
من المتخصصين في الأمن السيبراني وأمن المعلومات المشمولين بالاستطلاع في الولايات المتحدة والمملكة المتحدة كانوا يعانون ضغوطاً أو إرهاقاً أو احتراقاً وظيفياً مرتبطاً بالعمل

كيف يبدو ذلك داخل مركز العمليات

قد يمضي المحللون الجدد أسابيع في تعلم لغة الاستعلام الخاصة بنظام SIEM وحدها قبل أن يتمكنوا من إغلاق تحقيق واحد من دون عون.

ونتيجة لذلك، يُستدرج كبار المحللين إلى أعمال الفرز في المستوى الأول لأن طابور التنبيهات لا يحتمل انتظار نضج المبتدئين، وتتفاوت جودة التحقيقات من مناوبة إلى أخرى تبعاً لخبرة من يتولاها ومستوى مهارته. وحين يستقيل محلل كبير، تتدهور قدرة الاكتشاف شهوراً؛ لأن معرفة كيفية إجراء التحقيق كانت تقيم في رأس ذلك الشخص لا في المنصة ولا في إجراءاتها الموثقة.

فلو غادر أقوى محلليك غداً، فكم من قدرتك على اكتشاف التهديدات سيرحل معه؟

1 Hack The Box, HTB Report: Building a Firewall Against Cybersecurity Burnout (استطلاع أجرته Censuswide)، 2024.
https://www.hackthebox.com/blog/htb-report-building-a-firewall-against-cybersecurity-burnout

كيف يسهم التحديث في الحل

من أهداف التحديث تقليص الاعتماد على الخبرة الفردية عبر تحويل حكم الخبراء إلى مسارات عمل مقننة، ويمكن بلوغ ذلك بسبل شتى، منها على سبيل المثال:

- **واجهات البحث بمعالجة اللغات الطبيعية (NLP):** تمكن المحلل، أياً كان مستوى مهارته، من طرح أسئلته التحقيقية بلغة مبسطة بدل تعلم صيغة استعلام خاصة بالمنصة.
- **آليات إعادة البناء المؤتمتة للخط الزمني للأحداث:** تجمع التسلسل الزمني للحادثة من سجلات الأحداث الأساسية، فترفع عن كاهل المحلل عبء الاستعلام اليدوي في أنظمة متعددة وضم الأدلة بعضها إلى بعض يدوياً.
- **خصائص اقتراح الخطوات التالية وكتيبات الاستجابة الجاهزة الموثقة القابلة للتكرار:** ترشد المحلل المبتدئ خلال التحقيق، فلا تعود جودة الاستجابة رهينة مستوى مهارة من التقط التنبيه.
- **رسم خرائط التغطية وفق إطار MITRE ATT&CK:** يضع أمام الفريق مواضع فجوات الاكتشاف، فتتجه جهود التدريب والهندسة إلى حيث تكون أجدى.

إن التحديث يحسن الإجابة عن سؤال عملي يخص القوى العاملة:

كم من العمل التحقيقي المجدي يستطيع محلل المستوى الأول إنجازه في أسبوعه الأول من دون إسناد متواصل من كبار المحللين؟



2 معضلة الاقتصاديات:

حين تتجاوز أحجام البيانات طاقة أنظمة SIEM التقليدية

كلما رقمنت الجهات مزيداً من الخدمات، ونشرت أحمال عمل سحابية، ووصلت مزيداً من أصول التقنية التشغيلية، تعاظم حجم بيانات القياس الأمني عن بعد (Telemetry)؛ فكل نظام جديد يضيف بيانات يُنتظر من مركز العمليات جمعها والاحتفاظ بها والبحث فيها ومراقبتها.

وتفاقم منصات SIEM التقليدية المشكلة؛ لأن اقتصادياتها مصممة حول أحجام أدنى من بيانات القياس عن بعد، وبنية تحتية أكثر مركزية، وتراخيص قائمة على حجم استيعاب البيانات، وتخزين داخل مقار الجهات باهظ التوسعة.

كما أن كثيراً من هذه المنصات يشجع نهج «اجمع كل شيء» انطلاقاً من اعتقاد مفاده أن مزيداً من البيانات يعني اكتشافاً أفضل. غير أن هذا النهج يفضي إلى تكاليف متصاعدة، وإلى محللين يجتهدون في معالجة تنبيهات ضئيلة السياق.

أضف إلى ذلك الأعباء التشغيلية لتحديث محللات السجلات (Parsers)، وضبط قواعد الاكتشاف، وترقيات المنتج، فتجد الكلفة الإجمالية لإبقاء نظام SIEM تقليدي قيد التشغيل في صعود متواصل، من دون أن تتحسن قيمته الأمنية بالتناسب.

كيف يبدو ذلك داخل مركز العمليات

تقود تكاليف الاستيعاب والتخزين المتصاعدة إلى سلسلة من المفاضلات داخل المركز.

فقد تُستبعد بعض مصادر السجلات تقليصاً لإنفاق الاستيعاب والتخزين، وقد يُحتفظ بأخرى مدداً أقصر. وكلا القرارين يُحدث فجوات في الرؤية قد تمس التحقيقات، لا سيما حين تكون السجلات المطلوبة لم تخضع للجمع أصلاً، أو انقضت مدة الاحتفاظ بها، أو لم تكن متاحة بصيغة قابلة للبحث.

وتغدو نقاشات الموازنة بدورها أشد عسراً؛ فبدل التركيز على تغطية الاكتشاف وجودة التحقيقات وخفض المخاطر، ينزاح الحديث نحو حجم الاستيعاب، وحدود التخزين، ومصادر البيانات التي تقدر الجهة على تحمل كلفة الإبقاء عليها.

كيف يسهم التحديث في الحل

يستطيع التحديث تغيير طريقة التعامل مع بيانات القياس عن بعد منذ لحظة دخولها خط معالجة البيانات في المركز؛ فالتصميم القائم على أولوية خط المعالجة، مثلاً، لا يتعامل مع الاستيعاب بوصفه مجرد استقبال للسجلات، ولكن بوصفه النقطة التي يجري فيها إثراء بيانات القياس عن بعد، وترشيحها، وفهرستها، وتوجيهها، وتهيئتها للتخزين، والبحث، والتحقيق، والالتزام.

وهذا التصميم مدعوم عادة بالآليات الآتية:

- **إثراء البيانات أثناء حركتها:** يضيف سياقاً كمعلومات التهديدات الاستباقية (Threat Intelligence)، وبيانات الأصول، وهويات المستخدمين، وغيرها من التفاصيل التي تعين المحللين على تفسير الأحداث بدقة أكبر.
- **الجمع الانتقائي:** يتيح للمركز التركيز على بيانات القياس عن بعد الأوثق صلة بالاكتشاف والتحقيق والالتزام، بدل جمع كل شيء افتراضياً.
- **الفهرسة الكاملة عند الاستيعاب:** تمكّن المحللين من البحث في بيانات القياس عن بعد بسرعة فور انطلاق التحقيق.

- **التخزين بسعة سحابية:** يسمح بتنامي حجم السجلات من دون توسعات عتادية متكررة، فتغدو سعة التخزين وكلفته أيسر ضبطاً.
- **الاحتفاظ طويل الأمد بكلفة ميسورة:** يدعم متطلب الضوابط الأساسية للأمن السيبراني (ECC) بالاحتفاظ بالسجلات مدة 12 شهراً، لا سيما حين يلزم إعادة بناء الأدلة بعد شهور من وقوع الحدث.

إن التحديث يحسن الإجابة عن سؤال يخص اقتصاديات التشغيل:

هل يستطيع المركز الاحتفاظ ببيانات القياس عن بعد التي يحتاج إليها للاكتشاف والتحقيق والالتزام من دون فجوات رؤية تمليها الكلفة؟



3 معضلة السرعة:

الاكتشاف والاستجابة في ظل تدقيق الالتزام بضوابط ECC وOTCC

وجد تحليل حديث لسوق دول مجلس التعاون الخليجي، استند جزئياً إلى معلومات مراكز عمليات في دبي والرياض، أن سرعة إتمام الهجمات ارتفعت 65% في الربع الأول من عام 2026، وأن عدداً من الاختراقات الكبرى بلغ أثره التشغيلي في أقل من 40 ساعة.[2]

وهذا يمنح فرق المراكز وقتاً أقل لاكتشاف نشاط التهديد والتحقيق فيه وتصعيده واحتوائه مع صون الأدلة، ويضغط كذلك الوقتَ المتاح لاتخاذ قرارات يمكن الدفاع عنها، لا سيما حين يعمل المركز تحت حجم تنبيهات مرتفع وقدرة محدودة من كبار المحللين.

وفي دراسة أجرتها Forrester Consulting عام 2025 بتكليف من Google Cloud، قال 82% من كبار قادة تقنية المعلومات والأمن السيبراني إنهم قلقون أو شديدو القلق من أن جهاتهم قد تفوّت تهديدات أو حوادث حقيقية بسبب كم التنبيهات والبيانات الذي يواجهونه، فيما أفاد 72% بأن جهاتهم لا تزال في الغالب تتحرك برد الفعل حيال التهديدات السيبرانية.[3]

ففي بيئة خاضعة لنطاق الضوابط الأساسية للأمن السيبراني، يعمل هذا التضيّق في النافذة الزمنية، مقترناً بحجم التنبيهات، ضد التزامات المراقبة المستمرة وآليات الاكتشاف والاستجابة المحددة؛ إذ يجب أن يكون المركز قادراً على رؤية النشاط ذي الصلة وتقييمه وتصعيده وصون أدلته بسرعة تكفي لدعم عملية استجابة يمكن الدفاع عنها. فإذا تخلفت سرعة التحقيق عن سرعة الهجوم، فقد يتعثر المركز في إبراز الأدلة اللازمة لإثبات أن الضوابط عملت بفاعلية.

%82 من كبار قادة تقنية المعلومات والأمن السيبراني قلقون أو شديدو القلق من أن جهاتهم قد تفوّت تهديدات أو حوادث حقيقية بسبب كم التنبيهات والبيانات الذي يواجهونه

أما في بيئة خاضعة لنطاق ضوابط الأمن السيبراني للأنظمة التشغيلية (OTCC)، فالرهانات أعلى؛ فالحادثة السيبرانية في بيئة التقنية التشغيلية قد تمس الصحة والسلامة والظروف البيئية واستمرارية الخدمة والعمليات المادية. ومن ثم لا يكون الحكم على حسن توقيت الاستجابة بمجرد اتباع المركز للإجراءات، ويتعداه إلى مدى سرعته في التحرك لتقليص الأثر التشغيلي؛ فالتأخير الذي قد لا يتعدى ملاحظة تدقيق في بيئة تقنية معلومات قد يتحول إلى حدث سلامة أو انقطاع توافر في مصفاة نفط.

2 "Sovereignty, resilience top GCC's new cybersecurity priorities, says Help AG", tahawultech.com. https://www.tahawultech.com/news/sovereignty-resilience-top-gccs-new-cybersecurity-priorities-says-help-ag/

3 Forrester Consulting, Threat Intelligence Benchmark: Stop Reacting; Start Anticipating — دراسة بتكليف من Google Cloud، يوليو 2025. https://services.google.com/fh/files/misc/forrester_state_of_threat_intel_2025.pdf

كيف يبدو ذلك داخل مركز العمليات

تظهر الأعراض أولاً في طابور التنبيهات؛ فالمحللون يواجهون أحجاماً كبيرة من التنبيهات وبيانات التحقيق، ولذا فالمشكلة أكبر من مجرد أن الهجمات باتت أسرع، إذ إن الفريق بات يملك وقتاً أقل لفصل الحوادث الحقيقية عن الضجيج، وجمع الأدلة، وتقرير الخطوة التالية.

