Security Operations Center (SOC) Course Summary

ملخص كورس مركز عمليات الأمن

إعداد: إسماعيل محمد قطان

Prepared by: Ismail Muhammed Kattan

التاريخ: أكتوبر/ تشرين الأول 2025

Date: October, 2025



### تعريف مركز عمليات الأمن (SOC Definition)

#### ما هو مركز عمليات الأمن SOC؟

* هو **مركز القيادة المركزي** لأمن المعلومات في أي مؤسسة.
* مسؤوليته تشمل المراقبة، الكشف، التحليل، والاستجابة للحوادث الأمنية في الوقت الفعلي.
* يُعدّ مركز SOC خط الدفاع الأول لحماية البيانات، الأنظمة، والشبكات.

**لماذا هو مهم؟**

* الهجمات الإلكترونية مستمرة وتتطور باستمرار — ومركز SOC يضمن الحماية المستمرة.
* من دون SOC، يمكن أن تمرّ الاختراقات لفترات طويلة دون اكتشافها، مما يزيد الأضرار.
* يجمع SOC بين الأشخاص، والعمليات، والتكنولوجيا للحفاظ على أمان الأنظمة.

#### الهدف الرئيسي لمركز SOC

* الوقاية: تحديد التهديدات قبل أن تسبب الضرر.
* الكشف: ملاحظة الأنشطة المشبوهة والتحقق منها.
* الاستجابة: احتواء الهجمات والتعامل معها بسرعة.
* التعافي والتحسين: التعلم من الحوادث لتعزيز الدفاعات المستقبلية.

#### هيكل مركز SOC — لماذا توجد مستويات (Tiers) متعددة؟

يُنظّم مركز SOC على شكل مستويات (Tiers) لإدارة الحوادث حسب درجة تعقيدها:

| **المستوى (Tier)** | **الوظيفة** | **سبب وجوده** |
| --- | --- | --- |
| *المستوى الأول (Tier 1)* | مراقبة التنبيهات والتصنيف المبدئي | يضمن الاستجابة السريعة ويستبعد التنبيهات الخاطئة حتى لا يضيع وقت الخبراء. |
| *المستوى الثاني (Tier 2)* | التحقيق المتعمق والتنسيق | يتعامل مع الحوادث الحقيقية ويحدد تأثيرها الكامل. |
| *المستوى الثالث (Tier 3)* | الاستجابة المتقدمة وصيد التهديدات | يتعامل مع الهجمات المتقدمة مثل الثغرات الجديدة (Zero-Day). |
| *المدير / CISO* | القيادة والاستراتيجية | يضمن توافق السياسات والعمليات مع أهداف أمان المؤسسة. |

**ملاحظة مهمة**

نظام المستويات يسمح بـ **تصعيد فعال للحوادث** — القضايا البسيطة تُعالج بسرعة، والمعقدة تصل إلى الخبراء.

#### مفاهيم الثغرات الجديدة (Zero-Day) & برامج الفدية (Ransomware)

* Ransomware: برنامج خبيث يقوم بتشفير البيانات ويطلب فدية لفكّها.
* Zero-Day Attack: هجوم جديد غير معروف مسبقًا — لا يوجد له تصحيح أمني بعد.
* هذه الهجمات تتطلب مهارات متقدمة (Tier 3) واستجابة سريعة للحد من الأضرار.

#### أعضاء آخرون في مركز SOC

* CISO: المدير المسؤول عن الاستراتيجية الأمنية الشاملة.
* Red Team (الفريق الأحمر): يحاكي الهجمات لاختبار الدفاعات (هجومي).
* Blue Team (الفريق الأزرق): يدافع ضد تلك الهجمات (دفاعي).
* مهندسو الأمن: يبنون ويصونون أدوات المراقبة والأنظمة التقنية.

**لماذا هم مهمون؟**

هذه الأدوار الخارجية تعزّز فعالية SOC، وتضمن أن الأدوات والسياسات والاختبارات تواكب التهديدات الحديثة.

— — — — — — — — — — — — — — — —

### بيئة مركز عمليات الأمن (SOC) في يومنا

#### وقت البقاء (Dwell Time)

* التعريف: هو المدة الزمنية التي يقضيها المهاجم داخل الشبكة قبل اكتشافه.
* لماذا هو مهم:
  + كلما طال الوقت، زادت الأضرار المحتملة.
  + يُستخدم كمقياس لمدى فعالية مركز الأمن في اكتشاف التهديدات.
* الواقع الحالي: متوسط وقت الاكتشاف يتراوح بين 100 إلى 200 يومًا (وفق تقرير Cisco السنوي).
* هدف مركز العمليات الأمنية: تقليل وقت البقاء عبر الاكتشاف السريع والاستجابة الفورية.

**التدريب والممارسة في مراكز SOC:**

تقوم الفرق بتنفيذ تدريبات محاكاة للهجمات لمعرفة سرعة اكتشافها والاستجابة لها، مما يزيد من الجاهزية في الحالات الواقعية.

#### مصادر التهديدات السيبرانية

المهاجمون يأتون من مصادر متعددة:

1. الجريمة المنظمة — المصدر الرئيسي، بهدف الربح المالي.
2. جهات حكومية أو تابعة لدول — بهدف التجسس أو المصالح السياسية.
3. موظفون داخليون — إما عن قصد أو بسبب الإهمال.
4. مخترقون مبتدئون (Script Kiddies) — يستخدمون أدوات جاهزة من الإنترنت.

**لماذا هذا مهم:**

معرفة نوع المهاجم تساعد مركز الأمن على توقّع سلوكه ووضع دفاعات مناسبة له.

#### دوافع الهجمات

* الهدف الأساسي: الربح المالي (الفدية، سرقة الأموال، الاحتيال).
* أهداف ثانوية:
  + التجسس وجمع المعلومات.
  + إعادة استخدام الشيفرات لأغراض خفية وطويلة الأمد.

**الفكرة الأساسية:**

رغم تنوع الأسباب، تبقى الأموال والمعلومات المحركين الرئيسيين للهجمات.

#### أساليب الهجوم الشائعة

1. التصيّد الإلكتروني (Phishing)

* رسائل بريد إلكتروني مزيفة تبدو حقيقية.
* غالبًا تتضمن تهديدًا أو طلبًا عاجلاً للحصول على معلومات حساسة.
* تشكل المدخل الأساسي لمعظم الهجمات (مثل برامج الفدية).

