Ministry of Higher Education and Scientific Research

Emirates International University

Faculty of Engineering and IT

Department of Information

وزارة التعليم العالي والبحث العلمي

الجامعة الإماراتية الدولية

كلية الهندسة وتكنولوجيا المعلومات

قسم أمن معلومات

نظام تحليل التهديدات الأمنية والدفاع

Security System for Analyzing and Defending Threats

(SSADT)

أعضاء فريق المشروع:

أحمد شوقي عبد الله الجوفي	2021030254
باسل مسعد ناجي عيسى	2021030972
حميد أسعد حميد القماسي	2021030574
سام بليغ محمد المغربي	2021030149
عماد الدين فوزي عبد الله الحربي	2021030062
محمد يحيى يحيى طاهر	2021030342

إشراف:

أ.م.د. محمد الخولاني

مشرف مساعد:

م. علياء العراسي

مشروع تخرج تم تقديمه لقسم أمن معلومات لاستيفاء متطلبات الحصول على درجة البكالوريوس في أمن المعلومات.

2025-2024

قال تعالى في محكم التنزيل:

بسم الله الرحمن الرحيم

{يَرْفَعِ اللَّهُ الَّذِينَ آمَنُوا مِنكُمْ وَالَّذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ}

[سورة المجادلة: 11]

الملخص

في ظل التزايد المستمر للتهديدات السيبرانية وتعقيد أساليب الهجوم الرقمي، أصبحت المؤسسات بحاجة ماسّة إلى حلول أمنية متقدمة قادرة على التحليل الفوري والاستجابة الذكية. يهدف هذا المشروع إلى تطوير نظام متكامل لتحليل التهديدات الأمنية والدفاع الاستباقي، تحت مسمى "نظام تحليل التهديدات الأمنية والدفاع (SSADT)، بالاعتماد على أدوات مفتوحة المصدر تتمثل في Wazuh لرصد وتحليل سجلات الأنظمة، وSuricata لمراقبة حركة الشبكة واكتشاف الأنشطة غير الطبيعية.

يعتمد النظام على بنية SIEM موحدة تسهم في دمج البيانات وتحليلها من مصادر متعددة، مع تقديم واجهة رسومية مركزية تسهّل على المسؤولين الأمنيين مراقبة الأحداث واتخاذ قرارات فورية. تم تصميم SSADT ليكون قابلًا للاستخدام من قِبل الجهات ذات الخبرة المحدودة في الأمن السيبراني، من خلال واجهات مبسطة وتعليمات تثبيت واضحة.

يمثل SSADT خطوة فعالة نحو بناء قدرات دفاع سيبراني وطنية تعتمد على أدوات مرنة ومفتوحة المصدر، كما يفتح آفاقًا مستقبلية لتضمين الذكاء الاصطناعي وتحليل السلوك التنبئي في أنظمة الدفاع الرقمي.

Abstract

With the continuous rise of cyber threats and the growing sophistication of digital attack methods, organizations are increasingly in need of advanced security solutions capable of real-time analysis and intelligent response. This project presents the development of an integrated system for security threat analysis and proactive defense, named the Security System for Detection and Defending Threats (SSADT). The system leverages open-source tools specifically, Wazuh for system log monitoring and analysis, and Suricata for network traffic inspection and anomaly detection.

SSADT is built upon a unified SIEM architecture that enables the aggregation and analysis of data from multiple sources. It provides a centralized graphical interface that simplifies event monitoring and supports timely decision-making by security administrators. The system is designed to be user-friendly, even for organizations with limited cybersecurity expertise, offering simplified interfaces and clear installation guidelines.

Ultimately, SSADT represents a significant advancement toward establishing national cyber defense capabilities based on flexible and open-source technologies. It also lays the groundwork for future integration of artificial intelligence and predictive behavior analytics into digital defense systems.

تفويض

نفوض الجامعة الإماراتية الدولية كلية الهندسة وتكنولوجيا المعلومات بتزويد نسخ مشروع التخرج للمكتبات أو المنظمات أو الأفراد عند الطلب من الكلية.

كما يسمح باستخدامه في المسابقات الدولية والمحلية.

اسم الطالب	الرقم الجامعي	التوقيع
أحمد شوقي عبد الله الجوفي	2021030254	
باسل مسعد ناجي عيسى	2021030972	
حميد أسعد حميد القماسي	2021030574	
سام بليغ محمد المغربي	2021030149	
عماد الدين فوزي عبد الله الحربي	2021030062	
محمد يحيى يحيى طاهر	2021030342	

التاريخ:

الإهداء

إلى من كانوا سندنا في كل خطوة،

إلى آباؤنا الاعزاء، الذين علمونا معنى الإصرار والعمل الجاد،

وإلى أمهاتنا، نبع الحنان ومصدر الأمان،

اللذين كانا لنا العون والدعاء في كل لحظة.

إلى معلميّ الأفاضل،

شموع العلم التي أضاءت لنا دروب المعرفة،

والذين لم يبخلوا بعلمهم وتوجيههم حتى نصل إلى ما نحن عليه اليوم.

نهديكم هذا الإنجاز المتواضع، عربون شكر ووفاء،

راجين أن يكون بداية لمسيرة عطاء أكبر.

شكر وتقدير

الحمد لله الذي وفقنا وأعاننا على إتمام هذا المشروع، ونسأله أن يكون نافعًا ومباركًا.

نتقدم بخالص الشكر والتقدير إلى دكاترتنا الأفاضل، الذين لم يدخروا جهدًا في تعليمنا وتوجيهنا طوال مسيرتنا الدراسية، وكانت إرشاداتهم ونصائحهم خير معين لنا في إتمام هذا العمل ونخص بالشكر مشرف المشروع أ.م.د.محمد الخولاني والمشرف المساعد م.علياء العراسي.

ولا ننسى زملائنا وأصدقائنا الأعزاء، الذين كانوا لنا عونًا وسندًا، وشركاء في هذه الرحلة الطويلة.

لكم جميعًا نهدي هذا الإنجاز، فهو ثمرة عطائكم ودعمكم الدائم.

إقرار المشرف

أشهد بأن إعداد هذا المشروع بعنوان: **" Security System for Analyzing and Defending Threats"**

من إعداد:

- أحمد شوقي عبد الله الجوفي
- باسل مسعد ناجي عيسى
- حميد أسعد حميد القماسي
- سام بليغ محمد المغربي
- عماد الدين فوزي عبد الله الحربي
- محمد يحيى يحيى طاهر

تم تنفيذه تحت إشرافي في قسم أمن المعلومات استكمالًا جزئيًا لمتطلبات درجة البكالوريوس في أمن المعلومات.

اسم المشرف: أ.م.د. محمد الخولاني

التوقيع:

التاريخ:

لجنة الحكم والمناقشة

اسم المشروع: Security System for Analyzing and Defending Threats

المشرف

م	الاسم	التوقيع
1	أ.م.د. محمد الخولاني	

لجنة المناقشين

م	الاسم	التوقيع
1	د. جميل راشد	
2	د. هشام عقلان	

رئيس القسم:

.....

فهرس المحتويات

فهرس الجداول

فهرس الاشكال

الفصل 1: المقدمة

1.1 تمهيد

في عالمنا الرقمي المتسارع، أصبحت التهديدات الأمنية أمرًا لا يمكن تجاهله. تتنوع هذه التهديدات بين الهجمات السيبرانية مثل الفيروسات والاختراقات الإلكترونية، والتهديدات المادية التي تستهدف المواقع الحساسة. لذلك، أصبح تطوير أنظمة أمنية متقدمة للكشف المبكر عن التهديدات والدفاع عنها ضرورة ملحة لضمان حماية الأفراد والمؤسسات.

يساهم هذا النظام في تحسين مستوى الأمان، تقليل المخاطر، وضمان استمرارية الأعمال دون انقطاع. ويعمل من خلال جمع وتحليل البيانات من مصادر متعددة بهدف كشف أي نشاط غير طبيعي في بيئة العمل الرقمية، باستخدام أدوات فعّالة مثل Wazuh وSuricata. توفر هذه الأدوات تقنيات للكشف والتحليل والتنبيه في الوقت الفعلي، مما يعزز قدرة المؤسسات على التصدي للهجمات بسرعة وفعالية.

1.2 بيان المشكلة

تواجه الشركات الصغيرة والمتوسطة تحديات كبيرة في مجال الأمن السيبراني بسبب محدودية الموارد ونقص المعرفة التقنية. هذا يجعلها أهدافًا رئيسية للهجمات الإلكترونية مثل التصيد الاحتيالي، وهجمات DDoS، والبرامج الضارة، وحقن SQL. وتزداد هذه التحديات مع غياب نظام موحد لتتبع سلوك المستخدمين وتحليل الأحداث الأمنية بشكل مركزي، مما يؤدي إلى صعوبات مثل:

- عدم تتبع الهجمات والمهاجم.
- صعوبة معرفة الاختراقات.
- صعوبة تقييم حجم العمل.
- عدم وجود رؤية مركزية.
- نقص قدرات ربط البيانات.
- الاستجابة البطيئة للحوادث.
- نقص الموارد وارتفاع التكلفة.
- تنسيقات البيانات غير المتوافقة.

1.3 أهداف النظام

الهدف الأساسي من هذا المشروع هو تطوير نظام حاسوبي أمني متكامل يساهم في حماية نظم المعلومات الخاصة بالشركات الصغيرة والمتوسطة، من خلال إنشاء سجل أحداث للعمليات التي ينفذها المستخدمون داخل بيئة العمل. يعتمد المشروع على أدوات فعّالة مثل Wazuh لتحليل السجلات الأمنية ومراقبة سلوك المستخدمين، وSuricata لرصد حركة الشبكة وكشف التهديدات المتقدمة. يحقق النظام الأهداف التالية:

- تنفيذ نظام مركزي لجمع وتحليل البيانات الأمنية.
- تحسين سرعة الاستجابة للحوادث الأمنية.
- توفير لوحة معلومات شاملة وسهلة الاستخدام.
- تعزيز الكشف عن التهديدات المتطورة.
- خفض التكاليف وتحسين الأداء.
- معالجة تنوع تنسيقات البيانات.
- تنفيذ نظام إخطار آلي للحوادث الأمنية.
- اختبار النظام باستخدام سيناريوهات عملية.

1.4 أهمية المشروع

يتوقع أن يوفر النظام المقترح العديد من الفوائد التي تبرز أهميته، ومنها:

- سهولة تتبع المستخدمين وعملياتهم.
- سرعة اكتشاف الهجمات والثغرات.
- تخفيف الضغط على الأنظمة الأمنية التقليدية.
- تقليل الوقت المستغرق في مراقبة الأنشطة المشبوهة.
- الحفاظ على ديمومة واستمرارية عمل النظام.
- حماية البيانات الحساسة وضمان سريتها وسلامتها.
- تقليل الخسائر المالية الناتجة عن الهجمات.
- تعزيز ثقة المستخدمين بأنظمة المعلومات.