وقد تقبع الحوادث في ركام من التنبيهات غير المعالجة أو المعالجة جزئياً؛ لأن الطابور أعمق مما تستطيع كل مناوبة تصفيته. ويستنفد المحللون شطراً مفرطاً من التحقيق في جمع السجلات، والتنقل بين الأنظمة، وإعادة بناء الخطوط الزمنية، والتثبت من السياق الأولي قبل التمكن من اتخاذ قرار. وتتزاحم التنبيهات عالية الخطورة مع تنبيهات ضئيلة السياق، ولا تعكس تصنيفات الخطورة الثابتة دوماً الخطر الفعلي على الجهة.

وحين تتبعثر الأدلة عبر الأنظمة، يصبح إعداد تقارير الالتزام بدوره أبطأ وأعسر دفاعاً.

كيف يسهم التحديث في الحل

يسهم التحديث بتقصير المسافة بين التنبيه والاستجابة.

وثمة قدرات لها الأثر الأكبر هنا:

- **الفرز وترتيب الأولويات بمساندة الذكاء الاصطناعي:** يجمع الإشارات المترابطة، ويكتم الضجيج الواضح، ويرتب التنبيهات وفق السلوك المرصود، والهوية، وأهمية الأصل، وسياق الأعمال؛ فيعين المركز على البدء بالتنبيهات الأرجح تمثيلاً لخطر حقيقي.
- **إعادة البناء المؤتمتة للخط الزمني للأحداث:** تختصر الوقت الذي يقضيه المحللون في حياكة الأحداث عبر مصادر SIEM والأجهزة الطرفية والهوية والسحابة والشبكة والتقنية التشغيلية؛ فيتضح للفريق ما جرى، ومتى جرى، وأي المستخدمين، أو الأجهزة المضيفة، أو التطبيقات، أو الأصول التشغيلية كانت طرفاً فيه.
- كتيبات الاستجابة الجاهزة، تحوّل خطوات التصعيد والاحتواء والإبلاغ والتعامل مع الأدلة الشائعة إلى مسارات عمل قابلة للتكرار، بما يدعم تحركاً أسرع ونتائج أكثر اتساقاً.
- **إدارة الحالات مع تحصيل الأدلة بحكم التصميم:** تلتقط سجل التحقيق لحظة إنجاز العمل، بدل إرغام الفريق على إعادة بنائه لاحقاً. وذاك أمر جوهري في ظل تدقيق الالتزام بضوابط ECC وOTCC؛ إذ يجب أن يكون المركز قادراً على أن يُظهر أنه استجاب فحسب، علاوة على ما الذي رآه، وما الذي قرره، ومن الذي تصرف، ومتى تم اتخاذ الإجراء، وما الأدلة التي تسند الاستجابة.

إن التحديث يحسن الإجابة عن سؤال يخص جاهزية الاستجابة:

هل يستطيع المركز تمييز الخطر الحقيقي، والتحرك بسرعة تكفي لتقليص الأثر، وصون أدلة يمكن الدفاع عنها قبل أن تسبق سرعة الهجوم التحقيق؟

4 المركز المُدار خياراً افتراضياً:

الترخيص الإلزامي يغير قرار الشراء

يضع «الإطار التنظيمي لترخيص تقديم خدمات مركز عمليات الأمن السيبراني المُدار» الصادر عن الهيئة الوطنية للأمن السيبراني (NCA) اشتراطات صارمة على مقدمي الخدمات المرخصين من المستوى الأول، منها حد رأسمالي قدره 50 مليون ريال سعودي، وإلزام بإسناد أدوار المحللين إلى مواطنين سعوديين. كما يوجب بقاء مرافق المراقبة ومعالجة البيانات داخل المملكة، بما يحد من إمكانية تقديم خدمات المركز المُدار من خارجها.

أما مقدمو الخدمة المرخصون، فمن المنتظر منهم كذلك الوفاء بمؤشرات أداء رئيسة محددة لسرعة الاكتشاف ودقته، وتغدو تلك المؤشرات جزءاً من تقييم الخدمة المُدارة نفسها. ويمتد أثر هذه الإلزامات إلى ما هو أبعد من مقدمي الخدمة أنفسهم.

فمع تحول خدمات المراكز المُدارة إلى نموذج تشغيل افتراضي لدى كثير من الجهات السعودية، بات نظام الترخيص يصوغ طريقة شراء تقنيات مراكز العمليات في السوق بأسرها؛ فالمشتريات انتقلت من كونها تقييماً فنياً خالصاً، لتقييم للترخيص والالتزام أولاً، وتقييم فني ثانياً.

كيف يبدو ذلك في دورة الشراء

تبدأ دورات الشراء بمرشح الترخيص: هل يستطيع مقدم الخدمة، والمنصة التي يقوم عليها، العمل أصلاً ضمن متطلبات الهيئة؟ فالموردون الذين لا يملكون بنية تحتية داخل المملكة هم مستبعدون قبل أن يتسنى للمشترين استعراض قوائم خصائصهم.

ويُصار إلى إدراج التزامات مؤشرات الأداء لسرعة الاكتشاف ودقة التنبيهات في اتفاقية الخدمة، فتغدو تعاقدية لا طموحات معلنة. ولذا يجب أن تولّد المنصة تلك المؤشرات آلياً، بدل ترك الفريق يعيد بناءها يدوياً في كل دورة إبلاغ.

كيف يسهم التحديث في الحل

يسهم التحديث بدمج متطلبات ترخيص الهيئة في نموذج تشغيل المركز منذ البداية؛ ففي سياق المركز المُدار، يلزم أن تدعم منصة مقدم الخدمة وبنيته التحتية ونموذج توظيفه ومسارات إبلاغه نظام الترخيص قبل اعتبار الخدمة قابلة للاستمرار أصلاً.

وتتوقف تلك الجاهزية على عدة قدرات:

- **توطين البيانات داخل المملكة:** يضمن بقاء بيانات المراقبة وتخزين السجلات والمعالجة داخل المملكة، فيغدو الالتزام بالتوطين قدرة أساسية، أي أهم من كونه مجرد استثناء مفصل حسب الطلب.
- **وحدات التزام متوائمة مع متطلبات الهيئة:** تقلص الجهد اليدوي اللازم لمواءمة عمليات المركز مع الضوابط التنظيمية، لا سيما حيث يتعين على مقدمي الخدمة إثبات الوفاء بالتزامات المراقبة والاستجابة.
- **تقارير مؤشرات الأداء الرئيسة المدمجة في المنصة:** تعين على تتبع سرعة الاكتشاف وأداء الاستجابة ودقة التنبيهات وسائر مقاييس الخدمة التي قد تندرج في اتفاقيات المراكز المُدارة.
- **قدرة دعم وتدريب محلية:** تتيح لمقدمي الخدمة دعماً فنياً وتمكيناً وموارد لتطوير المحللين داخل المملكة، مما يلزم لاستدامة الخدمة في ظل متطلبات التوطين.

- **مرونة النشر:** تمكّن مقدمي الخدمة والمشترين من تلبية متطلبات عملاء متباينة، بما فيها البيئات السيادية والسحابية والهجينة، من دون فرض نموذج تشغيل واحد.

إن التحديث يحسّن الإجابة عن سؤال حاسم في المشتريات:

هل تستطيع خدمة المركز المُدار هذه إبقاء العمليات والبيانات داخل المملكة، والوفاء بتوقعات ترخيص الهيئة، وتحويل التزامات مؤشرات الأداء إلى تقارير قابلة للتدقيق من دون جمع يدوي للأدلة؟



5 مشتريات يقودها الالتزام:

حين تغربل الأطرُ الموردين

ليس ترخيص المراكز المُدارة الفيصل الوحيد المؤثر في قرارات شراء تقنيات مراكز العمليات؛ فنظام الترخيص يحسم ما إذا كان مقدم الخدمة ومنصته قادرَين على العمل ضمن متطلبات الهيئة للمراكز المُدارة. لكن ما إن يتم اجتياز اختبار الأهلية هذا، حتى يواجه المشترون مرشّحاً ثانياً: هل تستطيع المنصة دعم الالتزامات التنظيمية التي تحكم المركز بعد النشر؟

فقوانين وتنظيمات الأمن السيبراني وخصوصية البيانات، مثل ECC وOTCC وإطار الأمن السيبراني للبنك المركزي السعودي (SAMA CSF) ونظام حماية البيانات الشخصية (PDPL)، قلّما تسير في مسارات منفصلة؛ إذ تلتقي في كثير من الجهات السعودية عند الأنظمة نفسها ومصادر السجلات نفسها وسجلات التدقيق نفسها.

فمؤسسة مالية لديها بيانات عملاء وبنية تحتية للفروع وأجهزة صراف آلي وعمليات مراكز بيانات، مثلاً، قد يلزمها أن تفي في آن واحد بمتطلبات الأمن السيبراني للقطاع المالي، والتزامات الخصوصية، وضوابط الهيئة، وتوقعات المراقبة للأنظمة التي تسند عملياتها المادية والرقمية.

ونتيجة لذلك، تصبح الجاهزية للتدقيق جزءاً من الملاءمة الفنية؛ إذ انتقل تقييم منصة مركز العمليات من مدى إجادتها اكتشاف التهديدات أو البحث في البيانات أو عرض لوحات المعلومات فحسب، إلى أن يكون لزاماً عليها أيضاً إظهار قدرتها على الاحتفاظ بما سيطلبه المنظمون والمدققون وفرق الالتزام الداخلية بعد النشر وتنظيمه وإبرازه: من أدلة، وتقارير، وسجلات وصول، وخطوط زمنية للحوادث، وخرائط ربط للضوابط.

كيف يبدو ذلك في دورة الشراء

عند إعداد القوائم المختصرة، كثيراً ما يفضّل المشترون مقدمي الخدمة القادرين على إظهار جاهزية محلية إلى جانب القدرة الفنية؛ فقد تبلي منصة أداء جيداً في مقارنة عالمية، ثم تواجه مع ذلك عقبات في المشتريات السعودية إن لم يوائم نموذج نشرها أو توثيقها أو مسار تعاقدها أو بنية دعمها المتطلبات المحلية.

وقد يمتد العبء إلى ما بعد الاختيار؛ فتهيئة الالتزام قد تستغرق شهوراً إذا تعين بناء خرائط الربط بالأطر والتقارير ومسارات الأدلة يدوياً. وبدل التفرغ للاكتشاف والاستجابة، قد يضطر المحللون إلى إنفاق وقت معتبر في تجهيز أدلة على أن الضوابط تعمل كما هو مطلوب.

وقد يلزم تكرار العمل نفسه عبر أنشطة التزام مختلفة؛ فسجلات الوصول التي يتوقعها نظام حماية البيانات الشخصية وأدلة المراقبة التي يفحصها البنك المركزي السعودي قد تخص الأنظمة ومصادر السجلات ذاتها. لكن من دون ربط موحد بين الضوابط وبيانات القياس عن بعد والتقارير، يتحول كل تدقيق إلى عملية جمع أدلة مستقلة.