1. برامج الفدية (Ransomware)

* برمجيات خبيثة تشفّر البيانات وتطلب فدية مقابل فكها.
* الأنواع الحديثة تقوم أيضًا بسرقة البيانات وتهدد بنشرها.
* تبدأ عادة عبر رسائل التصيّد تحتوي على روابط أو مرفقات خبيثة.
* حتى مع النسخ الاحتياطية، يمكن أن تبقى الشركة في وضع حرج بسبب تسريب البيانات.

1. الهجمات من نوع "اليوم الصفري" (Zero-Day)

* تستغل ثغرات غير معروفة مسبقًا.
* لا يوجد لها تصحيح أو حماية جاهزة.
* يصعب اكتشافها وتتطلب استجابة متقدمة من محللين محترفين (المستوى الثالث).

#### الهندسة الاجتماعية (Social Engineering)

يعتمد المهاجمون على خداع الأشخاص نفسيًا للحصول على معلومات أو وصول.

مثال من المحاضرة: “جولي” تجمع معلومات من وسائل التواصل، وتكتب رسائل تبدو وكأنها من مدير الشركة.

* تدرس الضحية وسلوكها.
* تقلّد أسلوب التواصل الداخلي.
* تستغل الثقة والعجلة لإقناع الهدف.

**النقطة الأساسية:**

الهندسة الاجتماعية تتجاوز الدفاعات التقنية لأنها تهاجم العامل البشري — الحلقة الأضعف في الأمن.

#### التعاون بين مركز SOC والإدارات الأخرى

* يجب على مركز العمليات الأمنية التعاون مع الإدارات الداخلية (الموارد البشرية، القانونية، المالية، تكنولوجيا المعلومات...).
* لأن كل إدارة تمتلك أصولًا رقمية مهمة:
  + الموارد البشرية → بيانات شخصية وحسابات بنكية.
  + القانونية → الملكية الفكرية.
  + المالية → بيانات مالية ومعاملات.
* أثناء الحادث:
  + يتم تحديد ما تم اختراقه.
  + جمع الأدلة الرقمية (Artifacts) للتحليل الجنائي.
  + استعادة الأنظمة بشكل آمن.

**المفهوم الأساسي:**

الاستجابة للحوادث ليست تقنية فقط — بل تشمل جميع أقسام المؤسسة.

#### المعايير القانونية والدولية

* تتبع مراكز SOC معايير وإجراءات دولية معترف بها (مثل NIST، ISO/IEC 27035).
* الهدف منها:
  + ضمان سلامة الأدلة أثناء التحقيق.
  + جعلها قانونية ومعترف بها في المحاكم الدولية.
* الالتزام بالمعايير يعزز المصداقية والمساءلة والتعاون الدولي.

— — — — — — — — — — — — — — — —

### هدف مركز عمليات الأمن (Goal of a SOC)

#### ما هو الهدف من إنشاء مركز SOC؟

* الهدف الأساسي لأي مؤسسة تُنشئ مركز عمليات أمن (SOC) هو الحفاظ على استمرارية العمل (Business Continuity) ونزاهة البيانات والأنظمة (Integrity).
* لأن أي توقف في العمل بسبب الهجمات الإلكترونية يسبب خسائر مالية كبيرة،

بينما اختراق سمعة الشركة يمكن أن يكون أسوأ من الخسائر المادية نفسها.

#### الإستراتيجيات التي يستخدمها مركز SOC لتحقيق الأهداف

1. الاستراتيجية الاستباقية (Proactive Strategy)

الـSOC لا ينتظر الهجمات بل يحاول التفكير قبل القراصنة بخطوة واحدة.

ولتحقيق ذلك، يعتمد على معرفة شاملة بالشبكة من خلال:

* جرد الأصول (Asset Inventorying): معرفة كل الأجهزة والأنظمة في المؤسسة.
* المراقبة الأمنية المستمرة (Continuous Monitoring): مراقبة النظام على مدار الساعة.
* المسح للبحث عن ثغرات (Vulnerability Scanning): اكتشاف نقاط الضعف قبل أن تُستغل.
* اختبار الاختراق (Penetration Testing): محاكاة هجوم حقيقي لمعرفة مستوى الحماية.
* صيد التهديدات (Threat Hunting): البحث النشط عن علامات الهجمات.

كلما عرف فريق SOC نظامه أكثر، كان أسهل عليه التعرف على الهجمات والرد بسرعة.

1. تقليل أثر الاختراق (Minimizing Impact)

عندما يحدث اختراق فعلاً، يعمل الـSOC على تقليل الضرر بأقصى سرعة ممكنة.

* التركيز على سرعة الكشف (Detection Time): كلما قلّ الوقت بين الاختراق واكتشافه، قلّت الأضرار.
* استخدام ذكاء التهديدات (Threat Intelligence): لتحديد أولويات العمل بناءً على أخطر التهديدات الحالية في الصناعة.
* تحليل الحوادث السابقة: تُستخدم نتائج التحقيقات لتقوية السياسات والاستراتيجيات المستقبلية.

المعلومات التي يتم جمعها من استجابة الحوادث تساعد أيضًا في حساب المخاطر المالية الناتجة عن التهديدات السيبرانية.

#### مثال عملي: كيف يعمل الـSOC أثناء هجوم

1. الموظف يكتشف رسالة تصيّد (Phishing Email)

– يرسلها إلى فريق SOC بعد أن خضع لتدريب أمني.

1. محلل المستوى الأول (Tier 1 Analyst)

– يتحقق من أن الرسالة خبيثة بسبب وجود ملف تنفيذي مشبوه.

1. محلل المستوى الثاني (Tier 2 Analyst)

– يستخدم أدوات مثل Cisco Secure Malware Analytics لتأكيد أنها هجمة "Zero-Day" (غير معروفة مسبقاً).

1. الاستجابة (Mitigation)

– يقوم فريق SOC و KNOC (فريق الشبكة) بتنفيذ الإجراءات المناسبة مثل:

* حظر الملف على الأجهزة.
* استرجاع الرسالة من النظام البريدي.
* تفعيل أدوات الحماية مثل نظام كشف التسلل (IDS).

