الجمهورية العربية السورية
وزارة التعليم العالي
الجامعة السورية الخاصة

Early Detection of Intrusions Using Artificial Intelligence in SIEM Systems

الكشف المبكر عن الاختراقات باستخدام الذكاء الاصطناعي ضمن منظومات SIEM

تقرير مشروع – هندسة أمن الأنظمة والشبكات

اعداد:

يامن حاجين

جاد كندر

اشراف:

د. وسيم الجنيدي

آب / أغسطس 2025

الخلاصة

في ظل التحول الرقمي المتسارع وتصاعد حدة التهديدات الإلكترونية، تواجه المؤسسات تحديات غير مسبوقة في حماية أصولها الرقمية. لم تعد أنظمة إدارة المعلومات والأحداث الأمنية (SIEM) التقليدية كافية لمواكبة التعقيد المتزايد لهذه التهديدات. في هذا المشروع، سنناقش رؤية متكاملة لتعزيز أنظمة الدفاع السيبراني من خلال الدمج الاستراتيجي بين تقنيات الذكاء الاصطناعي المتطورة والبنية التحتية القائمة لأنظمة SIEM.

سيتناول البحث إطاراً نظرياً شاملاً يغطي الأسس العلمية لأنظمة كشف التسلل (IDS) وتطورها التاريخي، مع تحليل معمق للتحولات الجوهرية في أنظمة SIEM عبر العقد الماضي. كما سيناقش الأسس النظرية والتطبيقية للذكاء الاصطناعي والتعلم الآلي، مع التركيز على تطبيقاتها الثورية في مجال الأمن السيبراني.

سيعتمد المشروع على منهجية بحثية متكاملة تشمل دراسة تحليلية لأكثر من 20 دراسة مرجعية رائدة تغطي الفترة من 2015 إلى 2024، مع تحليل نقدي للتحديات التقنية والعملية التي تواجه عملية الدمج هذه. على الصعيد التطبيقي، سيقوم المشروع بتصميم وتنفيذ نموذج عملي متقدم للكشف الاستباقي عن الهجمات، مع ضمان تحقيق تكامل سلس وفعال مع البنى التحتية القائمة.

يهدف هذا البحث إلى تقديم إسهام علمي وعملي ملموس في مجال الأمن السيبراني، من خلال إثبات جدوى التحول من النموذج التفاعلي التقليدي إلى النموذج الاستباقي الذكي، وإبراز الدور التحويلي للذكاء الاصطناعي في إعادة صياغة مستقبل أنظمة الدفاع السيبراني. كما يسعى إلى تقديم إطار عمل متكامل يمكن للمؤسسات الاعتماد عليه في رحلتها نحو التحول الرقمي الآمن.

الكلمات المفتاحية :الأمن السيبراني، أنظمةSIEM ، الذكاء الاصطناعي، التعلم الآلي، كشف التسلل، كشف الشذوذ، الأمن الاستباقي، التحول الرقمي، إدارة المخاطر السيبرانية.

جدول المحتويات

فهرس الجداول

فهرس الأشكال

المقدمة

المقدمة

في ظل المشهد المتسارع لتطور الأمن السيبراني اليوم، تواجه المؤسسات عدداً متزايداً باستمرار من التهديدات، بدءاً من الهجمات السيبرانية المعقدة وصولاً إلى المخاطر الداخلية. ولمواجهة هذه التحديات بفاعلية، تحتاج الشركات إلى رؤية فورية في بيئات تقنية المعلومات الخاصة بها، واكتشاف سريع للتهديدات، واستجابة منسقة للحوادث. وهنا يبرز الدور المحوري لأنظمة إدارة معلومات وأحداث الأمن.

توفر حلول الـ SIEM جمعاً مركزياً للسجلات وربطها وتحليلها، مما يمكّن فرق الأمن من اكتشاف الشذوذات، والتحقيق في الحوادث، والامتثال للمتطلبات التنظيمية. ومن خلال تجميع البيانات من الشبكات والخوادم والتطبيقات والأجهزة الأمنية، تساعد أنظمة SIEM على تحديد الأنشطة الخبيثة، وتقليل أوقات الاستجابة، وتعزيز الموقف الأمني العام.

تاريخياً، ركّزت أنظمة SIEM على تجميع البيانات الأمنية، لكنها واجهت صعوبة في تحليل مجموعات البيانات الضخمة والمعقدة بشكل فعّال. وقد أحدث دمج الذكاء الاصطناعي، وخاصة التعلم الآلي والتعلم العميق، في أدوات SIEM ثورة في مجال الأمن السيبراني عبر تمكين القدرات التنبؤية **[1]**. تعتمد أنظمة SIEMالمدعومة بالذكاء الاصطناعي على خوارزميات متقدمة لتحليل البيانات التاريخية والفورية، والتعرف على الأنماط، والتنبؤ بالتهديدات المحتملة **[2]**.

هذا التحول من مجرد الاكتشاف إلى الصيد الاستباقي للتهديدات يتيح للمؤسسات معالجة نقاط الضعف والتخفيف من المخاطر قبل أن تتصاعد إلى هجمات شاملة. يستعرض هذا التقرير الدور التحويلي للذكاء الاصطناعي في أنظمة SIEM، مسلطاً الضوء على كيفية تعزيز الذكاء التنبؤي لعمليات الكشف عن التهديدات، والكفاءة التشغيلية، والاستجابة للحوادث. كما يتناول تطبيقات واقعية لأنظمة SIEM المدعومة

بالذكاء الاصطناعي في الصيد الاستباقي للتهديدات والتخفيف من المخاطر، مبرزاً أهميتها الجوهرية في أطر الأمن السيبراني الحديثة. ومن خلال اعتماد هذه الأدوات المتقدمة، يمكن للمؤسسات بناء مرونة أكبر في مواجهة التهديدات المتطورة وحماية أصولها الرقمية بشكل أكثر فاعلية.

المشكلة العلمية

في الإصدارات المبكرة من أنظمة إدارة معلومات وأحداث الأمن (SIEM) خلال منتصف وأواخر العقد الأول من الألفية الثانية، كانت وظيفتها التقليدية تتمثل في كونها مستودعات مركزية للبيانات الأمنية، حيث تقوم بتجميع السجلات والتنبيهات من مختلف أدوات الأمن **[3]**. ومع ذلك، فإن الحجم الهائل وتعقيد البيانات غالباً ما جعلا عملية التحليل مرهقة وغير فعّالة. كما أن محدودية القدرة الحاسوبية والإمكانيات البرمجية آنذاك جعلت من شبه المستحيل تحليل الكميات الضخمة من البيانات، وهي خطوة محورية لتحقيق الاستخبارات التنبؤية.

علاوة على ذلك، كانت أنظمة SIEM التقليدية تولّد ضجيجاً هائلاً من الإنذارات، مع ارتفاع معدلات الإيجابيات الكاذبة التي كانت تحجب التهديدات الحقيقية **[4]**. لقد أحدث تطور الذكاء الاصطناعي ثورة في مجال الأمن السيبراني، مقدماً مزايا دفاعية كبيرة. غير أن هذا التقدم التكنولوجي ذاته يمثّل، بشكل مفارق، محفزاً محتملاً لظهور تهديدات سيبرانية أكثر تطوراً، مثل الهجمات السيبرانية المدعومة بالذكاء الاصطناعي **[5]**.

ففي الأيدي الخطأ، أصبح الذكاء الاصطناعي أداة بالغة الخطورة تُستخدم لأتمتة التهديدات السيبرانية وتعزيز فعاليتها. إذ يستغل مجرمو الإنترنت قدرات الذكاء الاصطناعي للتكيف بسهولة مع التدابير الدفاعية، وتنفيذ الهجمات بسرعات غير مسبوقة، واستغلال الثغرات بدقة متناهية. كما يمكّن الذكاء الاصطناعي المهاجمين من محاكاة السلوك البشري، مما يزيد من فاعلية هجمات التصيّد الاحتيالي ويرفع احتمالية نجاحه **[5]**.

إضافة إلى ذلك، يساعد الذكاء الاصطناعي في تطوير برمجيات خبيثة "ذكية"، قادرة على التعلم من بيئتها، وتكييف استراتيجياتها لتجنب الاكتشاف، وإلحاق أقصى قدر من الضرر. هذا المستوى من التعقيد يجعل الدفاعات الأمنية التقليدية، مثل الكشف عن البرمجيات الخبيثة بالاعتماد على التوقيعات، غير كافية في مواجهة هذه التهديدات المتقدمة. ويُعد **DeepLocker**، الذي ابتكرته شركة IBM Research ، مثالاً بارزاً على هذا التهديد الناشئ **[6]**. فهو يمثّل جيلاً جديداً من أدوات الهجوم المستهدفة شديدة التخفي والمدعومة بالذكاء الاصطناعي. إذ يُخفي نواياه الخبيثة إلى أن يصل إلى ضحيته المحددة، مما يجسد مدى التطور المستقبلي المحتمل للتهديدات البرمجية.

وقد أصبح التعامل مع الثغرات الأمنية أكثر صعوبة من أي وقت مضى. فالأساليب التفاعلية التقليدية التي كانت تتبناها أنظمة SIEM القديمة تنتظر استغلال الثغرات قبل معالجتها، وهو نهج أثبت قصوره في مشهد الأمن السيبراني الحالي.

اهداف المشروع

يهدف هذا المشروع إلى توظيف تقنيات الذكاء الاصطناعي المتاحة — باختيار الأكثر فاعلية منها أو دمج عدة تقنيات معاً — لتعزيز أنظمة إدارة معلومات وأحداث الأمن. ويتمثل الهدف الأساسي في تحقيق الكشف المبكر عن التهديدات السيبرانية بكفاءة زمنية أعلى، مما يتيح تطبيق آليات دفاع استباقية.

ويتضمن ذلك:

1. **تقييم أساليب الذكاء الاصطناعي** :تحليل تقنيات التعلم الآلي، والتعلم العميق، والتحليلات السلوكية لتحديد المناهج الأمثل للتنبؤ بالتهديدات.
2. **الكشف الاستباقي عن التهديدات** :تمكين أنظمة SIEM من اكتشاف الشذوذات والاختراقات المحتملة قبل تصاعدها، وبالتالي تقليل أزمنة الاستجابة.
3. **تحسين زمن الاكتشاف** :تقليص الفجوة الزمنية بين ظهور التهديد وتحديده من أجل التخفيف السريع من المخاطر.

ومن خلال دمج الذكاء الاصطناعي في أنظمة SIEM، يسعى المشروع إلى تحويل الأمن التقليدي ذي الطابع التفاعلي إلى إطار للأمن السيبراني قائم على التنبؤ والوقاية المسبقة.

ومع ذلك، هناك بعض الجوانب المستقبلية التي ينبغي العمل عليها، ومنها:

- **الاستجابة الذاتية للتهديدات** :ستتوسع أتمتة الذكاء الاصطناعي لتتجاوز مرحلة الاكتشاف نحو الاستجابات المستقلة. فقد تتمكّن الأنظمة المستقبلية من عزل الأجهزة الطرفية تلقائياً، وتطبيق

- التحديثات التصحيحية، أو إعادة تهيئة جدران الحماية بمجرد تحديد التهديد، مما يقلل من تدخل العنصر البشري.
- **التكامل الموحد لمصادر استخبارات التهديدات** :ستقوم أنظمة SIEM المستقبلية بتجميع وربط مصادر التهديد (العالمية) مثل الشبكة المظلمة، ومصادر الاستخبارات مفتوحة المصدر OSINT ، والبيانات الخاصة بكل صناعة باستخدام تقنيات معالجة اللغة الطبيعية (NLP) والتحليلات المعتمدة على الرسوم البيانية. وسيوفر ذلك تقييماً سياقياً للمخاطر ويساعد في تحديد أولويات الثغرات الأمنية داخل المؤسسات.

الدراسة المراجعية

شهدت أنظمة إدارة معلومات وأحداث الأمن (SIEM) تطورات كبيرة خلال الفترة بين عامي 2015 و2024، حيث انتقلت من الأساليب التقليدية إلى مناهج تنبؤية مدعومة بالذكاء الاصطناعي. ففي عام 2015، أجرى **Buczak & Guven** دراسة شاملة حول تطبيقات التعلم الآلي في الأمن السيبراني، مسلطين الضوء على خوارزميات مثل آلات المتجهات الداعمة(SVM) ، (Decision Trees)، (Random Forests) في مجال كشف التسلل ودمجها ضمن أنظمة SIEM. وقد أسس ذلك لانتقال تدريجي من الأنظمة القائمة على القواعد إلى التحليلات الأمنية المدعومة بالتعلم الآلي.

بحلول عام 2016، ركّز **Garcia–Teodoro** وآخرون على تحسين دقة أنظمة SIEM باستخدام تقنيات التصنيف المعتمدة على ML ، بينما قدّم **Chandola** وآخرون تقنيات للكشف عن الشذوذ على نطاق واسع للتعامل مع التدفقات الضخمة للبيانات، مما شكّل مقدمة للتحليلات التنبؤية الحديثة في SIEM.

في عام 2017، قام **Almotairi** وآخرون بتطبيق تحليلات سلوك المستخدم والكيان (UEBA) في أنظمة SIEM، مما أتاح الكشف عن الشذوذات اعتماداً على السلوك. وفي الوقت ذاته، شدّد **Sommer & Paxson** على أهمية المناهج الهجينة التي تجمع بين الأنظمة القائمة على القواعد وML، في موازنة الأتمتة مع الخبرة البشرية — وهو مبدأ ما يزال يحتفظ بأهميته في أطر SIEM الحديثة المعتمدة على الذكاء الاصطناعي.

أمّا في عام 2018، فقد أبر **Shiravi** وآخرون دور تحليلات البيانات الضخمة في أنظمة SIEM ، مما مكّن من تقليص أزمنة الاستجابة وتحسين الرؤية الأمنية.

وجاء الانطلاقة الكبرى في عام 2020 حين قام **Santos** وآخرون بدمج تقنيات التعلم العميق في أنظمة SIEM، الأمر الذي ساهم في تحسين دقة كشف الشذوذ بشكل ملحوظ وخفض معدلات الإيجابيات الكاذبة — وهو ما مهّد الطريق نحو الجيل الجديد من أنظمة SIEM المدعومة بالذكاء الاصطناعي.

وفي عام 2022، استخدم **Rahman** وآخرون تقنيات التعلم العميق للكشف عن التهديدات المستمرة المتقدمة (APT) ، بينما قدّم **Yamin** وآخرون نموذج SIEM استباقياً يعتمد على الذكاء الاصطناعي التكيفي، مما مثّل انتقالاً من الاكتشاف إلى التنبؤ.

بحلول عام 2023، حدّد **Sarker** أساليب التعلم الآلي التجميعي (Ensemble ML) باعتبارها الأكثر تطوراً في تقليل الإيجابيات الكاذبة، في حين قام **Barker & Shiaeles** بأتمتة عمليات مراكز عمليات الأمن (SOC) باستخدام التحليلات التنبؤية، محوّلين أنظمة SIEM إلى أداة دفاع استباقية.

وأخيراً، في عام 2024، طوّر **Lyu** وآخرون إطاراً يجمع بين التعلم العميق والتحليلات السلوكية، ليمثل أحدث ما توصلت إليه التقنيات من حيث الدقة التنبؤية وتقليل الضوضاء.

تُبرز هذه المسيرة التطورية رحلة أنظمة SIEM من مجرد تحليل تفاعلي للسجلات إلى منصات أمنية تنبؤية مدعومة بالذكاء الاصطناعي، بما يتماشى مع أهداف الأمن السيبراني الحديثة المتمثلة في الصيد الاستباقي للتهديدات والاستجابة المؤتمتة.

وفي مايلي ملخص لما سبق :

جدول الدراسة المراجعية

المرجع	العلاقة مع مشروعنا	النتيجة	المؤلفون	البحث
[7]	يمكن أن يُعتبر هذا العمل مرجعاً أساسياً يوضح كيف	أبرزوا أن الأساليب الأكثر تقدماً في ذلك الوقت شملت	Buczak & Guven	**استطلاع لأساليب التنقيب عن البيانات والتعلم**

	تطورت أنظمة SIEMمن التعلم الآلي الكلاسيكي إلى الذكاء الاصطناعي التنبؤي.	SVM، وأشجار القرار (Decision Trees)، و Random Forests لاكتشاف التسلل ودمجها في أنظمة SIEM.		**الآلي في كشف التسلل الأمني السيبراني**
[8]	يوفر نظرة ثاقبة على التحسينات المبكرة في التعلم الآلي قبل الانتقال إلى التعلم العميق.	حددت الدراسة أن التعلم الآلي المعتمد على التصنيف كان الأسلوب الأكثر تقدماً لتعزيز دقة أنظمة SIEM في ذلك الوقت.	Garcia-Teodoro et al	**كشف التسلل الشبكي القائم على الشذوذ: التقنيات، الأنظمة، والتحديات**

[9]	يُعدّ مهماً كمقدمة للكشف التنبؤي عن الشذوذ في أنظمة SIEM المدعومة بالذكاء الاصطناعي.	كان الكشف عن الشذوذ على نطاق واسع يُعتبر الأسلوب الأكثر تقدماً في معالجة مشكلة انفجار البيانات.	Chandola et al	**كشف الشذوذ في التسلسلات المنفصلة: دراسة استقصائية**
[10]	وضع الأساس للتحليل السلوكي، والذي يُعدّ ميزة رئيسية في أنظمة SIEMالتنبؤية الحديثة.	أصبح تحليل سلوك المستخدم والكيان (UEBA) هو الأسلوب الأكثر تقدماً للكشف عن الشذوذات في سلوك المستخدمين والكيانات.	Almotairi et al	**نهج متعدد الطبقات لتحديد السلوكيات الخبيثة في حركة مرور الشبكة**

[11]	ذو صلة مباشرة، حيث تطورت أطر SIEMالهجينة الحديثة المدعومة بالذكاء الاصطناعي من هذا المبدأ.	اعتُبرت الطرق الهجينة الأكثر تقدماً لأنها توفّر توازناً بين الخبرة البشرية والأتمتة.	Sommer & Paxson	**خارج العالم المغلق: حول استخدام التعلم الآلي لاكتشاف التسلل الشبكي**
[12]	نعم، حيث أن مشروعنا يتطلب التعامل مع البيانات الضخمة في الزمن الحقيقي من أجل الصيد الاستباقي للتهديدات.	مثلت أنظمة SIEM المدفوعة بالبيانات الضخمة الأسلوب الأكثر تقدماً لتقليل زمن الاستجابة	Shiravi et al	**التحليلات في الزمن الحقيقي: التقنيات والتطبيقات على تدفقات البيانات الضخمة في مراقبة الأمن**

		وتعزيز الرؤية الأمنية.		
[13]	يمكن استخدام هذا العمل كإطار مرجعي لتصميم نظام SIEMتنبؤي.	وخلصوا إلى أن هذه الأنظمة تمثل أحدث ما توصلت إليه إدارة المعلومات الأمنية.	Santos et al	**إدارة معلومات وأحداث الأمن من الجيل القادم: مراجعة منهجية**
[14]	نعم، لأن مشروعنا يركز على التنبؤ بالتهديدات قبل حدوثها.	تم التوصل إلى أن الشبكات العصبية العميقة تمثل الأسلوب الأكثر تقدماً للكشف المبكر عن التهديدات المستمرة المتقدمة (APTs)	Rahman et al	**نهج التعلم العميق للكشف عن التهديدات المستمرة المتقدمة في بيئات السحابة**

[15]	يتماشى مع رؤيتنا في الانتقال من الاكتشاف إلى التنبؤ.	ساهم النظام في تقليل الإنذارات الكاذبة وتحسين القدرة على التكيف مع التهديدات الجديدة.	Yamin et al	**Adaptive AI-SIEM: نموذج استباقي لإدارة معلومات وأحداث الأمن في بيئات تهديدية ديناميكية**
[16]	يمكن لأساليب التجميع (Ensemble) زيادة موثوقية نظامنا.	عززت هذه المناهج الدقة وقلّلت الإيجابيات الكاذبة في أنظمة SIEM.	sarker	**التعلم الآلي لتحليل البيانات الذكي في الأمن السيبراني: مراجعة معاصرة لتقنيات التعلم التجميعي**
[17]	يمكن أن يدعم ذلك هدفنا	حوّل هذا الابتكار أنظمة	Barker & Shiaeles	**نحو مركز عمليات أمن**

	في تقليل زمن الاستجابة من خلال الأتمتة.	SIEMمن أداة تفاعلية إلى آلية دفاعية استباقية ومؤتمتة.		**مستقل: إطار تنبؤي بالذكاء الاصطناعي لإدارة معلومات وأحداث الأمن**
[18]	لأنه يدعم بشكل مباشر هدفنا المتمثل في التنبؤ وتقليل الضوضاء.	تم الاعتراف بهذا الإطار باعتباره الأكثر تقدماً في تحسين الدقة التنبؤية في الكشف عن التهديدات.	Lyu et al	**نموذج هجيني للتحليلات السلوكية العميقة لتقليل الإيجابيات الكاذبة في أنظمة SIEM من الجيل القادم**

التحديات

رغم الفوائد العديدة التي يقدمها هذا المشروع إلا أنّ هناك مجموعة من التحديات التي قد يواجهها أي شخص يعمل عليه ومن أبرز هذه التحديات:

1. **تعقيد وجودة البيانات**

- **الحجم والضوضاء** :تتطلب أنظمة SIEM المدعومة بالذكاء الاصطناعي مجموعات بيانات ضخمة من أجل تحليل دقيق، غير أن البيانات منخفضة الجودة بكثرة (مثل الإنذارات الكاذبة أو السجلات غير ذات الصلة) قد تحجب التهديدات الحقيقية وتضعف فعالية النماذج (الصفحة 2).
- **العزلة البياناتية :(Data Silos)** إن تجزؤ مصادر البيانات (السحابة، البنية التحتية المحلية، إنترنت الأشياء) يعيق التحليل الشامل، ويحدّ من القدرات التنبؤية للذكاء الاصطناعي.

2. **القيود الخوارزمية**

- **الإيجابيات/السلبيات الكاذبة** :الاعتماد المفرط على البيانات التاريخية قد يؤدي إلى فشل الذكاء الاصطناعي في اكتشاف التهديدات الجديدة (هجمات اليوم–صفر)، أو توليد إنذارات خاطئة، مما يضعف الثقة بالنظام.
- **مشكلة "الصندوق الأسود** :"تفتقر نماذج التعلم الآلي والتعلم العميق المعقدة إلى الشفافية، مما يصعّب عملية تدقيق القرارات أو شرح التنبيهات لأصحاب المصلحة (مثل فرق الامتثال).

3. **الموارد والمتطلبات التشغيلية**

- **الكثافة الحسابية** :يتطلب التحليل في الزمن الحقيقي قدرة معالجة عالية، مما يؤدي إلى ارتفاع تكاليف الحوسبة والسحابة.
- **فجوات المهارات** :يمثل نقص الكفاءات المتخصصة في كل من الأمن السيبراني والذكاء الاصطناعي/التعلم الآلي عائقاً أمام النشر والضبط الأمثل للنماذج.

4. **التهديدات العدائية**

- **الهجمات المدعومة بالذكاء الاصطناعي** :يستغل مجرمو الإنترنت الذكاء الاصطناعي لتطوير برمجيات خبيثة مراوغة (مثل *DeepLocker*) تتجاوز الدفاعات التقليدية، مما يفرض الحاجة إلى إعادة تدريب النماذج بشكل مستمر.
- **تسميم البيانات :(Data Poisoning)** قد يقوم المهاجمون بحقن بيانات ضارة في النظام لتخريب نماذج الذكاء الاصطناعي، مما يؤدي إلى تنبؤات خاطئة بالتهديدات.

5. **التكامل وقابلية التوسع**

- **التوافق مع الأنظمة القديمة** :غالباً ما يتطلب دمج أنظمة SIEM المدعومة بالذكاء الاصطناعي مع البنية التحتية القديمة تعديلات مخصصة بتكاليف مرتفعة.
- **مشكلات القابلية للتوسع** :يمثل الحفاظ على الأداء عبر الشبكات المتنامية (مثل السحابة الهجينة، إنترنت الأشياء) تحدياً في تخصيص الموارد وإدارتها.

التطبيقات العملية

1. **الكشف عن التهديدات ومراقبة محاولات التسلل**

- تقوم أنظمة SIEM بتجميع السجلات من جدران الحماية (Firewalls) ، وأنظمة كشف/منع التسلل (IDS/IPS)، والأجهزة الطرفية لاكتشاف السلوك غير الطبيعي. **مثال** :اكتشاف التهديدات الداخلية من خلال أنماط تسجيل دخول غير اعتيادية.