كيف يسهم التحديث في الحل

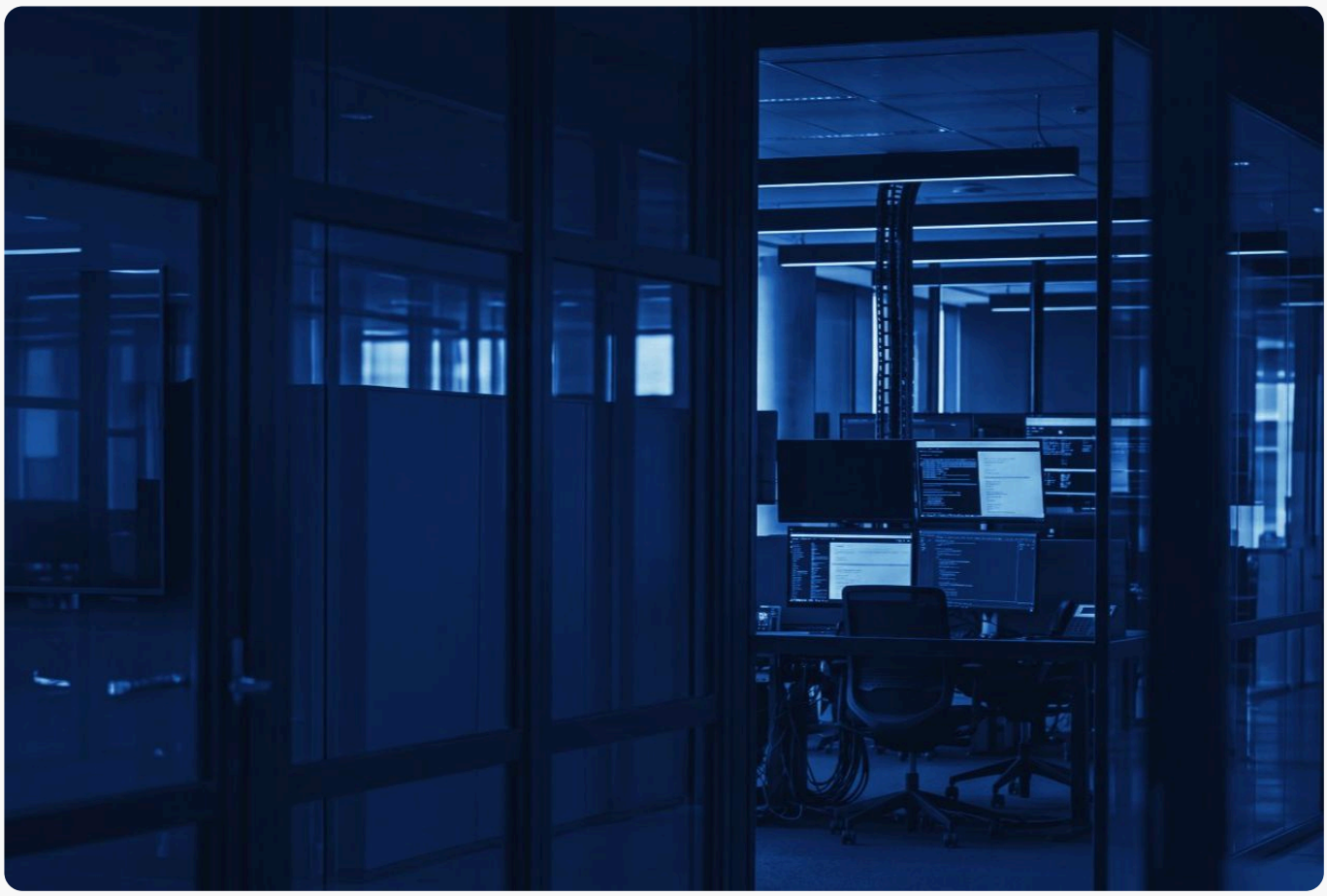
يسهم التحديث بمعاملة الالتزام بوصفه متطلباً معمارياً؛ فينبغي على منصة المركز الحديثة أن تيسر رؤية الضوابط المنطبقة، وبيانات القياس عن بعد التي تسندها، ومواضع تخزين الأدلة، والفجوات التي ما زالت بحاجة إلى سد.

ويعني ذلك البحث عن قدرات من قبيل:

- **ربط الأطر التنظيمية ببيانات القياس عن بعد:** يصل المتطلبات التنظيمية بمسارات عمل المركز ومصادر السجلات والتقارير ومسارات الأدلة التي تسندها، فيتبين للفريق أي الضوابط مغطاة وأين تبقى فجوات الأدلة.
- **الجمع المؤتمت للأدلة وإعداد التقارير:** يقلص الجهد اليدوي اللازم للتحضير للتدقيق، ويحول تقارير الالتزام إلى مسار عمل قابل للتكرار بدل اندفاع متكرر ومتجدد في كل مرة.
- **مرونة النشر:** تدعم البيئات داخل مقار الجهات والسحابة السيادية والبيئات الهجينة، لتبقى البيانات الخاضعة للتنظيم حيث يتوقع كل إطار أو متطلب من متطلبات التعامل مع البيانات بقاءها.
- **التوثيق بالعربية وبلغتين:** يمد فرق المشتريات والالتزام والتشغيل بالمواد التي تحتاج إليها لتقييم المنصة واعتمادها وتشغيلها بمصداقية في السوق السعودية.

إن التحديث يحسّن الإجابة عن سؤال يخص جاهزية الالتزام:

هل يستطيع المركز إثبات وفاء ضوابطه بالتزامات ECC وOTCC وSAMA CSF وPDPL من دون أن يتحول كل تدقيق إلى مشروع يدوي لجمع الأدلة؟



6 الواقع الهجين:
حين تلتقي هيمنة الاستضافة الداخلية بالتحليلات السحابية الأصيلة

مسنودة بسنوات من الاستثمار الرأسمالي ومعززة بأفضليات السيادة على أحمال العمل الحساسة، لا يزال أكثر من 70% من عمليات نشر الأمن السيبراني في المملكة داخل مقار الجهات. وفي الوقت نفسه، يواصل الطلب على الاكتشاف بمساندة الذكاء الاصطناعي وتحليل السلوكيات ومسارات التحقيق القابلة للتوسع صعوده، إذ من المتوقع أن تبلغ المراقبة المدعومة بالذكاء الاصطناعي 94% من الجهات السعودية الكبرى بحلول عام 2026.

ويوسع هذا التحول أيضاً محيط الهوية؛ ففي استطلاع Team8 لقادة الأمن (CISO Village Survey) لعام 2025، الذي شمل أكثر من 110 من قادة الأمن، صنف 37% تأمين وكلاء الذكاء الاصطناعي بوصفه أشد شواغلهم المرتبطة بالذكاء الاصطناعي إلحاحاً.[4] فمع إدخال الجهات مزيداً من الهويات غير البشرية والنشاط ذاتي التحرك، تحتاج المراكز إلى ربط تحليلي متسق للسلوك عبر المستخدمين وحسابات الخدمة والتطبيقات ووكلاء الذكاء الاصطناعي، أينما وقع ذلك النشاط.

ويولّد هذان الشرطان توتراً معمارياً؛ فالقدرات الإضافية التي بات كثير من مديري المراكز ينشدونها كثيراً ما تتطلب مستويات من التوسع والتكامل بين الأنظمة والأتمتة لم تُصمم كثير من عمليات نشر SIEM التقليدية داخل مقار الجهات لتقديمها بكفاءة. ومع ذلك، قليل من الجهات من يسوغ شطب استثمار قائم عامل في نظام SIEM، وأقل منها من يستطيع نقل جميع بيانات المركز ومساراته وتحليلاته إلى نموذج سحابي خالص في ظل القيود التنظيمية والسيادية الراهنة.

%70

لا يزال أكثر من 70% من عمليات نشر الأمن السيبراني في المملكة داخل مقار الجهات

%94

من المتوقع أن تبلغ المراقبة المدعومة بالذكاء الاصطناعي 94% من الجهات السعودية الكبرى بحلول عام 2026

%37

صنف 37% من قادة الأمن تأمين وكلاء الذكاء الاصطناعي بوصفه أشد شواغلهم المرتبطة بالذكاء الاصطناعي إلحاحاً

ولا تملك معظم المراكز حل هذا التوتر باختيار نموذج نشر خالص داخل المقار أو خالص في السحابة؛ فالهجين، لدى كثير من المراكز السعودية، هو المسار الأكثر عملية. ويكمن التحدي في جعل هذا النموذج أكثر تماسكاً وترابطاً وفاعلية.

4 Team8, CISO Village Survey 2025.
https://19935129.fs1.hubspotusercontent-na1.net/hubfs/19935129/CISO_Survey%202025_v10.pdf

كيف يبدو ذلك داخل مركز العمليات

قد تترك المعمارية الهجينة عمليات المركز موزعة على أنظمة منفصلة؛ فتبقى منصات المقار مسؤولة عن التسجيل الأساسي والبيانات الخاضعة للتنظيم وأدلة الالتزام، فيما يتم استحداث أدوات سحابية للتحليلات والبحث القابل للتوسع وحالات الاكتشاف الأحدث. وقد تكون كل مجموعة أدوات نافعة في ذاتها، لكن كلاً منها لا يرى إلا جزءاً من البيئة.

وحين لا تتكامل هذه الأنظمة جيداً، يضطر المحللون إلى التنقل بين لوحات تحكم متعددة لمتابعة تحقيق واحد؛ فقد يبحثون في منصة عن نشاط المقار، وفي أخرى عن النشاط السحابي، وفي ثالثة عن ملاحظات الحالة أو أدلة التقارير. وتتباطأ التحقيقات لأن تسلسل الأحداث يلزم إعادة بنائه يدوياً عبر الأنظمة.

ويزداد الانفصام والتجزؤ وضوحاً في الحوادث العابرة للبيئات؛ فبيانات هويات دخول مخترقة في بيئة المقار ثم يجري استخدامها لاحقاً ضد حمل عمل سحابي قد لا تحظى بالأولوية سريعاً إذا كانت الأحداث ذات الصلة خاضعة للتخزين والبحث والتحليل على حدة. فقد يملك المركز بيانات القياس عن بعد التي يحتاج إليها، لكن من دون سياق مشترك يكفي لربطها بسرعة.

كيف يسهم التحديث في الحل

يسهم التحديث بجعل العمليات الهجينة أكثر تماسكاً. وليس الهدف إرغام كل حمل عمل أو مصدر سجلات أو مسار تحقيق على بيئة واحدة، بل منح المراكز العاملة عبر أنظمة المقار والسحابة طريقة مشتركة لصون الرؤية، وربط بيانات القياس عن بعد، والتحقيق في الحوادث باتساق عبر البيئتين.

ويتطلب ذلك عدة قدرات:

- **رؤية عابرة للبيئات:** تمنح المحللين مشهداً موحداً للنشاط ذي الصلة عبر أنظمة المقار والسحابة والبيئات الهجينة، فتقل الحاجة إلى التنقل بين لوحات تحكم منفصلة أثناء التحقيق.
- **سياق مشترك لبيانات القياس عن بعد:** يعين المركز على تفسير الأحداث باتساق عبر البيئات، فيتسنى ربط بيانات الهوية والأصول والتنبيهات والسجلات خلال التحقيق وإعداد التقارير.
- **استمرارية التحقيق:**
تتيح للمحللين تتبع الحادثة وهي تعبر حدود البنى التحتية، بدل إعادة بناء تسلسل الأحداث يدوياً كلما انتقل النشاط بين الأنظمة.
- **خيارات نشر مرنة:** تسمح بأن تعكس معمارية المركز حساسية البيانات، والنطاق التنظيمي، وتوقعات السيادة، والاستثمارات القائمة في البنية التحتية.

إن التحديث يحسّن الإجابة عن سؤال يخص المعمارية الهجينة:

؟ هل يستطيع المركز التحقيق عبر بيئات المقار والسحابة من دون إحداث فجوات في الرؤية، أو ازدواج في مسارات العمل، أو فرض هجرة مربكة؟



قوى متشابكة وجذر واحد

ولا تعمل هذه القوى الست كلٌّ بمعزل عن الأخرى؛ فنقص الكفاءات يبطئ الاستجابة، فيعمّق معضلة السرعة. وضغط الكلفة يُحدث فجوات الرؤية التي تجعل إثبات الالتزام أعسر. وقواعد الترخيص والمشتريات تضيّق مجال الحلول المتاحة لمعالجة أي من ذلك. ومدير المركز الذي يحاول حل كل قوة على حدة، بأداة متخصصة هنا وتعيين جديد هناك، ينتهي به المطاف إلى إدارة ستة إصلاحات ناقصة بدل قدرة واحدة متماسكة. ويعرض الجدول التالي القوى الست في لمحة واحدة، بأثر كل قوة منها في التشغيل، واستجابة التحديث التي تعالجها.

الجدول 2: القوى الست في لمحة واحدة. كل قوة، وأثرها التشغيلي الرئيس، واستجابة التحديث التي تعالجها.