1.5 حدود المشروع

- يركز المشروع على حماية نظام المعلومات من التهديدات المرتبطة بسلوك المستخدمين والنشاطات داخل النظام، باستخدام سجل أحداث يتم إنشاؤه بواسطة أدوات مثل Wazuh.
- تُستخدم Suricata كمصدر لتحليل حركة مرور الشبكة، ولكن المشروع لا يشمل الإدارة الشاملة للشبكة.
- لا يتطرق المشروع إلى حماية نظام التشغيل أو إدارة البنية التحتية، بل يركز على مراقبة سلوك المستخدمين وتحليل الأحداث المرتبطة بأنظمة المعلومات.
- التركيز سيكون على بناء نظام فعال ومتكامل باستخدام الأدوات المختارة فقط.

1.6 منهجية المشروع

تم اختيار منهجية Agile لتنفيذ المشروع، وهي منهجية مرنة وتعاونية تركز على التطوير التدريجي والتحسين المستمر.

تُقسّم مراحل المشروع إلى دورات قصيرة (Sprints) تشمل التخطيط، التطوير، الاختبار، والتقييم.

تعزز هذه المنهجية التعاون بين أعضاء الفريق، وتسمح بتعديل المتطلبات حسب الحاجة خلال دورة حياة المشروع، مما يضمن إنتاج نظام أمني عالي الجودة يواكب المتغيرات ويُلبي احتياجات المستخدمين بشكل فعال والشكل يوضح هذه المنهجية:

الشكل 1-1: Agile Methodology

الفصل 2: الخلفية النظرية

2.1 المقدمة

يُعتبر تكامل أنظمة الكشف عن التهديدات والمراقبة الأمنية حجر الزاوية في تعزيز البنية التحتية للأمن السيبراني.

يركز هذا الفصل على الإطار النظري المُستخدم في المشروع، الذي يعتمد على تكامل نظامَي Wazuh (كمنصة لإدارة التهديدات ومراقبة السجلات) وSuricata (كمنصة لكشف التهديدات الشبكية في الوقت الفعلي)، بالإضافة إلى المفاهيم الأساسية لأمن الشبكات.

كما يستعرض الفصل الدراسات السابقة ذات الصلة، ويُبرز الفجوات البحثية التي يسدها هذا المشروع.

2.2 مفاهيم نظرية

2.2.1 نظام Wazuh: المراقبة الأمنية وإدارة التهديدات

Wazuh هو منصة مفتوحة المصدر متخصصة في المراقبة الأمنية (SIEM)واكتشاف التهديدات (XDR)، تعتمد على تحليل السجلات (Logs) وأنماط السلوك المشبوه. تتضمن مكوناته الرئيسية:

1. **العوامل (Agents):** تُنصَب على الأجهزة المستهدفة لجمع البيانات وإرسالها إلى الخادم المركزي.
2. **الخادم (Server):** يُعالج البيانات ويطبق قواعد الكشف عن التهديدات (مثل قواعد OWASP، MITRE ATT&CK).
3. **واجهة Elasticsearch/Kibana:** تُستخدم لتصور البيانات وتحليلها.
4. **قواعد مخصصة (Custom Rules):** تُمكّن من تحديد سلوكيات غير اعتيادية، مثل محاولات الوصول غير المصرح بها أو تغييرات في ملفات النظام.

يُعتبر Wazuh أداة حيوية في الكشف عن الثغرات الأمنية واستجابة الحوادث (Incident Response)، حيث يوفر تكاملاً مع أنظمة خارجية مثل Active Directory وDocker.

2.2.2 نظام Suricata: كشف التهديدات الشبكية في الوقت الفعلي

Suricataهو نظام مفتوح المصدر لكشف التسلل الشبكي (NIDS/NIPS) ، يتميز بقدرته على تحليل حركة المرور الشبكية باستخدام:

- قواعد التوقيعات (Signature-Based Detection): مثل قواعد Emerging Threats وETOpen.
- التحليل السلوكي (Anomaly-Based Detection): لاكتشاف الأنماط غير الاعتيادية (مثل هجمات DDoS).
- دعم بروتوكولات متقدمة: مثل TLS/SSL وHTTP/2.

تتمثل قوة Suricata في قدرته على معالجة حركة مرور عالية السرعة (Multi-Threading) وتكاملها مع أنظمة SIEM مثل Wazuh، مما يوفر طبقة دفاع متكاملة ضد الهجمات مثل التصيد الاحتيالي وهجمات حقن SQL.

2.2.3 أمن الشبكات: التحديات والحلول

تشمل التهديدات الرئيسية للشبكات:

- الهجمات الخارجية: مثل استغلال الثغرات (Zero-Day Exploits).
- الهجمات الداخلية: مثل تسريب البيانات عن طريق الموظفين.
- الهجمات الهجينة: تجمع بين أساليب متعددة (مثل هجمات Ransomware).

يتطلب التصدي لهذه التهديدات نهجاً متعدد الطبقات يشمل:

1. التقسيم الشبكي (Network Segmentation).
2. مراقبة حركة المرور (Traffic Analysis).
3. التحديث المستخدم لأنظمة التشغيل والتطبيقات.
4. التكامل بين أنظمة الكشف (مثل Wazuh + Suricata).

2.3 دراسات سابقة

2.3.1 دراسات حول تكامل SIEM وNIDS

- **دراسة (Ali et al., 2021):** قامت بدمج Wazuh مع Snort لتحسين كشف الهجمات، لكنها لم تتناول تحسين الأداء في البيئات عالية الحركة.
- **دراسة (Chen & Lee, 2022):** استخدمت Suricata مع Elasticsearch لتحليل الهجمات الشبكية، لكنها ركزت على الهجمات الخارجية فقط.

2.3.2 دراسات حول تحليل السلوك المشبوه

- **دراسة (Kumar et al., 2020):** طورت قواعد مخصصة في Wazuh لاكتشاف هجمات Ransomware، لكنها لم تُدمج مع أنظمة شبكية.
- **دراسة (Garcia, 2023):** استخدمت تعلم الآلة مع Suricata للتنبؤ بالهجمات، لكنها تطلبت موارد حاسوبية عالية.

2.3.3 الفجوات البحثية

- غياب حلول متكاملة تجمع بين تحليل السجلات (Wazuh) وحركة المرور (Suricata) في بيئة واحدة.
- محدودية الدراسات في معالجة الهجمات الهجينة التي تستهدف طبقات متعددة.
- الحاجة إلى تحسين الأداء عند معالجة كميات هائلة من البيانات في الوقت الفعلي.

2.4 الاستنتاج

من خلال الاطلاع على الدراسات السابقة يمكن إضافة العمليات التالية في هذا المشروع:

1. **التكامل المتقدم:** بين Wazuh وSuricata لمراقبة الطبقتين (Host-Based وNetwork-Based).
2. **قواعد مخصصة:** تجمع بين توقيعات Suricata وسجلات Wazuh لاكتشاف الهجمات الهجينة.
3. **تحسين الأداء:** استخدام تقنيات التوزيع (Distributed Architecture) لتقليل التأخير في المعالجة.

الفصل 3: التحليل

3.1 مقدمة

في هذا الفصل، سيتم التركيز على تحليل المتطلبات الفنية والوظيفية للمشروع، وتحديد الأدوات والتقنيات الأساسية المستخدمة في تطوير نظام SIEM باستخدام سجل الأحداث لحماية أنظمة المعلومات"، بالاعتماد على الأداتين Wazuh وSuricata

يشمل هذا الفصل:

- تحليل أنواع البيانات التي يجب جمعها من سجلات الأنظمة والشبكات.
- آلية معالجة وتحليل هذه البيانات لاكتشاف الأنماط المشبوهة والتهديدات.
- تحديد متطلبات النظام من الناحية الأمنية والبرمجية لضمان كفاءته في بيئة عمل حقيقية.

تأتي أهمية هذا الفصل من كونه يضع الأسس التقنية لتطوير النظام، ويواجه التحديات المحتملة بحلول تقنية حديثة. الأداتان Wazuh وSuricata تُشكلان العمود الفقري للنظام، إذ يتم استخدام Wazuh لتحليل سلوك المستخدمين والسجلات، بينما Suricata تُستخدم لاكتشاف التهديدات من خلال تحليل حركة مرور الشبكة (Network Traffic).

3.2 متطلبات المستخدمين

3.2.1 متطلبات وظيفية

- مراقبة سلوك المستخدمين (الإدخال، التعديل، الاستعلام، الحذف).
- كشف ومنع الحركات المشبوهة داخل النظام.
- تحديد نوع التهديد أو الهجمة حسب المستخدم والجهاز.
- توليد إحصائيات وتقارير يومية وشهرية.
- توفير تنبيهات لحظية لحالات الاشتباه أو الاختراق.
- استخدام Wazuh في تحليل سجلات الأنظمة والمستخدمين.
- استخدام Suricata لتحليل حركة المرور الشبكي وتحديد الأنشطة الضارة.

3.2.2 متطلبات غير وظيفية

- الخصوصية: حماية بيانات المستخدمين من الوصول غير المصرح.
- السرية: منع تسرب المعلومات الحساسة.
- الموثوقية: ضمان أن النظام يعمل بثبات دون أعطال.
- المرونة: القدرة على التوسع والتعديل بسهولة.
- التوافق: دعم أنظمة تشغيل مختلفة (Windows, Linux).
- التحديث المستمر: لدعم قواعد كشف التهديدات الحديثة.

3.3 دراسة الجدوى

3.3.1 الجدوى التقنية

تشمل الأدوات والامكانيات اللازمة لتطوير النظام وتشغيله ومنها:

- **Hardware:**
  - أجهزة حاسوب لا تقل على ان تكون بمعالج Core-i7 , RAM 16 ,HARD 1T.

- **Software:**

نظام التشغيل:

- Ubunto.

أدوات الأمن السيبراني

- Wazuh: لتحليل السجلات وكشف التهديدات بناءً على سلوك المستخدمين.
- Suricata: لمحرك كشف التسلل وتحليل الشبكة.

لغات البرمجة

- Python
- C#
- Bash Script
- MySQL

3.3.2 الجدوى الاقتصادية

الفرد	الوحدة	تكلفة السنة	تكلفة 5 سنوات
مسؤول الحماية cyber security	1	$2400	$12000
مسؤول ادخال ومراجعة البيانات log file	1→5	$2400→12000$	$12000→60000$
مسؤول مختص بأرشفة بيانات الشركة	4	$2400	$12000
الإجمالي	4→8	$7200→16800	$36000→84000$

جدول 1-3: تكاليف حماية الشركة بدون استخدام النظام المقترح

الفرد	الوحدة	تكلفة بدائية	تكلفة 5 سنوات
النظام	1	1000$	1000$
الصيانة	2	100$	500$
التحديثات	4	100$	500$
الأجهزة	5	3600$	3600$
الإجمالي	NULL	4800$	6600$

جدول 2-3: التكلفة مع نظامنا المقترح باستخدام Wazuh,Suricata

ومن خلال الجدول أعلاه يتيح ان النظام المقترح مجدي اقتصادياً.