1. محلل المستوى الثالث (Tier 3 Analyst)

– يبدأ صيد التهديدات للتأكد من أن الهجوم لم ينتشر داخليًا، مثل:

* فحص ما إذا نقر أحد المستخدمين على البريد.
* التحقق من توزيع الرسالة داخل الشركة أو خارجها.
* مراجعة أي نشاط حدث بعد فتح المرفق.

#### مقارنة: مؤسسة لديها SOC مقابل مؤسسة بدون SOC

| **الحالة** | **النتيجة** |
| --- | --- |
| ***مع وجود SOC*** | الاستجابة للحوادث سريعة، الضرر محدود، العمل مستمر بثقة. |
| ***بدون SOC*** | تأخر في اكتشاف الهجوم، خسائر مالية وسمعة سيئة، توقف العمل. |

الفرق بين المؤسستين هائل — مركز SOC لا يمنع الهجمات فقط، بل يحافظ على استقرار الشركة ويمنحها راحة بال.

— — — — — — — — — — — — — — — —

### تحديات مركز عمليات الأمن (SOC)

#### 1. التحديات التقنية

تشمل كل المكونات الحالية والمستقبلية من العتاد والبرمجيات، سواء في الموقع (On-premises) أو في السحابة.

كلما زادت التكنولوجيا من حيث الكمّ والتعقيد، زادت صعوبة إدارة مركز العمليات لها.

من أبرز التحديات:

* البنية التحتية لتقنية المعلومات أصبحت معقدة ومترابطة بين السحابة والمقرات.
* ضعف الرؤية الشاملة للشبكة يجعل من الصعب تتبع جميع الأجهزة وتدفقات البيانات.
* إدخال أجهزة وأنظمة جديدة يجعل من الصعب تحليل مصادر البيانات المختلفة.
* ازدياد الأجهزة يؤدي إلى زيادة الأحداث والتنبيهات، مما ينتج عنه كثرة الإنذارات الخاطئة (False Positives).

#### 2. التحديات البشرية

العنصر البشري هو أهم مورد يمتلكه مركز العمليات، لكنه يواجه تحديات كبيرة، منها:

* **إرهاق محللي الأمن (SOC Analyst Burnout):**

بسبب الكمّ الكبير من التنبيهات اليومية، حتى بعد التصفية باستخدام الأدوات، يبقى عدد كبير يجب التعامل معه يدويًا.

طبيعة العمل الرتيبة والضغط الزمني والمسؤولية العالية تؤدي إلى الإرهاق النفسي والوظيفي.

* **نقص الكفاءات وصعوبة الاحتفاظ بها:**

من الصعب الاحتفاظ بالمحللين المهرة، لذلك تضطر الشركات لإنفاق موارد إضافية لتدريب الموظفين الجدد أو تطوير القدامى.

* **ضعف التواصل الفعّال:**

غالبًا ما يكون التواصل بين المحللين مباشرًا وغير منظم، مما يؤدي إلى ضياع الوقت وضعف تبادل المعرفة.

الحل هو استخدام أدوات تعاون جماعي مثل Cisco SecureX و Splunk Phantom التي تسهل المشاركة المعرفية وتحفز الفريق.

#### 3. التحديات في العمليات

من المهم أن تكون العمليات داخل مركز العمليات موثقة وواضحة حتى يتم تنفيذها بكفاءة.

لكن كثيرًا من مراكز العمليات تفتقر إلى وثائق محددة لعملياتها، مما يؤدي إلى الارتباك وضعف الكفاءة.

ينبغي كتابة وتوزيع وثائق تحدد المعايير والتنظيمات التي تنطبق على المركز وتتكيف مع خصائصه التشغيلية.

#### 4. الحوكمة والامتثال (Governance & Compliance)

من مسؤوليات الحوكمة قياس أداء وكفاءة مركز العمليات.

لكن المشكلة أن المقاييس الحالية غالبًا لا تعكس أهداف المركز بدقة، لذلك هناك حاجة إلى مقاييس موحدة لقياس مدى تحقيق الأهداف الأمنية.

أما فيما يتعلق بالخصوصية، فهناك اختلافات كبيرة بين القوانين في دول مثل الاتحاد الأوروبي والولايات المتحدة، مما يجعل من الصعب على المؤسسات الدولية معرفة ما يُسمح بجمعه ومشاركته من بيانات عبر الحدود.

— — — — — — — — — — — — — — — —

### تفاعل مركز العمليات الأمنية (SOC) مع الأقسام الأخرى

مركز العمليات الأمنية (SOC) لا يعمل بشكل مستقل، بل يعتمد على تعاون وثيق مع أقسام أخرى داخل المؤسسة لتحقيق فعالية في الاستجابة للحوادث وحماية الأصول الرقمية.

#### أهمية التعاون بين SOC وبقية الأقسام

التهديدات مستمرة ومتعددة، لذلك يجب أن يعمل الـSOC بالتوازي مع الأقسام الأخرى لضمان تغطية شاملة لكل الجوانب التقنية، القانونية، والبشرية.

التعاون يضمن أن الاستجابة للحوادث تكون متكاملة (فنية + قانونية + تنظيمية).

يعزز الامتثال للمعايير والقوانين مثل GDPR وISO 27001.

#### الأقسام الأساسية التي يتفاعل معها الـSOC

| **القسم** | **دوره في الأمن السيبراني** | **أهمية التعاون** |
| --- | --- | --- |
| *NOC / IT Operations* | تنفيذ إجراءات الاستجابة (مثل عزل الأجهزة، إيقاف الخدمات المتأثرة، أو إصلاح الشبكة). | يسمح للـSOC بالتحكم السريع في التهديدات التقنية. |
| *القسم القانوني (Legal)* | مراجعة الخروقات القانونية، التواصل مع الجهات التنظيمية، وتقييم التبعات القانونية للخرق. | يضمن أن الاستجابة للحوادث تتوافق مع القانون وتحمي سمعة الشركة. |
| *الموارد البشرية (HR)* | التواصل مع الموظفين المتأثرين، وتدريب العاملين على الأمن السيبراني وتقليل الأخطاء البشرية. | يبني ثقافة أمنية داخل المؤسسة تقلل فرص الهجمات الناجحة. |

#### النتائج الأمنية للتعاون الجيد

* استجابة أسرع وأكثر تنسيقًا للحوادث.
* تقليل الأضرار الناتجة عن الهجمات.
* تحسين الوعي الأمني داخل الشركة.
* رفع النضج الأمني للمؤسسة ككل.