القوة	أثرها في عمليات المركز	استجابة التحديث
1 **معادلة الكفاءات**	بطء تأهيل الملتحقين الجدد؛ واستنزاف قدرات الكبار في أعمال الفرز الروتينية؛ وتفاوت جودة التحقيقات	التحقيق الموجه: بحث باللغة الطبيعية، وخطوط زمنية مؤتمتة، واقتراح للخطوات التالية، ورسم خرائط التغطية وفق ATT&CK
2 **اقتصاديات SIEM**	إنفاق على الاستيعاب يتجاوز القيمة الأمنية؛ وفجوات رؤية تمليها الكلفة	معمارية قائمة على أولوية خط المعالجة: إثراء عند الاستيعاب، وجمع انتقائي، وفهرسة كاملة، وتخزين قابل للتوسع سحابياً
3 **السرعة في ظل ECC وOTCC**	بطء الفرز؛ وإجهاد التنبيهات؛ وتلكؤ الاستجابة والتقارير	فرز بمساندة الذكاء الاصطناعي، وخطوط زمنية مؤتمتة، وكتيبات استجابة جاهزة، وإدارة حالات مع تحصيل الأدلة بحكم التصميم
4 **المركز المُدار خياراً افتراضياً**	متطلبات الترخيص تغربل المشتريات قبل الملاءمة الفنية	توطين البيانات داخل المملكة، ووحدات التزام متوائمة مع متطلبات الهيئة الوطنية للأمن السيبراني، ودعم محلي، وتقارير مؤشرات أداء مدمجة في المنصة
5 **مشتريات يقودها الالتزام**	شهور من التهيئة بعد النشر؛ والتحضير للتدقيق يستهلك ساعات المحللين	ربط الأطر التنظيمية ببيانات القياس عن بعد، وجمع مؤتمت للأدلة، ومرونة في النشر، وتوثيق ثنائي اللغة
6 **الواقع الهجين**	بيئات متجزئة؛ وتحقيقات تتعثر بين الأنظمة	رؤية عابرة للبيئات، وسياق مشترك لبيانات القياس عن بعد، واستمرارية التحقيق، ومرونة في النشر

وما تشترك فيه القوى الست هو جذر معماري، وذلك يشير إلى إجابة معمارية: معمارية واحدة لمركز العمليات تعالج القوى الست دفعة واحدة، ضمن واقع المملكة التنظيمي وبنيتها التحتية الهجينة. وذلك هو موضوع القسم التالي.



04

نهج المسارين لتحديث مراكز العمليات الأمنية في المملكة

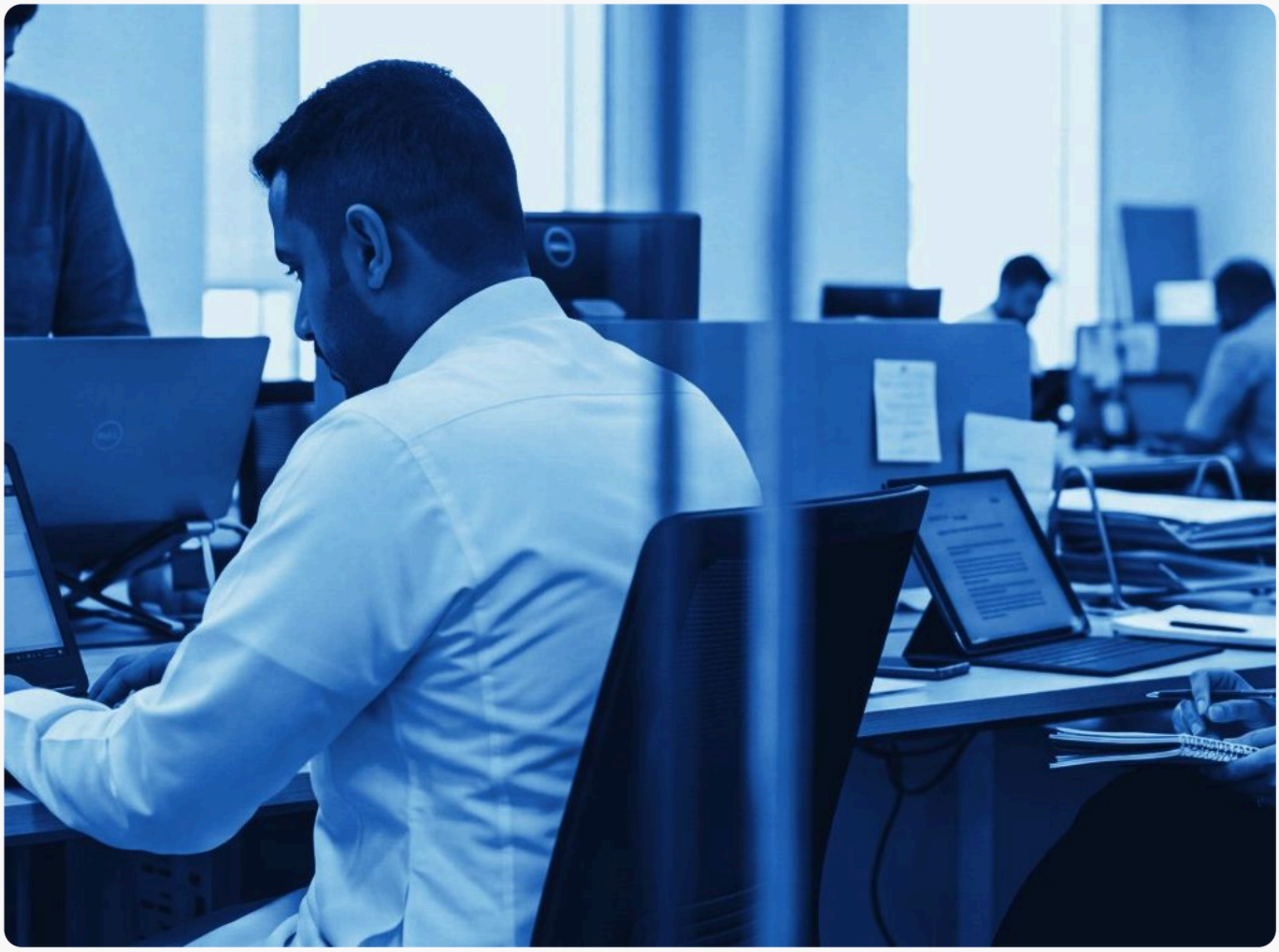
04

نهج المسارين لتحديث مراكز العمليات الأمنية في المملكة

اختُتم القسم الثالث بالقول إن القوى الست تشترك في جذر معماري، ومن ثم تستلزم إجابة معمارية. وهذا القسم يصف تلك الإجابة.

فليس ثمة نموذج نشر واحد يلائم السوق السعودية؛ إذ لا يزال أكثر من 70% من عمليات نشر الأمن السيبراني داخل مقار الجهات، وتُبقي متطلبات السيادة أحمال العمل المصنفة وأحمال البنية التحتية الحساسة هناك. وفي الوقت نفسه، يواصل الطلب على التحليلات المدفوعة بالذكاء الاصطناعي نموه، وهي قدرات يصعب تقديمها على نطاق واسع من بنية المقار وحدها.

والبنية المعمارية التي ترغم الجهات على الاختيار بين السيادة والتحليلات ستخفق في تخديم نصف السوق؛ ولذلك تدعم Exabeam مسارَين اثنين للنشر في المملكة، مع نموذج هجين للجهات التي تحتاج إلى الاثنين معاً.



طبقة موحدة للرؤية والتحليل

تحقيق واحد عبر البيئتين، دون الانتقال بين واجهات التحكم

المسار الأول

نشر سيادي داخل مقار الجهات

LogRhythm SIEM
استضافة ذاتية على بنية تحتية تتحكم بها الجهة

وحدة الالتزام بضوابط OTCC
تحقيق وتنبيه آنيان وفق الضوابط التي تحكم بيئات التقنية التشغيلية

LogRhythm Intelligence
يضيف تحليل السلوكيات إلى نظام SIEM المنشور في المقار، بالنماذج ذاتها العاملة على المنصة السحابية *

التقديم والدعم داخل المملكة
متاح ومدعوم عبر الشراكة مع شركة المعمر لأنظمة المعلومات (MIS)

يلائم الوزارات، والبنية التحتية الوطنية الحساسة، وأحمال العمل المصنفة وأحمال التقنية التشغيلية

المسار الثاني

سحابة داخل المملكة

Exabeam New-Scale Security Operations Platform
منطقة Google Cloud بالدمام (me-central2)

استيعاب على نطاق فائق
أكثر من مليوني حدث في الثانية، بنطاق يصعب على بيئات المقار التقليدية بلوغه بكفاءة

التحقيق بمساندة الذكاء الاصطناعي
تحقيق باللغة الطبيعية عبر Exabeam Nova، وإعادة رسم مؤتمتة لتسلسل الحوادث عبر Smart Timelines

تحليل سلوكيات أصلي في المنصة
يحدد السلوك المعتاد لكل مستخدم وكيان وينبّه إلى الانحرافات، ويرسم Outcomes Navigator خرائط التغطية وفق MITRE ATT&CK

يلائم الجهات التي تحتاج إلى استضافة بياناتها داخل المملكة، لكنها لا تحتاج إلى السيطرة المادية على البنية التحتية

النموذج الهجين | تعزيز القائم بدل استبداله

يبقى تسجيل الأحداث الأساسي، والبيانات الخاضعة للتنظيم، وأدلة الالتزام، على المنصة ذاتية الاستضافة.

* يضيف LogRhythm Intelligence تحليل السلوكيات، وتبقى المعالجة داخل المملكة.

تواصل الاستثمارات القائمة عملها، وتنمو القدرات حولها.

على المسارين كليهما، تستقبل المنصة بيانات السجلات، وتعالجها، وتخزنها، داخل المملكة العربية السعودية.

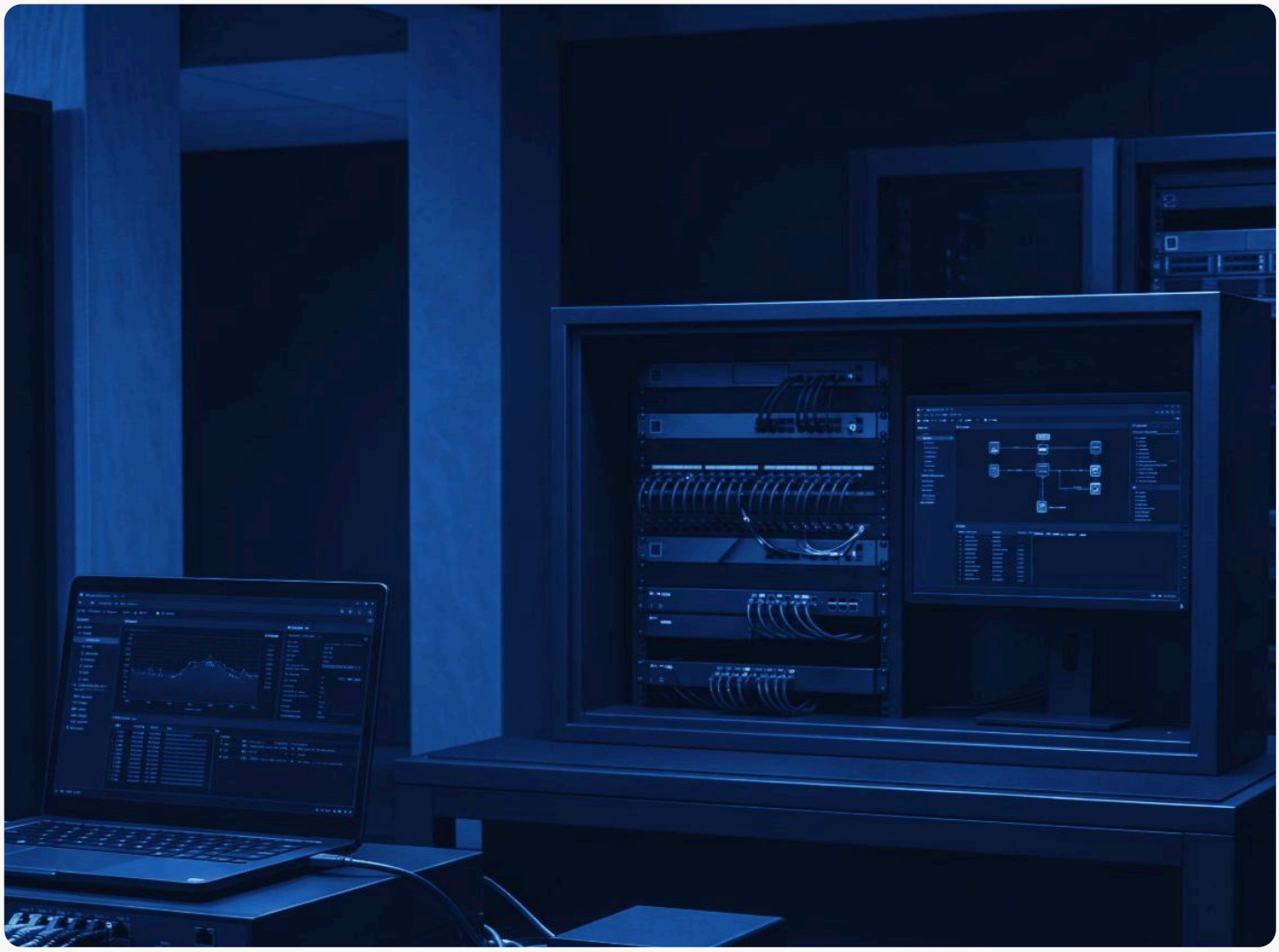
الشكل 2: معمارية المسارين: النشر السيادي داخل مقار الجهات، والسحابة داخل المملكة، والنموذج الهجين الجامع بينهما.