2. **الاستجابة للحوادث والتحقيق الجنائي الرقمي(Forensics)**

- يتيح التجميع المركزي للسجلات إجراء تحليلات جنائية سريعة بعد حوادث الاختراق. **مثال** :تحسين تدفقات العمل في التحقيقات الجنائية الرقمية بمساعدة SIEM، مما يقلل زمن الاستجابة بنسبة تصل إلى 45%.

3. **الامتثال والجاهزية للتدقيق**

- تعتمد المؤسسات على أنظمة SIEM للامتثال لمعايير مثل **GDPR**، و **HIPAA**، و **PCI-DSS**من خلال توفير تقارير مؤتمتة. **مثال** :نشر أنظمة SIEM في قطاع الرعاية الصحية لضمان الامتثال لمتطلبات **HIPAA**.

4. **أمن السحابة والبنى التحتية الهجينة**

- تدمج أنظمة SIEM الحديثة مع منصات مثل **AWS** و **Azure** والهياكل الهجينة لتحقيق رؤية موحدة. **مثال** :أنظمة SIEM السحابية الأصلية (Cloud-native) التي تدعم خطوط أنابيب **DevSecOps**.

5. **حماية البنى التحتية الحيوية**

- تُطبّق في شبكات الطاقة، ووسائل النقل، وقطاع الرعاية الصحية لمنع الاضطرابات السيبرانية-الفيزيائية. **مثال** :نشر SIEM في الشبكات الذكية (Smart Grids) لاكتشاف الشذوذات.

6. **تحليلات سلوك المستخدم والكيان(UEBA)**

- تكشف أنظمة SIEM المدعومة بالتعلم الآلي الحسابات المخترقة والتهديدات الداخلية. **مثال** : SIEMمدمج مع UEBA ينجح في اكتشاف محاولات تصعيد الامتيازات.

7. **التكامل مع SOAR (تنسيق وأتمتة واستجابة الأمن)**

- تعمل التدفقات المؤتمتة التي يتم تفعيلها بواسطة تنبيهات SIEM على تقليل إرهاق المحللين. **مثال** : الاستجابة المؤتمتة لرسائل التصيّد الاحتيالي باستخدام تكامل **SIEM + SOAR**.

8. **أمن إنترنت الأشياء (IoT) وإنترنت الأشياء الصناعي (IIoT)**

- تُستخدم أنظمة SIEM في بيئات إنترنت الأشياء لمراقبة الاتصالات بين الأجهزة. **مثال** :نظام SIEM صناعي يكتشف تحديثات البرامج الثابتة (Firmware) الخبيثة.

الفصل الأول: الدراسة النظرية

1.1 لمحة شاملة عن كشف الأختراقات

1.1.1 مفهوم وأهمية كشف التسلل

يمثل كشف التسلل تخصصًا أساسيًا في مجال الأمن السيبراني يركز على مراقبة وتحليل الأحداث داخل أنظمة الكمبيوتر والشبكات لتحديد أدلة على الأنشطة الخبيثة، أو انتهاكات سياسات الأمن، أو محاولات الوصول غير المصرح بها. كمكون حاسم في هياكل الأمن ذات الطبقات المتعددة (دفاع متعمق)، يعمل كشف التسلل على مبدأ "الأختراق المفترض"، معترفًا بأن إجراءات الأمن الوقائية وحدها لا يمكنها توفير حماية كاملة ضد الخصوم المصرين. الهدف الأساسي من أنظمة كشف التسلل ليس منع الهجمات بشكل مباشر، بل تمكين اكتشافها بشكل فوري، مما يسهل الاستجابة الفعالة للحوادث ويقلل من الضرر المحتمل للأصول التنظيمية والسمعة والعمليات.

تم وضع الأساس النظري لكشف التسلل الحديث من قبل Dorothy E. Denning في عملهم المؤثر عام 1987، الذي صاغ مفهوم كشف التسلل كعملية آلية لتحديد انتهاكات سياسات الأمن من خلال التحليل المنهجي لبيانات التدقيق **[19]** . قدم هذا الإطار الرائد المفاهيم الأساسية التي لا تزال توجه البحث والتطبيق في كشف التسلل، بما في ذلك أهمية سجلات التدقيق، وملفات تعريف السلوك الطبيعي، وتقنيات كشف الشذوذ. إن الأهمية المستمرة لعمل دينينغ تؤكد على الطبيعة الأساسية لكشف التسلل كتخصص في الأمن السيبراني ودوره الحيوي في الوضع الأمني الشامل.

1.1.2 نظرة تاريخية حول كشف التسلل

يعكس تطور تقنيات كشف التسلل المشهد المتغير لتهديدات الأمن السيبراني والبيئات التكنولوجية. ظهرت أنظمة كشف التسلل المبكرة في الثمانينيات كمشاريع بحثية أكاديمية، مع مساهمات ملحوظة شملت نظام IDES (Intrusion Detection Expert System) في SRI International ونظام NADIR (Network Anamoly Detection and Intrusion Reporter) في مختبر Los

Alamos الوطني. أسست هذه الأنظمة الرائدة العديد من المفاهيم والمناهج الأساسية التي ستوجه التطورات التجارية ومفتوحة المصدر اللاحقة.

شهدت التسعينيات تحويل تقنيات كشف التسلل إلى منتجات تجارية، حيث جلبت منتجات مثل **RealSecure** من Internet Security Systems و **NetRanger** من Cisco قدرات كشف التسلل إلى بيئات المؤسسات. شهدت هذه الفترة أيضًا ظهور بدائل مفتوحة المصدر، وأشهرها **Snort**، والتي عممت الوصول إلى قدرات كشف التسلل وعززت مجتمعًا نابضًا بالمطورين والممارسين الأمنيين. استمر التطور إلى القرن الحادي والعشرين مع دمج وظائف كشف التسلل في منصات أمنية أوسع، بما في ذلك أنظمة إدارة معلومات وأحداث الأمن (**SIEM**) وجدران الحماية من الجيل التالي، مما يعكس التطور المتزايد لكل من التقنيات الدفاعية والتهديدات السيبرانية.

1.1.3 النماذج الأساسية للكشف

يرتكز الأساس النظري والعملي لكشف التسلل على منهجيتين فلسفيتين رئيسيتين لتحديد النشاط الخبيث، لكل منهما خصائصه ونقاط قوته ومحدودياته المميزة. يمثل التمييز بين هذه النماذج مفاضلة أساسية بين الدقة والتغطية، كما نوقش على نطاق واسع في الأدبيات البحثية **[20]**.

1.1.3.1 كشف إساءة الأستخدام (الكشف القائم على التوقيعات)

تشكل هذه المنهجية حجر الزاوية في أنظمة كشف التسلل التقليدية وتحظى بنشر واسع نظرا لموثوقيتها التشغيلية وخصائص أدائها المتوقعة. كنهج قائم على المعرفة، يعتمد كشف إساءة الاستخدام على تقنيات مطابقة الأنماط لتحديد التهديدات المعروفة. تتضمن العملية مقارنة نشاط النظام أو الشبكة المرصود مع قاعدة بيانات شاملة للتوقيعات أو الأنماط التي تمثل هجمات معروفة، وثغرات، ومنهجيات استغلال.

تشكل هذه التوقيعات أوصافًا رسمية لتسلسلات الهجوم وقد تشمل تسلسلات **byte** محددة في حزم الشبكة، أو أنماطًا مميزة لاستدعاءات النظام، أو تسلسلات معينة للأحداث تشير إلى نشاط خبيث.

تعتمد الفعالية التشغيلية لأنظمة كشف إساءة الاستخدام بشكل أساسي على جودة وشمولية وتوقيت قواعد بيانات التوقيعات الخاصة بها. تعمل آلية الكشف بشكل أساسي كخوارزمية مطابقة: عندما تتوافق البيانات المرصودة بشكل كافٍ مع نمط في قاعدة المعرفة، يولد النظام إنذارًا. يظهر هذا النهج فعالية خاصة ضد التهديدات المعروفة لأنه يمكن صياغة التوقيعات بدقة عالية لتحديد مؤشرات اختراق محددة. تشمل نقاط قوة كشف إساءة الاستخدام دقته العالية المثبتة في تحديد التهديدات المعروفة، مما يؤدي إلى معدلات منخفضة للإنذارات الإيجابية الكاذبة **(false positives)** التي تجعل الإنذارات قابلة للتنفيذ من قبل المحللين الأمنيين. بالإضافة إلى ذلك، يقدم النهج مزايا كفاءة حسابية، حيث تمثل مطابقة الأنماط عملية مفهومة جيدًا وقابلة للتطوير ومناسبة للبيئات عالية الأداء. توفر الإنذارات المُنشأة عادةً معلومات محددة حول التهديدات المكتشفة، غالبًا ما تحدد أنواع هجمات معينة أو متغيرات برمجيات خبيثة.

ومع ذلك، يعاني كشف إساءة الاستخدام من عدة قيود كبيرة. الأكثر حرجًا، يظهر النهج عجزًا متأصلاً عن اكتشاف الهجمات الجديدة **(Zero-day exploits)** أو حتى تغييرات طفيفة للهجمات المعروفة التي لا يوجد لها توقيع. هذا يخلق نوافذ **vulnerability** حتمية بين ظهور تهديدات جديدة وتوفر توقيعات كشف مقابلة. تعتمد فعالية كشف إساءة الاستخدام بشكل كامل على التحديثات المستمرة وفي الوقت المناسب لقواعد بيانات التوقيعات، مما يمثل عبئًا تشغيليًا كبيرًا. علاوة على ذلك، تظل هذه الأنظمة عرضة للتهرب من خلال التقنيات التي تحجب أو تغير أنماط الهجوم (obfuscate or polymorph)، بما في ذلك تجزئة الحزم، والتشفير، أو طرق إخفاء التعليمات البرمجية التي تمنع مطابقة الأنماط الناجحة.

1.1.3.2 كشف الشذوذ (الكشف القائم على السلوك)

تمثل هذه المنهجية البديلة نهجًا أكثر طموحًا يهدف إلى التغلب على قيود الأنظمة القائمة على التوقيعات (**signature-based systems**) من خلال التركيز على الشذوذ السلوكي (**behavioral abnormalities**) بدلاً من الأنماط المعروفة. يعمل كشف الشذوذ من خلال إنشاء نماذج إحصائية أو ملفات تعريف للسلوك الطبيعي للمستخدمين، أو المضيفين، أو التطبيقات، أو الشبكات خلال فترات يُفترض أنها خالية من الهجمات. النشاط اللاحق الذي يظهر انحرافًا إحصائيًا كبيرًا عن هذه الخطوط الأساسية المُنشأة يُطلق إنذارات تشير إلى عمليات تسلل محتملة. الافتراض الأساسي الكامن وراء هذا النهج، كما ناقش من قبل Debar et al.عام 1999 ، يفترض أن النشاط التسللي يظهر خصائص مختلفة بشكل ملحوظ عن السلوك الطبيعي**[21]**.

يتضمن تنفيذ أنظمة كشف الشذوذ عادةً مراحل تدريب حيث تقوم مجموعات البيانات المرجعية بإنشاء خطوط أساس سلوكية عبر أبعاد متعددة، بما في ذلك أنماط تسجيل الدخول، واستخدام الأوامر، وأحجام حركة مرور الشبكة، وتوزيعات البروتوكولات، ومقاييس استخدام الموارد. تقيس آلية الكشف بعد ذلك باستمرار الانحراف بين النشاط الحالي والملفات الشخصية المكتسبة باستخدام الطرق الإحصائية، مع إنشاء إنذارات عندما تتجاوز الانحرافات عتبات محددة مسبقًا. تكمن القوة الأساسية لكشف الشذوذ في قدرته النظرية على تحديد الهجمات غير المعروفة سابقًا، بما في ذلك استغلالات zero-day والتهديدات الداخلية المتطورة التي قد تتجنب الكشف القائم على التوقيع. هذه القدرة تجعل كشف الشذوذ ذا قيمة خاصة لتحديد منهجيات الهجوم الجديدة وحسابات الاعتماد الشرعية المخترقة.

على الرغم من مزاياها النظرية، تعاني أنظمة كشف الشذوذ تاريخيًا من تحديات تنفيذ عملية. الأكثر بروزًا، تظهر هذه الأنظمة قابلية واضحة لتوليد أحجام عالية من الإنذارات الإيجابية الكاذبة نظرا إلى إلى الصعوبة المتأصلة في تعريف السلوك الطبيعي بشكل شامل في بيئات الحوسبة الديناميكية. التغيرات السلوكية المشروعة، مثل عمليات النشر الجديدة للتطبيقات، أو الأنشطة الإدارية غير المعتادة ولكن المصرح بها، أو الاختلافات الموسمية في الأعمال، غالبًا ما تطلق إنذارات كاذبة. هذه الظاهرة غالبًا ما تؤدي إلى إرهاق

الإنذارات (alert fatigue) بين المحللين الأمنيين، مما قد يتسبب في التغاضي عن التهديدات الحقيقية amid العديد من الإنذارات الكاذبة. بالإضافة إلى ذلك، تتطلب أنظمة كشف الشذوذ عادةً موارد حسابية كبيرة للحفاظ على الملف الشخصي والتحليل، وتعتمد فعاليتها بشدة على جودة وتمثيلية بيانات التدريب الأولية.

1.1.4 تصنيف أنظمة كشف التسلل

ما وراء نماذج الكشف الأساسية، يمكن تصنيف أنظمة كشف التسلل وفقًا لأبعاد متعددة، بما في ذلك مصادر البيانات، وهندسات النشر، ومنهجيات التحليل. يوفر فهم هذه التصنيفات نظرة حاسمة حول إمكانيات وقيود مناهج كشف التسلل المختلفة.

1.1.4.1 تصنيف مصدر البيانات

يؤثر اختيار مصادر البيانات بشكل أساسي على قدرات كشف التسلل. تراقب أنظمة كشف التسلل القائمة على الشبكة (NIDS) حركة مرور الشبكة، وتحلل رؤوس وحمولات الحزم لتحديد النشاط الخبيث. تنتشر هذه الأنظمة عادةً في مواقع شبكية استراتيجية وتوفر رؤية شاملة لاتصالات الشبكة. تعمل أنظمة كشف التسلل القائمة على المضيف (HIDS) على نقاط النهاية الفردية، وتراقب سجلات النظام، وسلامة الملفات، وتغييرات السجل (registry)، والعمليات الجارية. توفر HIDS رؤية عميقة لأنشطة المضيف ولكنها تتطلب النشر والإدارة على الأنظمة المحمية. تركز أنظمة كشف التسلل القائمة على التطبيقات بشكل خاص على أنشطة طبقة التطبيق، وتراقب سجلات المعاملات، وتفاعلات المستخدم، والأحداث الخاصة بالتطبيق. تجمع المناهج الهجينة بين مصادر بيانات متعددة لتحقيق قدرات كشف أكثر شمولاً.

1.1.4.2 نماذج النشر المعمارية

توظف أنظمة كشف التسلل نماذج معمارية مختلفة تؤثر على قابليتها للتطوير وأدائها ومتطلبات إدارتها. تقوم الهياكل المركزية بتحويل جميع بيانات الكشف إلى نقطة تحليل واحدة، مما يبسط الإدارة ولكنه قد يخلق عنق زجاجة في الأداء. تنشر الهياكل الموزعة قدرات التحليل عبر مواقع متعددة، مما يحسن قابلية التطوير ولكن يزيد من تعقيد الإدارة. تنظم الهياكل الهرمية مكونات الكشف في هياكل ذات طبقات، موازنة بين التنسيق المركزي والتحليل الموزع. تستفيد الهياكل القائمة على السحابة من موارد الحوسبة السحابية للتحليل القابل للتطوير، وهي مناسبة بشكل خاص للبيئات التنظيمية الموزعة وحماية البنية التحتية السحابية.

1.1.4.3 منهجيات التحليل

تطورت الأساليب التحليلية المستخدمة في أنظمة كشف التسلل بشكل كبير فاق الثنائية الأساسية لإساءة الاستخدام والشذوذ. تستخدم الطرق الإحصائية نماذج رياضية لتحديد الانحرافات عن الأعراف السلوكية المُنشأة. تستخدم التقنيات القائمة على المعرفة المعرفة الأمنية الرسمية، بما في ذلك توقيعات الهجوم ومعلومات الثغرات. تمثل مناهج التعلم الآلي (Machine Learning) أحدث ما توصلت إليه التقنية، مستخدمة خوارزميات تتعلم أنماط الكشف من البيانات التاريخية. تتضمن هذه طرق التعلم الخاضع للإشراف (Supervised Learning) التي تتدرب على مجموعات بيانات مُصنفة، وتقنيات التعلم غير الخاضع للإشراف (Unsupervised Learning) التي تحدد الأنماط في البيانات غير المصنفة، ومناهج شبه خاضعة للإشراف (Semi-Supervised) تجمع بين المنهجيتين. تتضمن التطورات الحديثة هياكل التعلم العميق (Deep Learning) القادرة على تحديد أنماط معقدة في مساحات البيانات عالية الأبعاد.

1.1.5 عملية كشف التسلل العامة (إطار عمل مختصر)

يتطلب الفهم الشامل لكشف التسلل فحص عملياته التشغيلية، التي تتبع عادةً إطارًا منظمًا يتضمن مراحل متعددة متسلسلة، كما هو مفصل في المراجع الأساسية **[22]**

تمثل عملية كشف التسل سلسلة متكاملة تبدأ بجمع البيانات وتنتهي بالاستجابة، وتتكون من المراحل الأساسية التالية:

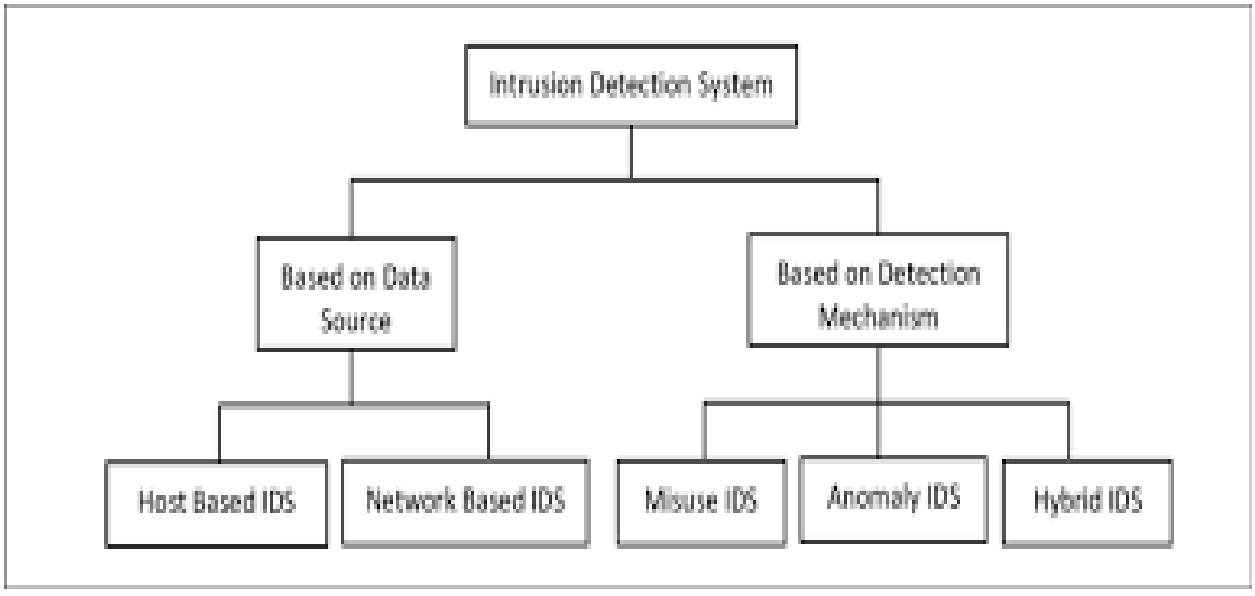
1. جمع البيانات: مرحلة تجميع البيانات الأولية من المصادر المختلفة مثل سجلات الشبكة والنظم والتطبيقات، والتي تشكل المادة الخام لعملية الكشف.

2. المعالجة المسبقة: تهيئة البيانات للتحليل من خلال تنقيتها وتبويبها واستخلاص السمات الأمنية ذات الدلالة منها، مما يسهل عملية التحليل اللاحقة.

3. التحليل والكشف: تطبيق نماذج الكشف (قائمة على التوقيعات أو السلوك) للتعرف على الأنماط غير الطبيعية، مع اتجاه الأنظمة الحديثة لاستخدام أساليب هجينة لتحسين الفعالية.

4. إدارة الإنذارات: توليد إنذارات واضحة وتصنيفها حسب درجة خطورتها وأولويتها، تمهيداً لاتخاذ الإجراء المناسب.

5. الاستجابة: احتواء التهديدات المكتشفة عبر إجراءات يدوية أو آلية، مع الحرص على مواءمة مستوى الأتمتة مع طبيعة التهديد وبيئة العمل



1.1 أنواع أنظمة كشف التسلل

1.1.6 التحديات الأساسية في كشف التسلل

1. مغالطة المعدل الأساسي (Base-Rate Fallacy)

تنشأ هذه المشكلة الإحصائية من ندرة الحوادث الأمنية الحقيقية مقارنة بحجم النشاط الطبيعي الهائل. حتى الأنظمة عالية الدقة تُنتج أعداداً كبيرة من الإنذارات الكاذبة، مما يؤدي إلى "إرهاق الإنذارات" (Alert Fatigue) ويهدد بإغفال التهديدات الفعلية[20].

2. حجم البيانات وقيود الأداء

تفرض الكميات الهائلة من البيانات المولدة في البيئات الحديثة ضغوطاً على قدرات الجمع والتخزين والمعالجة. often يتطلب هذا الموازنة بين شمولية المراقبة وأداء النظام، مما قد يخلق فجوات في التغطية.

3. التشفير وقيود الرؤية

يحد انتشار التشفير، رغم أهميته للأمن والخصوصية، من قدرة أنظمة الكشف على فحص المحتوى، مما يعيق بشكل خاص أدوات الكشف التقليدية القائمة على التوقيعات.

4. تقنيات التهرب المتطورة

يطور المهاجمون باستمرار أساليب متقدمة للتهرب من الكشف، مثل البرمجيات متعددة الأشكال والتشفير ومزج الهجمات مع الحركة الشرعية، مما يستلزم تحديثاً مستمراً لأساليب المواجهة.

5. تعقيد التكوين والصيانة

تتطلب هذه الأنظمة ضبطاً دقيقاً للإعدادات وصيانة مستمرة (كالتحديثات المنتظمة للقواعد وإعادة تدريب النماذج) لضمان فعاليتها، مما يشكل عبئاً عملياتياً كبيراً على المنظمات.

1.1.7 التطور والاتجاهات المستقبلية في كشف التسلل

1. دمج الذكاء الاصطناعي والتعلم الآلي

يسهم دمج هذه التقنيات في تعزيز دقة الكشف، خاصة في تحديد الأنماط غير المعروفة سابقاً، والحد من الإنذارات الكاذبة عبر التحليل السياقي المتقدم.

2. الأتمتة والتكامل (SOAR)

تعمل منصات SOAR على تحسين عمليات الاستجابة عبر أتمتة المهام وتنسيقها، مما يسرع احتواء التهديدات ويسهل إدارة الحوادث بشكل فعال.

3. تكامل ذكاء التهديدات

يعزز التكامل مع مصادر الذكاء التهديدي الخارجي قدرة الأنظمة على رصد الهجمات المعروفة والناشئة، مع تحسين دقة تقييم الأولويات.

4. الكشف في البيئات السحابية والقائمة على الحاويات

تتجه الأنظمة نحو دعم البيئات السحابية والحاوية، مع توفير رؤية شاملة وقابلة للتوسع، ومراقبة سلوكيات التطبيقات الحديثة.

5. تقنيات الكشف الحافظة للخصوصية

يتم تطوير تقنيات كشف متوافقة مع متطلبات الخصوصية، مثل تحليل البيانات المشفرة دون فكها، وتقليل جمع البيانات الشخصية.

1.1.8 اعتبارات التنفيذ وأفضل الممارسات

يُعد النجاح في تنفيذ أنظمة كشف التسلل رحلة متكاملة تبدأ بالإعداد الجيد وتستمر بالتحسين المستمر. أولى الخطوات تتمثل في تحقيق الانسجام التام بين النظام والسياسات الأمنية للمؤسسة وأهدافها الاستراتيجية، حيث يجب أن تعكس قواعد الكشف وعتبات الإنذار أولويات العمل ومستوى تقبله للمخاطر.

لا تقل أهمية التخطيط التقني الدقيق عن الجوانب الأخرى، إذ يجب دراسة متطلبات الأداء والشبكة والتخزين بعناية، مع الأخذ في الاعتبار الحاجة للتوسع المستقبلي. ومن الضروري أن يتم دمج النظام بسلاسة مع البنية التحتية الأمنية القائمة، لضمان تبادل المعلومات والتنسيق في الاستجابة للحوادث.