— — — — — — — — — — — — — — — —

### الخدمات الشائعة لمركز العمليات الأمنية (SOC)

مركز العمليات الأمنية (**SOC**) لا يكتفي فقط بالمراقبة أو كشف الحوادث، بل يقدم **مجموعة واسعة من الخدمات الأمنية** التي تغطي كامل دورة حياة الحادث:

**الكشف ⬅️ الاستجابة ⬅️ التعافي**.

#### مراحل عمل الـSOC وخدماته في كل مرحلة

# **مراحل دور SOC في إدارة الحوادث**

| **المرحلة** | **الدور الأساسي للـSOC** | **أهم الخدمات المقدَّمة** |
| --- | --- | --- |
| *1. ما قبل الحادث (Pre-Incident)* | التحضير والكشف المبكر عن التهديدات | 🔸 تحليل البيانات وتحسين التنبيهات عبر دمج نتائج التحقيقات السابقة.  🔸 استخدام معلومات التهديدات (Threat Intelligence).  🔸 مراقبة الأنظمة والشبكات بشكل مستمر. |
| *2. أثناء الحادث (Incident Response)* | احتواء الهجوم وتقليل الأضرار | 🔸 تحليل البرمجيات الخبيثة (Malware Analysis).  🔸 التنسيق مع الفرق الأخرى مثل NOC وفرق الأمن الداخلي.  🔸 تنفيذ إجراءات العزل، الحظر، أو إزالة التهديد.  🔸 توجيه عملية الاستجابة للحادث (Incident Response Guidance). |
| *3. بعد الحادث (Recovery & Post-Incident)* | التعافي والتحسين المستمر | 🔸 جمع الأدلة الرقمية (Digital Forensics).  🔸 إعداد تقارير مفصلة عن الحادث والدروس المستفادة.  🔸 التعاون مع الأقسام القانونية والامتثال (Legal & Compliance).  🔸 تحسين السياسات والإجراءات لمنع تكرار الحادث. |

#### مفاهيم رئيسية

* تحليل البرمجيات الخبيثة (Malware Analysis):

عملية فحص سلوك الملفات الضارة لتحديد آلية عملها وتأثيرها.

* التحليل الجنائي الرقمي (Digital Forensics):

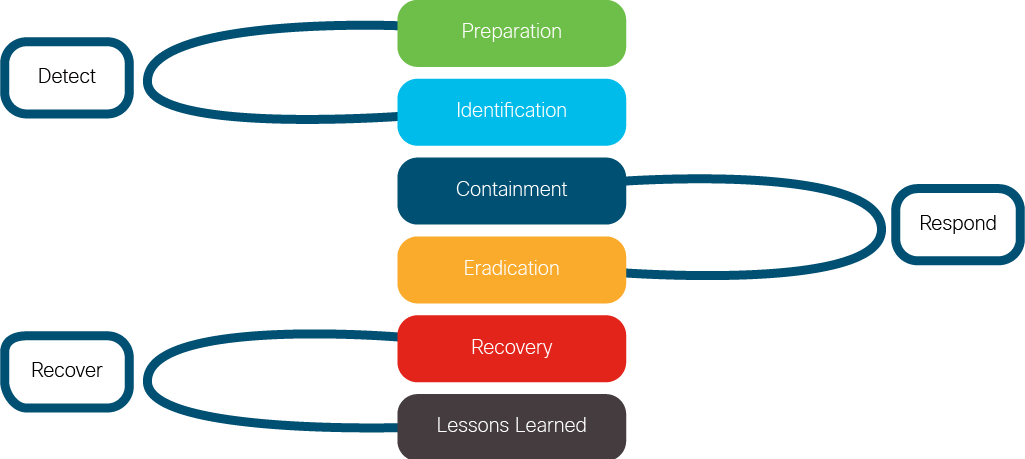
استخدام تقنيات تحقيق متقدمة لجمع الأدلة وحفظها بطريقة يمكن تقديمها للمحكمة.

* ذكاء التهديدات (Threat Intelligence):

جمع وتحليل معلومات حول التهديدات المحتملة لمساعدة الـSOC في اتخاذ قرارات استباقية.

#### أهمية تنسيق الـSOC مع الأقسام الأخرى

* القانوني (Legal): لضمان توثيق الأدلة بطريقة قانونية.
* الموارد البشرية (HR): لإدارة التواصل مع الموظفين المتأثرين أو المتسببين بالحادث.
* الامتثال (Compliance): لضمان توافق الإجراءات مع القوانين والسياسات الدولية.



— — — — — — — — — — — — — — — —

### أنواع مراكز العمليات الأمنية (SOC Types) واعتبارات التوظيف

كل منظمة لديها احتياجات أمنية مختلفة، ولهذا تختلف أهداف وطبيعة مركز العمليات الأمنية (SOC) فيها. بناءً على ذلك، يوجد ثلاثة أنواع رئيسية من مراكز الـSOC، يختص كل منها بنهج مختلف لحماية المنظمة.

#### الأنواع الثلاثة لمراكز الـSOC

| **النوع** | **الهدف الأساسي** | **الأنشطة والمجالات الرئيسية** | **المميزات** |
| --- | --- | --- | --- |
| *1. مركز تهديدي (Threat-Centric SOC)* | البحث الاستباقي عن التهديدات (Threat Hunting) | 🔸 الصيد الاستباقي للتهديدات (Threat Hunting).  🔸 النمذجة التهديدية (Threat Modeling).  🔸 تتبع الجهات المهاجمة (Threat Actor Tracking). | يعتمد على ذكاء التهديدات ويعمل على كشف الهجمات قبل وقوعها. |
| *2. مركز امتثال (Compliance-Based SOC)* | ضمان الالتزام بالقوانين والمعايير الأمنية | 🔸 مراقبة الالتزام بمعايير مثل PCI DSS، ISO 27001.  🔸 إعداد تقارير الامتثال والتدقيق.  🔸 توثيق العمليات والإجراءات. | مناسب للقطاعات المالية أو القانونية التي تتطلب التزاماً تنظيمياً صارماً. |
| *3. مركز تشغيلي (Operational-Based SOC)* | حماية الأصول والأنظمة الداخلية للمنظمة | 🔸 تحليل أصول المنظمة وتحديد الأصول الحساسة.  🔸 احتواء التهديدات وإزالتها والتعافي منها بسرعة.  🔸 تطوير التواقيع الأمنية الجديدة للهجمات الحديثة (Zero-Day). | يُعرف أيضاً باسم CSIRT (Computer Security Incident Response Team) ويركّز على العمليات الداخلية. |