3.4 طرق جمع البيانات

3.4.1 العيّنات (Sampling)

تم جمع عينات متنوعة من بيانات السجلات الأمنية من:

1. شركات خاصة تقدم خدمات الإنترنت أو تستضيف بيانات حساسة.
2. مراكز الإنترنت تحتوي على سجلات استخدام الأجهزة من قبل العملاء.

تم تحليل هذه البيانات لتحديد أنماط الهجمات الشائعة وطرق تسرب البيانات.

3.4.2 الملاحظات (Observation)

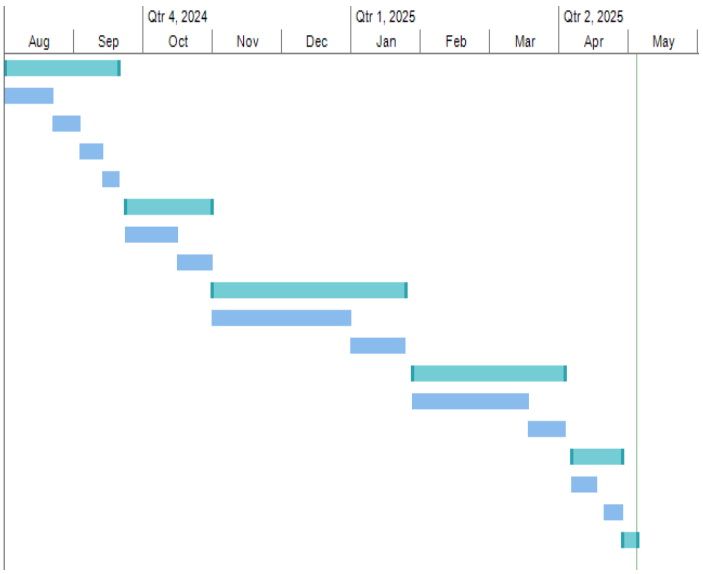
من خلال زيارات ميدانية ومراقبة مباشرة:

- تم ملاحظة أن السجلات غالبًا ما تُدار يدوياً أو عبر أدوات بسيطة.
- لا توجد أنظمة مركزية متقدمة تقوم بربط وتحليل البيانات تلقائيًا.
- قلة استخدام أدوات مثل Wazuh أو Suricata في البيئات الصغيرة، مما يخلق فرصة لتطبيق مشروع عملي فعّال.

3.5 الخطة الزمنية للمشروع

تم تقسيم الخطة الزمنية الى وحدات زمنية كل وحدة تمثل شهراً وتم توزيع الأنشطة على هذه الوحدات.

	Task Mode	اسم المهمة	Duration	Start	Finish
1		**التخطيط**	30 days	Thu 8/1/24 8:00 AM	Thu 9/19/24 5:00 PM
2		جمع المعلومات	12 days	Thu 8/1/24 8:00 AM	Wed 8/21/24 5:00 PM
3		إنشاء خطة المشروع	6 days	Thu 8/22/24 8:00 AM	Mon 9/2/24 5:00 PM
4		دراسة الجدوى	7 days	Tue 9/3/24 8:00 AM	Thu 9/12/24 5:00 PM
5		تحديد نطاق المشروع	5 days	Fri 9/13/24 8:00 AM	Thu 9/19/24 5:00 PM
6		**التحليل**	25 days	Mon 9/23/24 8:00 AM	Wed 10/30/24 5:00 PM
7		تحليل بيئة XDR	15 days	Mon 9/23/24 8:00 AM	Tue 10/15/24 5:00 PM
8		متطلبات التحليل	10 days	Wed 10/16/24 8:00 AM	Wed 10/30/24 5:00 PM
9		**التصميم**	50 days	Thu 10/31/24 8:00 AM	Thu 1/23/25 5:00 PM
10		إنشاء الأكواد	35 days	Thu 10/31/24 8:00 AM	Mon 12/30/24 5:00 PM
11		قابلية الاستخدام	15 days	Tue 12/31/24 8:00 AM	Thu 1/23/25 5:00 PM
12		**التنفيذ والتطوير**	40 days	Mon 1/27/25 8:00 AM	Thu 4/3/25 5:00 PM
13		كتابة الأكواد	30 days	Mon 1/27/25 8:00 AM	Tue 3/18/25 5:00 PM
14		تحسين المنصة	10 days	Wed 3/19/25 8:00 AM	Thu 4/3/25 5:00 PM
15		**الاختبار**	13 days	Mon 4/7/25 8:00 AM	Mon 4/28/25 5:00 PM
16		اختبار الأدوات	8 days	Mon 4/7/25 8:00 AM	Thu 4/17/25 5:00 PM
17		اختبار المنصة	5 days	Mon 4/21/25 8:00 AM	Mon 4/28/25 5:00 PM
18		**التوثيق**	4 days	Tue 4/29/25 8:00 AM	Mon 5/5/25 5:00 PM



الشكل 3-1: الخطة الزمنية

3.6 نمذجة المتطلبات

تعتبر هذه المرحلة مرحلة توصيف ونمذجة للعمليات القائمة في النظام الذي سيتم بناءه وذلك باستخدام UML (Unified Modeling Language)

3.6.1 السيناريو

يقوم مدير الأمن السيبراني في شركة تقنية متوسطة بتسجيل الدخول إلى لوحة تحكم نظام المراقبة الأمنية. تحتوي الشركة على 20 جهازًا و3 خوادم، وتتعامل بشكل يومي مع بيانات عملاء حساسة تتطلب أعلى درجات الحماية. بمجرد الدخول، يبدأ النظام تلقائيًا في عرض مؤشرات الأداء والتنبيهات النشطة. تم تجهيز البنية التحتية الأمنية بتثبيت Wazuh Agent على جميع الأجهزة والخوادم، بينما يعمل Wazuh Manager على خادم مركزي لجمع وتحليل السجلات الأمنية الواردة. إضافة إلى ذلك، تم تفعيل أداة Suricata على أحد الخوادم لمراقبة حركة الشبكة والتعرف على الأنشطة الخبيثة مثل Port Scanning وDNS Tunneling. يقوم Wazuh بمقارنة السجلات بالقواعد المحددة لرصد السلوكيات غير المعتادة. عند اكتشاف تهديد محتمل، يتم إرسال تنبيه فوري إلى لوحة التحكم، ويتلقى المدير إشعارًا عبر البريد الإلكتروني. بعد ذلك، يقوم محلل الأمن بمراجعة تفاصيل الحدث، وتحديد الجهاز والمستخدم المتورط، ثم اتخاذ الإجراءات اللازمة. وفي نهاية كل شهر، يُولّد النظام تقريرًا آليًا يتضمن إحصائيات الهجمات، وأكثر الأجهزة استهدافًا، وعدد الحوادث التي تم التعامل معها. وخلال أحد الأشهر، تمكن النظام من اكتشاف ثلاث محاولات SQL Injection، وسبع محاولات مسح شبكي تم حظرها، مع إرسال 12 تنبيهًا أمنيًا، منها 8 حقيقية و4 إنذارات كاذبة، ما ساعد على تقليص زمن اكتشاف التهديدات من 6 ساعات إلى أقل من 10 دقائق.

3.6.2 نموذج حالة المستخدم

الشكل 2-3: مخطط حالة المستخدم (Use Case Diagram)

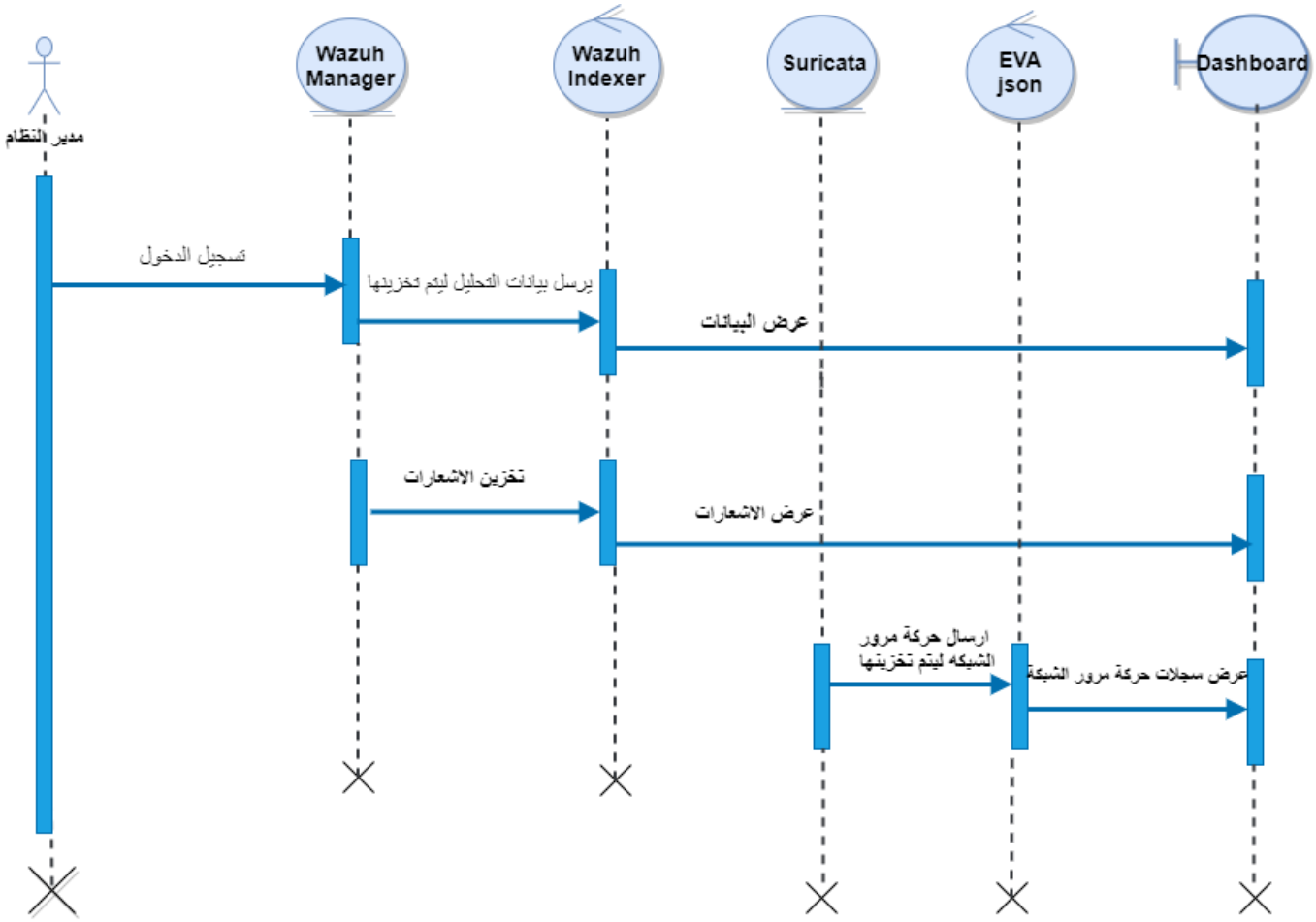
3.6.2.1 المستخدمون Actors

اسم المستخدم	نوع المستخدم	الصلاحية
مسؤول النظام	مستخدم نهائي	الوصول الكامل إلى النظام وإدارته.