المسار الأول: نشر سيادي داخل مقار الجهات بنظام LogRhythm SIEM

يستهدف المسار الأول الجهات التي تشترط أو تفضل منصة ذاتية الاستضافة: الوزارات، ومشغلي البنية التحتية الوطنية الحساسة، والجهات العاملة في قطاعات مثل النفط والغاز التي تُبقي أشد أحمالها حساسية على بنية تحتية محصنة خاضعة لسيطرة محلية. ولهذه الجهات تقدم Exabeam نظام LogRhythm SIEM لإدارة معلومات الأمن والأحداث في صيغة نشر سيادي داخل مقار الجهة.

ويتكيف هذا المسار مع السوق السعودية بعدة عناصر؛ أولها وحدة التزام مخصصة بضوابط الأمن السيبراني للأنظمة التشغيلية الصادرة عن الهيئة الوطنية للأمن السيبراني (NCA OTCC Compliance Module)، توائم التحقيق والتنبيه الآنيين مع الضوابط التي تحكم بيئات التقنية التشغيلية في المملكة. وثانيها التقديم المحلي: فنظام LogRhythm SIEM متاح ومدعوم داخل المملكة عبر شراكة Exabeam مع شركة المعمر لأنظمة المعلومات (MIS)، وهي من كبريات شركات تقنية المعلومات السعودية؛ بما يلبي توقعات الدعم داخل المملكة التي بيّن جزء «مشتريات يقودها الالتزام» (ص21) أنها باتت شرطاً مرجحاً في المشتريات.

أما تحليل السلوكيات فمتاح على هذا المسار عبر LogRhythm Intelligence، الذي يمد نظام SIEM المنشور في المقار بنماذج تعلم الآلة ذاتها العاملة على المنصة السحابية. ويصف النموذج الهجين، الذي يأتي بيانه لاحقاً، طريقة هذا النشر.



المسار الثاني: سحابة داخل المملكة بمنصة Exabeam New-Scale

يستهدف المسار الثاني الجهات التي تسعى إلى تحليلات على نطاق سحابي من دون إخراج البيانات من المملكة؛ فمنصة Exabeam New-Scale Security Operations Platform تعمل في منطقة Google Cloud بالدمام (me-central2)، وهي أولى مناطق Exabeam السحابية في الشرق الأوسط. يجري استقبال بيانات السجلات ومعالجتها وتخزينها داخل المملكة العربية السعودية، بما يفي بمتطلبات الهيئة الوطنية للأمن السيبراني لاستضافة البيانات داخل المملكة.

وفي الوقت ذاته، توفر المنصة قدرات يصعب على كثير من بيئات SIEM التقليدية داخل المقار تقديمها بكفاءة على نطاق واسع: استيعاب أكثر من مليوني حدث في الثانية، وتحقيق باللغة الطبيعية عبر Exabeam Nova، وإعادة رسم مؤتمتة لتسلسل الحوادث عبر Smart Timelines، ورسم خرائط تغطية الاكتشاف وفق إطار MITRE ATT&CK عبر Outcomes Navigator.

وتحليل السلوكيات قدرة متأصلة في هذه المنصة؛ فبدل مطابقة تواقيع معروفة، ترسم المنصة خط الأساس للسلوك المعتاد لكل مستخدم وكيان، ثم تنبه إلى الانحرافات ذات الدلالة. وهذا النموذج يناسب الهجمات التي تواجهها مراكز العمليات الأمنية فعلاً؛ إذ تظهر بيانات هويات الدخول المخترقة في 90% من الهجمات التي ترصدها r-tec، وهي شركة خدمات أمن سيبراني مقرها ألمانيا وشريكة Exabeam.[1]

فهذه ليست إصابات ببرمجيات ضارة يلتقطها الاكتشاف القائم على التواقيع، هي عمليات تسجيل دخول صحيحة يجري استعمالها على نحو غير مصرح به. والاكتشاف السلوكي مبني لهذا النمط تحديداً.

%90

تظهر بيانات هويات الدخول المخترقة في 90% من الهجمات التي ترصدها r-tec

أكثر من مليوني

حدث في الثانية



1 قصة عميل r-tec، Exabeam.
https://www.exabeam.com/customers/r-tec/

النموذج الهجين: تعزيز القائم بدل استبداله

لن تندرج معظم المنشآت السعودية بوضوح تحت مسار واحد، وليس عليها ذلك؛ فبالنسبة إلى الجهات الموصوفة في جزء «الواقع الهجين» (ص23)، ذات استثمارات SIEM عاملة في المقار وحاجات تحليلية متنامية، يظل التعزيز هو الطريق الواقعي.

فيبقى تسجيل الأحداث الأساسي والبيانات الخاضعة للتنظيم وأدلة الالتزام على منصة LogRhythm ذاتية الاستضافة، وتتم إضافة تحليل السلوكيات عبر LogRhythm Intelligence مع بقاء المعالجة داخل المملكة، ثم تتولى طبقة رؤية موحدة الربط التحليلي لبيانات القياس عن بعد عبر البيئتين، فيتسنى للمحللين متابعة التحقيق عبر الحد الفاصل بين المقار والسحابة من دون تبديل واجهات التحكم.

وتدعم الجدوى الاقتصادية هذا النموذج؛ فالتعزيز يجنب كلفة الاستبدال ذاتها. وتفيد NEC، وهي من عملاء حلول Exabeam التقنية، بانخفاض إجمالي كلفة الملكية بنسبة 35% نتيجة تعزيز الاستثمارات الأمنية القائمة بدل استبدالها.[2]

%35 انخفاض إجمالي كلفة الملكية بنسبة 35% نتيجة تعزيز الاستثمارات الأمنية القائمة بدل استبدالها

اختيار المسار: ما الذي يحدد الملاءمة

ليس تحديد المسار الملائم لجهة بعينها مسألة تفضيل، وهو متوقف على عوامل من قبيل حساسية البيانات، والنطاق التنظيمي، والبنية التحتية القائمة، وقدرات المحللين:

1 حساسية البيانات وتصنيفها

أحمال العمل المصنفة وأشد أنظمة البنية التحتية الوطنية الحساسة حساسية تشير إلى المسار السيادي داخل المقار. أما أحمال العمل التي توجب استضافة البيانات داخل المملكة من دون سيطرة مادية، فيمكن تشغيلها في منطقة الدمام.

2 النطاق التنظيمي

بيئات التقنية التشغيلية الخاضعة لنطاق OTCC تحقق أكبر استفادة من وحدة الالتزام المخصصة على المسار السيادي. أما الجهات المحكومة أساساً بالضوابط الأساسية للأمن السيبراني (ECC) أو إطار الأمن السيبراني للبنك المركزي السعودي (SAMA CSF) أو نظام حماية البيانات الشخصية (PDPL) فتستطيع الوفاء بالتزامات استضافة البيانات والمراقبة على أيٍّ من المسارين.

3 الاستثمار القائم في البنية التحتية

وجود نشر SIEM عامل يرجح كفة تعزيز القائم بدل استبداله. أما النظام الذي يقترب من نهاية عمره التشغيلي، أو المتعثر أصلاً في الكلفة أو التغطية، فيُضعف تلك الحجة.

4 تمرّس المحللين

الفرق التي يغلب عليها المحللون المبتدئون، الموصوفة في جزء «معادلة الكفاءات» (ص13)، هي الأكثر استفادة من قدرات التحقيق على المسار السحابي، التي تقلص الاعتماد على الخبرات الكبيرة الشحيحة.

2 دراسة حالة NEC، Exabeam.
https://www.nec.com.au/application/files/4716/8377/3621/exabeam-case-study-nec-australia.pdf

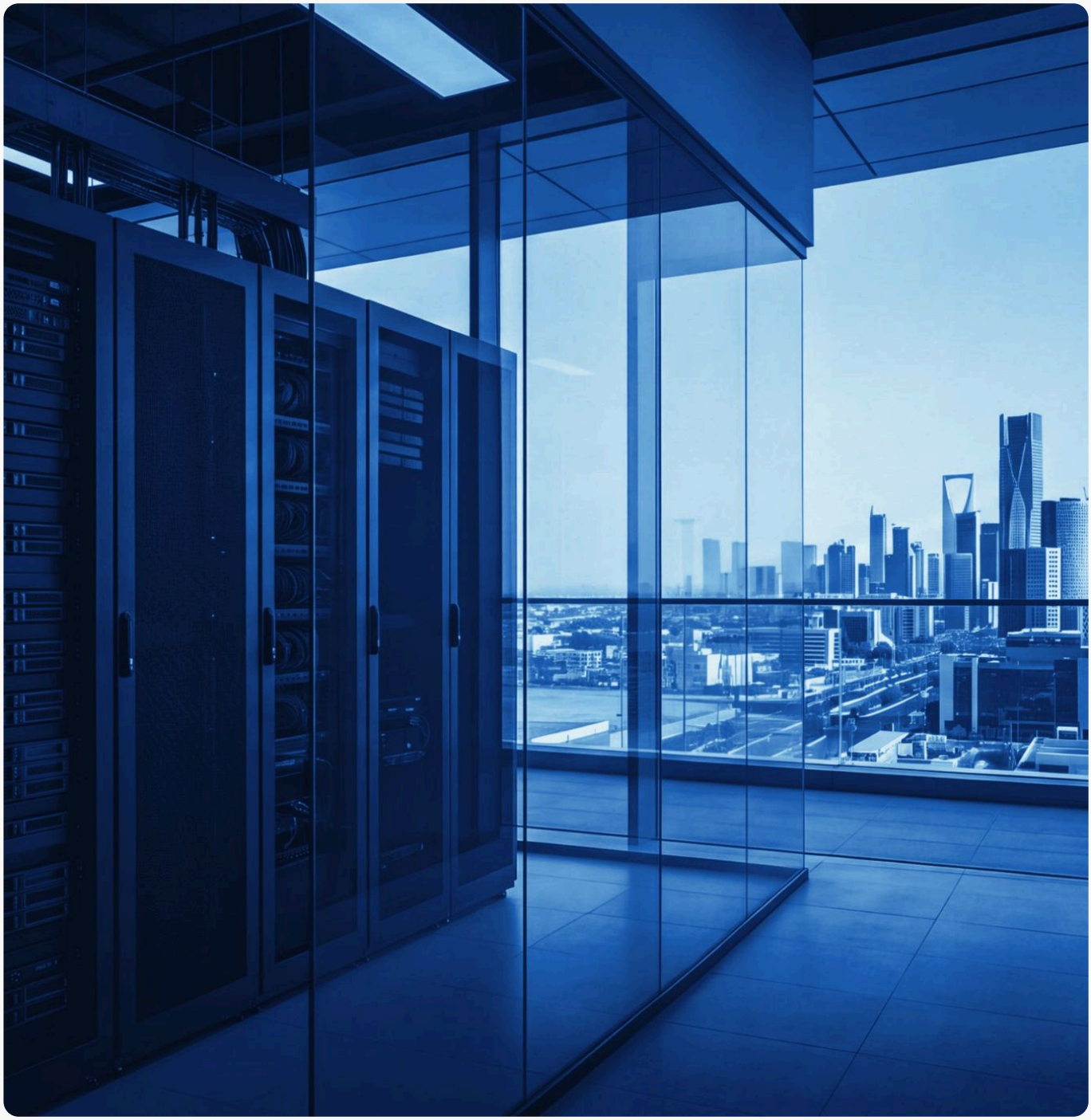


الشكل 3: مخطط تدفق قرار تعزيز القائم أو استبداله.