#### شرح إضافي للمفاهيم الأساسية

1. Threat Hunting (صيد التهديدات)

* البحث النشط عن الهجمات الخفية داخل الشبكة.
* يعتمد على فرضية أن المهاجم ربما اخترق النظام بالفعل.
* يستخدم مؤشرات الاختراق (IOCs) وذكاء التهديدات.

1. Threat Modeling (نمذجة التهديدات)

* تحديد الأصول الحساسة وتقييم نقاط الضعف.
* إنشاء ملف لخصم محتمل (Adversary Profile) يتضمن أهدافه وقدراته وأساليبه.
* الإجابة على أسئلة:
  + أين تكمن أكبر نقاط ضعفنا؟
  + ما التهديدات الأكثر احتمالًا؟
  + كيف نحمي أنفسنا منها؟

1. Threat Actor Tracking (تتبع الجهات المهاجمة)

* تحديد أنماط الهجوم وربطها بمجموعات مهاجمين معروفة.
* استخدام TTPs (التكتيكات، التقنيات، والإجراءات) لفهم طريقة عمل المهاجمين.
* الهدف: تسريع الاستجابة وتقليل الأضرار.

#### اعتبارات التوظيف (Staffing Considerations)

* نوع مركز الـSOC يحدد مهارات الموظفين المطلوبة:
  + Threat-Centric: يحتاج محللين ذوي خبرة في التحليل الاستخباراتي والصيد الاستباقي.
  + Compliance-Based: يحتاج مختصين في الامتثال والسياسات الأمنية.
  + Operational-Based: يحتاج تقنيين ذوي خبرة في البنية التحتية وأنظمة الاستجابة للحوادث.
* الفرق الواقعية (Real-World SOCs) غالباً ما تدمج بين أكثر من نوع واحد لتغطية جميع الجوانب الأمنية.

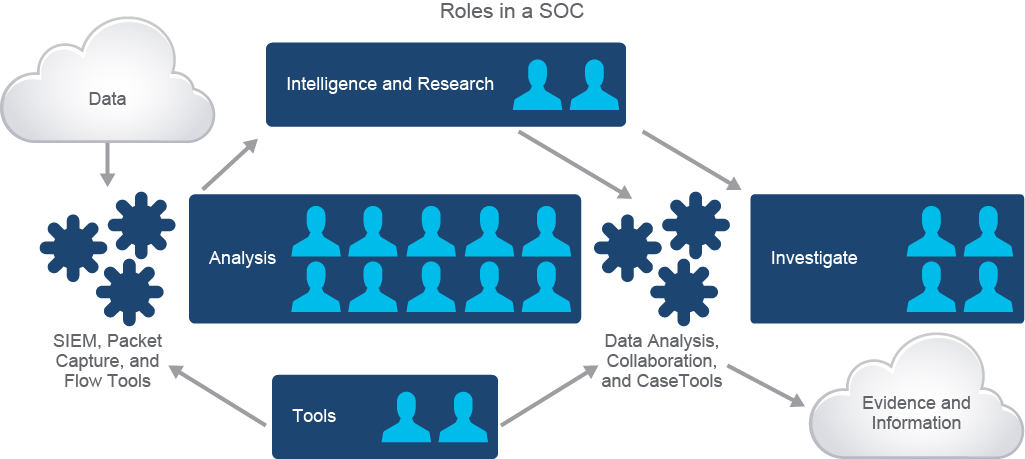
— — — — — — — — — — — — — — — —

### نماذج مراكز العمليات الأمنية (SOC Models)

| **نموذج SOC** | **الوصف (Description)** | **المميزات (Pros)** | **العيوب (Cons)** | **التكلفة (Cost)** |
| --- | --- | --- | --- | --- |
| *الداخلي (Internal SOC)* | في مقر المؤسسة (On-site)، يُدار بالكامل من قبل المؤسسة نفسها | 🔹 أفضل رؤية وتحكم (Best visibility)  🔹 إدارة بيانات حصرية (Exclusive data management)  🔹 قابلية تخصيص عالية (Most customizable)  🔹 طاقم داخلي متخصص (Dedicated in-house staff) | 🔸 الأعلى تكلفة (Most expensive)  🔸 صعوبة توظيف والاحتفاظ بالخبرات (Difficult to recruit and retain talent)  🔸 أبطأ في التنفيذ (Slowest implementation) | 💰💰💰 |
| *الافتراضي (Virtual SOC / vSOC)* | خدمة تُدار من طرف خارجي (Contracted service) | 🔹 الأقل تكلفة (Least expensive)  🔹 أسرع في التنفيذ (Quickest implementation)  🔹 أكثر مرونة وقابلية للتوسع (Most flexible and scalable) | 🔸 أقل رؤية وتحكم (Least visibility)  🔸 إدارة بيانات من طرف ثالث (Third-party data management)  🔸 أقل قابلية للتخصيص (Least customizable) | 💰 |
| *الهجين (Hybrid SOC)* | مزيج من الداخلي والافتراضي (Combination of Internal and Virtual) | 🔹 أسرع كشف واستجابة (Quickest detection and response)  🔹 أكثر أمانًا (Most secure – extra pair of eyes)  🔹 تبادل المعرفة بين الفريق الداخلي والطرف الثالث (Knowledge share) | 🔸 مكلف على المدى الطويل (Costly in long term)  🔸 يحتاج أجهزة إضافية (Additional hardware required)  🔸 إدارة بيانات من طرف ثالث (Third-party data management) | 💰💰 |

— — — — — — — — — — — — — — — —

### الأدوار في مركز العمليات الأمنية (SOC Roles)

مركز العمليات الأمنية (SOC) يعتمد على هيكل هرمي من الأدوار، حيث يتعاون جميع الأعضاء لرصد التهديدات، تحليلها، والاستجابة لها بشكل فعّال. هذه الأدوار تضمن سرعة الاستجابة وتقليل الأضرار الناتجة عن الهجمات السيبرانية.