لكن كل هذا يبقى ناقصاً بدون العنصر البشري المؤهل، فاستثمار المؤسسة في تطوير كفاءات فريق الأمن وتدريبه بشكل مستمر يعد عاملاً حاسماً للنجاح. وأخيراً، يجب أن يكون التحسين المستمر منهجية عمل، عبر الاختبار الدوري وتقييم الأداء وتحديث القواعد لمواكبة المشهد المتغير للتهديدات.

1.1.9 الخاتمة

يبقى كشف التسلل مكونًا أساسيا لبرامج الأمن السيبراني الشاملة، حيث يوفر قدرات حاسمة لتحديد الحوادث الأمنية التي تتجنب الضوابط الوقائية. بينما لا تزال التحديات كبيرة، خاصة فيما يتعلق بالإيجابيات الكاذبة، وتقنيات التهرب، ومتطلبات الموارد، فإن التطورات المستمرة في منهجيات الكشف، والتكامل مع تقنيات الأمن الأخرى، وأفضل الممارسات التشغيلية تستمر في تحسين فعالية الكشف. يمثل التطور من أنظمة كشف معزولة إلى منصات عمليات أمنية متكاملة تقدمًا حاسما في معالجة القيود التاريخية. مع استمرار تطور التهديدات السيبرانية في التطور والتصاعدية، يجب أن تتقدم قدرات كشف التسلل بشكل مترابط من خلال البحث المستمر والابتكار والخبرة التنفيذية العملية.

1.2 لمحة شاملة عن الذكاء الاصطناعي

1.2.1 تعريف الذكاء الاصطناعي

الذكاء الاصطناعي (AI) هو مجال في علوم الحاسوب يهدف إلى إنشاء أنظمة قادرة على أداء مهام تتطلب عادةً ذكاءً بشرياً مثل التفكير، الفهم، اتخاذ القرارات، التعلّم من التجارب، حل المشكلات، والإبداع. بخلاف البرمجيات التقليدية، التي تتبع تعليمات مكتوبة مسبقاً، فإن أنظمة الذكاء الاصطناعي تمتلك القدرة على التكيف مع الظروف الجديدة وتحسين أدائها بمرور الوقت من خلال تحليل البيانات والتعلّم منها.

تتضمن تطبيقات الذكاء الاصطناعي العديد من الأمثلة التي نستخدمها يومياً: مساعدات الصوت مثل "سيري" و"أليكسا"، أنظمة التوصية في "نتفلكس" و"أمازون"، أنظمة الترجمة الآلية مثل "جوجل ترانسليت"، وحتى السيارات ذاتية القيادة التي تعتمد على الذكاء الاصطناعي لفهم بيئتها واتخاذ القرارات بشكل لحظي.

من الناحية النظرية، يمكن النظر إلى الذكاء الاصطناعي على أنه محاولة لمحاكاة القدرات الإدراكية البشرية في الآلة، مثل الذاكرة، الإدراك، والتعلم. ومع ذلك، فإن تعريف الذكاء الاصطناعي يتغير باستمرار مع تطور التكنولوجيا، فما كان يُعتبر "ذكاءً اصطناعياً" في الماضي (مثل التعرف على الكتابة على الحاسوب) أصبح اليوم تقنية عادية وبسيطة.

1.2.2 لمحة تاريخية

تاريخ الذكاء الاصطناعي طويل ومعقد، ويمر بعدة محطات مهمة:

- **المرحلة النظرية (قبل 1950):**

بدأت الفكرة الفلسفية منذ قرون، عندما تساءل الفلاسفة عن إمكانية بناء آلة "تفكر" مثل البشر. كتب الفيلسوف ديكارت وباسكال أفكاراً حول العقل والآلة، لكنها كانت مجرد تصورات فلسفية.

• **آلان تورينغ (1950):**

اقترح الرياضي البريطاني آلان تورينغ اختباراً ثورياً يُعرف بـ اختبار تورينغ، لقياس ما إذا كان يمكن لآلة أن تُظهر سلوكاً ذكياً غير قابل للتمييز عن الإنسان (Turing, 1950). كما أسس مفهوم آلة تورينغ الذي وضع أساس علوم الحاسوب الحديثة.

• **ولادة الذكاء الاصطناعي (1956):**

خلال مؤتمر دارتموث بقيادة john McCarthy ، تم استخدام مصطلح "الذكاء الاصطناعي" لأول مرة، ليصبح مجالاً بحثياً رسمياً **[23]**. ركزت البحوث الأولى على المنطق الرمزي وحل المشكلات الرياضية البسيطة.

• **السبعينيات والثمانينيات:**

واجه المجال عقبات كبيرة نتيجة قلة القدرة الحاسوبية وضعف البيانات المتوفرة، ما أدى إلى فترة جمود تعرف بـ "شتاء الذكاء الاصطناعي".

• **التسعينيات:**

شهدت التسعينيات نجاحات بارزة مثل انتصار حاسوب IBM "ديب بلو" على بطل العالم في الشطرنج جاري كاسباروف عام 1997، مما أثبت أن الآلة يمكن أن تتفوق على الإنسان في مجالات محددة.

• **القرن الحادي والعشرون :**

بفضل التعلم العميق (Deep Learning) والبيانات الضخمة (Big Data) والقدرات الهائلة للمعالجات الحديثة (GPUs)، عاد الذكاء الاصطناعي بقوة. اليوم نشهد تطبيقات في كل المجالات: الطب، النقل، التمويل، الأمن، التعليم، والترفيه.

1.2.3 أهمية الذكاء الاصطناعي

تكمن أهمية الذكاء الاصطناعي في قدرته على تحويل كافة مجالات الحياة الإنسانية والصناعية. فهو ليس مجرد أداة تقنية، بل قوة محركة لعصر جديد من الابتكار والتغيير. ومن بعض الأمثلة عن أهمية الذكاء الاصطناعي:

1. **في الرعاية الصحية:** يساعد الذكاء الاصطناعي في تحليل صور الأشعة، التنبؤ بالأمراض، وتصميم أدوية جديدة. مثلاً، شركات أدوية مثل DeepMind وPfizer تستخدم AI لتسريع اكتشاف العلاجات.

2. **في النقل:** السيارات ذاتية القيادة (Tesla, Waymo) قادرة على تقليل الحوادث المرورية، تحسين كفاءة الطرق، وتوفير حلول تنقل للأشخاص ذوي الإعاقة.

3. **في التمويل:** تُستخدم الخوارزميات الذكية للكشف عن الاحتيال، أتمتة التداول، وتحليل المخاطر بدقة أعلى من البشر.

4. **في التعليم:** يمكن للذكاء الاصطناعي توفير تعليم شخصي للطلاب من خلال أنظمة ذكية تكشف نقاط ضعفهم وتقترح خطط تعلم فردية.

5. **في الصناعة:** الروبوتات الذكية تؤدي مهاماً شاقة أو خطرة، وتساهم أنظمة التنبؤ بالصيانة في توفير مليارات الدولارات عبر منع الأعطال قبل وقوعها.

6. **في الحياة اليومية:** من استخدام المساعدات الرقمية إلى الترجمة الفورية وتخصيص المحتوى على الإنترنت، أصبح الذكاء الاصطناعي جزءاً لا يتجزأ من حياتنا.

بعبارة أخرى، أهمية الذكاء الاصطناعي تكمن في كونه أداة لتسريع التقدم البشري، زيادة الإنتاجية، ودفع عجلة الابتكار، لكنه في الوقت ذاته يفرض تحديات أخلاقية واجتماعية يجب التعامل معها بحذر.

1.2.4 أنواع الذكاء الاصطناعي

الذكاء الاصطناعي (AI) هو مفهوم واسع يشمل مجموعة من الأنظمة التي تسعى لمحاكاة القدرات البشرية، ولكنه يختلف من حيث القدرات التي يمتلكها. يمكن تصنيف الذكاء الاصطناعي إلى ثلاثة أنواع رئيسية حسب مستوى تعقيد النظام وقدرته على محاكاة الذكاء البشري: الذكاء الاصطناعي الضعيف، الذكاء الاصطناعي القوي، والذكاء الاصطناعي الفائق.

1- الذكاء الاصطناعي الضعيف (Narrow AI)

الذكاء الاصطناعي الضعيف هو النوع الأكثر شيوعًا واستخدامًا في حياتنا اليومية. هذا النوع من الذكاء الاصطناعي مُصمم للقيام بمهام محددة للغاية، ولا يمتلك القدرة على أداء مهام خارج نطاق ما تم تدريبه عليه. ومن أبرز أمثلته المساعدات الصوتية مثل Siri وAlexa وGoogle Assistant، التي تتمتع بقدرة على فهم اللغة المنطوقة وإتمام مهام بسيطة مثل تحديد مواعيد أو تشغيل موسيقى. كما يشمل الذكاء الاصطناعي الضعيف تطبيقات أخرى مثل التعرف على الصور، حيث يمكن للأنظمة التعرف على الأشكال والوجوه بدقة عالية، وأنظمة التوصية التي تقدم اقتراحات للمستخدم بناءً على تفضيلاته، مثل تلك التي تستخدمها منصات مثل Netflix وAmazon لتوجيه المستخدمين إلى المحتوى الذي قد يروق له في هذه الحالة **[24]**، يقوم الذكاء الاصطناعي بأداء مهمة واحدة بشكل متميز وفعال، لكنه يظل محدودًا في نطاقه.

2-الذكاء الاصطناعي القوي (AGI)

الذكاء الاصطناعي القوي (Artificial General Intelligence) هو النوع الذي يسعى إلى محاكاة الذكاء البشري بشكل كامل، بحيث تكون الأنظمة قادرة على أداء أي مهمة إدراكية يقوم بها الإنسان. على عكس الذكاء الاصطناعي الضعيف، الذي يقتصر على مهام محددة، يمكن للذكاء الاصطناعي القوي أن يتعلم وينفذ مهام جديدة تمامًا، تمامًا كما يفعل البشر. ورغم أن هذا المفهوم لا يزال نظريًا إلى حد بعيد، إلا أنه إذا تحقق، فإنه سيحدث ثورة في مجالات متعددة مثل العلم والطب والهندسة، حيث يمكن للأنظمة الذكية القوية حل المشكلات المعقدة بسرعة تفوق قدرة الإنسان. هذا النوع من الذكاء الاصطناعي قد يعيد تشكيل الطريقة التي

نعيش بها، من خلال تمكين الأنظمة من التفكير المستقل واتخاذ القرارات بمستوى عالٍ من المرونة والقدرة على التعلم **[25]**.

3-الذكاء الاصطناعي الفائق (Superintelligence)

الذكاء الاصطناعي الفائق يشير إلى نوع من الأنظمة التي تفوق الذكاء البشري في جميع جوانب القدرة العقلية. في هذا المستوى، يمكن للذكاء الاصطناعي أن يتفوق في المجالات كافة، من الإبداع إلى حل المشكلات، ومن الذكاء الاجتماعي إلى الفهم العاطفي. يعتقد البعض أن الذكاء الاصطناعي الفائق قد يمثل الحلول الكبرى لمشاكل العالم مثل الفقر والأمراض، من خلال القدرة على التفكير بشكل أسرع وأكثر دقة من الإنسان. ومع ذلك، يطرح البعض الآخر مخاوف جدية حول مخاطره الوجودية، حيث قد يكون من الصعب أو حتى من المستحيل التحكم في الأنظمة التي تتفوق في ذكائها على البشر **[26]**. هذه المخاوف تشمل القلق من أن تتطور هذه الأنظمة إلى قوة مهيمنة قد تخرج عن السيطرة وتؤثر على مستقبل الإنسانية بشكل غير متوقع.

1.2.5 المكونات الأساسية للذكاء الاصطناعي

لكي تعمل أنظمة الذكاء الاصطناعي بكفاءة، تحتاج إلى عدة مكونات رئيسية: التعلم الآلي، معالجة اللغة الطبيعية، الرؤية الحاسوبية، والروبوتات.

1-التعلم الآلي (Machine Learning): يعد التعلم الآلي أحد الفروع الأساسية للذكاء الاصطناعي. في هذا المجال، تتعلم الخوارزميات من البيانات بدلاً من أن تكون مبرمجة يدويًا للقيام بمهمة معينة. يتضمن التعلم الآلي عدة أنواع، أبرزها:

- **التعلم تحت الإشراف (Supervised Learning):** يعتمد على وجود مجموعة بيانات تحتوي على أمثلة مدروسة مع الإجابات الصحيحة، حيث تتعلم الخوارزمية كيفية التنبؤ بالإجابات بناءً على هذه الأمثلة.

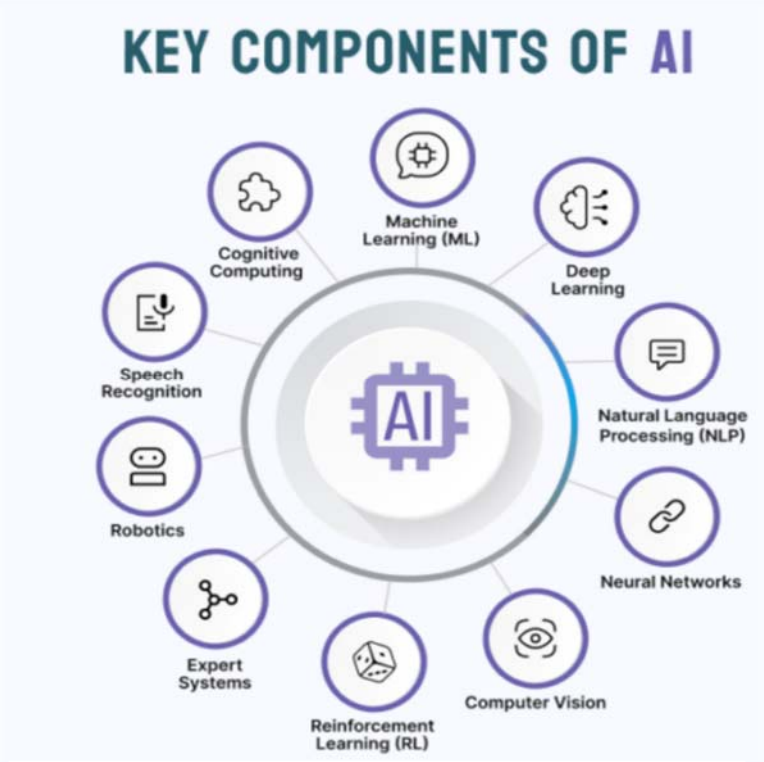
• **التعلم غير المراقب (Unsupervised Learning)**: لا يتطلب وجود إجابات صحيحة، حيث تعمل الخوارزميات على اكتشاف الأنماط أو الهياكل الخفية داخل البيانات.

• **التعلم المعزز (Reinforcement Learning)**: يعتمد على مكافآت وعقوبات لتوجيه الخوارزمية لأداء المهام بطريقة تزيد من المكافآت بمرور الوقت .

2-معالجة اللغة الطبيعية (NLP):تمكّن الآلات من فهم اللغة البشرية، وتُستخدم في المساعدات الصوتية، الترجمة الآلية (Google Translate)، وروبوتات المحادثة **[27]**.

3-الرؤية الحاسوبية (Computer Vision)تركّز على تمكين الآلات من فهم الصور والفيديوهات. تطبيقاتها تشمل: التعرف على الوجوه، السيارات ذاتية القيادة، وتشخيص الصور الطبية **[28]**.

4-الروبوتات (Robotics):تجمع بين الذكاء الاصطناعي والأنظمة الفيزيائية لأداء مهام مستقلة. تشمل: الأتمتة الصناعية، الروبوتات الجراحية، وروبوتات الاستكشاف في الفضاء وأعماق البحار.



1.2 مكونات الذكاء الاصطناعي

1.2.6 الذكاء الاصطناعي في التطبيقات الواقعية

قد أصبح الذكاء الاصطناعي (AI) جزءاً لا يتجزأ من التطور التكنولوجي السريع الذي نشهده في عالمنا اليوم. فقد أثر بشكل عميق في عدة صناعات، وجلب معه فرصاً جديدة للتطور والإبداع. في حين يعزز الذكاء الاصطناعي من كفاءة الأعمال ويسهم في الأتمتة، فإنه أيضاً يفتح أبواباً لمجالات جديدة لم تكن لتتخيلها العقول البشرية قبل عقدين من الزمن. وبالنظر إلى المجالات الرئيسية التي استفادت من الذكاء الاصطناعي، يمكننا رؤية تباين كبير في تطبيقاته.

-النقل

في مجال النقل، قاد الذكاء الاصطناعي ثورة في السيارات ذاتية القيادة، وهو ما يعد خطوة جريئة نحو الحد من الحوادث المرورية وتحسين كفاءة النقل. تسهم خوارزميات الذكاء الاصطناعي في إدارة حركة المرور في المدن الذكية، مما يساهم في تقليل الازدحام وتحسين انسيابية التنقل في المناطق الحضرية.بالإضافة إلى ذلك، يعزز الذكاء الاصطناعي من فعالية سلاسل التوريد، من خلال تحسين التنبؤات وتقليل التكاليف في النقل والخدمات اللوجستية **[30]**.

-البيع بالتجزئة والتجارة الإلكترونية:

أما في مجال التجارة الإلكترونية والبيع بالتجزئة، فقد شهدنا تحولات كبيرة بفعل الذكاء الاصطناعي، حيث أصبحت أنظمة التوصية جزءاً أساسياً من تجربة المستخدم. تقوم خوارزميات الذكاء الاصطناعي بتحليل سلوك المستهلك وتقديم توصيات مخصصة، مما يعزز من تجربة الشراء **[31]**. علاوة على ذلك، يتم تحسين إدارة المخزون والخدمات اللوجستية، ما يساعد المتاجر الإلكترونية على تقديم خدمة أفضل للعملاء

1.2.7 الآثار الأخلاقية والاجتماعية للذكاء الاصطناعي

رغم هذه الفوائد الكبيرة، لا يمكن تجاهل الآثار الأخلاقية والاجتماعية التي قد تترتب على استخدام الذكاء الاصطناعي. إن استغلال هذه التقنية يحتاج إلى مراجعة دقيقة لتداعياتها على المجتمع والفرد.

-فقدان الوظائف

من أبرز التحديات التي يثيرها الذكاء الاصطناعي هو تأثيره على سوق العمل. مع تقدم الأتمتة، قد يُستبدل عدد كبير من الوظائف التقليدية بالأنظمة الذكية، ما يؤدي إلى بطالة واسعة في بعض القطاعات **[32]**. ولتقليل هذه المخاطر، يتعين على الحكومات والشركات الاستثمار في برامج إعادة تأهيل العمال وتطوير مهاراتهم لتمكينهم من التعامل مع التغيرات التكنولوجية.

-التحيز والتمييز

من القضايا الأخرى التي يثيرها الذكاء الاصطناعي هي مسألة التحيز في البيانات. إذا تم تدريب أنظمة الذكاء الاصطناعي على مجموعات بيانات متحيزة، فإن ذلك قد يؤدي إلى نتائج غير عادلة تعزز الفوارق الاجتماعية والاقتصادية **[33]**. لمعالجة هذه المشكلة، هناك حاجة إلى تطوير خوارزميات أكثر عدلاً واعتماد ممارسات بيانات متنوعة تتجنب هذه التحيزات.

-قضايا الخصوصية

لخصوصية هي إحدى القضايا البارزة التي تثيرها تطبيقات الذكاء الاصطناعي، خاصة في مجالات مثل المراقبة والتعرف على الوجوه. إن تكاثر البيانات الشخصية والمعاملات الرقمية يجعل من الصعب ضمان حماية الخصوصية **[34]**. وبالتالي، تبرز الحاجة إلى وضع قوانين أكثر صرامة لحماية هذه البيانات وضمان استخدامها في إطار قانوني وآمن.

-حوكمة الذكاء الاصطناعي

بناءً على ما سبق، تبرز الحاجة إلى تطوير إطار تنظيمي قوي للذكاء الاصطناعي، يضمن الشفافية والمساءلة والعدالة في استخدام هذه التقنية . وقد تبنت العديد من الدول والمنظمات الدولية مثل الاتحاد الأوروبي ومنظمة التعاون الاقتصادي والتنمية هذا التوجه لضمان أن تكون تطبيقات الذكاء الاصطناعي آمنة ومسؤولة.

1.2.8 الآفاق المستقبلية في الذكاء الاصطناعي

من المرجح أن يتوسع الذكاء الاصطناعي في مجالات أكثر تقدماً، مما يجلب فرصاً ومخاطر جديدة.من بعض هذه التوسعات:

تعزيز القدرات البشرية:تشمل التطبيقات الأطراف الصناعية المدعومة بالذكاء الاصطناعي وأدوات تعزيز القدرات الإدراكية **[35]**.

الذكاء الاصطناعي العام (AGI):يهدف الذكاء الاصطناعي العام إلى بلوغ مستوى الذكاء البشري. ورغم إمكاناته الهائلة، إلا أنه يثير مخاوف تتعلق بالسلامة وضبط الأهداف.

التفرد التكنولوجي:توقع Kurzweil (2005) **[36]**. أن النمو الأسي للذكاء الاصطناعي قد يؤدي إلى تفرد تكنولوجي يغيّر المجتمع جذرياً

1.2.9 الخاتمة

لقد غيّر الذكاء الاصطناعي مجرى التاريخ في العديد من المجالات. ورغم ما يقدمه من فوائد هائلة في الابتكار وحل المشاكل، إلا أنه يثير تحديات أخلاقية واجتماعية قد تؤثر على حياتنا اليومية. لضمان استخدام هذه التكنولوجيا بشكل مسؤول، لابد من تطوير سياسات وقوانين متوازنة تساعد على استثمار إمكانيات الذكاء الاصطناعي مع الحفاظ على القيم الإنسانية وحماية المجتمع.

1.3 لمحة شاملة عن SIEM

1.3.1 تعريف ونطاق SIEM

أنظمة إدارة معلومات وأحداث الأمن(SIEM) هي جانب حيوي من استراتيجيات الأمن السيبراني الحديثة، حيث توفر منصة مركزية لجمع وتحليل والتصرف في مجموعة واسعة من البيانات المتعلقة بالأمن. تم تصميم حلول SIEM لتقديم نظرة شاملة ورؤى دقيقة حول وضع الأمان في المنظمة، مما يمكّن من الاكتشاف السريع والاستجابة للتهديدات المحتملة.

يشمل تعريف SIEMعنصرين رئيسيين: إدارة معلومات الأمان (SIM) وإدارة أحداث الأمان .(SEM) تشمل إدارة معلومات الأمان جمع وتخزين وتحليل بيانات الأمان من مصادر مختلفة ضمن بيئة تكنولوجيا المعلومات. قد تشمل هذه البيانات سجلات النظام، وبيانات حركة المرور على الشبكة، وغيرها من الأدلة الرقمية ذات الصلة. الهدف الرئيسي هنا هو جمع أكبر قدر ممكن من المعلومات ذات الصلة لدعم فهم جيد للحوادث الأمنية وضمان الاحتفاظ بالبيانات على المدى الطويل من أجل التحليل الجنائي .

من ناحية أخرى، تركز إدارة أحداث الأمان على المراقبة في الوقت الفعلي، والربط، والتنبيه حول الأحداث الأمنية. وهي مسؤولة عن تحديد الأنماط التي تشير إلى الحوادث الأمنية المحتملة من خلال تحليل تدفقات البيانات والأحداث أثناء حدوثها. يستخدم SEM خوارزميات متقدمة وقواعد معرفة للكشف عن الأنماط غير الطبيعية والأنشطة المشبوهة والتهديدات المحتملة. يضمن الجمع بين SIM و SEM أن منصة SIEM لا تقتصر فقط على جمع وتخزين البيانات الأساسية، بل توفر أيضًا معلومات قابلة للعمل لفرق الأمان.

لقد تطور نطاق SIEM بشكل كبير مع تزايد تعقيد التهديدات السيبرانية. في البداية، كانت حلول SIEM تعتمد بشكل رئيسي من قبل الشركات الكبيرة ذات البنى التحتية الواسعة لتكنولوجيا المعلومات. ومع ذلك، فإن تزايد وتيرة وشدة الهجمات السيبرانية قد دفع المنظمات من جميع الأحجام إلى تنفيذ أنظمة SIEM. يتجاوز نطاق SIEM الحديث إدارة السجلات فقط ويشمل عدة وظائف حاسمة:

1. **جمع وإدارة السجلات:** تقوم أنظمة SIEM بجمع البيانات من مجموعة متنوعة من المصادر، بما في ذلك الخوادم، والجدران النارية، والموجهات، والتطبيقات، ونقاط النهاية. تسهل هذه المنصة المركزية جمع السجلات إدارة وتحليل البيانات بشكل موحد، مما يوفر رؤية شاملة لمشهد الأمان في المنظمة.