تحديث بلا اضطراب

أياً كان المسار المنطبق، فمبدأ النشر واحد: يمضي التحديث على مراحل، وليس فيه ما يستلزم إحلالاً كاملاً واستبدالاً؛ فبوسع الجهة أن تبدأ بإضافة طبقة تحليل السلوكيات فوق نظام SIEM القائم لديها، وأن تثبت القيمة في حالة استخدام أو اثنتين من الحالات عالية الخطورة، ثم تتوسع من هناك بإيقاعها الخاص. فتظل الاستثمارات القائمة تعمل فيما تُضاف حولها القدرات المدفوعة بالذكاء الاصطناعي.

تلك هي البنية المعمارية. ويقرن القسم التالي كل قوة من القوى الست الواردة في القسم الثالث بقدرة Exabeam التي تعالجها.





05

كيف تسدّ Exabeam الفجوات

05

كيف تسدّ Exabeam الفجوات

توفر معمارية المسارين الموصوفة في القسم الرابع الأساسَ لتحديث مراكز عمليات الأمن السيبراني عبر البيئات السحابية الأصيلة وذاتية الاستضافة والهجينة. غير أن قيمتها العملية تكمن في التحسينات التشغيلية التي تحدثها داخل المركز. ولبيان كيفية تحقق تلك التحسينات، يقرن هذا القسم قدرات Exabeam بالقوى التشغيلية الست المحددة في القسم الثالث.

معالجة معضلة القوى العاملة

تواجه المراكز السعودية نقصاً في المحللين المتمرسين وحدوداً لما تستطيع الفرق القائمة استيعابه من عمل في آن واحد. وتوسّع Exabeam Nova الطاقة التشغيلية عبر التعاضد بين الإنسان والوكلاء؛ إذ تضيف سبعة وكلاء ذكاء اصطناعي إلى طاقة المركز التشغيلية، يعملون على مدار الساعة طوال أيام الأسبوع جنباً إلى جنب مع المحللين البشر لإسناد البحث، والفرز، والتحقيق، وتقدير درجات خطورة التهديدات، وتحليل الوضع الأمني.

ومن بين هؤلاء، يسند وكيل البحث (Search Agent) التحقيقَ باللغة الطبيعية عبر بيئة السجلات كلها. ويقدم وكيل مساعد المحلل (Analyst Assistant Agent) السياقَ وتقدير درجات المخاطر والخطوات التالية الموصى بها قبل أن يشرع المحلل في الفرز التفصيلي، فيما يجمّع وكيل التحقيق (Investigation Agent) الأدلة والخطوط الزمنية السلوكية في حالة واحدة. وتعين هذه القدرات مجتمعة المحللين المبتدئين على الإسهام مبكراً، وتخفف الأعباء الروتينية عن الكوادر الكبيرة، وتتيح للمحللين المتمرسين التفرغ للقرارات التي تستلزم حصافة وسياق أعمال.

تحسين اقتصاديات SIEM

يتولى نموذج المعلومات الموحد لدى Exabeam (Common Information Model) توحيد صيغ بيانات القياس وتصنيفها وإثراءها لحظة دخولها المنصة. ويسرّع أكثر من 10,000 من محللات السجلات (Parsers) الجاهزة عملية ربط مصادر السجلات، ويقلص الجهد الهندسي المتواصل المقترن ببناء المحللات المخصصة وصيانتها. وتدعم معمارية New-Scale استيعاباً يتجاوز مليوني حدث في الثانية، فتستطيع الجهات مواكبة أحجام بيانات القياس المتنامية من دون توسيع البنية التحتية التقليدية مرة بعد أخرى.

ولأن Exabeam قادرة على تعزيز نظام SIEM قائم بدل اشتراط استبداله الفوري، تستطيع الجهات إضافة التحليلات والأتمتة مع صون الاستثمارات العاملة، وتجنّب كلفة هجرة الاقتلاع والاستبدال واضطرابها.

تسريع الاكتشاف والاستجابة

يرسّخ تحليل السلوكيات لدى Exabeam النشاطَ المعتاد للمستخدمين والكيانات، ثم يُسند درجات خطورة إلى الانحرافات ذات الدلالة. وتتولى قدرتا Nova في تقدير درجات خطورة التهديدات (Threat Scoring) والتحقيق تجميعَ الاكتشافات المترابطة، وإبراز النشاط الأعلى خطورة، وجمع الأدلة الداعمة، وتوليد ملخص تحقيق مشفوع بالإجراءات الموصى بها. فيبدأ المحللون من حالة مرتبة الأولوية بدل تنبيه خام، بما يقصّر المسافة من الاكتشاف إلى استجابة يمكن الدفاع عنها.

إسناد نموذج تشغيل المراكز المُدارة

بالنسبة إلى مقدمي خدمات المراكز المُدارة، يجب أن تلائم القدرةُ الفنية نموذجَ الترخيص لدى الهيئة الوطنية للأمن السيبراني. فمنصة Exabeam New-Scale تعمل في منطقة Google Cloud بالدمام، مبقيةً المعالجة والتخزين السحابيين داخل المملكة. وتستطيع الجهات التي توجب تشغيلاً ذاتي الاستضافة استخدام LogRhythm SIEM، بما فيه وحدة الالتزام المخصصة لضوابط OTCC الصادرة عن الهيئة، مع تقديم ودعم محليين عبر MIS. ويتيح المساران لمركز مُدار خدمةَ عملاء متباينين في متطلبات السيادة والنشر من دون بناء نماذج تشغيل منفصلة.

تمتين الجاهزية للالتزام

تصل Exabeam بين المراقبة والتحقيق وتوليد الأدلة، بدل معاملة الالتزام تمريناً منفصلاً لإعداد التقارير. فوحدة OTCC تقدم إسناداً مهيأً مسبقاً لبيئات التقنية التشغيلية. ويرسم Outcomes Navigator خرائط تغطية الاكتشاف وفق إطار MITRE ATT&CK، ويستطيع ربط التغطية الأمنية بالمتطلبات التنظيمية، فيما تجمع مسارات التحقيق لدى Exabeam الآثارَ الرقمية الداعمة والأدلة المجموعة وملخصات الحالات في موضع واحد. كما تتيح مرونة النشر بقاء البيانات الخاضعة للتنظيم في البيئة الملائمة لتصنيفها وللإطار الذي يحكمها.



جعل العمليات الهجينة متماسكة

عبر البيئات السحابية الأصيلة وذاتية الاستضافة والهجينة، تعين Exabeam على الحفاظ على تجربة تحليلات وتحقيق متسقة؛ فبوسع Exabeam إضافة تحليل السلوكيات ومسارات العمل المسنودة بالذكاء الاصطناعي إلى نظام SIEM قائم، فيما يمدّ LogRhythm Intelligence النماذجَ السلوكية إلى عمليات النشر ذاتية الاستضافة. ويعين نموذجُ بيانات مشترك وتجربةُ تحقيق متكاملة المحللين على تتبع نشاط الهوية والأصول والأحداث عبر البيئات المختلطة. ويمكّن ذلك من تحديث متدرج تقوده حالات الاستخدام: فيحسّن المركز مجالاً واحداً ذا أولوية — كاكتشاف تهديدات بيانات هويات الدخول، أو التحقيق في مخاطر التهديدات الداخلية، أو تقارير الالتزام — ثم يتوسع من دون انتظار هجرة كاملة للمنصة. ويجمع الجدول التالي ما تقدم، فيقابل كل قوة من القوى الست بقدرة Exabeam التي تعالجها، والمحصلة التشغيلية المترتبة عليها.

الجدول 3: كيف تتقابل قدرات Exabeam مع القوى الست

القوة	قدرة Exabeam	المحصلة التشغيلية
1 **معادلة الكفاءات**	وكلاء Nova: وكيل البحث، ووكيل مساعد المحلل، ووكيل التحقيق	تأهيل أسرع للملتحقين الجدد، وتحقيقات موجَّهة، واعتماد أقل على الخبرات الكبيرة الشحيحة
2 **اقتصاديات SIEM**	نموذج المعلومات الموحد، وأكثر من 10,000 من محللات السجلات، واستيعاب على نطاق فائق، وتعزيز SIEM	ربط أسرع للسجلات، ومعالجة قابلة للتوسع، وصون الاستثمارات القائمة
3 **السرعة في ظل ECC وOTCC**	تقدير درجات الخطورة السلوكي، وThreat Scoring، ووكيل التحقيق، وأتمتة الاستجابة	تقديم الحالات الأعلى أولوية، وتجميع الأدلة مبكراً، وطريق أقصر إلى الاحتواء
4 **المركز المُدار خياراً افتراضياً**	منطقة الدمام السحابية، وLogRhythm SIEM السيادي، ووحدة OTCC، ودعم MIS	عمليات داخل المملكة بخيارات نشر تلائم متطلبات العملاء والترخيص المتباينة
5 **مشتريات يقودها الالتزام**	محتوى الالتزام بضوابط OTCC، وOutcomes Navigator، وأدلة الحالات، ومرونة النشر	جمع يدوي أقل للأدلة، ومواءمة أوضح بين الضوابط وبيانات القياس والتقارير
6 **الواقع الهجين**	تعزيز SIEM، وLogRhythm Intelligence، ونموذج بيانات مشترك موجه للأمن	استمرارية التحقيق عبر البيئات المختلطة من دون هجرة اقتلاع واستبدال مربكة

وتغدو البرهنة على القيمة التشغيلية لهذه القدرات أيسر متى أمكن قياس التحسينات المترتبة عليها. وينتقل القسم التالي بهذه المحصلات التشغيلية إلى مؤشرات أداء رئيسة يستطيع مديرو المراكز رفعها إلى قيادات الأمن ومجلس الإدارة.



06

قياس ما يستحق القياس:

مؤشرات أداء يثق بها مجلس الإدارة

06

قياس ما يستحق القياس:

مؤشرات أداء يثق بها مجلس الإدارة

قد يعالج مركز عمليات الأمن السيبراني مزيداً من التنبيهات ويغلق مزيداً من التذاكر من دون أن يخفض الخطر السيبراني على الأعمال خفضاً ملموساً، بل قد يحسّن أرقام النشاط تلك فيما تظل التهديدات الحقيقية غير مكتشفة مدداً أطول.

فحجم التنبيهات وأعداد التذاكر المغلقة نافعان لإدارة أعباء العمل، لكنهما لا يخبران القيادة بما يحققه ذلك النشاط: هل يجري اكتشاف التهديدات أبكر؟ وهل يكتمل احتواء الحوادث أسرع؟ وهل تتحسن طاقة المحللين؟ وهل الاستمرارية التشغيلية مصونة؟ وحين يكون النشاط هو الدليل الوحيد المعروض، تنقلب نقاشات الموازنة جدلاً حول الكلفة لا حول القيمة.