#### المستوى الأول – Tier 1: Triage Specialist (أخصائي الفرز)

* أول نقطة اتصال في SOC، يتعامل مع التنبيهات الأولية الصادرة من أدوات المراقبة مثل SIEM أو ITSM.
* يقوم بتحديد مدى خطورة التنبيه (criticality) ويقرر ما إذا كان يحتاج تصعيدًا.
* يضبط ويُدير أدوات المراقبة الأمنية.
* يُثري التنبيهات بالمعلومات ذات الصلة (Enrichment with relevant data).
* إذا لم يُحل التهديد، يتم تصعيده إلى Tier 2.

#### المستوى الثاني – Tier 2: Incident Handler (مُعالج الحوادث)

* يتولى تحليل الحوادث المُصعّدة من المستوى الأول بعمق.
* يحدد نطاق وطبيعة الهجوم والأنظمة المتأثرة.
* يضع وينفذ استراتيجيات الاحتواء (containment) والمعالجة (remediation) والاستعادة (recovery).
* يضيف بيانات إضافية وتحليل سياقي (telemetry data) لتحسين قواعد الكشف المستقبلية.
* إذا تعقدت الحالة، يصعّدها إلى Tier 3.

#### المستوى الثالث – Tier 3: Threat Hunter (صائد التهديدات)

* أعلى مستويات التحليل الفني داخل SOC.
* يبحث بشكل استباقي عن التهديدات ونقاط الضعف غير المكتشفة.
* يدرس تقنيات الهجوم الجديدة ويطور نماذج تهديدات تناسب بيئة المؤسسة.
* يدعم المستويات الأدنى بالتحليل العميق أثناء الحوادث الكبرى.
* يمتلك خبرة كبيرة في تحليل البيانات واستخدام أدوات الذكاء التهديدي (Threat Intelligence).

#### المستوى الرابع – SOC Manager (مدير مركز العمليات الأمنية)

* يشرف على الفريق بأكمله من حيث التوظيف، التدريب، وتقييم الأداء.
* يُدير التقارير الأمنية والاتصالات أثناء الأزمات.
* يتابع الالتزام بالقوانين والسياسات الأمنية.
* يُنسق مع CISO (رئيس أمن المعلومات) ويُشرف على الميزانية والعمليات.

أدوات SOC الأساسية:

* SIEM (Security Information and Event Management) a: مراقبة وتحليل الأحداث في الوقت الحقيقي (مثل Splunk).
* ITSM (IT Service Management) b: إدارة التذاكر والتنبيهات (مثل ServiceNow).‬‏
* Intrusion detection systems (IDS) and intrusion prevention systems (IPS) c: اكتشاف ومنع التسللات (مثل Cisco Firepower، Cisco Secure Endpoint).
* Vulnerability Scanners: فحص الثغرات (مثل Nessus).
* Threat Intelligence Services: جمع وتحليل معلومات التهديدات (مثل Cisco Talos).
* Forensics Tools: تحليل الأدلة الرقمية (مثل Encase، Velociraptor، Redline).

— — — — — — — — — — — — — — — —

### 

### تفاعل الأدوار داخل مركز العمليات الأمنية (SOC Interaction)

مركز العمليات الأمنية (Security Operations Center - SOC) يعمل كفريق متكامل من المحللين والمديرين الذين يتعاونون مع أقسام داخلية وخارجية للكشف عن التهديدات، تحليلها، واحتوائها بسرعة وفعالية.

#### 1. التفاعل الداخلي داخل الـ SOC

يتطلب نجاح SOC تنسيقًا مستمرًا بين عدة مستويات من المحللين، بالإضافة إلى أقسام داخل المؤسسة مثل:

* NOC (Network Operations Center): للتنسيق أثناء عزل الأجهزة أو الشبكات المصابة.
* HR (الموارد البشرية): عند تأثر أجهزة الموظفين أو بياناتهم.
* Legal (القسم القانوني): لضمان التزام الاستجابة باللوائح والقوانين.
* IT Department: لتطبيق التصحيحات (patches) ونشر التحديثات الأمنية.
* CISO/CIO: لتقديم التقارير التنفيذية وتقييم المخاطر.

يتم هذا التعاون غالبًا أثناء الاستجابة للحوادث Incident Response التي تشمل مراحل:

الكشف ⬅️ التحليل ⬅️ الاحتواء ⬅️ الإزالة ⬅️ التعافي ⬅️ الدروس المستفادة.

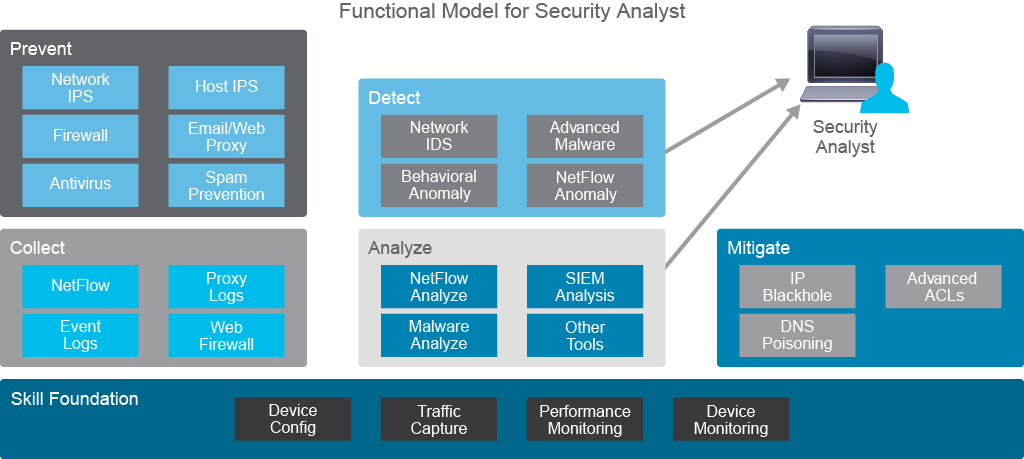
#### 2. التفاعل الخارجي

في بعض الحالات، يتواصل الـSOC مع جهات خارجية مثل:

* الجهات القانونية (Legal entities) لمتابعة الإجراءات القضائية.
* الجهات الإعلامية (Media sources) في حال حدوث تسريب أو دعاية سلبية.
* الهيئات الحكومية الأمنية (مثل US-CERT / CISA) عند وجود تهديد وطني أو عالمي.
* المحاكم الدولية (International courts of law) عند توثيق الأدلة الجنائية الرقمية.