جدول 3-3: المستخدمون (Actors)

3.6.3 نماذج الكائنات Objects Model

3.6.3.1 مخطط التسلسل Sequence Diagram



الشكل 3-3: مخطط التسلسل لعمليات مدير النظام (Sequence Diagram)

الفصل 4: تنفيذ النظام

4.1 المقدمة

يتناول هذا الفصل الجوانب العملية لتنفيذ نظام إدارة أمن المعلومات والكشف عن التهديدات السيبرانية (SIEM) باستخدام الأداتين Wazuh وSuricata، حيث يتم عرض الخطوات التي تم اتباعها لبناء النظام وتكوينه، بدءًا من إعداد بيئة العمل المناسبة وتكوين الأدوات الأمنية، مرورًا بتهيئة Wazuh لجمع وتحليل سجلات الأنظمة، وتفعيل Suricata لمراقبة حركة الشبكة، وصولاً إلى اختبار النظام باستخدام سيناريوهات واقعية لمحاكاة الهجمات وتحليل الاستجابة لها. كما يتضمن الفصل عرضًا للنتائج التي تم التوصل إليها بعد الانتهاء من مراحل التطوير والتجربة. يهدف هذا الفصل إلى توثيق الجانب العملي للمشروع بشكل شامل، بما يعكس الجهد المبذول لتحويل المفاهيم النظرية إلى نظام أمن سيبراني متكامل وفعّال يدعم احتياجات المؤسسات الصغيرة والمتوسطة في مواجهة التهديدات الرقمية.

4.2 بناء الواجهات

تعتبر واجهات النظام سهلة الفهم وليست معقدة بحيث يمكن استخدامها بسهولة ومن أهم وجهات النظام الأساسية:

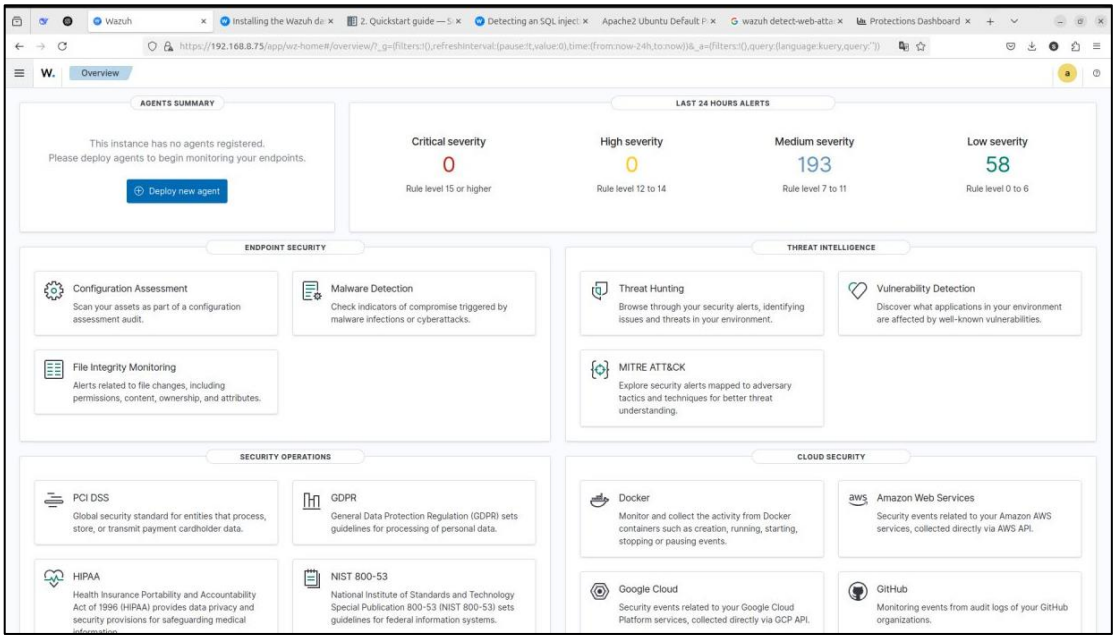
4.2.1 واجهة تسجيل الدخول

تعتبر أول واجهة تظهر للمستخدم عند فتح النظام.

الشكل 1-4: واجهة تسجيل الدخول

4.2.2 واجهة النظرة العامة (Overview)

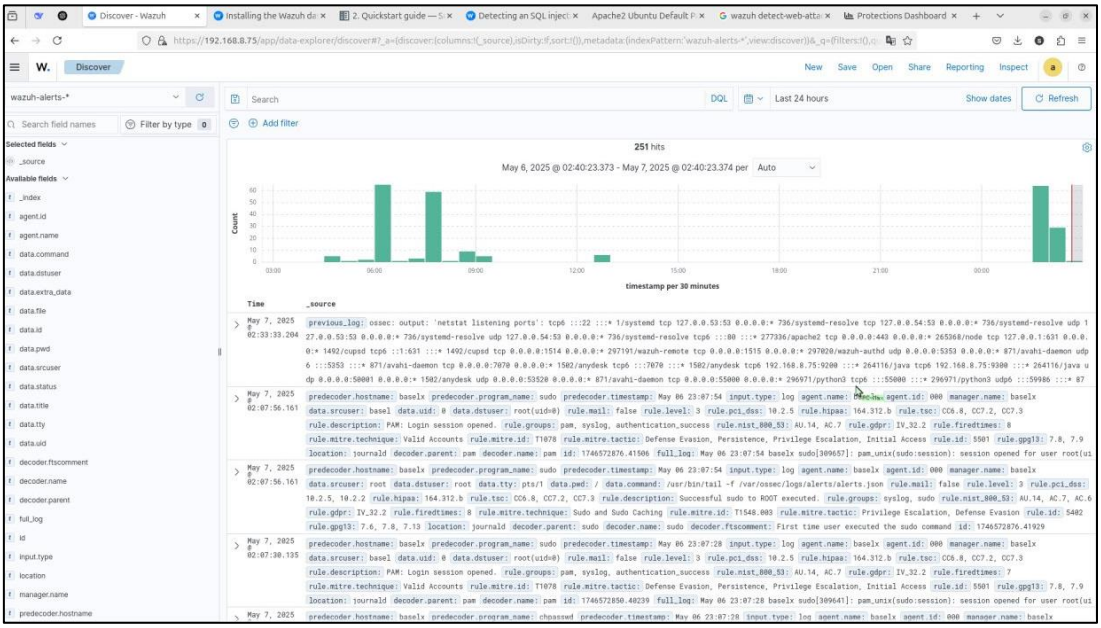
تعرض ملخصًا لحالة الأمان الكلي للنظام، مثل عدد التنبيهات، الأجهزة المتصلة، التهديدات المكتشفة، وأكثر الأحداث نشاطًا.



الشكل 2-4: واجهة النظرة العامة (Overview)

4.2.3 واجهة الاستكشاف (Discover)

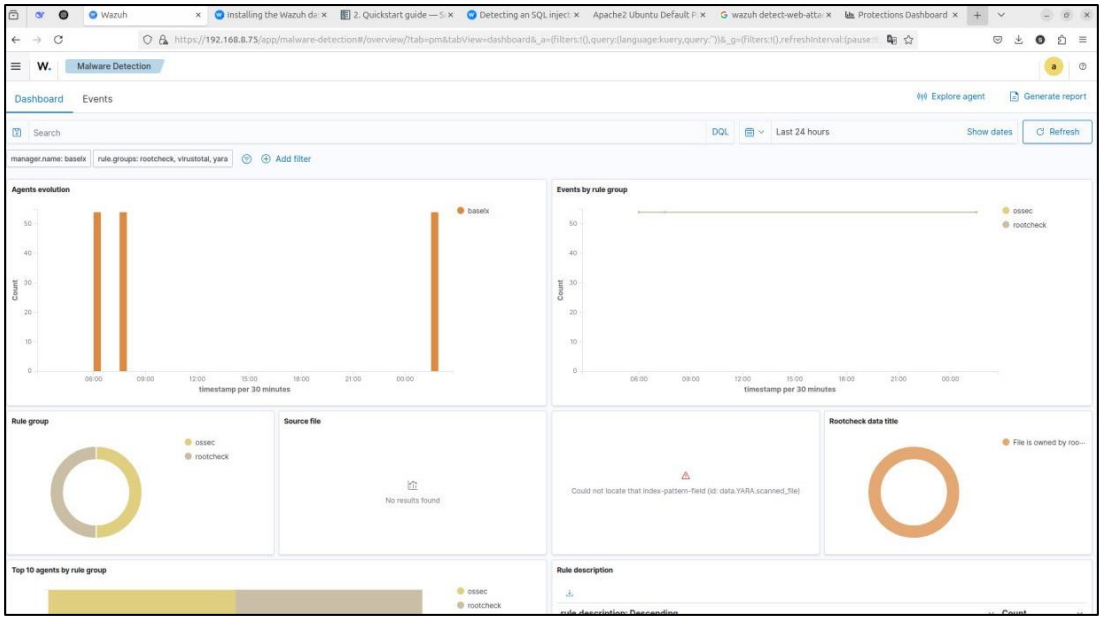
تستخدم لاستعراض وتحليل بيانات السجلات (Logs) الخام المجمعة من الوكلاء، بطريقة مشابهة لـ Kibana، عبر فلترة وتخصيص الأعمدة والبحث.



الشكل 3-4: واجهة الاستكشاف (Discover)

4.2.4 واجهة كشف البرمجيات الخبيثة

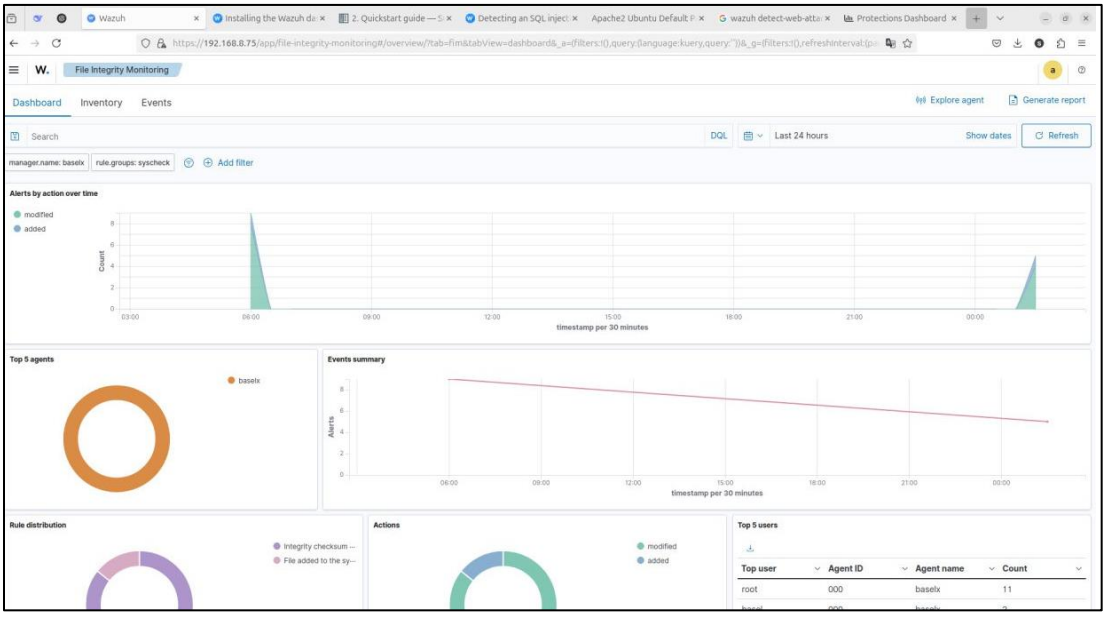
عرض النتائج المتعلقة باكتشاف البرمجيات الخبيثة استنادًا إلى قواعد فحص الملفات والسجلات.