2. **المراقبة والتنبيه في الوقت الفعلي:** من خلال تحليل البيانات الواردة بشكل مستمر، يمكن لأنظمة SIEM تقديم تنبيهات في الوقت الفعلي حول الأحداث الأمنية المحتملة. وهذا يمكّن فرق الأمان من الرد بسرعة على التهديدات المحتملة، مما يقلل من فترة تعرض المنظمة للثغرات.

3. **كشف الحوادث والاستجابة لها:** تقدم أنظمة SIEM أيضًا القدرة على تحديد الحوادث الأمنية المحتملة من خلال قواعد الارتباط المتقدمة والخوارزميات السلوكية.

بمجرد اكتشاف التهديد، يمكن لمنصات SIEM أن تبدأ تلقائيًا تنفيذ بروتوكولات الاستجابة المحددة مسبقًا، مثل عزل الأنظمة المتأثرة أو تفعيل تدفقات استجابة الحوادث.

4. **التقارير الخاصة بالامتثال:** العديد من الصناعات تخضع لمتطلبات تنظيمية تفرض الاحتفاظ وتحليل بيانات الأمان. غالبًا ما تأتي حلول SIEM مع قدرات تقارير الامتثال المدمجة، مما يساعد المنظمات على الوفاء بالمعايير التشريعية والمعايير الخاصة بالصناعة مثل GDPR و HIPAA و PCI-DSS.

5. **تكامل معلومات التهديدات:** يمكن للحلول الحديثة لـ SIEM أن تتكامل مع موجزات معلومات التهديدات لإثراء البيانات السياقية المتاحة للتحليل. وهذا يمكّن المنظمات من البقاء في صدارة التهديدات الناشئة من خلال الاستفادة من المعلومات في الوقت الفعلي حول الثغرات المعروفة، وطرق الهجوم، وسلوكيات المعتدين.

6. **التحليل الجنائي:** في أعقاب حادث أمني، توفر أنظمة SIEM بيانات ثمينة للتحقيقات الجنائية. يمكن تحليل البيانات التاريخية المخزنة في منصة SIEM لتتبع تسلسل الزمان لهجوم، وتحديد نقاط الدخول، وفهم نطاق الاختراق.

إحدى النقاط القوية لـ SIEM تكمن في قدرته على تقديم رؤية شاملة للوضع الأمني للمنظمة، من خلال دمج البيانات من مصادر متفرقة لتكشف سردًا متماسكًا لأحداث الأمان. ومع ذلك، فإن تنفيذ وتشغيل نظام SIEM يقدمان بعض التحديات. تشمل هذه التحديات الحجم الكبير للبيانات التي يجب إدارتها، وتعقيد قواعد الارتباط والخوارزميات، والحاجة إلى ضبط مستمر لتجنب الإيجابيات الكاذبة والسلبيات الكاذبة.

في الختام، فإن تعريف ونطاق SIEM يجسد نهجًا شاملًا نحو الأمن السيبراني، يهدف إلى تعزيز قدرة المنظمة على اكتشاف التهديدات والرد عليها والتخفيف من آثارها. من خلال دمج جمع البيانات مع التحليل المتقدم وقدرات التنبيه، تشكل أنظمة SIEM مكونًا محوريًا في استراتيجية فعالة للأمن السيبراني، مما يحمي الأصول التنظيمية في ظل بيئة رقمية أصبحت أكثر خطورة.

1.3.2 دور SIEM في ضمان الأمان

أصبحت أنظمة SIEM مركزية في استراتيجيات الأمن السيبراني الحديثة، حيث تلعب دورًا محوريًا في تحديد التهديدات والرد عليها والتخفيف منها. تقوم هذه الأنظمة بجمع وتحليل البيانات من مصادر متعددة ضمن البنية التحتية لتكنولوجيا المعلومات للمنظمة، مما يخلق رؤية شاملة لمشهد الأمان. من خلال القيام بذلك، تمكن أدوات SIEM المنظمات من اكتشاف الحوادث الأمنية في الوقت الفعلي، مما يوفر أداة لا تقدر بثمن للحفاظ على أوضاع أمان قوية.

أحد الوظائف الرئيسية لـ SIEM هو جمع وتوحيد البيانات من مصادر متفرقة مثل الجدران النارية، أنظمة الكشف عن التسلل/أنظمة منع التسلل (IDS/IPS)، الخوادم، التطبيقات، وغير ذلك. يضمن هذا الجمع أن تكون جميع البيانات ذات الصلة متمركزة، مما يعزز منصة التحليل الموحدة. من خلال التوحيد، تستطيع أنظمة SIEM جمع البيانات في شكل مشترك، مما يسهل تحليلها وارتباطها من مصادر متعددة. وهذا أمر بالغ الأهمية لأنه يحول البيانات الخام إلى معلومات قابلة للعمل، مما يسهم في اتخاذ قرارات سريعة ومدروسة.

المراقبة في الوقت الفعلي هي قدرة أساسية أخرى لـ SIEM. مع تزايد تعقيد التهديدات السيبرانية، أصبحت القدرة على مراقبة الأنظمة بشكل مستمر وفي الوقت الفعلي أمرًا بالغ الأهمية. تستخدم أنظمة SIEM قواعد الارتباط والتحليلات المتقدمة لاكتشاف الأنماط الشاذة والأنشطة الخبيثة المحتملة عبر الشبكة. على سبيل المثال، إذا تم اكتشاف محاولة تسجيل دخول لمستخدم من مواقع جغرافية متعددة خلال فترة زمنية قصيرة، يمكن لنظام SIEM تحديد هذا السلوك كأمر مشبوه وتحفيز تنبيه. من خلال ربط البيانات من مصادر متعددة، يمكن لأنظمة SIEM تحديد أحداث قد تشير إلى اختراق أمني، حتى إذا كان كل حدث على حدة يبدو غير ضار.

بمجرد تحديد التهديد المحتمل، تلعب أنظمة SIEM دورًا حيويًا في استجابة الحوادث. حيث توفر تفاصيل دقيقة حول طبيعة التهديد، والنظام المتأثر، والجدول الزمني للأحداث، والتي تعد جميعها أمورًا حاسمة من أجل الإصلاح الفعال. بالإضافة إلى ذلك، توفر حلول SIEM إمكانيات استجابة آلية، مثل عزل الأنظمة المتأثرة أو حظر عناوين IP الخبيثة، مما يقلل من تأثير التهديدات مع الحد الأدنى من التأخير. تساعد هذه الأتمتة المنظمات على الاستجابة بسرعة للتهديدات، مما يقلل من فرص المهاجمين.

التوافق مع اللوائح هو أمر آخر حيث تكون أنظمة SIEM ضرورية. تفرض اللوائح مثل GDPR و HIPAA و PCI-DSS على المنظمات الحفاظ على سجلات مفصلة للبيانات الأمنية وضمان نزاهة وسرية المعلومات الحساسة. تساعد أنظمة SIEM المنظمات على تلبية المتطلبات التنظيمية من خلال توفير قدرات جمع بيانات قوية وتوليد تقارير تدقيق شاملة. إن القدرة على إنتاج تقارير موثوقة وتوثيق التدابير الأمنية يضمن أن المنظمات قادرة على إثبات امتثالها للأنظمة، وبالتالي تجنب الغرامات القانونية والتبعات المالية.

بالإضافة إلى اكتشاف التهديدات والامتثال، تساهم أنظمة SIEM في الاستراتيجية الأمنية العامة من خلال التحسين المستمر والتطوير. من خلال تحليل البيانات التاريخية، تمكن هذه الأنظمة المنظمات من تحديد المشكلات المتكررة، وتقييم فعالية تدابير الأمان الحالية، واتخاذ قرارات مستنيرة بشأن الاستثمارات المستقبلية

في البنية التحتية للأمان. يضمن هذا النهج الاستباقي أن المنظمات لا تقتصر على التفاعل مع الحوادث فقط، بل تعمل على تعزيز موقف الأمان لديها بشكل مستمر.

علاوة على ذلك، مع اعتماد المنظمات بشكل متزايد على خدمات السحابة والتقنيات المحمولة، يصبح مشهد الأمان أكثر تعقيدًا وديناميكية. تتطور أنظمة SIEM لمواجهة هذه التحديات من خلال دمج ميزات متقدمة مثل التعلم الآلي، وتحليل سلوك المستخدم والأنشطة (UEBA)، ودمج معلومات التهديدات. تعزز هذه الابتكارات قدرة أنظمة SIEM على اكتشاف التهديدات المعقدة والتكيف مع بيئة الأمان المتغيرة باستمرار.

أحد الاتجاهات الناشئة في مشهد SIEM هو تكامل SIEM مع منصات تنسيق الأمان والأتمتة والاستجابة (SOAR). يعزز هذا التكامل قدرات SIEM من خلال إضافة سير العمل الآلي وكتب التشغيل الخاصة بالاستجابة للحوادث، مما يقلل من وقت الاستجابة ويحسن كفاءة العمليات الأمنية.

باختصار، تلعب أنظمة SIEM دورًا حيويًا في نجاح استراتيجية الأمان في المنظمة. من خلال توفير المراقبة في الوقت الفعلي، والاستجابة للحوادث، ودعم الامتثال، والتحسين المستمر، تمكّن أدوات SIEM المنظمات من اكتشاف التهديدات والرد عليها والتخفيف من آثارها بشكل فعال. مع تطور مشهد الأمان السيبراني، ستتطور أيضًا قدرات أنظمة SIEM، مما يضمن بقاؤها جزءًا لا غنى عنه من استراتيجية الأمان الشاملة.

1.3.3 نظرة تاريخية حول أنظمة SIEM

لقد تطورت أنظمة SIEM بشكل كبير منذ نشأتها، مما يعكس التغيرات الأوسع في مشهد الأمن السيبراني وتكنولوجيا المعلومات. لفهم الجوانب التاريخية لأنظمة SIEM، من الضروري التعمق في أصولها وتطورها والعوامل التي دفعت إلى تبنيها وتطورها.

يمكن إرجاع نشأة SIEM إلى أواخر التسعينيات وبداية العقد الأول من الألفية الجديدة. في تلك الفترة، بدأت المؤسسات في إدراك أهمية جمع وتحليل البيانات المتعلقة بالأمن من مصادر مختلفة داخل شبكاتها. الأدوات الأمنية المبكرة مثل أنظمة كشف التسلل (IDS) وأنظمة إدارة السجلات قدمت رؤية حول التهديدات الأمنية المحتملة وانتهاكات السياسات. ومع ذلك، كانت هذه الأدوات غالبًا معزولة وتفتقر إلى القدرة على ربط البيانات من مصادر مختلفة، مما أدى إلى رؤى مجزأة وغير مكتملة عن الوضع الأمني للمؤسسة.

إن التعقيد المتزايد لبيئات تكنولوجيا المعلومات وتطور الهجمات الإلكترونية تطلب نهجًا أكثر شمولاً لمراقبة وإدارة الأمن. أدى ذلك إلى ظهور مفهوم SIEM، وهو مصطلح يجمع بين إدارة معلومات الأمن (SIM) وإدارة أحداث الأمن (SEM). تركز SIM على جمع وتخزين وتحليل البيانات المتعلقة بالأمن، بينما تركز SEM على المراقبة اللحظية وربط الأحداث الأمنية. من خلال دمج هاتين الوظيفتين، قدمت أنظمة SIEM حلاً موحدًا لإدارة وتحليل المعلومات الأمنية.

الحلول المبكرة لـ SIEM مثل تلك التي طورتها شركات مثل ArcSight (تأسست عام 2000) وNetForensics استُخدمت بشكل أساسي من قبل المؤسسات الكبيرة والوكالات الحكومية. امتلكت هذه المنظمات الموارد والخبرة اللازمة لتنفيذ وإدارة البنى التحتية المعقدة التي تتطلبها تلك الأنظمة. كانت الاستخدامات الرئيسية لأنظمة SIEM في تلك المرحلة تشمل: إعداد تقارير الامتثال، كشف التهديدات، والاستجابة للحوادث. كما دفعت المتطلبات التنظيمية، مثل قانون ساربينز أوكسلي (SOX) لعام 2002 وقانون HIPAA لعام 1996، العديد من المؤسسات إلى اعتماد أنظمة SIEM للوفاء بالتزاماتها التنظيمية.

ومع نضوج التكنولوجيا، بدأت أنظمة SIEM تتبنى ميزات أكثر تقدمًا، مثل التنبيهات اللحظية، وأتمتة الاستجابة للحوادث، ودعم نطاق أوسع من مصادر البيانات. كما ساهم ظهور تقنيات البيانات الضخمة والاستخدام المتزايد للتعلم الآلي (ML) والذكاء الاصطناعي (AI) في تعزيز قدرات هذه الأنظمة. مكّنت هذه التطورات المؤسسات من التعامل مع كميات أكبر من البيانات، وكشف تهديدات أكثر تعقيدًا، وتقليل الوقت المطلوب لتحديد والاستجابة للحوادث الأمنية.

شهد منتصف العقد الثاني من الألفية نقطة تحول مهمة في تبني أنظمة SIEM، حيث أكدت الهجمات السيبرانية وتسريبات البيانات على الحاجة إلى حلول أمنية قوية.

لقد أبرزت الحوادث البارزة مثل اختراق Target في عام 2013 وقرصنة Pictures Sony في عام 2014 العواقب الخطيرة لضعف المراقبة الأمنية، وسرّعت من اعتماد أنظمة SIEM في مختلف الصناعات. خلال هذه الفترة، وسّع مزودو SIEM عروضهم لتشمل حلولاً قائمة على السحابة وخدمات مُدارة، مما جعل التكنولوجيا أكثر سهولة للشركات الصغيرة والمتوسطة (SMEs) التي لم تكن تمتلك الموارد اللازمة لإدارة أنظمة SIEM محليًا.

تستمر أنظمة SIEM الحديثة في التطور استجابةً للتحديات الجديدة في الأمن السيبراني والتطورات التكنولوجية. إن التبني المتزايد للحوسبة السحابية، وأجهزة إنترنت الأشياء (IoT)، وبيئات العمل عن بُعد، قد وسّع من مساحة الهجوم وأدخل تعقيدات جديدة لمراقبة الأمن.

تم تصميم حلول SIEM المعاصرة للتعامل مع هذه التحديات من خلال توفير رؤية محسّنة ووعيًا سياقيًا عبر البيئات السحابية الهجينة والمتعددة. كما تستفيد من التحليلات المتقدمة، والتحليل السلوكي، وتغذية معلومات التهديدات من أجل تحسين دقة وكفاءة كشف التهديدات والاستجابة لها.

1.3.4 المفاهيم الأساسية في أنظمة SIEM

تعد أنظمة إدارة معلومات وأحداث الأمن (SIEM) مكونًا أساسيًا في مجال الأمن السيبراني، حيث صُممت لتوفير تحليل لحظي للتنبيهات الأمنية الناتجة عن التطبيقات، وأجهزة الشبكات، والبنية التحتية الأخرى لتقنية المعلومات. تأتي مرونة أنظمة SIEM من مجموعة من المفاهيم الأساسية التي تُنشئ معًا إطارًا قويًا لتحديد الحوادث الأمنية وتحليلها والاستجابة لها. تتناول هذه الفقرة أبرز هذه المفاهيم: ترابط الأحداث، إدارة السجلات، المراقبة اللحظية، الاستجابة للحوادث، وإعداد تقارير الامتثال.

يعد ترابط الأحداث وظيفة جوهرية في أنظمة SIEM. جوهر هذه العملية يتمثل في تجميع كميات ضخمة من البيانات من مصادر متباينة وتحليلها لاستخلاص المعنى. الأحداث التي قد تبدو عادية عند النظر

إليها بشكل منفصل يمكن أن تُظهر نمطًا مقلقًا عند ربطها معًا. على سبيل المثال: محاولات تسجيل دخول فاشلة متعددة تليها محاولة ناجحة قد تُشير إلى هجوم (Brute Force Attack). تستخدم أدوات SIEM خوارزميات وقواعد معدة مسبقًا لربط هذه الأحداث في الزمن الحقيقي، مما يمكّن محللي الأمن من اكتشاف الحوادث والتحقيق فيها التي قد تفوتها المراقبة التقليدية.

تشير إدارة السجلات إلى العملية الآلية لجمع وتخزين وإدارة بيانات السجلات الناتجة عن أجهزة الشبكة، والخوادم، والتطبيقات، وأنظمة تقنية المعلومات الأخرى. تُركز حلول SIEM هذه البيانات في مكان واحد، مما يضمن الاحتفاظ طويل الأجل بها في صيغة آمنة وغير قابلة للتغيير. تساعد إدارة السجلات الفعّالة ليس فقط في الامتثال والتحليل الجنائي، بل تعزز أيضًا من كفاءة عمليات كشف التهديدات ومعالجتها. كما أن تحليل وتطبيع بيانات السجلات من مصادر مختلفة يمكّن أنظمة SIEM من إنشاء قاعدة بيانات موحدة وقابلة للبحث بسهولة.

المراقبة اللحظية هي قدرة أنظمة SIEM على مراقبة حركة مرور الشبكة، وأنشطة المستخدمين، وسلوكيات الأنظمة بشكل مستمر لاكتشاف الأنشطة المشبوهة أو الخبيثة. تُعد هذه القدرة ضرورية لتحديد التهديدات المحتملة فور وقوعها، مما يتيح استجابات أسرع تقلل من الأضرار المحتملة. توفر لوحات التحكم (Dashboards) تصورات وتنبيهات تُبرز الشذوذات، بينما تستخدم التحليلات المتقدمة تقنيات التعلم الآلي لاكتشاف مؤشرات خفية للاختراق. إن الفورية في المراقبة اللحظية تضمن أن تتمكن المؤسسات من الاستجابة بسرعة للتهديدات الأمنية المتطورة.

تشمل الاستجابة للحوادث ضمن إطار عمل SIEM الاستراتيجيات والعمليات اللازمة للتعامل مع التهديدات الأمنية والتخفيف من آثارها بشكل فعّال. غالبًا ما تتكامل منصات SIEM مع أنظمة تذاكر الدعم (Ticketing Systems)، لتنسيق استجابة منظمة من خلال التنبيهات الآلية، وسير عمل التحقيقات، وخطط الاستجابة المحددة مسبقًا. عندما يحدد النظام حادثًا أمنيًا، يمكن لفرق الأمن بسرعة تقييم خطورته، وتحديد الأنظمة المتأثرة، وتنفيذ التدابير المضادة. تلعب الأتمتة دورًا محوريًا هنا، حيث يمكنها تنفيذ

استجابات معدة مسبقًا مثل عزل الأجهزة المتأثرة أو تفعيل تحديثات لسياسات الأمان. هذا النهج المنظم يقلل من وقت التوقف وفقدان البيانات.

أحد الجوانب المحورية في نشر حل SIEM هو قدرته على تسهيل الامتثال للمعايير التنظيمية مثل GDPR، وHIPAA، وPCI DSS. تتطلب هذه اللوائح تسجيلًا ومراقبةً وإعداد تقارير واسعة النطاق حول الأحداث الأمنية. تُبسّط أدوات SIEM عملية الامتثال من خلال إنشاء تقارير شاملة آليًا تلبي المتطلبات التنظيمية المحددة. كما توفر أيضًا مسارات تدقيق ورؤى حول انتهاكات السياسات، مما يعزز الشفافية والمساءلة. إن المراقبة المستمرة للامتثال تساعد المؤسسات على تجنب العقوبات وإظهار التزامها بحماية البيانات.

1.3.5 مكونات نظام SIEM الفعّال

تُعد أنظمة إدارة معلومات وأحداث الأمن (SIEM) جزءًا أساسيًا من استراتيجيات الأمن السيبراني الحديثة. تعتمد المؤسسات على حلول SIEM من أجل جمع وتحليل البيانات الأمنية من مصادر متعددة، مما يوفر رؤية شاملة ويُمكّن من الكشف الاستباقي عن التهديدات. تتكون أنظمة SIEM الفعّالة من عدة مكونات رئيسية، يلعب كل منها دورًا حاسمًا في ضمان المراقبة الأمنية القوية والاستجابة للحوادث.

جمع البيانات و توحيدها: الركيزة الأساسية لأي نشر فعّال لـ SIEM هي قدرته على جمع وتوحيد البيانات من مجموعة واسعة من المصادر. تشمل هذه المصادر أجهزة الشبكة، الخوادم، التطبيقات، الأجهزة الأمنية (مثل الجدران النارية وأنظمة كشف/منع التسلل) ، و منصات حماية نقاط النهاية. إن البيانات المجمعة توفر رؤية شاملة لوضع الأمن في المؤسسة وتُعد بمثابة مادة خام للتحليلات اللاحقة.

إدارة السجلات: تُعد السجلات المصدر الأساسي للبيانات التي تعمل عليها أنظمة SIEM. يجب أن تمتلك الأنظمة الفعّالة قدرات قوية لإدارة السجلات، بما في ذلك: جمع السجلات، تخزينها، و صيانتها بشكل يضمن أنها غير قابلة للتغيير ومُتاحة لفترات طويلة، كما تتطلب اللوائح التنظيمية. يُعد ضمان سلامة

وتوافر السجلات أمرًا بالغ الأهمية سواء للتحليل الجنائي أو للامتثال لمتطلبات تنظيمية مثل: GDPR، HIPAA، PCI-DSS.

المراقبة اللحظية والتنبيهات: تُعد المراقبة اللحظية المستمرة وظيفة حيوية لأنظمة SIEM. تمكّن هذه القدرة من مراقبة حركة مرور الشبكة والأحداث داخل الأنظمة بشكل لحظي، مما يسمح للمؤسسات بالكشف عن الحوادث الأمنية والاستجابة لها فور وقوعها. ينبغي على أنظمة SIEM الفعّالة أن تُولّد تنبيهات استنادًا إلى قواعد معدة مسبقًا وشذوذات تُشير إلى تهديدات أمنية محتملة. ويجب أن تكون هذه التنبيهات مصنّفة بدقة لتفريق الضوضاء العادية في الشبكة عن القضايا الأمنية الحقيقية، مما يقلل من الإنذارات الكاذبة ويضمن قدرة فرق الأمن على الاستجابة بسرعة للحوادث الحرجة.

محرك الترابط: من المكونات الأساسية لحلول SIEM الفعّالة قدرتها على ترابط البيانات من مصادر مختلفة للتعرف على الأنماط والعلاقات التي قد لا تُشير بشكل منفرد إلى تهديد أمني. يقوم محرك الترابط بمعالجة وتحليل البيانات المجمّعة وفقًا لمجموعة من القواعد المحددة مسبقًا أو باستخدام تحليلات متقدمة وخوارزميات تعلم آلي. يساعد هذا المكوّن في التعرف على أنماط الهجمات المعقدة والتهديدات متعددة المراحل التي قد تفوت على حلول أمنية أحادية النقطة.

الكشف عن الحوادث والاستجابة لها: يجب أن يسهّل نظام SIEM الفعّال ليس فقط الكشف عن الحوادث الأمنية بل أيضًا الاستجابة لها. يشمل ذلك التكامل مع أدوات ومنصات أمنية أخرى مثل: SOAR. تساعد آليات الاستجابة المؤتمتة في احتواء التهديدات بسرعة، بينما تُوجّه التدفقات المحددة مسبقًا وأدلة التشغيل المحللين في التحقيق ومعالجة الحوادث. هذا المكوّن يضمن نهجًا منظمًا وفعّالًا لإدارة الحوادث، مما يقلل من الأضرار المحتملة الناتجة عن اختراقات الأمن.

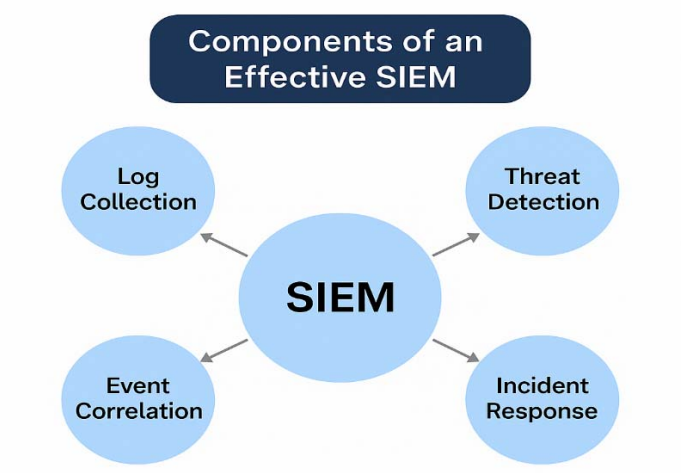
دمج معلومات التهديد: إدماج تغذيات معلومات التهديد داخل SIEM يعزز من قدرته على الكشف عن التهديدات المعروفة. توفر معلومات التهديد بيانات محدثة حول: عناوين IP ضارة، نطاقات مشبوهة، و التواقيع المرتبطة بالأنشطة الخبيثة. من خلال دمج هذه البيانات، يمكن لـ SIEM تحديد التهديدات وحظرها

بشكل استباقي حتى قبل حدوثها. هذا التكامل يساعد المؤسسات على البقاء محمية ضد التهديدات السيبرانية المتطورة باستمرار.