#### 3. دور مدير مركز العمليات الأمنية (SOC Manager)

* يشرف على جميع أنشطة المركز ويضمن سير العمليات اليومية بسلاسة.
* يضع SOPs (Standard Operating Procedures) أي الإجراءات التشغيلية القياسية للاستجابة للحوادث.
* يُحدد المهارات المطلوبة للمحللين في كل مستوى (Tier).
* يُنسق الاتصالات مع الأقسام الداخلية والخارجية.
* يضمن تحسين الأداء بشكل مستمر عبر جلسات مراجعة ودروس مستفادة (Lessons Learned).



#### 4. مستويات محللي SOC ومسؤولياتهم

| **المستوى** | **المسمى** | **المهام الرئيسية** |
| --- | --- | --- |
| *Tier 1* | Triage Specialist / Alert Analyst | - مراقبة التنبيهات بشكل مستمر.  - تحليل أولي للحوادث وتحديد إذا كانت حقيقية أو إيجابية كاذبة (False Positive).  - جمع البيانات الأولية لتصعيدها إلى المستوى الثاني.  - مراقبة صحة الحساسات الأمنية وأجهزة الـEndpoint. |
| *Tier 2* | Incident Responder / Analyst | - تحليل الحوادث بعمق باستخدام مصادر متعددة.  - تحديد الأنظمة أو البيانات المتأثرة.  - توجيه وتنفيذ إجراءات الإصلاح (Remediation).  - تطوير أساليب تحليل جديدة لاكتشاف التهديدات. |
| *Tier 3* | Threat Hunter / Senior Analyst | - صيد التهديدات بشكل استباقي قبل حدوث الهجمات.  - تحليل البرمجيات الخبيثة (Malware Analysis) والهندسة العكسية.  - تحسين خوارزميات الكشف والتحليل.  - استخدام أدوات Threat Intelligence وMITRE ATT&CK. |
| *SOC Manager* | Operations Lead / Security Manager | - قيادة الفريق وتنظيم الأولويات.  - إدارة الحوادث الكبرى والتنسيق مع CISO وLegal.  - تطوير الإجراءات والسياسات الأمنية. |

#### 5. مهارات محلل SOC

* Tier 1: معرفة أساسية في الشبكات، تحليل حركة المرور (Traffic Analysis)، ومراقبة الأجهزة.
* Tier 2: تحليل متقدم، correlate بين البيانات من مصادر متعددة، وفهم دورة حياة الهجوم.
* Tier 3: خبرة في الـForensics، التحليل العميق للبرمجيات الخبيثة، والـThreat Hunting.

#### 6. أهمية التعاون بين الأدوار

* يتيح الاستجابة السريعة وتقليل الأضرار.
* يمنع انتشار الهجمات داخل الشبكة.
* يعزز جودة التحليل ورفع مستوى الحماية المستقبلية.
* يساعد في بناء ثقافة أمنية قوية داخل المؤسسة.

— — — — — — — — — — — — — — — —

### أنواع البيانات التي يتعامل معها محلل مركز العمليات الأمنية (SOC Analyst)

محلل مركز العمليات الأمنية (SOC Analyst) يحتاج لتحليل أنواع مختلفة من البيانات أثناء التحقيق في التهديدات الأمنية.

تأتي هذه البيانات من مصادر متعددة، ويجب على المحلل معرفة كيفية تحليلها لتحديد التهديدات المحتملة بدقة.

يتم استخدام هذه البيانات في مراحل مختلفة من التحقيق، وغالباً ما تتضمن الوصول إلى أدوات أو منتجات مختلفة.

#### أنواع بيانات المراقبة الأمنية (Network Security Monitoring Data Types)

لا يوجد نوع واحد من البيانات يعطي صورة كاملة، لذلك يجب على المحلل تحليل عدة أنواع من بيانات الأحداث (Event Data) تشمل:

* Session Data
* Full Packet Capture
* Transaction Data
* Extracted Content
* Statistical Data
* Alert Data
* External Data

#### Session Data (بيانات الجلسة)

تمثل محادثة مختصرة بين جهازين على الشبكة.

تشبه فاتورة الهاتف — لا تُظهر محتوى المكالمات، ولكن تُظهر من اتصل بمن، ومتى، ومدة الاتصال.

**تتضمن البيانات:**

* الـ5-tuple (بروتوكول النقل، عنوان IP المصدر، منفذ المصدر، عنوان IP الوجهة، منفذ الوجهة)
* الطوابع الزمنية (Time Stamps)
* كمية البيانات المتبادلة
* المعايير الشائعة: NetFlow v5, NetFlow v9, IPFI

**مثال**: يمكن للمحلل معرفة أن جهازاً مصاباً بدأ يتواصل بشكل متكرر مع خادم خارجي مجهول (Beaconing).

#### Full Packet Capture (الالتقاط الكامل للحزم)

يشبه التنصت على الخط (Wiretap) في العالم الواقعي.

يُسجِّل رؤوس الحزم (Headers) والمحتوى الكامل (Payload) — أي كل ما تم تبادله بين جهازين.

🔸 المزايا:

* يوفر تفاصيل دقيقة جداً عن الاتصالات
* يمكن استخراج البيانات الأصلية (مثل المرفقات أو الملفات المنقولة)

🔸 العيوب:

* يتطلب مساحة تخزين ضخمة
* تحليله معقد وبطيء

غالباً يُستخدم ملف .PCAP لتخزين البيانات

**مثال**: يمكن استخدامه لتحليل كيفية انتقال برمجية الفدية (Ransomware) داخل الشبكة.

#### Transaction Data (بيانات المعاملات)

تُبرز العمليات التي تحدث نتيجة الجلسات أو نشاط الأنظمة.