الشكل 4-4: واجهة كشف البرمجيات الخبيثة

4.2.5 واجهة مراقبة سلامة الملفات

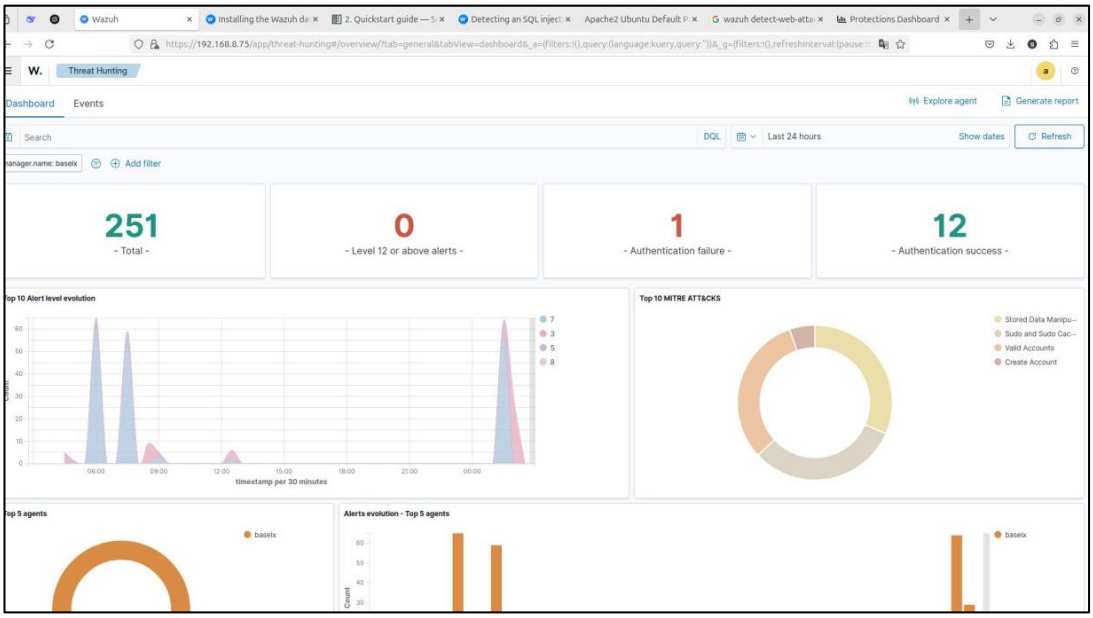
يراقب التغييرات على الملفات الحساسة (مثل ملفات النظام أو التكوين)، ويرسل تنبيهات عند تعديلها.



الشكل 4-5: واجهة مراقبة سلامة الملفات

4.2.6 واجهة صيد التهديدات

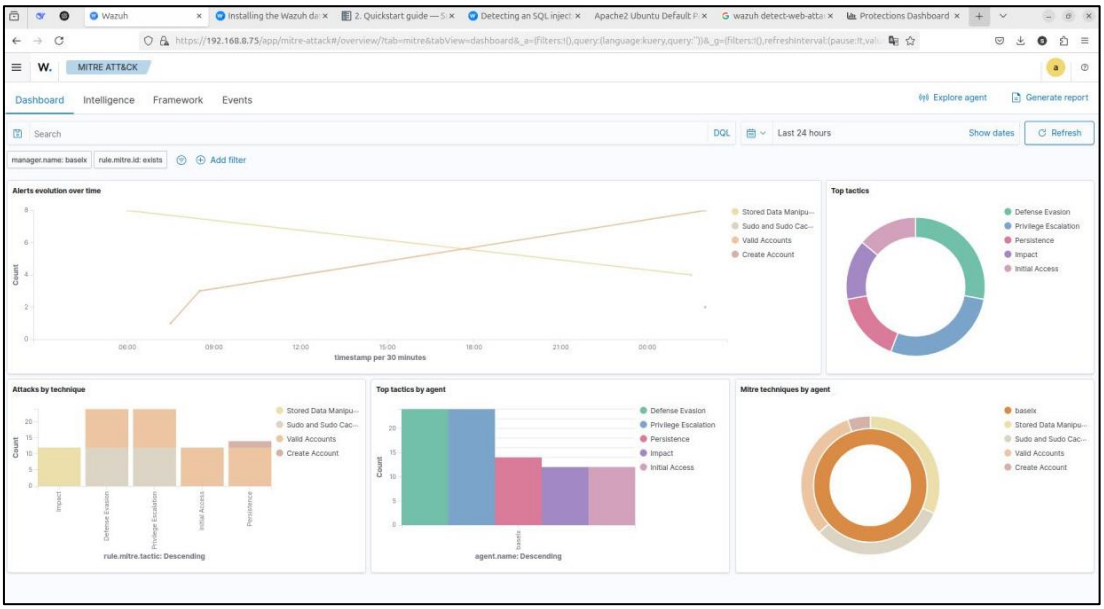
أداة تحليلية لاستعراض الأنشطة المشبوهة يدويًا، مثل تحليلIPs ، العمليات النشطة، أو سجلات الدخول والخروج.



الشكل 4-6: واجهة صيد التهديدات

4.2.7 واجهة إطار الهجمات

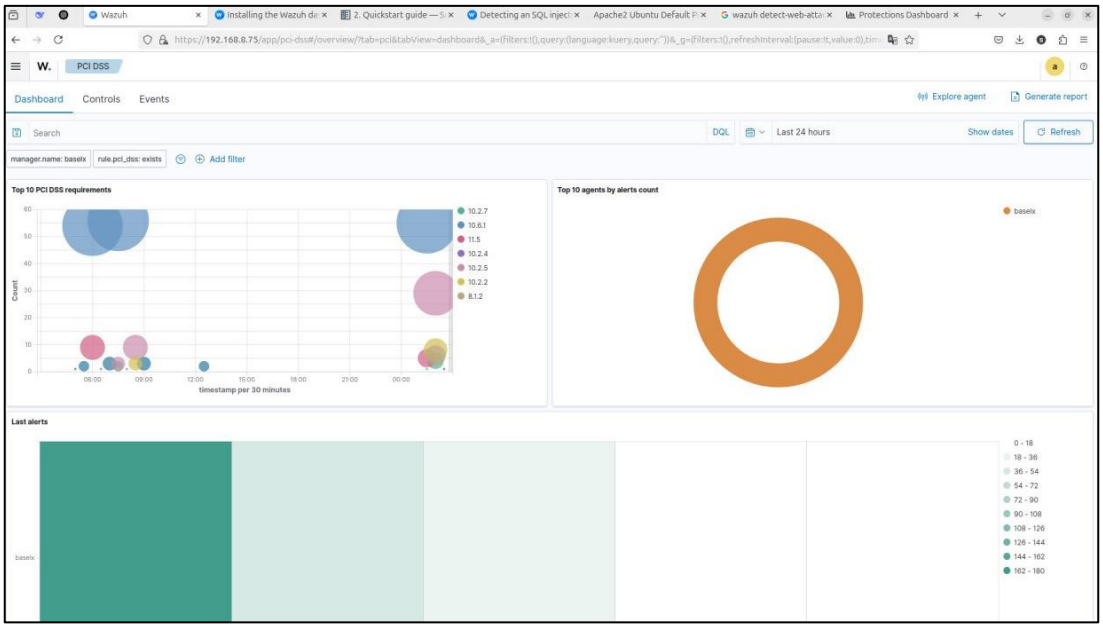
يربط التنبيهات المكتشفة بتكتيكات وتقنيات MITRE ATT\&CK لمعرفة نوع الهجوم وسلوكه.



الشكل 4-7: واجهة اطار الهجمات

4.2.8 واجهة PCI DSS

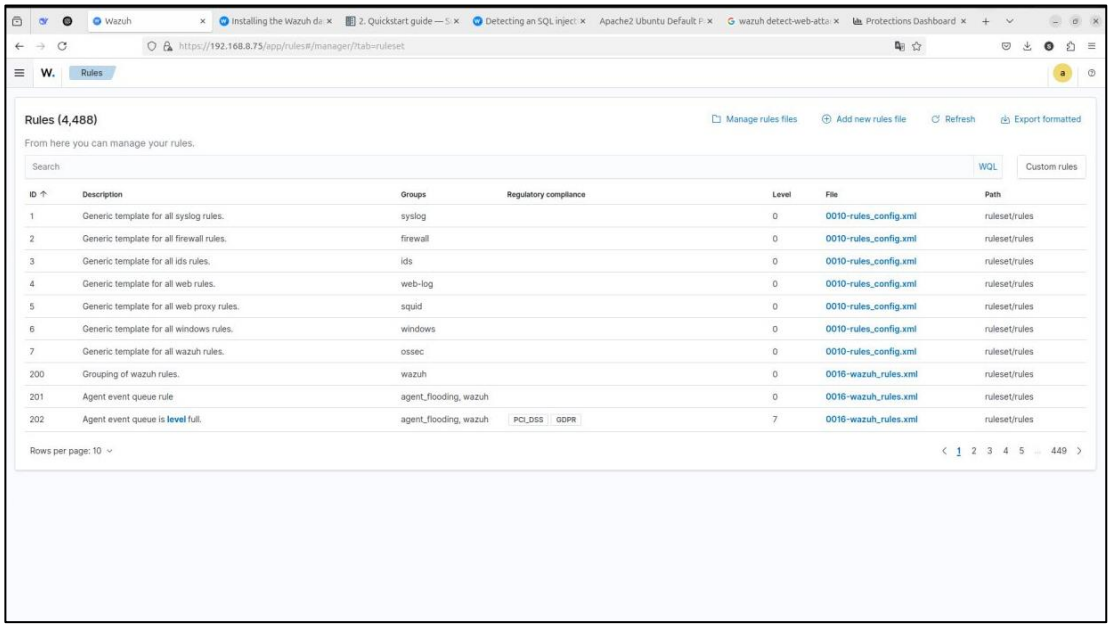
لحماية بيانات بطاقات الدفع.