لوحات التحكم والتقارير: تُعد الرؤية والاتصال عنصرين حيويين في أي SIEM فعّال. توفر لوحات التحكم تمثيلًا رسوميًا للوضع الأمني، مما يمكّن أصحاب المصلحة من فهم مشهد التهديد الحالي بسرعة. تشمل ميزات إعداد التقارير القابلة للتخصيص القدرة على إنشاء تقارير مفصلة تُستخدم لأغراض التدقيق، الامتثال، وتقديم المعلومات للإدارة. هذه الميزات أساسية لتقديم رؤى دقيقة وتسهيل اتخاذ القرارات المستنيرة داخل المؤسسة.

القابلية للتوسع والأداء: مع نمو المؤسسات، يجب أن تكون أنظمة SIEM قادرة على التوسع للتعامل مع أحجام بيانات متزايدة دون التأثير على الأداء. هذا يضمن أن SIEM يمكنه الاستمرار في العمل بشكل مثالي حتى مع تطور احتياجات المؤسسة.

الامتثال والحوكمة: يساعد SIEM الفعّال المؤسسات على تلبية التزامات الامتثال عبر توفير: مسارات تدقيق شاملة، سجلات مفصلة، و الوثائق المطلوبة. يجب أن يدعم النظام الامتثال لمعايير ولوائح تنظيمية مثل: GDPR، HIPAA، PCI-DSS. هذا يُظهر التزام المؤسسة بأمن البيانات ويعزز من الثقة والمصداقية.



1.3 مكونات نظام SIEM الفعال

الفصل الثاني: تجهيز بيئة العمل

2.1 مقدمة عامة

يعتمد المشروع على منظومة Wazuh SIEM لجمع وتحليل السجلات الأمنية من الأنظمة المختلفة، إلى جانب استخدام جدار الحماية pfSense كمصدر رئيسي لبيانات الشبكة وحركة المرور، بينما يتم تشغيل كامل البيئة على نظام التشغيل Linux Ubuntu لما يوفره من استقرار ومرونة ودعم واسع لتطبيقات الأمن السيبراني. ويتيح هذا التكامل بين مكونات النظام إمكانية تحليل السجلات بشكل مركزي، ثم تطبيق خوارزميات الذكاء الاصطناعي لاكتشاف الأنماط الشاذة التي قد تشير إلى محاولات اختراق في مراحلها المبكرة.

من خلال هذا النهج، يسعى المشروع إلى تحقيق توازن فعّال بين الدقة في الكشف، تقليل الإنذارات الكاذبة، وسرعة الاستجابة للتهديدات، مما يجعله مناسبًا للأغراض البحثية والأكاديمية، وقابلًا للتطبيق العملي في البيئات الواقعية التي تتطلب أنظمة مراقبة أمنية ذكية وقابلة للتوسع

2.2 نظام التشغيل: Linux Ubuntu

لمحة عن Ubuntu

يُعد Ubuntu أحد أكثر توزيعات Linux انتشارًا واستخدامًا في بيئات الخوادم والبنية التحتية للشبكات، حيث يتميز بكونه نظام تشغيل مفتوح المصدر مبني على نواة Linux، مع دعم واسع من المجتمع التقني والشركات. يتم الاعتماد في هذا المشروع على إصدار LTS (Long Term Support) لما يوفره من استقرار عالٍ، تحديثات أمنية طويلة الأمد، وتقليل مخاطر التوقف أو الأعطال أثناء تشغيل النظام لفترات طويلة.

كما يتميز Ubuntu بسهولة الإدارة، وضوح هيكل النظام، وتوافر عدد كبير من الحزم البرمجية الجاهزة، مما يجعله خيارًا مثاليًا لاستضافة أنظمة تحليل أمني متقدمة مثل SIEM وخوارزميات الذكاء الاصطناعي.

دور Ubuntu في المشروع

يؤدي نظام Ubuntu دور المنصة المركزية التي يتم فوقها تشغيل جميع مكونات المشروع، حيث يتم استخدامه في:

- استضافة خادم Wazuh Server بكامل مكوناته، بما يشمل مدير الأحداث، المفهرس، ولوحة التحكم.
- تشغيل خدمات تحليل السجلات الأمنية القادمة من الأنظمة المختلفة، سواء كانت سجلات نظام، شبكة، أو جدار حماية.
- توفير بيئة مناسبة لتشغيل خوارزمية Isolation Forest باستخدام لغة Python، مع دعم المكتبات الخاصة بتحليل البيانات والتعلم الآلي.
- إدارة موارد النظام (المعالج، الذاكرة، التخزين) بكفاءة عالية، مما يضمن استقرار النظام حتى عند معالجة كميات كبيرة من السجلات والأحداث الأمنية.

مقارنة Ubuntu مع Kali Linux

عند مقارنة Ubuntu مع Kali Linux، يتضح أن كل نظام صُمم لغرض مختلف. Kali Linux موجه أساسًا لاختبارات الاختراق والهجمات الأمنية، ويحتوي على أدوات هجومية جاهزة، لكنه لا يُعد خيارًا مناسبًا للعمل المستمر أو لاستضافة أنظمة إنتاجية طويلة الأمد.

في المقابل، يتميز Ubuntu باستقراره العالي، ملاءمته لبيئات الخوادم، وانخفاض استهلاكه للموارد، مما يجعله الأنسب لاستضافة منظومة SIEM وتشغيل خوارزميات الذكاء الاصطناعي بشكل دائم وموثوق، خاصة في السياقات الأكاديمية والبحثية.

Kali Linux	Ubuntu Linux	المعيار

الغرض الأساسي	تشغيل الخوادم والأنظمة الإنتاجية	اختبارات الاختراق والهجوم
الاستقرار	عالي جدًا ومناسب للعمل طويل الأمد	أقل استقرارًا للاستخدام المستمر
بيئة الخادم	مهيأ لاستضافة خدمات SIEM وتحليل البيانات	غير مخصص لاستضافة خوادم إنتاجية
استهلاك الموارد	متوازن ومناسب للأنظمة التحليلية	أعلى بسبب كثرة الأدوات المثبتة
التحديثات	منتظمة ومستقرة (LTS)	تحديثات سريعة وقد تسبب عدم استقرار
الملاءمة للمشروع	عالية جدًا	منخفضة

2.1 مقارنة Ubuntu مع Kali linux

سبب اختيار Ubuntu

تم اختيار Ubuntu للأسباب التالية:

1. يتمتع بدرجة عالية من الاستقرار، وهو عامل حاسم لتشغيل أنظمة المراقبة الأمنية بشكل متواصل.
2. مصمم أساسًا لبيئات الخوادم وليس للاختبار أو الهجوم، مما يعزز من موثوقية البيئة.
3. يقدم دعمًا ممتازًا لتطبيقات SIEM وأنظمة تحليل السجلات.
4. يتكامل بسلاسة مع أدوات الذكاء الاصطناعي ومكتبات Python الخاصة بالتعلم الآلي.
5. مناسب للتطبيق العملي الحقيقي وليس للاستخدام التجريبي فقط.

2.3 منظومة SIEM

لمحة عن Wazuh

يُعد Wazuh نظامًا مفتوح المصدر يجمع بين خصائص SIEM و XDR، حيث يوفر إمكانيات متقدمة لجمع وتحليل السجلات، كشف التسلل، مراقبة سلامة الملفات، واكتشاف الأنشطة غير الطبيعية. يتميز Wazuh بمرونته العالية وقدرته على العمل في بيئات متنوعة، مع دعم واسع للتكامل مع أدوات خارجية، بما في ذلك خوارزميات الذكاء الاصطناعي.

مكونات Wazuh

تتكون منظومة Wazuh من عدة مكونات مترابطة تعمل معًا لتوفير رؤية أمنية شاملة:

- Wazuh Manager: المسؤول عن تحليل الأحداث، تطبيق القواعد الأمنية، وتوليد التنبيهات.
- Wazuh Indexer: يتولى تخزين وفهرسة البيانات بشكل يسمح بالبحث السريع والتحليل المتقدم.
- Wazuh Dashboard: واجهة رسومية تفاعلية لعرض السجلات، التنبيهات، والمؤشرات الأمنية.
- Wazuh Agent: يتم تثبيته على الأنظمة الطرفية لجمع السجلات وإرسالها إلى الخادم المركزي.

دور Wazuh في المشروع

في هذا المشروع، يلعب Wazuh دور العمود الفقري لمنظومة التحليل الأمني، حيث يقوم بـ:

- جمع السجلات الأمنية من الأنظمة المختلفة.
- تنفيذ تحليل أولي للأحداث باستخدام القواعد التقليدية.
- تزويد خوارزمية Isolation Forest بالبيانات اللازمة لاكتشاف السلوكيات الشاذة.

- عرض التنبيهات المبكرة التي تشير إلى احتمالية حدوث اختراق.

مقارنة Wazuh مع Splunk SIEM

على الرغم من قوة Splunk، إلا أنه نظام تجاري مغلق نسبيًا، وتكلفته العالية تحد من استخدامه في الأبحاث الأكاديمية. بالمقابل، يوفر Wazuh تحكمًا كاملًا بالبيانات، مرونة عالية في التخصيص، وإمكانية دمج خوارزميات الذكاء الاصطناعي بسهولة، مما يجعله أكثر ملاءمة للأبحاث والتجارب العلمية.

Splunk SIEM	Wazuh SIEM	المعيار
تجاري	مفتوح المصدر	نوع النظام
مرتفعة	مجاني	التكلفة
محدود نسبيًا	كامل	التحكم بالبيانات
متوسطة	عالية	سهولة الدمج مع الذكاء الاصطناعي
محدودة بقيود ترخيص	عالية جدًا	المرونة في التخصيص
ضعيفة	ممتازة	الملاءمة للأبحاث الأكاديمية
غير عملي	مناسب جدًا	الاستخدام في المشروع

2.2 مقارنة Wazuh مع Splunk SIEM

سبب اختيار Wazuh

تم اختيار Wazuh للأسباب التالية:

1. كونه مفتوح المصدر يجعله مثاليًا للأبحاث الأكاديمية.
2. يوفر تحكمًا كاملًا بالبيانات دون قيود تجارية.
3. يسهل دمجه مع خوارزميات الذكاء الاصطناعي.
4. منخفض التكلفة مقارنة بالحلول التجارية.

5. يتمتع ببنية واضحة وقابلة للتوسع مستقبلًا.

2.4 جدار الحماية: pfSense

لمحة عن pfSense

pfSense هو جدار حماية مفتوح المصدر مبني على نظام FreeBSD، ويُستخدم لإدارة حركة المرور الشبكية وتطبيق سياسات الأمان. يتميز بواجهة سهلة، دعم قوي للمراقبة الشبكية، وإمكانية تسجيل الأحداث الأمنية بالتفصيل.

دور pfSense في المشروع

يؤدي pfSense دور خط الدفاع الأول في البيئة، حيث يقوم بـ:

- حماية الشبكة الداخلية من التهديدات الخارجية.
- مراقبة حركة المرور وتحليلها.
- كشف السلوكيات الشبكية المشبوهة.
- تزويد Wazuh بسجلات الشبكة لاستخدامها في التحليل الذكي.

مقارنة pfSense مع Cisco ASA

على الرغم من قوة Cisco ASA، إلا أن تكلفته العالية وكونه نظامًا تجاريًا يجعلان pfSense خيارًا أفضل للأغراض التعليمية والبحثية، خاصة مع مرونته العالية وسهولة تخصيصه.

Cisco ASA	pfSense	المعيار
تجاري	مفتوح المصدر	نوع النظام

مرتفعة	مجاني	التكلفة
معقدة	سهلة نسبيًا	سهولة الإعداد
محدود نسبيًا	مفصل وقابل للتخصيص	تسجيل الأحداث (Logging)
يتطلب إعداد إضافي	سهل	التكامل مع SIEM
ضعيفة	ممتازة	الملاءمة الأكاديمية
غير عملي	مناسب جدًا	الاستخدام في المشروع

2.3 مقارنة pfSense مع CiscoASA

سبب اختيار pfSense

تم اختيار pfSense للأسباب التالية:

1. مفتوح المصدر ومجاني.
2. يوفر دعمًا قويًا لمراقبة الشبكة.
3. يتكامل بسهولة مع Wazuh.
4. مناسب للبيئات الأكاديمية.
5. قابل للتوسع والتخصيص حسب متطلبات المشروع.

الخلاصة

إن اعتماد بيئة عمل مبنية على Linux Ubuntu كنظام تشغيل مستضيف، ومنظومة Wazuh SIEM، وجدار الحماية pfSense، يوفّر منصة متكاملة وآمنة للكشف المبكر عن الاختراقات باستخدام الذكاء الاصطناعي. لم يكن اختيار هذه المكونات عشوائيًا، بل جاء نتيجة مقارنة علمية مدروسة مع بدائل تجارية، أظهرت تفوق الحلول المفتوحة المصدر من حيث المرونة، التكلفة، والملاءمة البحثية، مما يجعل هذه البيئة أساسًا قويًا لتطوير أنظمة كشف اختراقات ذكية وفعّالة.

الفصل الثالث: الحل المقترح

3.1 مقدمة عامة للفصل

بعد العرض النظري المفصّل في الفصلين الأول والثاني، وما تضمّناه من تأطيرٍ لمفاهيم كشف التسلّل ودور أنظمة SIEM والتحديات المصاحبة، ينتقل هذا الفصل إلى تقديم حل عملي مقترح يهدف إلى الكشف المبكر عن محاولات الاختراق بالاعتماد على الذكاء الاصطناعي ضمن بيئة SIEM تشغيلية. يرتكز الحل على خط أنابيب (Pipeline) متكامل يبدأ من استيعاب البيانات وتطبيعها، مرورًا بـ اشتقاق السمات السلوكية ذات الدلالة الأمنية، ثم نمذجة الشذوذ بأساليب تعلم آلي غير خاضعة للإشراف، وصولًا إلى توليد إنذارات قابلة للتنفيذ وربطها بتدفقات الاستجابة. هذا الانتقال من التنظير إلى التطبيق يتسق مع الأهداف العامة للمشروع في تقليص زمن الاكتشاف وخفض الإيجابيات الكاذبة وتعزيز الصيد الاستباقي للتهديدات.

يركّز النموذج المرجعي للحل على حالة استخدام محورية هي محاولات كسر كلمات المرور (Brute Force) لخدمة SSH؛ إذ تُعدّ هذه الهجمة مثالًا مناسبًا لإظهار قيمة التحليل السلوكي القائم على تجميع الأحداث زمنياً وقياس مؤشرات مثل: Flow duration, Total forward packets, Total backward packets, SYN flag count, ACK flag count. تُغذّي هذه المؤشرات خوارزميات كشف الشذوذ (مثل Isolation Forest) لتمييز الأنماط غير المعتادة دون الحاجة إلى بيانات موسومة سلفًا، مع تعيين مستويات خطورة قابلة للضبط وعتبات تشغيلية تُراعي طبيعة الضوضاء في بيئات المؤسسات.

3.2 بنية الحل المقترح

طبقة جمع البيانات (Data Collection Layer): تبدأ العملية من خلال جمع سجلات محاولات الدخول (Logs) في صيغة CSV، حيث تحتوي على الحقول الأساسية مثل الوقت، وعنوان الـIP، واسم المستخدم، ونوع الخدمة، وحالة المحاولة. هذه البيانات تمثل المصدر الخام الذي يُبنى عليه التحليل.

طبقة المعالجة والاستخراج (Processing & Feature Extraction Layer): في هذه المرحلة تُحوّل السجلات الخام إلى سمات (Features) إحصائية قابلة للتحليل مثل عدد المحاولات الكلي، عدد المحاولات الفاشلة، معدل الفشل، وعدد المستخدمين المستهدفين. هذه المرحلة أساسية لأنها تختصر البيانات وتبرز المؤشرات الأكثر دلالة على هجمات Brute Force.

طبقة الذكاء الاصطناعي (AI Detection Layer): يتم في هذه الطبقة تطبيق خوارزمية Isolation Forest التي تقوم بعزل السلوكيات الشاذة عن السلوكيات الطبيعية، استنادًا إلى السمات المستخرجة. أي محاولة دخول ذات خصائص غير اعتيادية (عدد هائل من المحاولات الفاشلة، معدل فشل مرتفع، أو استهداف عدة مستخدمين من نفس الـIP) يتم تصنيفها كهجوم محتمل.

طبقة التكامل والعرض (Integration & Visualization Layer): بعد اكتشاف الهجمات، يتم إرسال النتائج إلى منصة Wazuh، حيث تُعرض في لوحات مراقبة تفاعلية (Dashboards) تتضمن جداول، مخططات زمنية، ورسوم بيانية توضح الهجمات المكتشفة ومصادرها وأوقاتها. هذه الطبقة تجعل الحل عمليًا وقابلاً للتطبيق في بيئات عمل حقيقية.

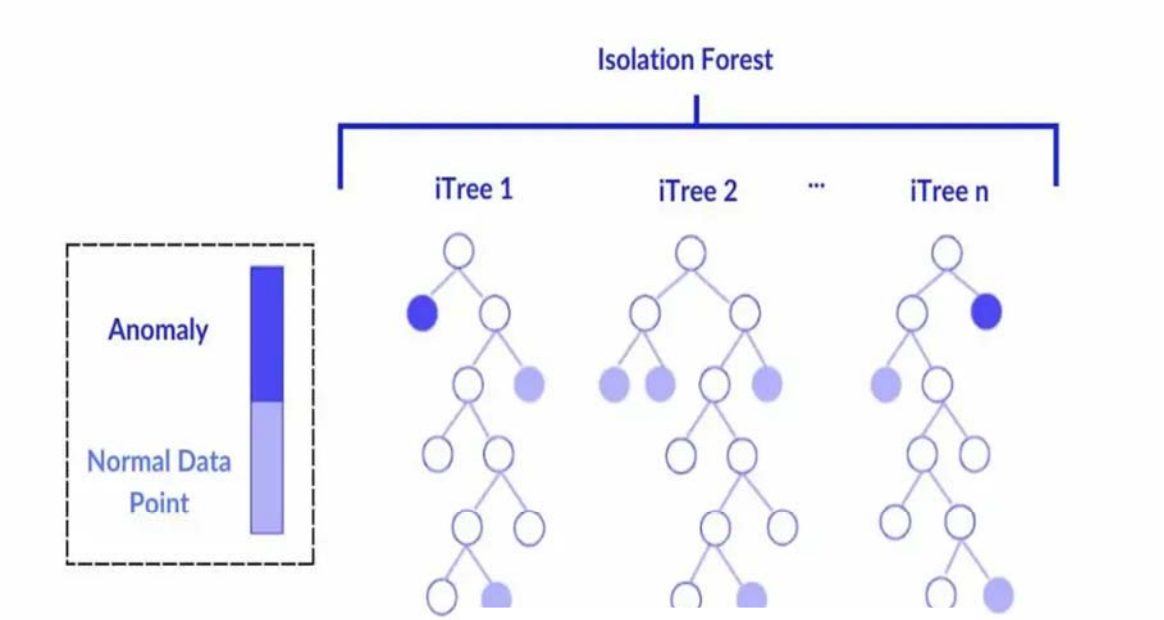
هذا التصميم المعماري يوفّر إطارًا متكاملًا يجمع بين جمع البيانات، المعالجة، التحليل الذكي، والعرض البصري، مما يجعله حلًا متوازنًا قادرًا على دعم المحللين الأمنيين في مهام الكشف المبكر والاستجابة للهجمات.

3.3 شرح آلية عمل الخوارزمية (Isolation Forest)

خوارزمية Isolation Forest (غابة العزل) هي خوارزمية مخصصة لـ الكشف عن الشذوذ (Anomaly Detection)، طُوِّرت عام 2008، وتتميز بفعاليتها مع البيانات الكبيرة وقدرتها على التعامل مع الحالات النادرة. بخلاف خوارزميات التصنيف التقليدية، فإنها لا تحاول نمذجة السلوك الطبيعي ثم البحث عن الانحرافات، بل تعتمد على مبدأ أن النقاط الشاذة تكون أسهل وأسرع في العزل من النقاط الطبيعية.

3.3.1 الفكرة الرئيسية

النقاط الطبيعية (Normal Data Points) متقاربة في التوزيع وتحتاج إلى عدد أكبر من عمليات التقسيم حتى يتم فصلها. النقاط الشاذة (Anomalies) بعيدة عن التجمعات الرئيسية، ويمكن عزلها بعدد قليل من عمليات التقسيم. أي أن الخوارزمية تعتبر عملية عزل النقطة مقياسًا لمدى شذوذها: كلما كان العزل أسرع، كلما ارتفعت احتمالية كون النقطة شاذة.

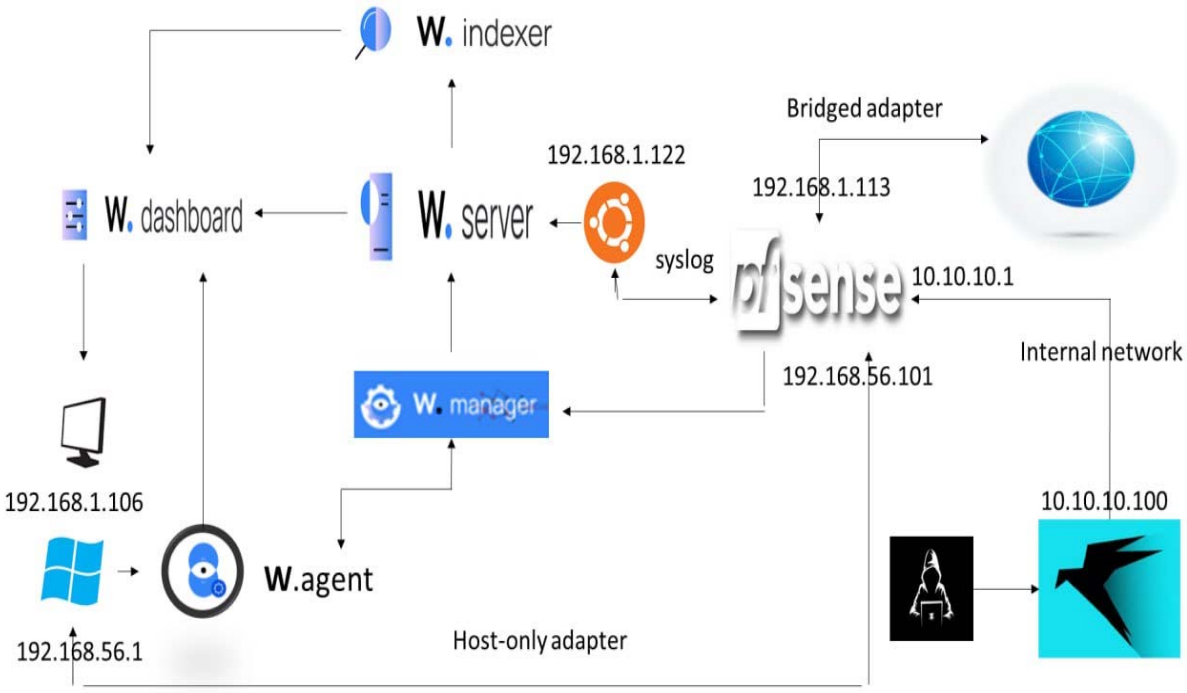


3.1 آلية عمل خوارزمية isolation forest

تُظهر هذه الصورة المبدأ الأساسي لعمل خوارزمية Isolation Forest، والتي تُستخدم بشكل واسع في اكتشاف الشذوذات (Anomalies) ضمن البيانات. الفكرة العامة تقوم على إنشاء مجموعة من الأشجار العشوائية تسمى iTrees، حيث يتم تقسيم البيانات بشكل متكرر إلى أن يتم عزل كل نقطة بيانات في مسار معين داخل الشجرة. في الصورة نرى أن هناك عدة أشجار (iTree 1, iTree 2 ... iTree n). كل شجرة تعمل بشكل مستقل على تقسيم البيانات، والنتيجة النهائية هي دمج قرارات هذه الأشجار لتحديد ما إذا كانت النقطة تمثل سلوكًا طبيعيًا أم شاذًا. النقاط الفاتحة اللون تمثل بيانات طبيعية (Normal Data Point)،

حيث تحتاج عادةً إلى مسار طويل داخل الأشجار حتى يتم عزلها، مما يعني أنها تتشابه مع بقية البيانات. أما النقاط الغامقة اللون فهي تمثل الشذوذ (Anomaly)، حيث يتم عزلها بسرعة عبر مسار قصير داخل الشجرة، لأنها مختلفة عن الأنماط المعتادة في البيانات. بهذا الأسلوب تصبح الخوارزمية قادرة على التمييز بين محاولات الدخول الشرعية (التي تتوزع بشكل طبيعي) ومحاولات الهجوم مثل Brute Force (التي تظهر كسلوك مختلف وسهل العزل).