وتغدو قيمة القدرات الموصوفة في القسم السابق أوضح متى استطاع المركز إظهار ما الذي تغير بعد التطبيق؛ فالتأهيل الأسرع، وتجميع الأدلة الأبكر، والاعتماد الأقل على الخبرات الكبيرة، والجاهزية الأمتن للالتزام، واستمرارية التحقيق عبر البيئات المختلطة، كلها محصلات تشغيلية. ولتأمين استمرار الاستثمار، يجب على مديري المراكز ترجمة تلك المحصلات إلى مقاييس تفهمها القيادة.

فمجلس الإدارة يحتاج إذن إلى مقاييس قائمة على المحصلات تجيب عن الأسئلة المطروحة في مستهل هذا الدليل العملي، ومنها:

1. ما مدى سرعة اكتشاف التهديدات واحتوائها؟
2. كم من وقت المحللين تستهلكه التنبيهات الخاطئة؟
3. هل يمكن إثبات الالتزام بتوطين البيانات وسائر الالتزامات التنظيمية بأدلة يمكن الدفاع عنها؟
4. إلى أي حد لا تزال العمليات رهينة الخبرات الكبيرة الشحيحة؟
5. وهل يثمر التحديث تحسينات قابلة للقياس بمرور الوقت؟

ويترجم الجدول التالي مقاييس المركز هذه إلى محصلات الأعمال التي تعبّر عنها.

الجدول 4: ترجمة مؤشرات أداء المركز إلى محصلات بلغة مجلس الإدارة

المؤشر بعد التحديث	ترجمته بلغة مجلس الإدارة
متوسط زمن الاكتشاف (MTTD)	ما مدى سرعة إدراك الجهة أنها معرّضة للخطر
متوسط زمن الاستجابة (MTTR)	طول نافذة الأثر المحتمل على الأعمال بعد الاكتشاف
زمن المكوث (Dwell Time)	كم يستطيع المهاجم العمل قبل أن يرصد المركز نشاطه
معدل التنبيهات الخاطئة	وقت المحللين وكلفة التشغيل اللذان يلتهمهما الضجيج
ساعات المحللين المستردة ومعدل التصعيد إلى كبار المحللين	طاقة تحقيقية إضافية تتولد من دون نمو موازٍ في التوظيف، واعتماد أقل على الخبرات الكبيرة الشحيحة
معدل جاهزية أدلة الالتزام	نسبة الضوابط التنظيمية المنطبقة التي تستطيع الجهة أن تقدم لها أدلة كاملة ومحدّثة ويمكن الدفاع عنها، بما فيها أدلة توطين البيانات، ضمن الإطار الزمني المطلوب
التغطية المتحقق منها للأولويات وفق MITRE ATT&CK	نسبة أساليب الخصوم ذات الأولوية التي اختبر المركز قدرته على اكتشافها، بما يُظهر مواضع الانكشاف المتبقي ومواطن الحاجة إلى مزيد من الاستثمار

وينبغي قياس خطوط أساس لهذه المؤشرات قبل انطلاق التحديث، ثم تتبعها بوصفها اتجاهات زمنية.

فانخفاض متوسط زمن الاستجابة يدل على خفض المخاطر وتمتين الاستمرارية التشغيلية. وقلة التنبيهات الخاطئة وازدياد ساعات المحللين المستردة يبرهنان على تجنّب الكلفة ويخففان العبء عن الكوادر الكبيرة. وجاهزية أدلة الالتزام وتوطين البيانات الأمتن تُظهر أن الجهة قادرة على إبراز أدلة يمكن الدفاع عنها حين يطلبها المنظمون، فيما يمنح تحسّن التغطية وفق ATT&CK القيادةَ أساساً رصيناً لتقرير وجهة الاستثمار التالية.

ويسند Exabeam Outcomes Navigator عملية التحسين المستمر هذه بقياس التغطية الأمنية والوضع الأمني قياساً على حالات الاستخدام الاستراتيجية، وأساليب MITRE ATT&CK، وأطر الالتزام، ونظراء القطاع؛ فيحدد الفجوات، ويوصي بالخطوات التالية، ويتتبع التقدم بمرور الوقت. ويحوّل وكيل المستشار المدمج فيه (Nova Advisor Agent) هذه الرؤى إلى تقارير تنفيذية وخطط تحسين مرتبة الأولويات، عاملاً جنباً إلى جنب مع رئيس الإدارة المعنية بالأمن السيبراني (CISO) طوال رحلة تحسين المركز.

ومكاسب الطاقة الممكنة معتبرة؛ إذ تفيد Exabeam بأن Nova قادرة على:

- توفير ثلاث ساعات من أعمال فرز التنبيهات لكل محلل في كل مناوبة، بما يمثل زيادة في الإنتاجية قدرها 37.5%؛
- وخفض الجهد اللازم لإعداد ملخصات الحوادث بنسبة 50%؛

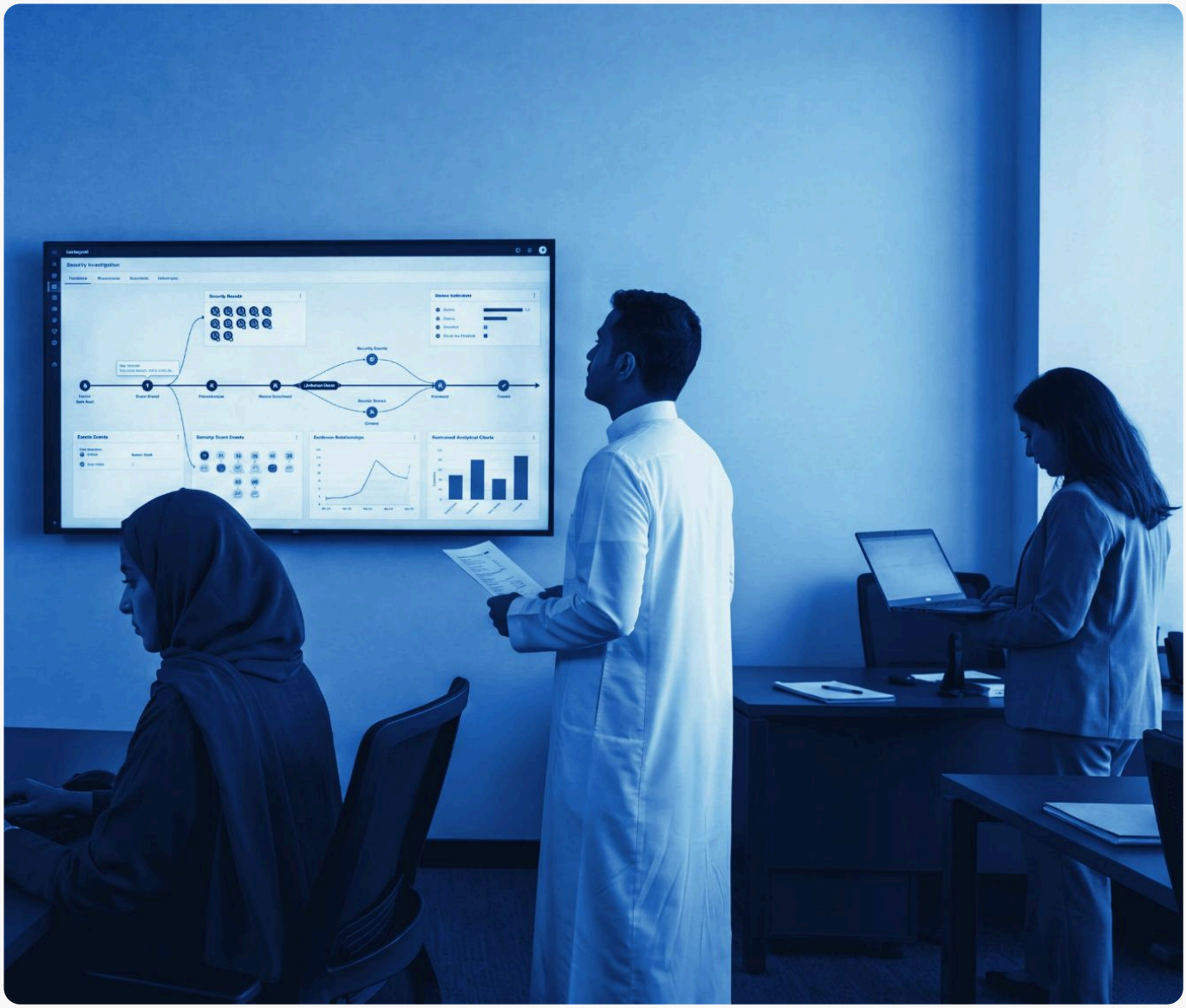
- وخفض جهد جمع الأدلة بنسبة 26%؛
- وخفض الجهد الإجمالي لاكتشاف التهديدات والتحقيق فيها والاستجابة لها (TDIR) بنسبة تصل إلى 80% مقارنة بالبيئات الخالية من تحليل السلوكيات ومن TDIR القائم على وكلاء الذكاء الاصطناعي.

%37.5 توفير ثلاث ساعات من أعمال فرز التنبيهات لكل محلل في كل مناوبة، بما يمثل زيادة في الإنتاجية قدرها 37.5%

بحسب Exabeam

وفي سوق ارتفعت فيها رواتب محللي المستويين الثالث والرابع بنسبة تتراوح بين 30% و40% خلال عام واحد، يغدو استرداد طاقة الخبراء محصلة قابلة للقياس على صعيدي القوى العاملة والكلفة، أكثر من كونه مجرد مكسب إنتاجية.

ويتخذ القسم التالي من هذه المؤشرات أساساً لخارطة طريق تحديث تمتد تسعين يوماً.





07

خارطة طريق التسعين يوماً لتحديث مركز عمليات الأمن السيبراني

07

خارطة طريق التسعين يوماً لتحديث مركز عمليات الأمن السيبراني

لا يكتمل تحديث مركز عمليات الأمن السيبراني في تسعين يوماً؛ لكن دورة مركزة من تسعين يوماً قد تكفي لإرساء خط أساس يمكن الدفاع عنه، واتخاذ القرارات المعمارية المفصلية، ونشر حالة استخدام أو اثنتين من ذوات الأولوية، والوقوف على ما إذا كان نموذج التشغيل الجديد قد بدأ يثمر قيمة قابلة للقياس.

وتسير خارطة الطريق على دورة تسعينية قابلة للتكرار: تقييم الحالة الراهنة، ثم تصميم الحزمة التالية من التحسينات، ثم نشرها والتحقق منها على مراحل.

1 الأيام من 1 إلى 30: التقييم

يرسي الشهر الأول خط أساس للحالة الراهنة للبيئة المختارة وحالات الاستخدام ذات الأولوية قبل إدخال تغييرات التحديث الكبرى؛ فمن دون ذلك الخط، قد يتحسن المركز ثم يعجز مع ذلك عن إثبات قيمة تلك التحسينات.

ابدأ بالمقاييس القائمة على المحصلات المحددة في القسم السادس (الجدول 4): سجّل القيم الحالية لمتوسط زمن الاكتشاف، ومتوسط زمن الاستجابة، وزمن المكوث، ومعدل التنبيهات الخاطئة، ووقت المحللين المستهلك في الفرز، ومعدل التصعيد إلى كبار المحللين، وجاهزية أدلة الالتزام، والتغطية المتحقق منها لأساليب MITRE ATT&CK ذات الأولوية. وحيثما لا توجد أرقام موثوقة، وثّق البيانات اللازمة لاحتسابها ومن سيتولى جمعها.