الشكل 4-8: واجهة PCI DSS

4.2.9 واجهة القواعد (Roles)

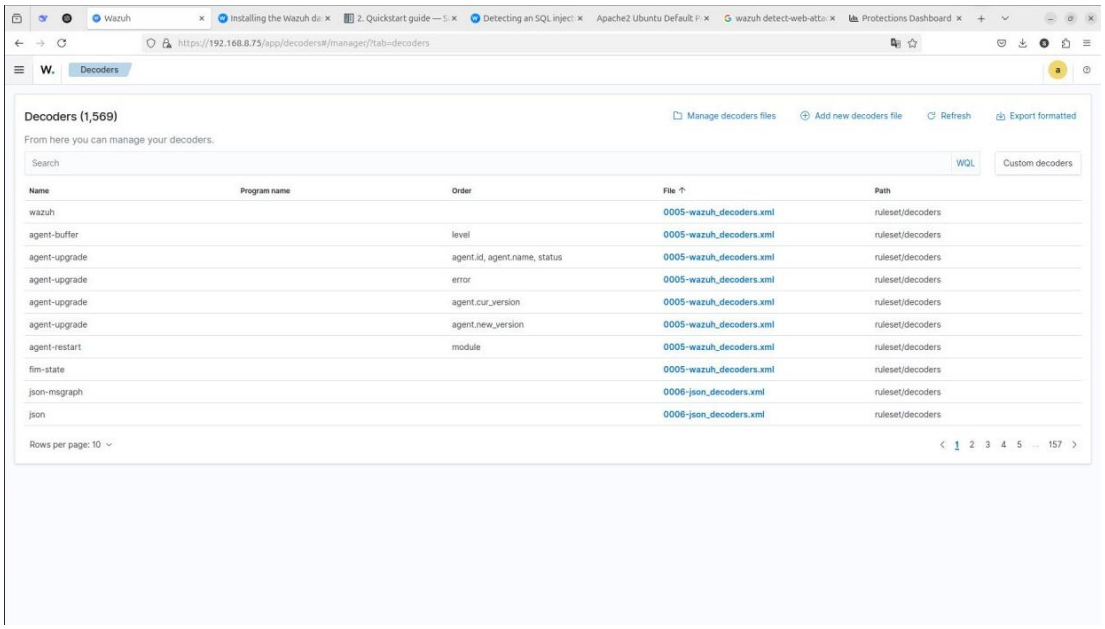
القواعد التي تحدد متى يتم إطلاق التنبيهات.



الشكل 4-9: واجهة القواعد (Roles)

4.2.10 واجهة (Decoders)

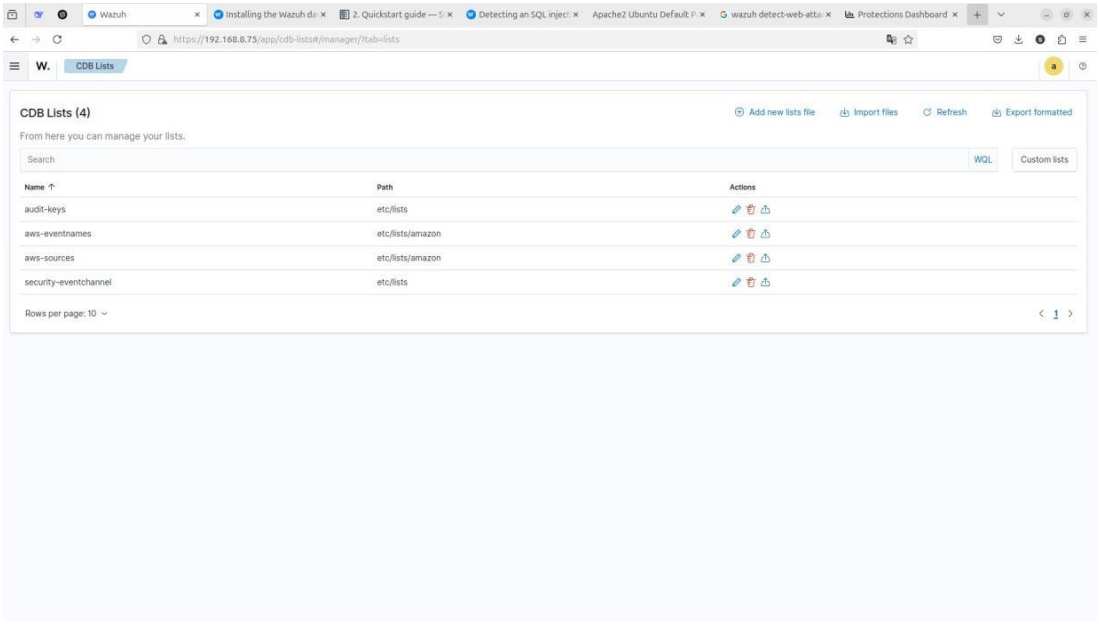
تفسر تنسيقات السجلات المختلفة.



الشكل 4-10: واجهة (Decoders)

4.2.11 واجهة القوائم (Lists)

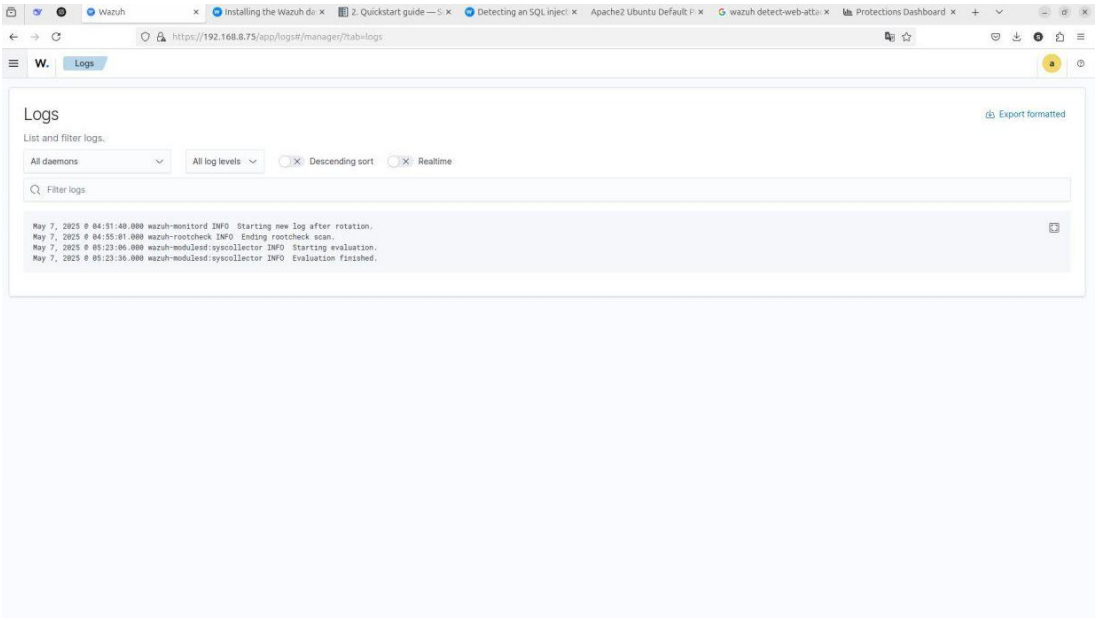
قوائم قابلة للتحديث لتطابق قواعد معينة مثل IPs أو كلمات مرور.



الشكل 4-11: واجهة القوائم (Lists)

4.2.12 واجهة السجلات (Logs)

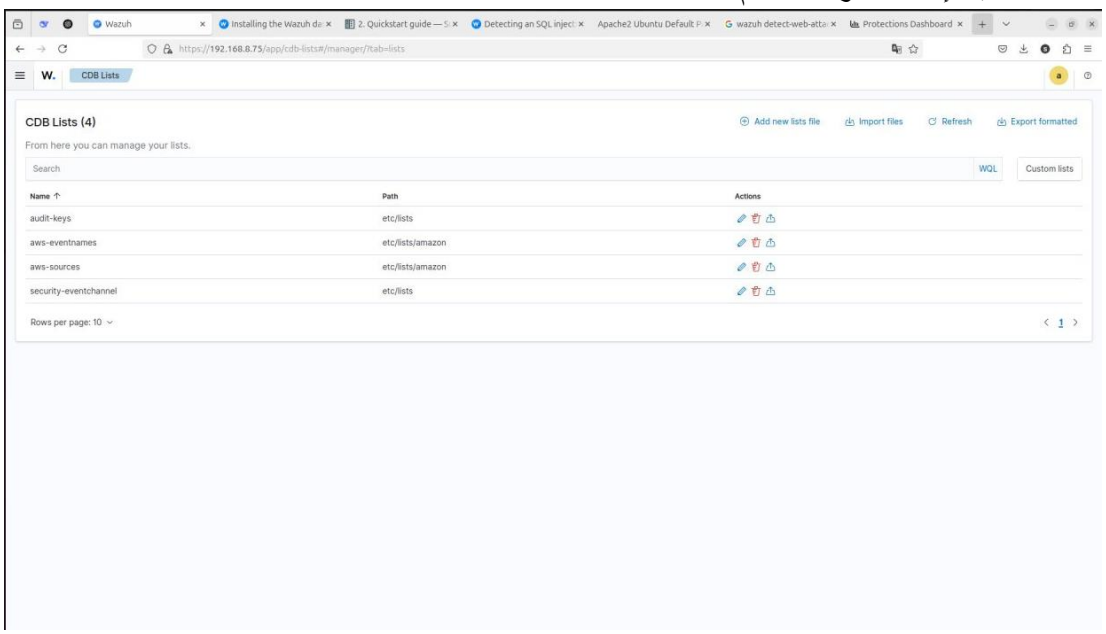
الاطلاع على سجلات النظام.



الشكل 12-4: واجهة السجلات (Logs)

4.2.13 واجهة الاعدادات (Settings)

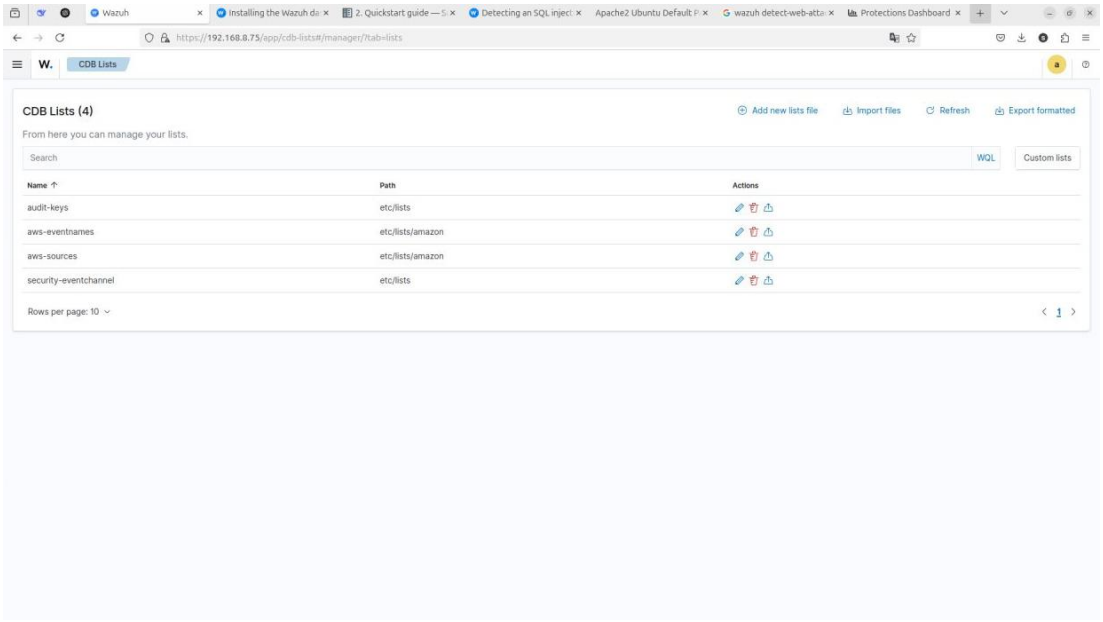
ضبط إعدادات لوحة التحكم.