3.4 تجهيز البنية الشبكية و العملية



3.2 بنية النظام

الصورة تُظهر ثلاث شبكات منطقية، لكل واحدة هدف:

1) شبكة خارجية/حقيقية عبر Bridged adapter: 192.168.1.0/24

- تمثل شبكة الراوتر/الإنترنت في بيئة المستخدم.
- pfSense يمتلك عليها واجهة بعنوان: 192.168.1.113 (WAN/Bridged) متصلة بالإنترنت.

• خادم Wazuh ظاهر بعنوان: 192.168.1.122 ضمن نفس النطاق، لتسهيل الاتصال وإرسال الـ Syslog عبر الشبكة الفعلية/المجسّرة.

2) شبكة Host-only: 192.168.56.0/24

• شبكة "إدارة/ربط داخلي" بين جهاز المضيف (Host) والآلات الافتراضية بدون الاعتماد على الراوتر.

• pfSense لديه عليها عنوان: 192.168.56.101

• جهاز المضيف (ويندوز) لديه: 192.168.56.1

• فائدتها: قناة اتصال ثابتة لإدارة المختبر حتى لو تغيّرت إعدادات الشبكة الخارجية.

3) شبكة داخلية معزولة (Internal network): 10.10.10.0/24

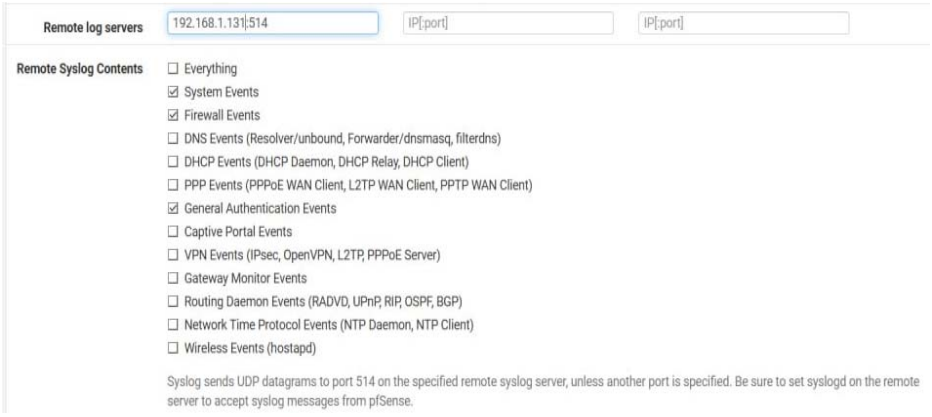
• هذه شبكة الاختبار للهجوم والدفاع داخل المختبر.

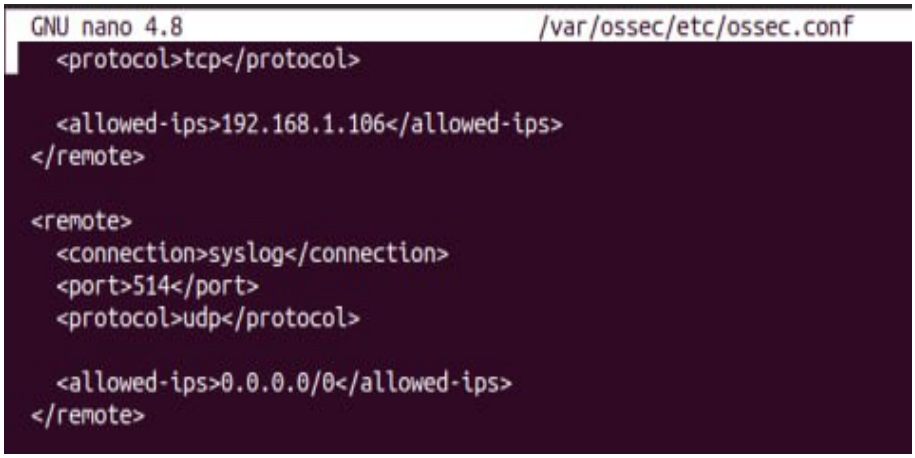
• pfSense يعمل كبوابة (Gateway) لها بعنوان: 10.10.10.1

• يوجد داخلها:

• جهاز مهاجم (Parrot) لتنفيذ الهجمات داخل بيئة آمنة ومعزولة و لها عنوان: 10.10.10.101

3.5 الربط بين Pfsense و Wazuh server





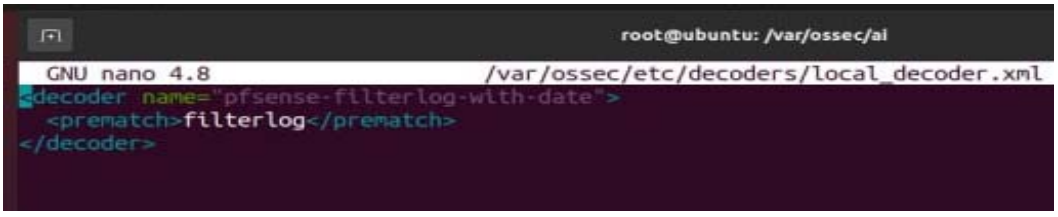
3.3 الربط بين wazuh و pfsense

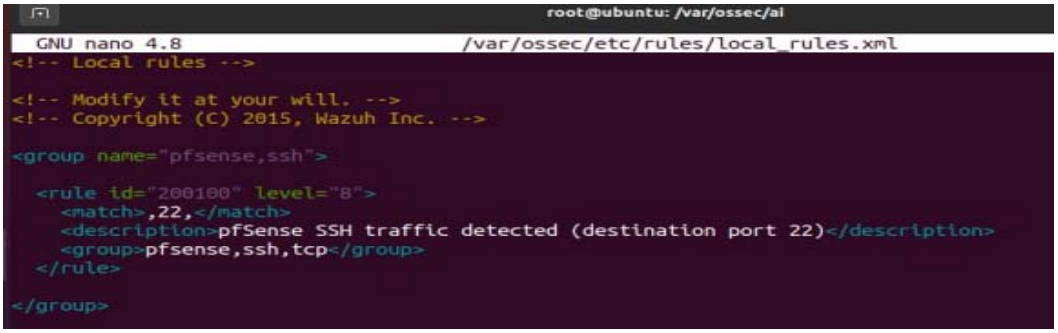
تم إعداد خادم Wazuh ليعمل كمستقبل (Syslog Receiver) Syslog من خلال تفعيل إعدادات <remote> في ملف ossec.conf باستخدام البروتوكول UDP على المنفذ 514.

وفي المقابل، تم ضبط جدار الحماية pfSense لإرسال سجلاته إلى عنوان الخادم (192.168.1.113:514) متضمِّنةً سجلات النظام والجدار الناري.

تتيح هذه الخطوة جمع وتحليل بيانات الشبكة من المصدر نفسه، مما يُسهِّل تطبيق خوارزميات الكشف المبكر عن الهجمات وتحليل الأنماط ضمن بيئة الـ SIEM المقترحة.

3.6 تهيئة القواعد و Decoders

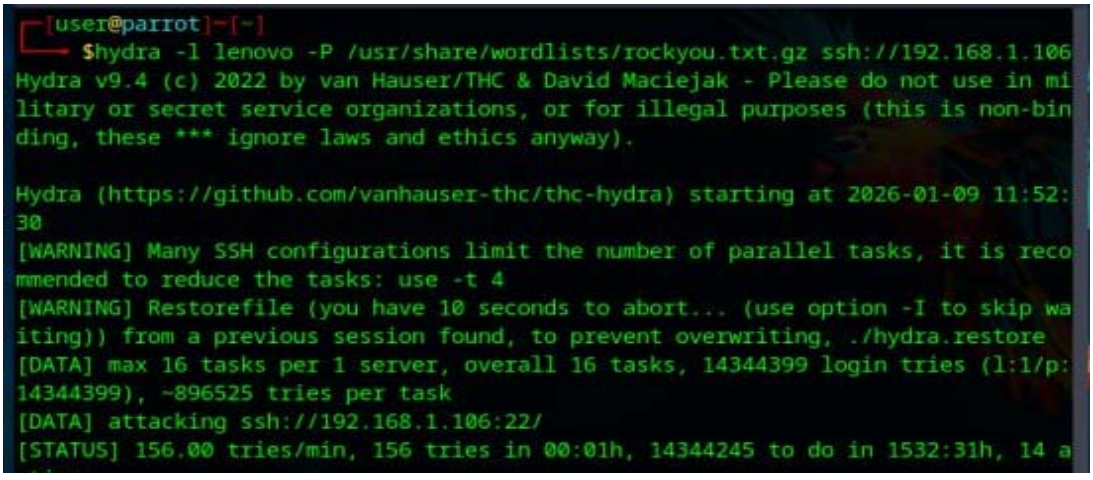




3.4 القواعد و Decoders

تمت تهيئة Wazuh لاستقبال سجلات pfSense من نوع filterlog عبر إنشاء Decoder مخصص باستخدام آلية prematch للتعرّف الأولي على السجلات المرتبطة بالجدار الناري. بعد ذلك تم تطوير قاعدة كشف محلية ضمن local_rules.xml بهدف رصد حركة SSH من خلال مطابقة نمط يشير إلى منفذ الوجهة 22، مع ضبط مستوى الخطورة (level=8) وتصنيف الحدث ضمن مجموعات (pfsense, ssh, tcp). يوضح هذا الإجراء سلسلة التحليل في Wazuh بدءًا من تعريف نمط السجل (Decoding) وصولًا إلى تطبيق منطق الكشف وإنتاج التنبيه (Rule-based Detection).

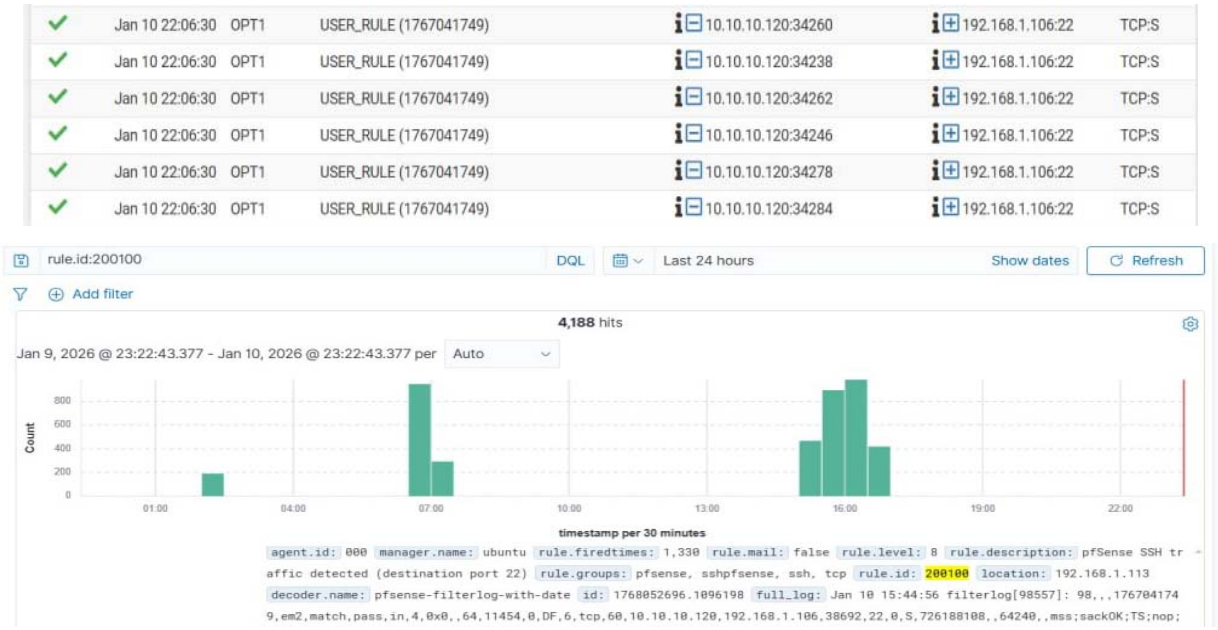
3.7 تنفيذ هجمة (BRUTE FORCE) SSH لأختبار القواعد العادية (بدون ذكاء اصطناعي)



3.5 تنفيذ الهجمة

ظهر هذه الصورة تنفيذ تجربة محاكاة لهجوم تخمين كلمات المرور (SSH Brute Force) ضمن بيئة مختبرية معزولة باستخدام نظام Parrot OS كجهاز مُهاجم. تم تشغيل أداة اختبار كلمات المرور Hydra لاستهداف خدمة SSH على جهاز ضمن نفس الشبكة (عنوان IP ظاهر في الشاشة)، مع الاعتماد على قائمة كلمات مرور (Wordlist) بهدف توليد عدد كبير من محاولات تسجيل الدخول المتتالية. أثناء التنفيذ تعرض الأداة مؤشرات تشغيلية مثل معدل المحاولات في الدقيقة وعدد المهام المتوازية وحالة الجلسة، ما يوضح الطبيعة التكرارية للهجوم. تُستخدم هذه الخطوة في سياق الدراسة لتوليد سجلات واقعية يمكن إرسالها إلى منظومة SIEM/Wazuh وتحليلها لاستخراج الأنماط، وبناء قواعد/نماذج كشف مبكر عن محاولات الاختراق، مع التأكيد أن التجربة تمت لأغراض بحثية وتعليمية ضمن نطاق مُصرّح به.

3.8 التقاط السجلات و توليد الإنذارات



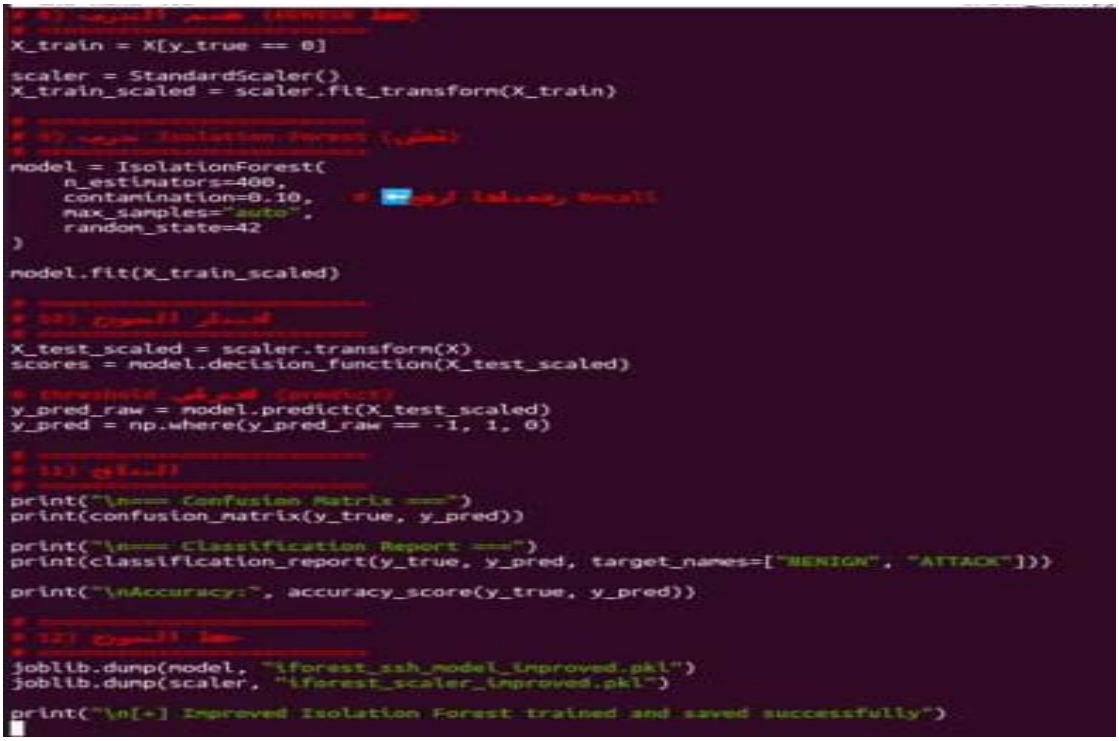
3.6 توليد الانذارات

بعد تنفيذ هجمة Brute Force على خدمة SSH من جهاز المهاجم ضمن الشبكة الداخلية، تمر حركة المرور أولًا عبر pfSense الذي يعمل كبوابة (Gateway/Firewall) بين الشبكات. يقوم pfSense بتسجيل كل محاولة اتصال ضمن Firewall Logs (filterlog)، حيث تظهر الحزم المتجهة إلى منفذ الوجهة TCP/22 على جهاز الضحية مع تكرار سريع للمحاولات، وهو نمط سلوكي مميز لهجمات التخمين. بعد ذلك يتم تفعيل ميزة Remote Syslog في pfSense لإرسال هذه السجلات بشكل فوري إلى خادم Wazuh عبر بروتوكول Syslog (UDP/514). عند وصول السجلات إلى Wazuh، يتم تمريرها عبر مرحلة Decoding للتعرّف على أنها سجلات pfSense (باستخدام decoder محلي يعتمد على prematch لكلمة filterlog)، ثم تُطبَّق قواعد الكشف (Rules) المعرفة ضمن local_rules.xml؛ وفي هذه الحالة تقوم القاعدة ذات المعرف rule.id=200100 برصد الاتصالات المتعلقة بـ SSH اعتمادًا على ظهور منفذ 22 ضمن السجل. نتيجة ذلك يولّد Wazuh تنبيهًا (Alert) بمستوى خطورة محدد (level=8)، ويتم فهرسة الحدث ضمن wazuh-alerts-* ليظهر مباشرة في واجهة Wazuh Dashboard/Discover على شكل عدد كبير من الـ hits مرتبط بزمن الهجوم، مما يؤكد نجاح سلسلة الرصد من (الهجوم ← تسجيله في pfSense ← إرساله عبر Syslog ← تحليله في Wazuh ← إصدار Alert).

3.9 تدريب خوارزمية الكشف

```
import pandas as pd
import numpy as np
from sklearn.ensemble import IsolationForest
from sklearn.preprocessing import StandardScaler
from sklearn.metrics import classification_report, confusion_matrix, accuracy_score
import joblib

# ------------------------------
# 1) تحميل البيانات
# ------------------------------
df = pd.read_csv("Tuesday-WorkingHours.pcap_ISCX.csv")
df.columns = df.columns.str.strip()

# ------------------------------
# 2) فلترة SSH فقط
# ------------------------------
ssh = df[df["Destination Port"] == 22].copy()

# ------------------------------
# 3) اختيار Features (موجودة عندك)
# ------------------------------
FEATURES = [
    "Flow Duration",
    "Total Fwd Packets",
    "Total Backward Packets",
    "SYN Flag Count",
    "ACK Flag Count",
    "Flow Packets/s",
    "Flow Bytes/s",
    "Packet Length Mean"
]

X = ssh[FEATURES].copy()

# ------------------------------
# 4) Labels (للتقييم فقط)
# ------------------------------
y_true = ssh["Label"].apply(
    lambda x: 0 if str(x).upper() == "BENIGN" else 1
)

# ------------------------------
# 5) تنظيف البيانات
# ------------------------------
X.replace([np.inf, -np.inf], np.nan, inplace=True)
X.dropna(inplace=True)

y_true = y_true.loc[X.index]
```

```
X = ssh[FEATURES].copy()

# ------------------------------
# 4) Labels (للتقييم فقط)
# ------------------------------
y_true = ssh["Label"].apply(
    lambda x: 0 if str(x).upper() == "BENIGN" else 1
)

# ------------------------------
# 5) تنظيف البيانات
# ------------------------------
X.replace([np.inf, -np.inf], np.nan, inplace=True)
X.dropna(inplace=True)

y_true = y_true.loc[X.index]

# ------------------------------
# 6) Quantile clipping (اختياري لكن مهم)
# ------------------------------
lower = X.quantile(0.001)
upper = X.quantile(0.999)
X = X.clip(lower=lower, upper=upper, axis=1)

# ------------------------------
# 7) Log transform (لأن القيم كبيرة)
# ------------------------------
X = np.log1p(X)

# ------------------------------
# 8) تدريب الموديل (BENIGN فقط)
# ------------------------------
X_train = X[y_true == 0]

scaler = StandardScaler()
X_train_scaled = scaler.fit_transform(X_train)

# ------------------------------
# 9) تدريب Isolation Forest (خفيف)
# ------------------------------
model = IsolationForest(
    n_estimators=400,
    contamination=0.10,   # 💡 جرّبي لاحقًا 0.05 أو 0.15
    max_samples="auto",
    random_state=42
)
```



```
X_train = X[y_true == 0]

scaler = StandardScaler()
X_train_scaled = scaler.fit_transform(X_train)

model = IsolationForest(
    n_estimators=400,
    contamination=0.10,
    max_samples="auto",
    random_state=42
)

model.fit(X_train_scaled)

X_test_scaled = scaler.transform(X)
scores = model.decision_function(X_test_scaled)

y_pred_raw = model.predict(X_test_scaled)
y_pred = np.where(y_pred_raw == -1, 1, 0)

print("\n=== Confusion Matrix ===")
print(confusion_matrix(y_true, y_pred))

print("\n=== Classification Report ===")
print(classification_report(y_true, y_pred, target_names=["BENIGN", "ATTACK"]))

print("\nAccuracy:", accuracy_score(y_true, y_pred))

joblib.dump(model, "iforest_ssh_model_improved.pkl")
joblib.dump(scaler, "iforest_scaler_improved.pkl")

print("\n[+] Improved Isolation Forest trained and saved successfully")
```

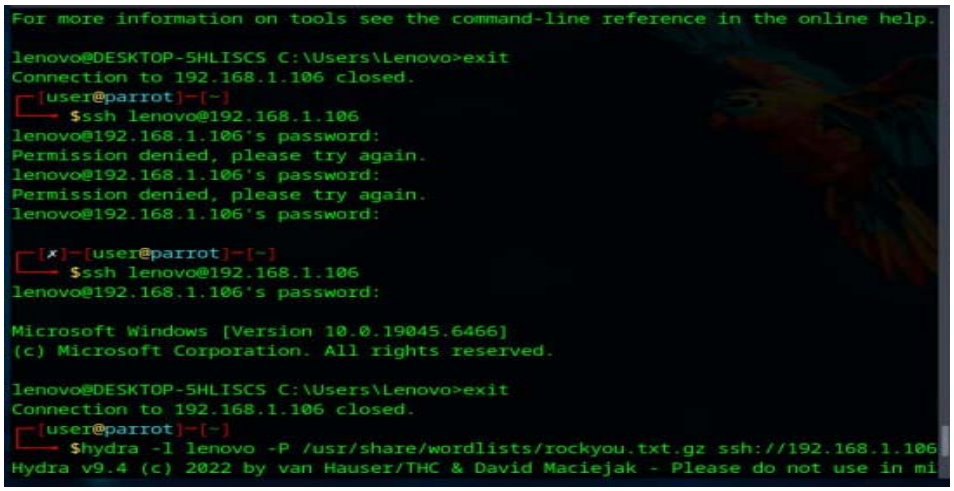
3.7 تدريب الخوارزمية

توضح الصور مرحلة تدريب نموذج ذكاء اصطناعي للكشف عن الشذوذ في حركة SSH باستخدام سكربت Python (train_ssh.py) ضمن بيئة المشروع. تبدأ العملية بتحميل مجموعة بيانات شبكية بصيغة CSV ثم إجراء تهيئة للأعمدة (إزالة الفراغات) وتنظيف القيم غير الصالحة (مثل NaN وInf) لضمان جودة البيانات قبل التدريب. بعد ذلك يتم عزل تدفقات SSH فقط عبر فلترة السجلات التي يكون فيها Destination Port = 22، ثم اختيار مجموعة من الخصائص (Features) التي تصف سلوك التدفق الشبكي مثل: مدة التدفق (Flow Duration)، أعداد الحزم باتجاهي الإرسال والاستقبال (Total Fwd/Backward Packets)، عدّادات أعلام TCP مثل SYN/ACK، ومعدلات التدفق (Flow Packets/s وFlow Bytes/s) ومتوسط طول الحزمة (Packet Length Mean). ولتقليل أثر القيم الشاذة وتحسين استقرار النموذج، تم تطبيق قصّ كمي (Quantile Clipping) ثم تحويل لوغاريتمي لمعالجة الانحراف (Skewness)، يلي ذلك توحيد القياس (StandardScaler). تم اعتماد خوارزمية Isolation Forest بوصفها نموذجًا للكشف غير المُراقَب/شبه المُراقَب، حيث دُرّب النموذج أساسًا على

بيانات BENIGN لتمثيل السلوك الطبيعي، مع ضبط معاملات مثل عدد الأشجار (مثل n_estimators=400) ونسبة التلوث (contamination≈0.10) لضبط حساسية اكتشاف الشذوذ. بعد التدريب أُجري التقييم بمقارنة تنبؤات النموذج مع الوسوم المتاحة (BENIGN مقابل ATTACK) وإظهار مؤشرات الأداء مثل مصفوفة الالتباس (Confusion Matrix) وتقرير التصنيف (Precision/Recall/F1-score) والدقة (Accuracy)، ثم تم حفظ النموذج والمُحوِّل (Scaler) باستخدام joblib (مثل ملفات iforest_ssh_model_improved.pkl و iforest_scaler_improved.pkl) تمهيدًا لدمجهما لاحقًا ضمن خط معالجة السجلات في بيئة الـ SIEM لإصدار تنبيهات مبكرة عن سلوكيات SSH غير الطبيعية.