ثم افحص الأسس الكامنة خلف تلك المقاييس:

- **جرد بيانات القياس.** حدد أي مصادر السجلات تُجمع وتُحلَّل وتُربط تحليلياً وتكون قابلة للبحث ومحفوظة للمدة المطلوبة. وسجّل المصادر المفقودة، والصيغ غير المدعومة، والتغذيات المكررة، والبيانات المستبعدة لأسباب تتعلق بالكلفة أو بقيود فنية.
- **رسم النطاق التنظيمي ونطاق البيانات.** حدد الأنظمة الخاضعة لالتزامات ECC وOTCC وSAMA CSF وPDPL. وتثبّت من مواضع استيعاب بيانات القياس الأمنية وسجلات التحقيق وبيانات الحالات ذات الصلة ومعالجتها وتخزينها ونسخها احتياطياً والوصول إليها، وحدد الأدلة المطلوبة خلال أي تقييم أو تدقيق.
- **تقييم قدرات المحللين.** وثّق من يستطيع أداء أعمال المستويات الأول والثاني والثالث من دون مساعدة، وأي التحقيقات تستلزم تصعيداً إلى الكبار، وأين لا تزال المعرفة متركزة في أفراد لا في مسارات عمل قابلة للتكرار.
- **توثيق المعمارية القائمة كما هي.** ارسم مكونات المقار والسحابة والبيئات الهجينة؛ وعمليات التكامل؛ ونقاط تسليم التحقيقات؛ وإجراءات إدارة الحالات؛ واستثمارات SIEM القائمة الجديرة بالصون.

وينبغي أن يكون الناتج تقييماً للحالة الراهنة يحدد الفجوات الأعلى خطورة، ويرسي خط الأساس الذي سيُقاس عليه التحسن.

2 الأيام من 31 إلى 60:
التصميم

يحوّل الشهر الثاني التقييم إلى معمارية وخطة تشغيل.

اختر مسار النشر الموصوف في القسم الرابع: سيادي داخل المقار، أو سحابة داخل المملكة، أو هجين. وابنِ ذلك القرار على حساسية البيانات، والنطاق التنظيمي، والبنية التحتية القائمة، وتمرّس المحللين. ولا يُستبدل نظام SIEM عامل لمجرد توافر منصة أحدث؛ فحدد ما سيبقى، وما سيُعزز بالتحليلات والأتمتة، وما ينبغي سحبه من الخدمة.

ثم انتقِ من ثلاث إلى خمس حالات استخدام مرتبطة مباشرة بالتقييم. وتُعد إساءة استخدام بيانات هويات الدخول والحركة الجانبية نقطتَي انطلاق قويتين حيثما كانت مخاطر الهوية بارزة. وقد تشمل الأولويات الأخرى مخاطر التهديدات الداخلية، أو مراقبة التقنية التشغيلية، أو جمع الأدلة، أو التحقيق العابر للبيئات. وحدد لكل حالة استخدام: التهديد أو فجوة الضابط، وبيانات القياس المطلوبة، ومسار عمل التحقيق، والمسؤول عن الاستجابة، وطريقة التحقق، ومقياس النجاح.

وحدد في الوقت نفسه نموذج تشغيل المركز الذي سيسند المعمارية الجديدة: اربط الضوابط التنظيمية ببيانات القياس والتقارير وسجلات الحالات والأدلة التي تثبتها. وقرر كيف سيقلص البحثُ باللغة الطبيعية والخطوط الزمنية المؤتمتة وتقدير درجات الخطورة والإجراءات المقترحة وأدلة الاستجابة الجاهزة اختناقاتِ مهارات بعينها. وعيّن المسؤولين عن الضبط والمعايرة، والتحقيق، والتصعيد، ومراجعة الأدلة، وتقارير مؤشرات الأداء الرئيسة.

وأخيراً، اتفقوا على إيقاع القياس: أي الأرقام تُرفع شهرياً، وأي الاتجاهات تُراجع فصلياً، وكيف تجيب النتائج عن الأسئلة المطروحة في الرسالة الافتتاحية إلى رئيس الإدارة المعنية بالأمن السيبراني.

وينبغي أن يكون الناتج معماريةً مستهدفة متفقاً عليها، وخارطة طريق لحالات الاستخدام مرتبة الأولويات، وخطة قياس بمسؤولين ومعايير تحقق ومحصلات مستهدفة.

3 الأيام من 61 إلى 90:
النشر والتحقق وإظهار القيمة المبكرة

يضع الشهر الأخير التصميم موضع التشغيل من دون تحويل التحديث إلى هجرة دفعة واحدة عالية المخاطر.

انشر حالة استخدام أو اثنتين تجمعان بين قيمة أعمال عالية وخطر تنفيذ يمكن ضبطه: اربط بيانات القياس المطلوبة، وتحقق من التحليل والإثراء، وهيّئ مسارات عمل التحقيق، واختبر نقاط التسليم بين المحللين والمسؤولين عن الاستجابة. وحيثما بقي نظام SIEM قائم في مكانه، شغّل القدرة الجديدة إلى جانبه مدة تكفي للتثبت من التكامل والتغطية واستمرارية التحقيق قبل سحب أي شيء من الخدمة.

وينبغي أن يستند التحقق إلى نتائج مقيسة، لا إلى انطباعات متفرقة وحدها: أجرِ تمرين محاكاة افتراضياً للتحقق من الأدوار والقرارات ومسارات التصعيد، واستخدم محاكاة مضبوطة لاختبار مسار العمل الفني من الإشارة الأولى حتى الاحتواء والإبلاغ. وتأكد من قدرة المحللين على إعادة بناء الأحداث، وتحديد المستخدمين والأصول المتأثرين، وتوثيق القرارات، وصون الأدلة، والتصعيد باتساق. وأشرك المحللين المبتدئين لاختبار ما إذا كان مسار العمل يقلص فعلاً الاعتماد على الخبرات الكبيرة.

واستعمل Outcomes Navigator لمقارنة الوضع الأمني المحدَّث بخط الأساس، ومراجعة خطواته التالية الموصى بها، وتحويل تلك الأولويات إلى خطة التحسين لدورة التسعين يوماً التالية.

وفي ختام هذه المرحلة، أعد احتساب مؤشرات اليوم الأول التي تتوافر لها بيانات كافية، وسجّل مؤشرات مبكرة لما تبقى. وقارن زمن التحقيق، وعبء التنبيهات الخاطئة، والتصعيدات إلى الكبار، وجاهزية الأدلة، وتغطية الاكتشاف المتحقق منها، بخط الأساس.

وسجّل مواضع تحسّن الأداء ومواضع تعثره، وما إذا كان الفارق راجعاً إلى التقنية أو جودة البيانات أو تصميم الإجراءات أو التدريب.

ثم استعمل النتائج لوضع إيقاع الإبلاغ المتفق عليه موضع التطبيق: لوحة معلومات تشغيلية شهرية، وسرد فصلي لقيادات الأمن، ومراجعة نضج دورية. وينبغي لدورة التسعين يوماً التالية أن توسّع حالات الاستخدام الناجحة، وتصحح عمليات التكامل الضعيفة، وتسد فجوات بيانات القياس المتبقية، وتتحقق من أساليب إضافية وفق ATT&CK.



الشكل 4: خارطة طريق التسعين يوماً لتحديث المركز

4 أسئلة لتوجيهها إلى المورّدين قبل التوقيع

اسأل كل مورد بلغ القائمة المختصرة:

- أين ستقيم فعلياً سجلاتنا وبيانات حالاتنا ونسخنا الاحتياطية وبيانات المعالجة بالذكاء الاصطناعي، وهل تستطيعون التأكيد كتابةً أنها لن تغادر المملكة العربية السعودية؟
- أي متطلبات ECC وOTCC وSAMA CSF وPDPL تدعمونها بخرائط ربط أو تقارير أو محتوى التزام جاهز، وأيها يستلزم تهيئة مخصصة؟
- ما الذي يستطيع محلل المستوى الأول فعله من يومه الأول مما يستلزم اليوم أحد كبار المحللين؟
- هل تستطيع منصتكم تعزيز نظام SIEM القائم لدينا؟ وما أعمال التكامل وازدواج البيانات والصيانة المستمرة التي سيتطلبها ذلك؟

- ما الذي توفرونه من دعم محلي، وتدريب، وتوثيق بالعربية، وقدرات شريك إقليمي معتمد؟
- كيف تحافظ خدماتكم السحابية وإجراءات دعمكم وترتيبات التعافي من الكوارث لديكم وخصائص الذكاء الاصطناعي عندكم على متطلباتنا في السيادة وتوطين البيانات؟

ويصف القسمان الرابع والخامس نموذج نشر Exabeam والقدرات ذات الصلة بهذه الأسئلة.

5 مزالق شائعة ينبغي تجنبها

- لا تبدأ بقائمة منتجات مختصرة قبل تحديد المحصلات المنشودة.
- لا تستبدل منصة عاملة حيثما كان التعزيز قادراً على تقديم القيمة أسرع وبأقل اضطراب.
- لا تستهن بأعباء تنقية بيانات القياس، والتكامل، والتوطين، وتهيئة الالتزام.
- لا تنشر حالات استخدام كثيرة دفعة واحدة.

وفوق ذلك كله، لا تتجاوز خط أساس اليوم الأول؛ فمن دونه لن تستطيع مراجعة التسعين يوماً أن تُظهر ما إذا كان التحديث يخفض المخاطر، أو يسترد الطاقات، أو يمتّن الجاهزية للالتزام. إن الأيام التسعين الأولى ترسي انضباطاً تحديثياً قابلاً للتكرار: قِس، ورتّب الأولويات، وانشر، وتحقق، وحسّن.



المساهمون



سلطان العنزي

المدير الإقليمي لمكتب المملكة العربية السعودية

LogRhythm - Exabeam



مازن عدنان الدوه جي

النائب الأول للرئيس والمدير العام لمنطقة الهند والشرق الأوسط وتركيا وأفريقيا

LogRhythm - Exabeam



محمد عطا النويشي

كبير مهندسي الحلول

LogRhythm - Exabeam

تواصل معنا

سايبر كاست

البريد

الهاتف

الموقع cybersecuritycast.com

LogRhythm exabeam

البريد

الهاتف

الموقع exabeam.com

عن Exabeam

تُعد Exabeam شركة عالمية متخصصة في الأمن السيبراني وعمليات الأمن، وتجمع بين خبرات وتقنيات Exabeam وLogRhythm لتقديم حلول متقدمة تساعد المؤسسات على تعزيز قدراتها في اكتشاف التهديدات السيبرانية والتحقيق فيها والاستجابة لها. وتوظف الشركة الذكاء الاصطناعي وتحليلات السلوك والبيانات الأمنية لتمكين فرق الأمن من فهم التهديدات واتخاذ الإجراءات المناسبة بكفاءة.

وتخدم Exabeam المؤسسات في مختلف القطاعات والأسواق حول العالم، من خلال حلول تدعم تطوير عمليات أمنية أكثر كفاءة وفاعلية، وتساعد فرق الأمن على التعامل مع التهديدات المتطورة وتعزيز قدرتها على حماية بيئاتها الرقمية.

عن سايبركاست

سايبركاست منصة إعلامية سعودية متخصصة في الأمن السيبراني، تُعنى بإنتاج وتطوير المحتوى المتخصص الذي يخدم القيادات وصنّاع القرار في القطاع، ويواكب أبرز التطورات والتوجهات والتقنيات والقضايا المؤثرة في المشهد السيبراني. وتقدم المنصة محتوى متنوعاً يشمل التقارير والدراسات والمقابلات والمواد التحريرية والمرئية.

وتعمل سايبركاست بالشراكة مع شركات الأمن السيبراني والمؤسسات والجهات المتخصصة على تطوير محتوى مهني عالي الجودة، وتحويل الخبرات والمعارف المتخصصة إلى مواد إعلامية متخصصة، إلى جانب نشر هذا المحتوى وتوزيعه عبر قنواتها الإعلامية وشبكاتها المتخصصة.



دليل تحديث مراكز العمليات الأمنية في المملكة

Saudi SOC Modernization Playbook



LogRhythm®

exabeam™

exabeam.com

سايبر كاست

cybersecuritycast.com

© 2026 Exabeam وسايبركاست. جميع الحقوق محفوظة.