الشكل 13-4: واجهة الاعدادات (Settings)

4.2.14 واجهة Dev Tools

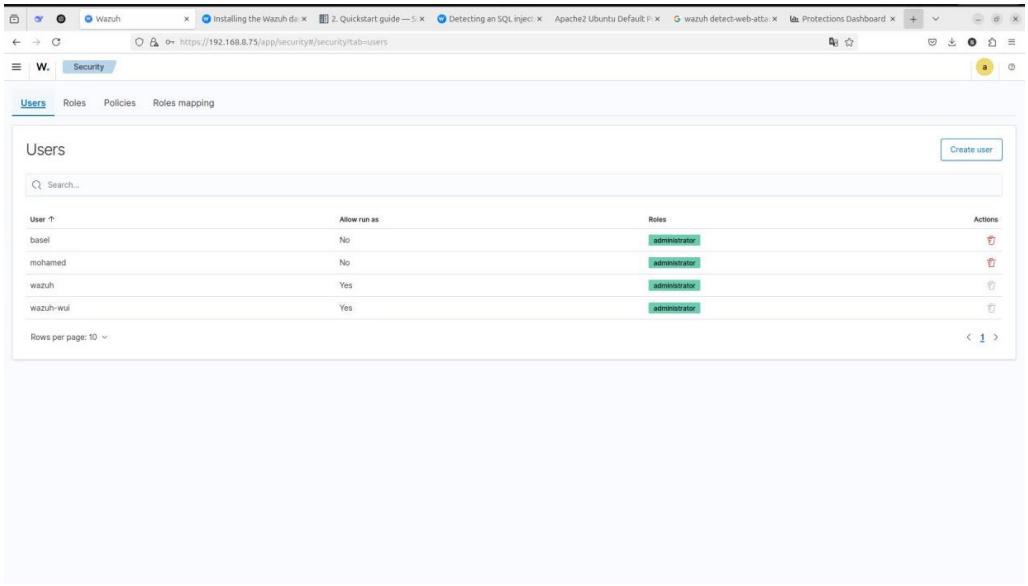
أدوات المطورين مثل استعلامات.OpenSearch



الشكل 4-14: واجهة Dev Tools

4.2.15 واجهة إدارة المستخدمين

إدارة صلاحيات المستخدمين والتحكم في الوصول.



الشكل 4-15: واجهة إدارة المستخدمين

4.3 دليل المستخدم

تم تصميم نظام تحليل التهديدات الأمنية والدفاع SSADT بواجهة إشرافية بسيطة وواضحة من خلال لوحة تحكم مركزية، تتيح لمدير النظام أو المسؤول الأمني التنقل بسهولة بين أقسام المراقبة والتنبيهات وإعدادات الحماية، دون الحاجة إلى خبرة تقنية معقدة في أدوات الأمن السيبراني.

يوفر النظام تعليمات مبسطة ضمن صفحة الإعدادات تشرح للمستخدم طريقة تثبيت وكيل Wazuh (Wazuh Agent) على الأجهزة المستهدفة، بالإضافة إلى خطوات ربط Suricata لمراقبة حركة الشبكة. تتضمن الإرشادات أوامر جاهزة للتنفيذ في الطرفية (Terminal)، مع شرح مفصل لكل خطوة لتسهيل الإعداد حتى على غير المختصين.

كما يتضمن الدليل أمثلة حقيقية على سيناريوهات التهديدات وطريقة اكتشافها ومعالجتها داخل النظام، مما يساعد المستخدم على فهم آلية عمل SSADT والاستفادة منه بشكل عملي وفعّال في حماية بيئة العمل الرقمية الخاصة بالمؤسسة.

4.4 تكامل واختبار النظام

4.4.1 اختبار التكامل

تم دمج جميع مكونات نظام SSADT بنجاح، حيث شمل التكامل كل من أداة Wazuh الخاصة بمراقبة السجلات وتحليل سلوك الأنظمة، وأداة Suricata الخاصة بمراقبة حركة الشبكة واكتشاف التهديدات في الوقت الفعلي. بعد دمج الأداتين ضمن منصة SIEM موحدة، تم تنفيذ اختبارات تكامل شاملة لضمان التفاعل السليم بين الوحدات، مثل إرسال التنبيهات، معالجة الأحداث، وعرض التقارير المركزية. وقد أثبتت نتائج الاختبار أن النظام يعمل كوحدة متكاملة بدون أي تعارض أو أخطاء.

4.4.2 اختبار النظام

- **اختبار قابلية الاستخدام**

تم التركيز في هذا الاختبار على تجربة مدير النظام والمستخدمين الأمنيين، حيث تم التأكد من سهولة التعامل مع لوحة التحكم الخاصة بـ SSADT، وكذلك طريقة عرض تنبيهات Suricata عبر واجهة Wazuh. أظهرت النتائج أن المستخدمين تمكنوا من استيعاب وظائف النظام الأساسية بسهولة دون الحاجة إلى تدريب معقد، مما يؤكد أن التصميم يدعم قابلية الاستخدام حتى لمن ليست لديهم خبرة متقدمة في الأمن السيبراني.

- **اختبار واجهات المستخدم**

شمل هذا الاختبار التحقق من عمل واجهة Wazuh Web UI بسلاسة ضمن بيئة SSADT، واستجابة جميع العناصر الرسومية. تم اختبار الواجهة على متصفحات وأنظمة تشغيل مختلفة، وتم التأكد من توافقها مع مختلف قياسات الشاشات (شاشات كمبيوتر، أجهزة لوحية، هواتف محمولة). كما تم التأكد من أن تقارير التهديدات وسجلات الأحداث تُعرض بشكل منظم وسهل القراءة.

- **اختبار قابلية الوصول**

تم اختبار الوصول إلى النظام من خلال متصفحات مختلفة (مثل Chrome، Firefox، Microsoft Edge) وعلى أنظمة تشغيل متنوعة (Windows، Linux)، وتم التأكد من أن SSADT يعمل بكفاءة ولا يعتمد على مكونات إضافية غير مدعومة. كما تم اختبار إمكانية الوصول من شبكات مختلفة للتحقق من أمان وربط واجهة النظام بشكل مناسب مع قيود الشبكة.

- **اختبار الموثوقية**

تم تشغيل نظام SSADT على بيئة افتراضية ذات أحمال متزايدة لمحاكاة عمله في ظروف واقعية. كما تم إدخال كمّ كبير من السجلات ومراقبة الاستجابة والأداء. لم تُسجّل أي حالات تعطل أو فقدان بيانات، وأظهر النظام استقرارًا عاليًا في معالجة الطلبات والتنبيهات، مما يعكس موثوقيته للاستخدام في بيئة مؤسسية حقيقية.

4.5 نتائج المشروع

حقق نظام تحليل التهديدات الأمنية والدفاع SSADT النتائج الأساسية المخطط لها بنجاح، حيث تمكن من تلبية جميع الأهداف التي وُضعت له منذ بداية المشروع. أثبت النظام فعاليته في مراقبة سلوك المستخدمين واكتشاف التهديدات الأمنية في الوقت الفعلي، مع توفير سجل أحداث شامل يمكن الاعتماد عليه في تحليل الأنشطة المشبوهة.

كما أظهر SSADT أداءً مستقرًا، وتكاملًا مرنًا بين مكوناته، واستجابة فورية للحوادث. ساهمت الواجهة الرسومية البسيطة في تمكين مسؤولي النظام من استخدامه بسهولة دون الحاجة إلى خبرة تقنية متقدمة. هذه النتائج تؤكد نجاح SSADT في تعزيز أمن المؤسسات الصغيرة والمتوسطة، وتشير إلى إمكانية توسيعه مستقبلًا ليشمل قدرات تحليل متقدمة وتكاملات إضافية.

الفصل 5: الأعمال المستقبلية والتوصيات

5.1 نظرة عامة

يهدف هذا الفصل إلى تقديم رؤية مستقبلية لنظام تحليل التهديدات الأمنية والدفاع (SSADT)، استنادًا إلى التجربة العملية والنتائج التي تم تحقيقها خلال مراحل تطوير النظام واختباره. كما يتناول هذا الفصل مجموعة من المقترحات التي يمكن تنفيذها في المستقبل لتعزيز قدرات النظام، إلى جانب توصيات عامة لضمان كفاءته واستدامته في بيئات العمل المختلفة، خصوصًا في الشركات الصغيرة والمتوسطة.

5.2 الأعمال المستقبلية

- دمج خوارزميات ذكية تعتمد على التعلم الآلي لتحسين قدرات النظام على التنبؤ بالتهديدات غير المعروفة.
- تطوير وحدة تحليل متقدمة لسلوك المستخدم (UEBA) لتمييز السلوكيات الاعتيادية عن الأنشطة المشبوهة.
- تعزيز التكامل مع أنظمة أخرى مثل الجدر النارية (Firewall) وأنظمة مكافحة الفيروسات لزيادة فعالية الاستجابة التلقائية.
- إضافة وحدة لتحليل بيانات الشبكة في الزمن الحقيقي باستخدام أدوات مفتوحة المصدر متقدمة.

5.3 التوصيات

- يُوصى بتدريب موظفي الشركات على كيفية التعامل مع التنبيهات الأمنية وقراءة التقارير لفهم طبيعة المخاطر والاستجابة المناسبة.
- التأكد من تحديث قواعد البيانات الخاصة بالهجمات والتهديدات بشكل منتظم ليبقى النظام محدثًا بأحدث الأساليب المستخدمة من قبل المهاجمين.
- تكوين نظام نسخ احتياطي دوري لبيانات النظام لتجنب ضياع المعلومات في حال وقوع هجوم كبير أو عطل فني.