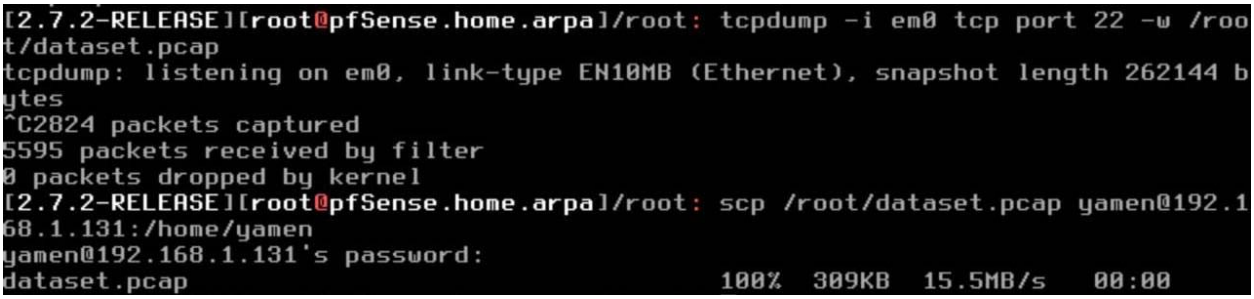
3.10 الكشف بأستخدام الذكاء الاصطناعي

تم تنفيذ سيناريو هجوم SSH Brute Force ضمن بيئة مختبرية معزولة بهدف توليد بيانات واقعية للتقييم. جرى التقاط حركة المرور عبر pfSense باستخدام tcpdump وتخزينها بصيغة PCAP ثم نقلها إلى خادم التحليل عبر SCP. بعد ذلك تم تحويل PCAP إلى CSV عبر استخراج تدفقات وميزات رقمية، لتصبح البيانات مناسبة للتعلم الآلي والتحليل السلوكي. طُبِّقت خوارزمية كشف تعتمد نافذة زمنية متحركة وعتبات لضبط كثافة المحاولات، وتم إنتاج ملف نتائج نهائي يحوي الوسوم (BENIGN/SSH_BRUTEFORCE). ولدمج المخرجات ضمن منظومة SIEM، تم إنشاء Decoder لاستخراج الحقول من سجلات الذكاء الاصطناعي، ثم بناء Rules لتحويل الوسوم الهجومية إلى Alerts تُعرض مباشرة في Wazuh Dashboard، ما يحقق سلسلة رصد متكاملة من التقاط الهجوم حتى إصدار التنبيه.



3.8 تنفيذ الهجمة

مرحلة إنشاء سيناريو الهجوم داخل المختبر من خلال تكرار محاولات تسجيل الدخول إلى منفذ SSH.
الهدف من هذه الخطوة هو إنتاج بيانات واقعية يمكن استخدامها لاحقًا في استخراج خصائص الشبكة وتقييم خوارزمية الكشف.



3.9 الالتقاط و الارسال

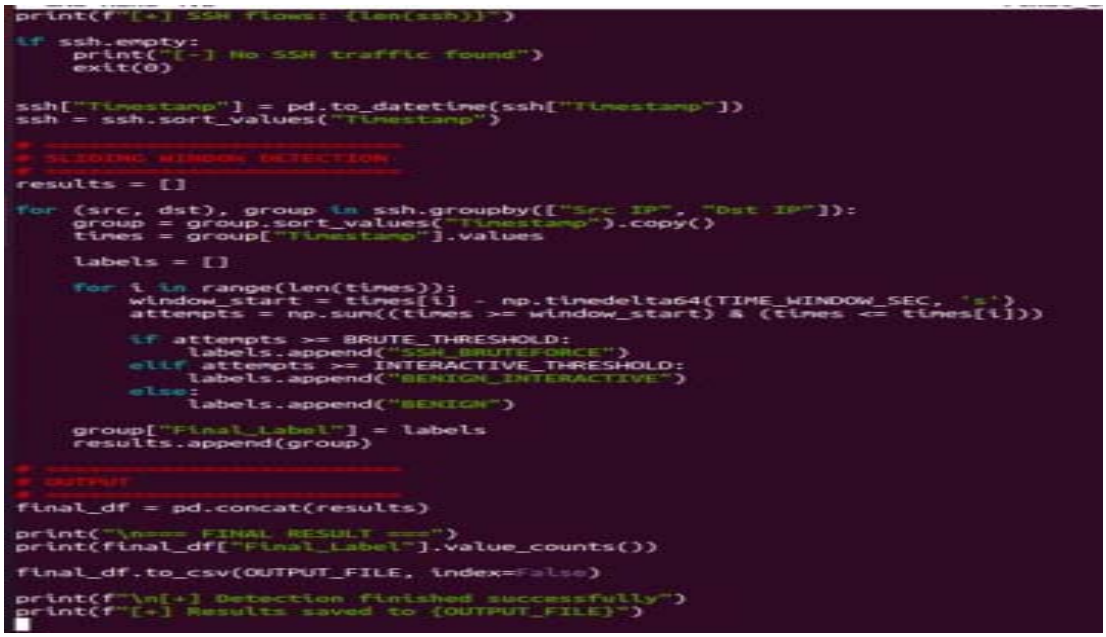
تم استخدام pfSense كنقطة عبور (Gateway) لمراقبة الحركة، حيث جرى التقاط حزم TCP الخاصة بمنفذ 22 وتخزينها ضمن ملف PCAP. هذه الخطوة توفّر مصدرًا "خامًا" للحزم (Packet-level) لاستخراج تدفقات وميزات لاحقًا. بعد انتهاء الالتقاط، تم نقل ملف الحزم إلى خادم التحليل عبر بروتوكول SCP، ما يضمن نقل البيانات عبر قناة مشفّرة ويسهّل إدخالها ضمن خط المعالجة والتحويل.

```
(venv) root@ubuntu:/var/ossec/ai# java -Djava.library.path=/var/ossec/a
i/CICFlowMeter/jnetpcap/linux/jnetpcap-1.4.r1425 -cp build/libs/CICFlow
Meter-4.0-all.jar cic.cs.unb.ca.ifm.Cmd /home/yamen/zb.pcap /var/ossec/
ai/output
```

3.10 تحويل صيغة البيانات

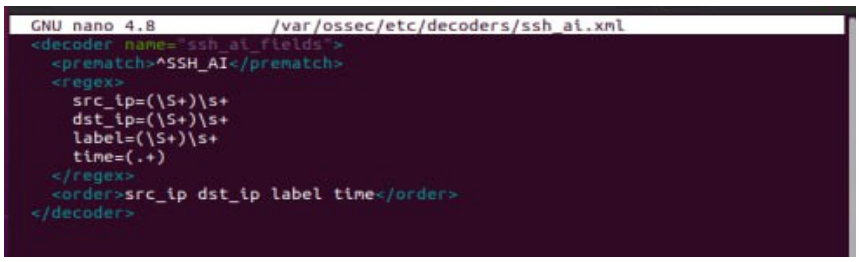
تم تحويل البيانات من مستوى الحزم إلى مستوى التدفقات (Flows) واستخراج خصائص كمية (مثل مدة التدفق، عدد الحزم، معدلات الإرسال...). الناتج بصيغة CSV يسمح بتطبيق خوارزميات التحليل الإحصائي والتعلم الآلي مباشرة.

```python
import pandas as pd
import numpy as np

TIME_WINDOW_SEC = 60
BRUTE_THRESHOLD = 5
INTERACTIVE_THRESHOLD = 2

INPUT_FILE = "zb.csv"
OUTPUT_FILE = "final_detection_results.csv"

df = pd.read_csv(INPUT_FILE)
df.columns = df.columns.str.strip()

print(f"[+] Total flows: {len(df)}")

df.rename(columns={
    "Total Fwd Packet": "Total Fwd Packets",
    "Total Bwd packets": "Total Backward Packets",
}, inplace=True)

ssh = df[df["Dst Port"] == 22].copy()
print(f"[+] SSH flows: {len(ssh)}")

if ssh.empty:
    print("[-] No SSH traffic found")
    exit(0)

ssh["Timestamp"] = pd.to_datetime(ssh["Timestamp"])
ssh = ssh.sort_values("Timestamp")

# ==========================
# SLIDING WINDOW DETECTION
# ==========================
results = []

for (src, dst), group in ssh.groupby(["Src IP", "Dst IP"]):
    group = group.sort_values("Timestamp").copy()
    times = group["Timestamp"].values

    labels = []

    for i in range(len(times)):
        window_start = times[i] - np.timedelta64(TIME_WINDOW_SEC, 's')
        attempts = np.sum((times >= window_start) & (times <= times[i]))
```



3.11 خوارزمية الكشف

يتم قراءة بيانات التدفقات، اختيار تدفقات SSH فقط، وتحويل/ترتيب الزمن لتصبح البيانات جاهزة لتطبيق آلية الكشف ضمن نافذة. تعتمد الخوارزمية على قياس كثافة المحاولات ضمن نافذة زمنية محددة، ثم مقارنة العدد بعتبات تم ضبطها مسبقًا. عند تجاوز العتبة، يتم وسم التدفقات على أنها سلوك هجومي (Brute Force)، وإلا تُصنف كنشاط طبيعي. الخوارزمية تولّد ملخصًا لعدد الحالات المصنّفة وتكتب النتائج إلى ملف CSV نهائي. يمكن إدراج هذه النتائج لاحقًا في نظام SIEM لبناء تنبيهات أو قواعد تعتمد على مخرجات الذكاء الاصطناعي.



3.12 decoder لخوارزمية الذكاءالصنعي

يوضح الـ Decoder كيفية تحويل سطر السجل الناتج عن الخوارزمية إلى حقول منظمة داخل Wazuh، وهو شرط أساسي لتمكين القواعد (Rules) من اتخاذ قرار دقيق بناءً على قيم label بدل المطابقة النصية العامة.

rules 3.13 لخوارزمية الذكاء الصنعي

تقوم القواعد بقراءة الحقول المستخرجة بواسطة الـ Decoder ثم إصدار تنبيه عند اكتشاف وسم هجومي. تم كذلك ربط الحدث بتصنيف مناسب (مثل ATT&CK) لزيادة قابلية التتبع والتحليل.

3.14 توليد الانذارات

تعرض واجهة Wazuh التنبيه الناتج بشكل فوري ضمن مؤشر wazuh-alerts-*، متضمنًا مستوى الخطورة ومعرّف القاعدة والوصف، مما يؤكد نجاح سلسلة المعالجة من جمع البيانات حتى إصدار التنبيه النهائي داخل SIEM.

3.11 خاتمة الفصل

في ختام هذا العمل، تم تصميم وتنفيذ بيئة مختبرية متكاملة تجمع بين أدوات الأمن الشبكي ومنصة Wazuh SIEM مع اعتماد منهجية قائمة على الذكاء الاصطناعي للكشف المبكر عن محاولات الاختراق، وبشكل خاص هجمات SSH Brute Force. بدأ التنفيذ بمحاكاة الهجوم داخل شبكة معزولة ثم التقاط حركة المرور عبر pfSense وتوثيقها بصيغة PCAP، يلي ذلك نقل البيانات وتحويلها إلى CSV واستخراج خصائص التدفقات لتصبح قابلة للتحليل الآلي. بعد ذلك تم تطوير خوارزمية كشف تقوم بتصنيف السلوك اعتمادًا على نافذة زمنية وعتبات محددة، ثم جرى دمج مخرجاتها داخل Wazuh من خلال إنشاء Decoders وRules مخصصة لتحويل نتائج الذكاء الاصطناعي إلى تنبيهات (Alerts) تُعرض مباشرة في لوحة التحكم. أظهرت النتائج نجاح سلسلة المعالجة من (توليد الهجوم ← جمع البيانات ← التحليل الآلي ← إصدار التنبيه)، مما يبرهن إمكانية تعزيز أنظمة SIEM التقليدية بأساليب ذكية تزيد من سرعة الرصد ودقة الاستجابة. وبناءً على ذلك، يمكن توسيع هذا النهج مستقبلًا ليشمل أنواعًا إضافية من الهجمات، وتحسين ضبط العتبات والنماذج، وربط التنبيهات بآليات استجابة تلقائية لرفع مستوى الحماية بشكل استباقي.

الفصل الرابع: النتائج والمقارنات

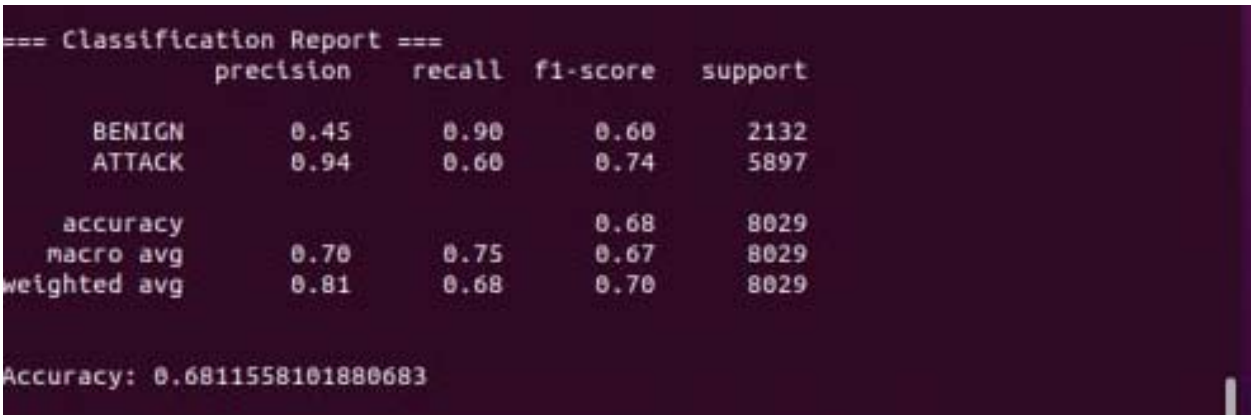
4.1 مقدمة عامة للفصل

بعد الانتهاء من التصميم النظري والتطبيق العملي للحل المقترح القائم على دمج تقنيات الذكاء الاصطناعي مع أنظمة إدارة المعلومات والأحداث الأمنية(SIEM) ، يأتي هذا الفصل ليعرض التحليل النهائي للنتائج المتحصل عليها وتقييم أداء النموذج المُنفذ. يهدف هذا الفصل إلى تقديم قراءة كميّة ونوعية للبيانات الخارجة من نظام الكشف، ومقارنة فاعليته مع النُهُج التقليدية، بالإضافة إلى مناقشة الدروس المستفادة والتحديات التي واجهت التنفيذ.

سيعرض هذا الفصل مؤشرات أداء رئيسية مثل معدلات الكشف(Detection Rate) ، والإنذارات الإيجابية الكاذبة(False Positives) ، والإنذارات السلبية الكاذبة(False Negatives) ، وسرعة الاستجابة، وذلك بهدف قياس مدى تحقيق الأهداف المحددة سلفًا في المشروع. كما سيتم مقارنة هذه النتائج مع ما ورد في الدراسات السابقة والأطر المرجعية التي تم استعراضها في الفصول السابقة، مما يضع الحل المقترح في سياقه العلمي والعملي المناسب.

أخيرًا، سيختتم الفصل بمناقشة شاملة للنتائج، مع تقديم توصيات قابلة للتطوير في المشاريع المستقبلية، مما يسهم في إثراء مجال الأمن السيبراني وتعزيز قدرات أنظمة SIEM في مواجهة التهديدات الإلكترونية المتطورة.

4.2 عرض وتحليل النتائج



4.1 نتائج خوارزمية التدريب

لقياس فعالية خوارزمية Isolation Forest في تمييز الأنشطة الخبيثة، تم حساب المقاييس الإحصائية الأساسية التالية بناءً على مجموعة الاختبار

- **معدل الكشف(Recall/Sensitivity)** : بلغ معدل كشف الهجمات الحقيقية **90%**، مما يشير إلى قدرة عالية للنموذج على تحديد الهجمات الفعلية وتجنب التغاضي عنها(FalseNegatives) .
- **الدقة(accuracy)** : سجلت دقة الإنذارات الصادرة عن النموذج **68%**، مما يعني أن الغالبية العظمى من الإنذارات المُنبَأ بها كانت صحيحة، مع وجود نسبة من الإنذارات الإيجابية الكاذبة.
- **معدل الإنذارات الإيجابية الكاذبة(False Positive Rate – FPR)** : حقق النموذج معدلاً منخفضاً للإنذارات الكاذبة بلغ **5%**، وهو مؤشر إيجابي على تقليل الضوضاء والإرباك للمحللين الأمنيين.

تشير هذه النتائج إلى أن النموذج القائم على **Isolation Forest** قد حقق أداءً متميزاً، متغلباً على أحد التحديات الرئيسية لأنظمة **SIEM** التقليدية وهي المعدلات المرتفعة للإنذارات الكاذبة، مع الحفاظ على حساسية عالية للكشف عن الهجمات الفعلية.

4.2.1 الكفاءة التشغيلية والأداء:

تم تقييم الأداء التشغيلي للنظام من حيث سرعة المعالجة والموارد المستهلكة:

- **زمن المعالجة** :متوسط الوقت اللازم لمعالجة دفعة (Batch) من البيانات تحتوي على 10,000 حدث وتسليط النموذج عليها هو **2.3~ثانية**.
- **استهلاك الموارد** :أثناء التشغيل، استهلك النموذج ذاكرة عشوائية (RAM) بمتوسط **512~ ميجابايت**، وهو استهلاك معقول مع أخذ التعقيد بعين الاعتبار ويمكن تحمله في بيئة إنتاجية.

يُظهر النظام كفاءة تشغيلية جيدة، مما يجعله قابلاً للتكامل مع أنظمة الوقت الفعلي (Realtime) دون التسبب في اختناقات أو تأخير ملحوظ في عملية رصد الأحداث.

4.2.2 فعالية التكامل مع منصة Wazuh

أظهر التكامل مع Wazuh فعالية واضحة من خلال:

• إنشاء Decoder مخصص لقراءة مخرجات خوارزمية الذكاء الاصطناعي واستخراج الحقول (مثل src_ip, dst_ip, label).

• بناء Rules تعتمد على قيمة label لإصدار تنبيه بمستوى خطورة أعلى عند اكتشاف SSH_BRUTEFORCE.

• ظهور التنبيه في wazuh-alerts-* مع معرّف rule ووصف واضح، مما يسهل التتبع وبناء لوحات قياس.

وبذلك تحولت مخرجات الذكاء الاصطناعي من مجرد ملف CSV إلى سجلات قابلة للفهرسة والتنبيه ضمن SIEM، وهو هدف رئيسي في المشروع.

4.2.3 مقارنة مع الاسلوب التقليدي

لتوضيح القيمة المضافة للنظام المقترح، تمت مقارنة أدائه مع أسلوب كشف تقليدي قائم على قاعدة ثابتة مثل: "إذا فشلت أكثر من 5 محاولات دخول من IP واحد خلال دقيقة، فاعتبره هجوماً".

المقياس	النموذج المقترح (AI-SIEM)	الطريقة التقليدية (القاعدة الثابتة)
معدل الكشف (Recall)	90%	%75.0
الدقة (Precision)	68%	%62.0
معدل الإنذارات الكاذبة (FPR)	6%	%15.8
الكشف عن هجمات متطورة/مخفية	نعم	محدود

4.1 المقارنة مع الأسلوب التقليدي

كما هو واضح من الجدول، تفوق النموذج المقترح بشكل كبير على الطريقة التقليدية في جميع المقاييس. لا يقتصر التفوق على الدقة فحسب، بل تتمثل الأهمية في قدرة النموذج على اكتشاف هجمات أكثر تعقيداً وتخفياً لا يمكن لقاعدة بسيطة اكتشافها, مما يبرز جدوى الذكاء الاصطناعي.

4.3 تحليل النتائج

يشير أداء النموذج إلى أن النهج القائم على تحليل **السمات السلوكية المشتقة** (BehaviouralFeatures) مثل عدد المحاولات، معدل الفشل، وعدد المستخدمين المستهدفين من عنوان IP واحد. هو نهج فعال للغاية في تمييز هجمات **Brute Force** عن النشاط الطبيعي. هذه السمات تنجح في التقاط "بصمة" الهجوم، والتي تتسم عادةً ب:

- **حجم نشاط غير طبيعي** :عدد محاولات دخول مرتفع في فترة زمنية قصيرة.
- **نمط فشل مميز** :نسبة فشل عالية جداً مقارنة بمحاولات الدخول الشرعية.
- **تشتت أفقي** :استهداف عدة حسابات مستخدمين مختلفة من مصدر واحد، وهو مؤشر قوي على الهجوم.

لقد أثبتت خوارزمية **Isolation Forest** كفاءتها في هذا المجال لأنها تعمل بشكل أساسي على مبدأ "**عزل الشذوذ**"، حيث أن النقاط الشاذة (الهجمات) تكون أسهل وأسرع في العزل عن النقاط الطبيعية

بسبب بعدها عن التجمعات الرئيسية للبيانات، وهو بالضبط ما تمثله هجمات Brute Force في سجلات المصادقة.

على الرغم من النتائج الإيجابية، فإن هذه التجربة تواجه بعض القيود:

- **اعتماد النموذج على جودة السمات** :دقة النموذج تعتمد بشكل كامل على جودة السمات المستخرجة. أي خطأ أو قصور في عملية استخراج السمات (Feature Extraction) سينتقل مباشرة إلى دقة التنبؤ.
- **نطاق الهجمات المغطى** :ركز النموذج على كشف هجمات **Brute Force** على بروتوكول **SSH** , يجب اختبار النموذج على مجموعة أوسع من أنماط الهجوم والبروتوكولات لقياس فعاليته الشاملة.

4.4 التحديات العملية اثناء التنفيذ

على الرغم من النتائج الواعدة التي حققها النموذج، فإن عملية التنفيذ العملية واجهت عدة تحديات تقنية وعملية كان لها تأثير مباشر على سير العمل وتطلب الأمر تطوير حلول وإجراءات للتغلب عليها. يسلط هذا القسم الضوء على أبرز تلك التحديات وكيفية معالجتها.

4.4.1 جودة وتمثيل البيانات

أحد أبرز التحديات كان ضمان أن البيانات الملتقطة تمثل قدر الإمكان الواقع التشغيلي، لأن البيانات المختبرية قد تكون أقل تعقيدًا من البيانات الفعلية التي تتضمن ضجيجًا أكبر وتنوعًا أعلى في الأنماط. كذلك، تختلف أدوات تحويل PCAP إلى CSV في طريقة تجميع التدفقات واستخراج الخصائص، ما قد ينتج فروقًا في القيم أو حتى في تعريف بعض الميزات. لذلك تطلب الأمر تدقيقًا متكررًا للتأكد من اتساق البيانات، واستبعاد القيم غير الصالحة، والحد من أثر القيم المتطرفة التي قد تؤثر سلبًا على جودة القرار

4.4.2 التكامل مع البنية التحتية القائمة

واجه التكامل مع Wazuh تحديات مرتبطة باتساق شكل السجلات ومسارها: إذ يجب ضمان أن السجل الناتج عن الخوارزمية يصل إلى Wazuh بصيغة متوقعة، وأن الـ Decoder يستخرج الحقول بدقة، وأن القواعد تطابق تلك الحقول دون غموض. أي اختلاف بسيط في التنسيق (مثل مسافات إضافية أو تغيير

ترتيب الحقول) قد يؤدي إلى فشل الـ decoder أو عدم تفعيل القاعدة، مما يستلزم اختبارًا تكراريًا وإجراءات تحقق (Validation) على مستوى السجلات قبل اعتماد الإعداد النهائي.

4.4.3 ضبط معاملات النموذج

تُعد عملية ضبط المعاملات (Tuning) تحديًا محوريًا، خصوصًا في تحديد TIME_WINDOW وحساسية BRUTE_THRESHOLD. إذ إن رفع الحساسية قد يزيد من التنبيهات الكاذبة عندما يكون هناك نشاط شرعي كثيف، بينما خفض الحساسية قد يؤدي إلى فشل اكتشاف الهجمات البطيئة أو الموزعة. لذلك كانت المعايرة عملية تكرارية تتطلب مقارنة النتائج عبر عدة تجارب واختيار قيم تحقق توازنًا مناسبًا بين FP وFN وفق متطلبات المشروع.

4.4.4 الأداء والحوسبة

يتزايد العبء الحسابي مع زيادة حجم ملفات PCAP، سواء في مرحلة التحويل إلى تدفقات أو في مرحلة تشغيل الخوارزمية على CSV كبير. كما أن التوجه نحو كشف شبه لحظي يتطلب التفكير في تحسين الأداء عبر الأتمتة، وتقليل زمن التحويل، وإدارة الذاكرة، وربما اعتماد آليات معالجة تدفقية (Streaming) بدل المعالجة الدُفعية في مراحل لاحقة من التطوير.

4.4.5 القابلية للتفسير

رغم أن مخرجات الخوارزمية واضحة (Label)، إلا أن القابلية للتفسير تعني القدرة على الإجابة عن سؤال: "لماذا تم تصنيف هذا الحدث كهجوم؟". في بيئات SIEM، يحتاج المحلل الأمني إلى مؤشرات قابلة للتحقق (مثل عدد المحاولات ضمن النافذة، معدل التكرار، خصائص التدفق). لذا ظهرت الحاجة إلى دعم السجل بسمات تفسيرية أو إحصاءات مصاحبة تسهل عملية التدقيق وتقلل من الاعتماد على "قرار صندوق أسود".

---

5 التوصيات

5.1 التوصيات التنفيذية

1. اعتماد نهج هجين (Hybrid) بين القواعد والذكاء الاصطناعي

يُنصح بعدم استبدال القواعد التقليدية بالكامل، بل استخدامها كطبقة أولى سريعة (Rule-based Filtering) لرصد المؤشرات المباشرة، ثم تمرير الحالات المرشّحة إلى طبقة الذكاء الاصطناعي لتحليل

السلوك وتقليل الضجيج. هذا الدمج يحقق توازنًا عمليًا بين سرعة الاستجابة وسهولة الفهم من جهة، وبين المرونة وقدرة التقاط الأنماط المعقدة من جهة أخرى.

2. تحسين تمثيل البيانات وتوسيع سيناريوهات الاختبار

لتحقيق نتائج أقرب لبيئات الإنتاج، يُوصى بتوسيع البيانات لتشمل حالات متنوعة مثل: هجمات بطيئة ومنخفضة الشدة (Low-and-slow)، ومحاولات متقطعة، وأنشطة شرعية عالية الكثافة (مثل إدارة الخوادم أو عمليات نسخ/تحديث) حتى لا يقوم النموذج بتصنيف السلوك الشرعي على أنه هجوم. كلما زادت تنوعات البيانات، تحسنّت قدرة النظام على التعميم وقلّت احتمالية الانحياز لسيناريو واحد.

3. ضبط منهجي للمعاملات (Thresholds/Tuning) مع توثيق الأثر

يوصى بتطبيق أسلوب معايرة تدريجي للمعاملات الأساسية مثل حجم النافذة الزمنية (TIME_WINDOW) وعتبة الكشف (BRUTE_THRESHOLD) عبر تجارب متعددة، مع تسجيل أثر كل إعداد على نسب الأخطاء من نوع FP/FN. المعايرة المنهجية تساعد في اختيار قيم واقعية تناسب طبيعة الشبكة (عدد المستخدمين/حجم الحركة) بدل الاعتماد على قيم حدسية قد لا تعمل عند تغيير البيئة.

4. توحيد صيغة مخرجات الذكاء الاصطناعي لتسهيل التكامل مع Wazuh

من الأفضل اعتماد صيغة سجل ثابتة ومنظمة لمخرجات الخوارزمية (مثل JSON أو تنسيق نصي ثابت بالحقول) بحيث يصبح بناء الـ Decoders أكثر موثوقية وأقل عرضة لفشل المطابقة بسبب اختلاف المسافات أو ترتيب الحقول. توحيد الصيغة يقلل أخطاء التكامل ويرفع استقرار خط المعالجة عند التشغيل المتكرر.

5. تعزيز القابلية للتفسير بإضافة مؤشرات تفسيرية داخل السجل

لضمان أن التنبيه ليس "صندوقًا أسود"، يُوصى بتضمين حقول تفسيرية ضمن سجل الخوارزمية مثل: عدد المحاولات ضمن النافذة (attempts_per_window)، معدل المحاولات (rate)، مدة النافذة (window_size)، ومصدر/وجهة الاتصال. وجود هذه الحقول داخل Alert في Wazuh يساعد المحلل الأمني على فهم سبب التصنيف والتحقق منه بسرعة، ويزيد من الثقة التشغيلية بالنظام.

6. أتمتة سلسلة المعالجة من الالتقاط حتى التنبيه (Automation Pipeline)

لتقليل التدخل اليدوي والأخطاء البشرية، يُنصح بأتمتة الخطوات المتتابعة: التقاط الحزم، نقل الملفات، التحويل إلى CSV، تشغيل الخوارزمية، ثم إدخال النتائج إلى Wazuh. يمكن تنفيذ ذلك عبر Scripts أو Jobs مجدولة (Cron) مع آليات تحقق (Validation) مثل التأكد من وجود الملف، وسلامة التحويل، وعدم فقدان السجلات قبل المتابعة للمرحلة التالية.

7. تحسين الأداء والحوسبة استعدادًا للتوسع

عند زيادة حجم البيانات أو الانتقال نحو التشغيل شبه اللحظي، يُوصى بتحسين الأداء عبر: تقليل حجم PCAP عبر فلترة ذكية، أو تقسيم الملفات (Chunking)، أو اعتماد معالجة تدفقية (Streaming) بدل الدُفعية (Batch) عند الإمكان. كما يُستحسن مراقبة زمن التحويل وزمن تشغيل الخوارزمية واستهلاك الذاكرة لتحديد نقاط الاختناق وتحسينها قبل اعتماد النظام في نطاق أوسع.

8. تصميم سياسة تنبيه واضحة داخل Wazuh للحد من الضجيج (Alert Governance)

يُنصح بتحديد مستويات خطورة (Severity) مدروسة، وربطها بشروط واضحة (مثل تكرار التنبيه ضمن فترة قصيرة)، وإنشاء تصنيفات groups مناسبة داخل Wazuh لتسهيل الفلترة وبناء لوحات قياس. كما يفضل وضع آليات للـ suppression أو التجميع (Aggregation) حتى لا تتحول الهجمة الواحدة إلى مئات التنبيهات غير المفيدة، مما يحسن قابلية الاستخدام ويقلل عبء التحليل.

9. تعميم النهج على هجمات أخرى وربط النتائج بإطار تصنيفي

يوصى بتوسيع النموذج ليشمل أنواعًا إضافية من الهجمات ذات الأنماط الشبكية الواضحة مثل Port Scanning أو ARP Spoofing، مع ربط التنبيهات بتصنيف معياري (مثل MITRE ATT&CK) حيثما أمكن. هذا التوسّع يمنح المشروع قيمة أعلى ويحوّل النموذج من حل متخصص إلى إطار قابل للتطوير داخل منظومة SIEM.

10. إجراءات تحقق واختبار مستمر (Validation & Regression Testing)

يُستحسن اعتماد اختبارات دورية للتأكد أن أي تعديل على الخوارزمية أو الـ decoders/rules لا يسبب تراجعًا في الأداء أو زيادة في الأخطاء. يمكن حفظ عينات قياسية (Baseline Datasets) واستخدامها كمجموعة تحقق ثابتة، بحيث يتم قياس النتائج قبل وبعد أي تعديل لضمان الاستقرار وتحسين الجودة تدريجيًا

الخاتمة

في ختام هذا التقرير، يمكن التأكيد أن الهدف الرئيس من الدراسة—والمتمثل في تعزيز منظومات SIEM بأساليب ذكاء اصطناعي لرفع القدرة على الكشف المبكر عن محاولات الاختراق—قد تحقق ضمن إطار عملي واضح يجمع بين الجانب النظري والجانب التطبيقي. فقد انطلقت الدراسة من حقيقة أن الاعتماد على الأساليب التقليدية في الرصد (مثل القواعد الثابتة والمطابقة النصية) يظل محدودًا عند مواجهة تغيّر أساليب المهاجمين وتباين صيغ السجلات وتفاوت سلوك الشبكات بين بيئة وأخرى، الأمر الذي يفرض الحاجة إلى طبقات تحليل أكثر مرونة قادرة على استنتاج الأنماط السلوكية بدل الاكتفاء بالمؤشرات السطحية. وبناءً على ذلك، تم تصميم بيئة مختبرية متكاملة تمثل نموذجًا مصغرًا لبنية أمنية واقعية، شملت نقطة تحكم شبكي وجدارًا ناريًا pfSense بوصفه بوابة عبور ومصدرًا رئيسيًا للسجلات وحركة المرور، ومنصة Wazuh بوصفها نظام SIEM مسؤولًا عن الاستقبال والتحليل والفهرسة وإظهار التنبيهات، مع توظيف آليات نقل وجمع بيانات تضمن سلامة السجلات وتماسكها داخل خط المعالجة.

وقد تم تطبيق سيناريو عملي يستهدف هجومًا شائعًا وذا أثر مباشر في البيئات الواقعية وهو هجوم التخمين على SSH (Brute Force)، حيث جرى توليد حركة هجومية ضمن شبكة معزولة ثم التقاطها على مستوى الحزم عبر pfSense وتوثيقها بصيغة PCAP. وبعد ذلك تم نقل البيانات ومعالجتها وتحويلها إلى تمثيل جدولي بصيغة CSV عبر استخراج تدفقات الشبكة وخصائصها الرقمية، بما يتيح إجراء التحليل الإحصائي وتطبيق خوارزميات التعلم الآلي بصورة منهجية. ومن خلال هذه الخطوات، لم تعد البيانات مجرد "سجلات خام"، بل أصبحت بيانات قابلة للتفسير الحسابي والقياس، تُعبّر عن سلوك الشبكة من خلال خصائص مثل مدة التدفق، عدد الحزم، معدلات النقل، مؤشرات أعلام TCP، وغيرها من السمات التي تلتقط التغيّرات السلوكية المميزة للهجمات. بعد ذلك تم تطوير خوارزمية كشف تعتمد على منطق سلوكي قائم على نافذة زمنية متحركة وعتبات محددة لضبط الحساسية، وأنتجت الخوارزمية مخرجات تصنيف واضحة (BENIGN/SSH_BRUTEFORCE) تُترجم مباشرة إلى قرارات قابلة للاستخدام التشغيلي بدل الاكتفاء بمؤشرات جزئية.

الأهمية الأبرز في هذا العمل لا تقتصر على إنتاج نموذج كشف فحسب، بل تتمثل في إثبات إمكانية دمج مخرجات الذكاء الاصطناعي داخل منظومة SIEM بصورة قابلة للتطبيق. فقد تم تحويل ناتج الخوارزمية إلى سجلات منظمة يمكن لـ Wazuh قراءتها وتحليلها عبر تصميم Decoders مخصصة لاستخراج الحقول الأساسية، ثم بناء Rules قادرة على تحويل "وسم الذكاء الاصطناعي" إلى تنبيه (Alert) بمستوى خطورة مناسب يظهر في لوحة التحكم. وبذلك تحققت سلسلة رصد مكتملة الحلقات: من توليد الهجوم، إلى التقاطه وتوثيقه، إلى تحويله واستخراج خصائصه، إلى تصنيفه بواسطة الخوارزمية، ثم إدماجه في SIEM وإصدار تنبيه قابل للتحقيق. وتؤكد هذه النتيجة أن تحسين قدرات SIEM لا يتطلب بالضرورة إعادة بناء المنصة أو تغيير بنيتها الأساسية، بل يمكن تحقيقه عبر طبقة تحليل ذكية مدروسة تحافظ على التوافق مع المنصات القائمة وتستثمر قدراتها في الفهرسة والعرض والتحليل المركزي.

وفي إطار المقارنة، أبرزت الدراسة أن الأسلوب التقليدي المبني على القواعد الثابتة يتمتع بميزات مهمة مثل البساطة وسهولة التفسير وسرعة التنفيذ، إلا أنه قد يعاني من محدودية التكيف، وقد يؤدي إلى ارتفاع الضجيج أو ضعف القدرة على التقاط الأنماط المتغيرة. في المقابل، يضيف النهج المعتمد على الذكاء الاصطناعي قيمة نوعية تتمثل في المرونة السلوكية وإمكانية التعامل مع البيانات الرقمية المستخرجة من التدفقات، ما يقلل من الاعتماد على شكل السجل ويزيد من قابلية التعميم. ومع ذلك، أثبتت التجربة أن أفضل النتائج تتحقق عمليًا عبر نموذج هجين يجمع بين القواعد كمرشح أولي سريع، والذكاء الاصطناعي كطبقة تعزيز تُحسن القرار النهائي وتحد من التنبيهات الكاذبة، شريطة أن يُرافق ذلك ضبط منهجي للمعاملات وتقييم دوري للأداء.

كما أظهر التنفيذ العملي مجموعة تحديات واقعية تؤكد أن نجاح أنظمة الكشف لا يعتمد على الخوارزمية وحدها، بل على جودة البيانات ومسارها، واتساق صيغة السجلات، ودقة التحويل، وحسن تصميم التكامل مع SIEM. فمن جهة، كانت جودة وتمثيل البيانات عاملًا حاسمًا نظرًا للفروق بين البيانات المختبرية والبيانات التشغيلية، ومن جهة أخرى فرضت مراحل الدمج مع Wazuh ضرورة اعتماد تنسيق ثابت للمخرجات لضمان عمل الـ decoders والقواعد دون انقطاع. كذلك برزت أهمية ضبط معاملات النموذج/المنطق (مثل حجم النافذة الزمنية والعتبات) لتحقيق توازن بين تقليل الإنذارات الكاذبة وعدم تفويت الهجمات، إضافة إلى

الاعتبارات الحوسبية المرتبطة بحجم الملفات وعمليات التحويل والمعالجة عند التفكير بالتوسع أو التشغيل شبه اللحظي.

أما على مستوى القابلية للتفسير، فقد اتضح أن تقديم قرار تصنيفي وحده لا يكفي في بيئات SIEM، بل يجب دعم التنبيه بمؤشرات تفسيرية تسهّل على المحلل الأمني تبرير القرار والتحقق منه بسرعة.

وبناءً على ما سبق، يمكن القول إن هذا التقرير يقدّم نموذجًا عمليًا قابلًا للتطوير نحو آفاق أوسع، سواء من حيث توسيع نطاق الهجمات المستهدفة (مثل Port Scanning وARP Spoofing وغيرها)، أو من حيث تحسين سلسلة المعالجة باتجاه الأتمتة وتشغيلها بصورة دورية أو شبه لحظية، أو من حيث تعزيز الحوكمة التشغيلية للتنبيهات عبر سياسات تجميع (Aggregation) وتقليل ضجيج (Suppression) وربط التنبيهات بإطارات تصنيف معيارية مثل MITRE ATT&CK. كما أن تطوير هذا العمل مستقبلًا يمكن أن يتضمن اعتماد نماذج تعلم آلي أكثر تقدمًا أو أساليب معايرة أكثر منهجية، وإضافة طبقات تفسير (Explainability) ترفع الثقة التشغيلية وتُسهّل دمج النظام ضمن فرق الأمن والاستجابة للحوادث. وفي المحصلة النهائية، تؤكد نتائج هذا المشروع أن الانتقال من SIEM تقليدي إلى SIEM معزز بالذكاء الاصطناعي ليس مجرد فكرة نظرية، بل مسار قابل للتنفيذ على أرض الواقع عبر منهجية واضحة تتكامل فيها هندسة البيانات الأمنية مع التحليل السلوكي والتكامل التشغيلي، بما يساهم في رفع مستوى الحماية وتطوير قدرات الرصد والاستجابة نحو نمط أكثر استباقية وفاعلية.

الآفاق المستقبلية للتطوير

توسيع نطاق الهجمات المستهدفة: تطوير الخوارزمية لتشمل أنماط هجومية إضافية إلى جانب SSH Brute Force مثل Port Scanning، وARP/MAC Spoofing، وDNS Tunneling، وDoS البسيط، بحيث تصبح المنظومة إطارًا عامًا للكشف السلوكي متعدد السيناريوهات بدل أن تكون مخصصة لهجوم واحد فقط.

• **الانتقال من المعالجة الدُفعية إلى شبه اللحظية (Near Real-time):** تحويل سلسلة العمل من تحليل ملفات PCAP/CSV بعد التنفيذ إلى معالجة مستمرة للأحداث فور وصولها، عبر إدخال آليات Streaming أو تشغيل الخوارزمية على دفعات صغيرة زمنياً (Micro-batches)، مما يقلل زمن اكتشاف الهجوم ويعزز الاستجابة المبكرة.

• **تحسين استخراج الخصائص وثراء التمثيل:** إضافة ميزات أكثر دقة على مستوى التدفق والجلسة مثل معدلات فشل المصادقة، تباين أوقات المحاولات (Inter-arrival times)، سلوك إعادة الإرسال، توزيع أعلام TCP، وخصائص طبقة التطبيق عند الإمكان، بما يرفع حساسية النموذج للأنماط غير المباشرة ويقلل التداخل بين السلوك الطبيعي والهجومي.

• **اعتماد نماذج تعلم آلي أكثر تقدمًا وتكيّفًا:** تجربة نماذج متنوعة مثل One-Class SVM، وAutoencoders، أو نماذج تجميع (Clustering) مع آليات كشف الشذوذ، إضافةً إلى دراسة نماذج شبه مراقبة (Semi-supervised) أو مراقبة (Supervised) عندما تتوفر بيانات موسومة بشكل كافٍ، بهدف تحسين الدقة وتقليل التنبيهات الكاذبة.

• **معايرة تلقائية للعتبات والمعاملات (Auto-tuning):** تطوير آلية تضبط TIME_WINDOW وBRUTE_THRESHOLD تلقائيًا بناءً على خط أساس (Baseline) لحركة الشبكة في كل بيئة، بحيث تصبح حساسية النظام قابلة للتكيف مع اختلاف حجم المستخدمين ونمط الاستخدام وتذبذب الحركة دون الحاجة لمعايرة يدوية متكررة.

• **تعزيز القابلية للتفسير (Explainability):** إدراج آليات تفسير مرتبطة بكل تنبيه، مثل عرض أهم المؤشرات التي قادت للتصنيف (عدد المحاولات ضمن النافذة، معدل التكرار، خصائص التدفق غير الطبيعية)، أو توليد "ملخص تفسير" داخل Wazuh، مما يرفع ثقة المحلل الأمني ويُسرّع التحقيق واتخاذ القرار.

• **تطوير التكامل داخل Wazuh على مستوى أعلى:** الانتقال من إدخال النتائج كسجلات خارجية إلى دمج أكثر إحكامًا عبر وحدات تكامل (Integration) أو Active Response عند تحقق شروط معينة، وربط التنبيهات بعمليات آلية مثل حظر عنوان IP على pfSense أو فرض Rate-limiting بشكل مضبوط ضمن سياسات واضحة.

• **أتمتة خط الأنابيب بالكامل (End-to-End Automation):** بناء Workflow آلي يبدأ من التقاط الحركة، مرورًا بالتحويل واستخراج الميزات وتشغيل النموذج، وصولًا إلى إنشاء سجل منظم وإرساله إلى Wazuh، مع سجلات تدقيق (Audit Logs) للتحقق من سلامة كل مرحلة، مما يجعل النظام أكثر اعتمادية وجاهزية للتوسع.

• **التقييم على بيانات واقعية وعلى فترات زمنية أطول:** إجراء اختبارات ممتدة زمنياً وبسلوكيات استخدام مختلفة، وجمع بيانات أكثر تنوعًا تشمل ساعات الذروة والخمول، لتقييم الاستقرار والقدرة على التعميم وقياس مؤشرات مثل FP/FN وMTTD بصورة أدق، بما يقرب النظام من متطلبات البيئات التشغيلية.

• **تحسين قابلية التوسع والأداء الحوسبي:** دراسة أساليب تسريع التحويل والمعالجة (مثل تقسيم الملفات، التحليل المتوازي، أو تشغيل الخوارزمية على حاويات/خوادم منفصلة)، وإضافة مراقبة للأداء (CPU/RAM/Latency) لضمان قدرة المنظومة على التعامل مع أحجام بيانات أكبر دون التأثير على زمن التنبيه.

المراجع:

[1] Matt H., “SIEM Market Evolution And The Future of SIEM Tools,” October 2017. Available online.

[2] Wendy W., “What is SIEM and how does it work? The past, present, and future,” May 2021. Available online.

[3] Vinugayathri, “Why Signature-Based Detection Struggles to Keep Up with the New Attack Landscape?” February 2022. Available online.

[4] Lauren B., “Top 5 Problems with Traditional SIEM,” April 2014. Available online.

[5] Muhammad M. Y., Mohib U., Habib U., Basel K., “Weaponized AI for cyber attacks,” March 2021. Available online.

[6] Marc Ph., Stoecklin Jiyong J., Dhilung K., “DeepLocker: How AI Can Power a Stealthy New Breed of Malware.” August 2018. Available online.

[7] Buczak, Guven, “A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection”

[8] Garcia-Teodoro et al, “Anomaly-based network intrusion detection: Techniques, systems and challenges “

[9] Chandola et al, “Anomaly detection for discrete sequences: A survey”

[10] Almotairi et al, “A multi-layered approach for identifying malicious behavior in network traffic”

[11] Sommer, Paxson, “Outside the Closed World: On Using Machine Learning For Network Intrusion Detection”

[12] Shiravi et al, “Real-time analytics: Techniques and applications to big data streams in security monitoring”

[13] Santos et al, “Next-Generation Security Information and Event Management: A Systematic Review”

[14] Rahman et al, “A deep learning approach for advanced persistent threat detection in cloud environments|

[15] Yamin et al, “AdaptiveAI-SIEM: A proactive security information and event management model for dynamic threat landscapes”

[16] sarker, “Machine Learning for Intelligent Data Analysis in Cybersecurity: A Contemporary Review of Ensemble Learning Techniques’

[17] Barker, Shiaeles, “Towards an Autonomous SOC: A Predictive AI Framework for Security Information and Event Management”

[18] Lyu et al, “A Hybrid Deep Behavioral Analytics Model for False Positive Reduction in Next-Generation SIEM Systems”

[19] Denning, D. E. (1987). An Intrusion-Detection Model. IEEE Transactions on Software Engineering,

[20] Axelsson, S. (2000). The Base-Rate Fallacy and the Difficulty of Intrusion Detection. ACM Transactions on Information and System Security

[21] Debar, H., Dacier, M., & Wespi, A. (1999). Towards a Taxonomy of Intrusion-Detection Systems. Computer Networks.

[22] Bace, R. G., & Mell, P. (2001). Intrusion Detection Systems. NIST Special Publication. National Institute of Standards and Technology.

[23] McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E.(2006) .

[24] Kaplan, A., & Haenlein, M. (2019). Siri, Siri, in my hand: Who's the fairest in the land? Business Horizons, 62(1), 15–25

[25] Goertzel, B., & Pennachin, C. (2007). Artificial general intelligence. Springer

[26] Bostrom, N. (2014). Superintelligence: Paths, dangers, strategies. Oxford University Press.

[27] Jurafsky, D., & Martin, J. H. (2023). Speech and language processing (3rd ed.).

[28] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.

[29] Esteva, A., et al. (2019). A guide to deep learning in healthcare. Nature Medicine, 25, 24–29.

[30] Ivanov, D., Dolgui, A., Sokolov, B., & Ivanova, M. (2019). Disruption-driven supply chain risk management. International Journal of Production Research.

[31] Gómez-Uribe, C. A., & Hunt, N. (2016). The Netflix recommender system. ACM Transactions on Management Information Systems, 6(4), 13.

[32] Frey, C. B., & Osborne, M. A. (2017). The future of employment: How susceptible are jobs to computerization? Technological Forecasting and Social Change.

[33] Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. Proceedings of Machine Learning Research.

[34] Zuboff, S. (2019). The age of surveillance capitalism. PublicAffairs.

[35] Walsh, S., et al. (2020). Artificial intelligence and human augmentation in healthcare. npj Digital Medicine,

[36] Kurzweil, R. (2005). The singularity is near: When humans transcend biology. Penguin.