5.4 الخاتمة

في ختام هذا المشروع، تم بحمد الله الانتهاء من تطوير نظام تحليل التهديدات الأمنية والدفاع (SSADT)، والذي يُعد أداة أمنية متكاملة تهدف إلى تعزيز حماية أنظمة المعلومات في المؤسسات الصغيرة والمتوسطة. تم تصميم النظام ليكون سهل الاستخدام، وقابلًا للتخصيص، ويعتمد على أدوات مفتوحة المصدر فعّالة مثل Wazuh وSuricata، مما يجعله حلاً اقتصاديًا وعمليًا في الوقت نفسه.

يعتمد SSADT على فكرة جمع وتحليل السجلات الأمنية والأنشطة المرتبطة بالمستخدمين، بهدف اكتشاف أي نشاط غير طبيعي في الوقت الحقيقي، مع توفير تقارير تنبيهية دقيقة تساعد مسؤولي النظام على اتخاذ قرارات سريعة. وخلال مراحل التطوير،

المراجع

1. Wazuh Documentation, 2023.

2. Suricata User Guide, 2023.

3. Chen, L., & Lee, S. (2022). "Integrating NIDS with SIEM for Advanced Threat Detection ."

4. Garcia, M. (2023). "Machine Learning Approaches in Network Security."

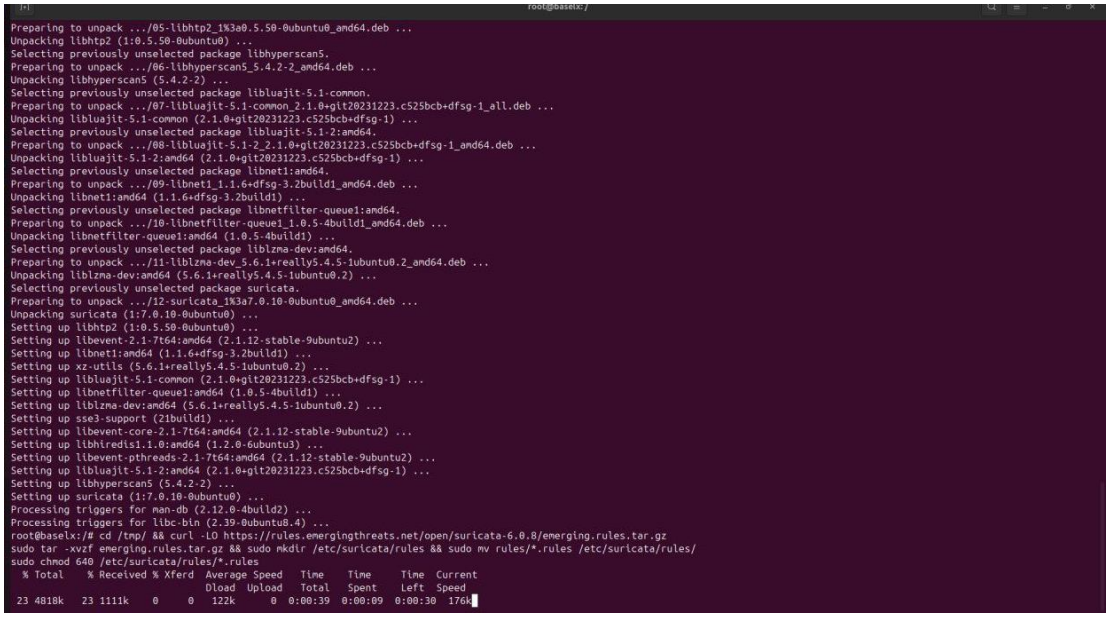
5. Collins, M. (2023). *"Network Security Through Data Analysis".* O'Reilly Media.

6. Kumar, R., et al. (2020). *"Custom Rule-Based Threat Detection in Wazuh for Ransomware Attacks".* ACM Digital Library.

7. Ali, H., et al. (2021). *"Integration of SIEM and NIDS for Enhanced Threat Detection in Enterprise Networks".* IEEE Xplore.

الملحقات

وهنا سوف نقوم بإرفاق بعض من اكواد النظام



```
and many more great features -
https://suricata.io/features/all-features/
More info: https://launchpad.net/~oisf/+archive/ubuntu/suricata-stable
Adding repository.
Press [ENTER] to continue or Ctrl-c to cancel.
Found existing deb entry in /etc/apt/sources.list.d/oisf-ubuntu-suricata-stable-noble.sources
Hit:1 http://archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:3 http://archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:4 http://archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:5 https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu noble InRelease
Reading package lists... Done
Hit:1 http://archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:3 http://archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:4 http://archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:5 https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu noble InRelease
Reading package lists... Done
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
suricata is already the newest version (1:7.0.10-0ubuntu0).
0 upgraded, 0 newly installed, 0 to remove and 208 not upgraded.
root@baselx:/# cd /tmp/ && curl -LO https://rules.emergingthreats.net/open/suricata-6.0.8/emerging.rules.tar.gz
sudo tar -xvzf emerging.rules.tar.gz && sudo mkdir /etc/suricata/rules && sudo mv rules/*.rules /etc/suricata/rules/
sudo chmod 640 /etc/suricata/rules/*.rules
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 4822k  100 4822k    0     0   120k      0  0:00:40  0:00:40 --:--:--  199k
rules/
rules/BSD-License.txt
rules/LICENSE
rules/botcc.portgrouped.rules
rules/botcc.rules
rules/ciarmy.rules
rules/classification.config
rules/compromised-ips.txt
rules/compromised.rules
rules/drop.rules
rules/dshield.rules
rules/emerging-activex.rules
rules/emerging-adware_pup.rules
rules/emerging-attack_response.rules
rules/emerging-chat.rules
rules/emerging-coinminer.rules
```

```
oot@baselx:/# sudo add-apt-repository ppa:oisf/suricata-stable
udo apt-get update
udo apt-get install suricata -y
epository: 'Types: deb
RIs: https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu/
uites: noble
omponents: main

escription:
uricata IDS/IPS/NSM stable packages
ttps://suricata.io/
ttps://oisf.net/

uricata IDS/IPS/NSM - Suricata is a high performance Intrusion Detection and Prevention System and Network Security Monitoring engine.

pen Source and owned by a community run non-profit foundation, the Open Information Security Foundation (OISF). Suricata is developed by the OISF, its supporting vendors and the commu
ity.

his Engine supports:

 Multi-Threading - provides for extremely fast and flexible operation on multicore systems.
 Multi Tenancy - Per vlan/Per interface
 Uses Rust for most protocol detection/parsing
 TLS/SSL certificate matching/logging
 JA3 TLS client fingerprinting
 JA3S TLS server fingerprinting
 IEEE 802.1ad (QinQ) and IEEE 802.1Q (VLAN) support
 VXLAN support
 All JSON output/logging capability
 IDS runmode
 IPS runmode
 IDPS runmode
 NSM runmode
 eBPF/XDP
 Automatic Protocol Detection and logging - IPv4/6, TCP, UDP, ICMP, HTTP, SMTP, TLS, SSH, FTP, SMB, DNS, NFS, TFTP, KRB5, DHCP, IKEv2, SNMP, SIP, RDP
 SCADA automatic protocol detection - ENIP/DNP3/MODBUS
 File Extraction HTTP/SMTP/FTP/NFS/SMB - over 4000 file types recognized and extracted from live traffic.
 File MD5/SHA1/SHA256 matching
 Gzip Decompression
 Fast IP Matching
 Datasets matching
 Rustlang enabled protocol detection
 Lua scripting

nd many more great features -
```

```
Notice: suricata: This is Suricata version 7.0.10 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 8
Info: suricata: Running suricata under test mode
Info: suricata: Setting engine mode to IDS mode by default
Info: exception-policy: master exception-policy set to: auto
Info: logopenfile: fast output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: eve.json
Info: logopenfile: stats output device (regular) initialized: stats.log
Info: detect: 52 rule files processed. 42873 rules successfully loaded, 0 rules failed, 0
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 42876 signatures processed. 1223 are IP-only rules, 5067 are inspecting packet payload, 36553 inspect application layer, 0 are decoder event only
Notice: suricata: Configuration provided was successfully loaded. Exiting.
root@baselx:/#
```

```
##
## Configure Suricata to load Suricata-Update managed rules.
##

default-rule-path: /var/lib/suricata/rules

rule-files:
  - suricata.rules
  - "*.rules"
##
## Auxiliary configuration files.
##

classification-file: /etc/suricata/classification.config
reference-config-file: /etc/suricata/reference.config
# threshold-file: /etc/suricata/threshold.config

##
## Include other configs
##

# Includes:  Files included here will be handled as if they were in-lined
# in this configuration file. Files with relative pathnames will be
# searched for in the same directory as this configuration file. You may
# use absolute pathnames too.
#include:
#   - include1.yaml
#   - include2.yaml
```

```
root@baselx:/# sudo add-apt-repository ppa:oisf/suricata-stable
sudo apt-get update
sudo apt-get install suricata -y
Repository: 'Types: deb
URIs: https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu/
Suites: noble
Components: main
'
Description:
Suricata IDS/IPS/NSM stable packages
https://suricata.io/
https://oisf.net/

Suricata IDS/IPS/NSM - Suricata is a high performance Intrusion Detection and Prevention System and Network Security Monitoring engine.

Open Source and owned by a community run non-profit foundation, the Open Information Security Foundation (OISF). Suricata is developed by the OISF, its supporting vendors and the commu
nity.

This Engine supports:

- Multi-Threading - provides for extremely fast and flexible operation on multicore systems.
- Multi Tenancy - Per vlan/Per interface
- Uses Rust for most protocol detection/parsing
- TLS/SSL certificate matching/logging
- JA3 TLS client fingerprinting
- JA3S TLS server fingerprinting
- IEEE 802.1ad (QinQ) and IEEE 802.1Q (VLAN) support
- VXLAN support
- All JSON output/logging capability
- IDS runmode
- IPS runmode
- IDPS runmode
- NSM runmode
- eBPF/XDP
- Automatic Protocol Detection and logging - IPv4/6, TCP, UDP, ICMP, HTTP, SMTP, TLS, SSH, FTP, SMB, DNS, NFS, TFTP, KRB5, DHCP, IKEv2, SNMP, SIP, RDP
- SCADA automatic protocol detection - ENIP/DNP3/MODBUS
- File Extraction HTTP/SMTP/FTP/NFS/SMB - over 4000 file types recognized and extracted from live traffic.
- File MD5/SHA1/SHA256 matching
- Gzip Decompression
- Fast IP Matching
- Datasets matching
- Rustlang enabled protocol detection
- Lua scripting

and many more great features -
```

```
Notice: suricata: This is Suricata version 7.0.10 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 8
Info: suricata: Running suricata under test mode
Info: suricata: Setting engine mode to IDS mode by default
Info: exception-policy: master exception-policy set to: auto
Info: logopenfile: fast output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: eve.json
Info: logopenfile: stats output device (regular) initialized: stats.log
Info: detect: 52 rule files processed. 42873 rules successfully loaded, 0 rules failed, 0
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 42876 signatures processed. 1223 are IP-only rules, 5067 are inspecting packet payload, 36553 inspect application layer, 0 are decoder event only
Notice: suricata: Configuration provided was successfully loaded. Exiting.
root@baselx:/#
```