مثلاً، خادم ويب (HTTP Server) يُنشئ سجلات طلبات المستخدمين، أو خادم بريد (SMTP Server) يسجّل الرسائل الواردة والصادرة.

🔸 الاستخدام:

* تحديد أصل البريد الإلكتروني الذي حمل المرفق الضار
* تحليل سلوك الخوادم أو المستخدمين

📁 كل ملف سجل (Log File) يحتوي على Transaction Data.

#### Extracted Content (المحتوى المستخرج)

هي الملفات أو الأجزاء المستخرجة من حركة مرور الشبكة (Traffic)، مثل:

* مرفقات البريد الإلكتروني
* الملفات التي تم تنزيلها من الإنترنت
* أسماء النطاقات (DNS)
* عناوين الأجهزة (Hosts)

يمكن استخراجها مباشرة من الشبكة أو من ملفات Full Packet Capture (PCAP).

🟢 هذه البيانات تُستخدم كأدلة رقمية (Digital Artifacts) في التحقيقات.

#### Statistical Data (البيانات الإحصائية)

تجمع بيانات الشبكة في صورة إحصاءات لفهم النشاط الطبيعي (Baseline).

مثلاً:

* عدد الاتصالات في الدقيقة إلى خادم معين خلال شهر
* مقارنة النشاط الحالي بالنشاط الطبيعي لاكتشاف الشذوذ (Anomalies)

🔸 تشمل:

* Baseline Graphs (الرسوم الأساسية)
* Top Reports (تقارير الأعلى استخدامًا)

🟢 مثال: يمكن معرفة أي الأجهزة ترسل أكبر كمية من بيانات HTTP أو تطلب أكثر عدد من نطاقات DNS.

#### Alert Data (بيانات التنبيهات)

هي البيانات التي تولدها أنظمة الكشف (IDS / IPS) عند تطابق حركة المرور مع قواعد محددة.

هذه البيانات هي النتيجة النهائية بعد تحليل كميات ضخمة من البيانات تلقائياً.

🔸 الفائدة: تقلل الجهد اليدوي الكبير.

🔸 التحدي: قد تحتوي على إيجابيات كاذبة (False Positives) أو سلبيات كاذبة (False Negatives).

🧠 محللو Tier 1 SOC Analysts هم أول من يتعامل مع هذه البيانات ويقررون ما إذا كانت التنبيهات حقيقية أو خاطئة.

#### External Data (البيانات الخارجية)

تتكون من المعلومات القادمة من خارج المؤسسة، مثل:

* Threat Intelligence Feeds (تغذيات استخبارات التهديدات)
* Indicators of Compromise (IoCs)

🔸 الهدف:

تحديث أنظمة الكشف بشكل مستمر لمواكبة تطور الهجمات.

تحسين دقة التنبيهات (Alert Fidelity) وتوفير سياق أوسع للحوادث.

#### ملخص

| **🔢 نوع البيانات** | **📝 الوصف** | **🎯 الفائدة / الاستخدام** | **⚠️ ملاحظات مهمة** |
| --- | --- | --- | --- |
| ***بيانات الجلسة (Session Data / Flow Data)*** | تمثل محادثة مختصرة بين جهازين على الشبكة، وتشمل البروتوكول، عناوين IP، المنافذ، الوقت، وحجم البيانات. | تساعد في التعرف على الاتصالات غير المألوفة أو المشبوهة بين الأجهزة. | تشبه "فاتورة الهاتف" — لا تحتوي على محتوى الاتصال. تُستخدم مع معايير مثل NetFlow وIPFIX. |
| ***الالتقاط الكامل للحزم (Full Packet Capture - PCAP)*** | يسجل كل حزمة بيانات بالكامل (الرأس + المحتوى) بين جهازين على الشبكة. | يتيح تحليلًا عميقًا للهجمات واستخراج الأدلة مثل المرفقات الضارة. | يتطلب مساحة تخزين كبيرة جدًا، ويصعب تحليله بشكل يدوي. |
| ***بيانات المعاملات (Transaction Data)*** | تسجل الأنشطة الناتجة عن الجلسات، مثل سجلات HTTP، أو البريد الإلكتروني SMTP، أو سجلات النظام. | تساعد في تتبع مصدر التهديد، وانتشاره بين الأنظمة. | لا يوجد تطابق دائم بين الجلسة والمعاملة — قد توجد معاملات كثيرة في جلسة واحدة. |
| ***المحتوى المستخرج (Extracted Content)*** | ملفات أو بيانات يتم استخراجها من الحزم مثل مرفقات البريد أو الملفات المنزلة. | تُستخدم في التحليل الجنائي لتحديد محتوى الهجوم والملفات الضارة. | يمكن استخراجها من بث مباشر أو من ملفات PCAP بعد التحليل. |
| ***البيانات الإحصائية (Statistical Data)*** | بيانات مجمعة تلخص النشاط الشبكي عبر الزمن لتحديد السلوك الطبيعي (baseline). | تُستخدم لاكتشاف الأنماط غير الطبيعية والأنشطة المشبوهة. | تشمل الرسوم البيانية والتقارير التي تُظهر الاتجاهات (مثل أكثر المضيفين نشاطًا). |
| ***بيانات التنبيه (Alert Data)*** | ناتجة عن أنظمة كشف التسلل (IDS/IPS) عندما تطابق حركة الشبكة قاعدة محددة. | توفر الوقت عبر تنبيه المحلل مباشرة حول نشاط مشبوه. | قد تحتوي على إنذارات كاذبة (false positives) ويجب أن يتحقق منها المحلل يدويًا. |
| ***البيانات الخارجية (External Data)*** | معلومات من خارج المؤسسة مثل تغذيات التهديد (Threat Intelligence Feeds) ومؤشرات الاختراق (IoCs). | تساعد في الدفاع الاستباقي وتحديث القواعد والتوقيعات ضد التهديدات الحديثة. | مصدر أساسي لتقوية قدرات الكشف والتنبؤ بالهجمات. |

— — — — — — — — — — — — — — — —

### أدوات مركز العمليات الأمنية (SOC Tools & Features)

مركز العمليات الأمنية (SOC) يعتمد على مجموعة من الأدوات المتكاملة التي تمكّن المحللين من:

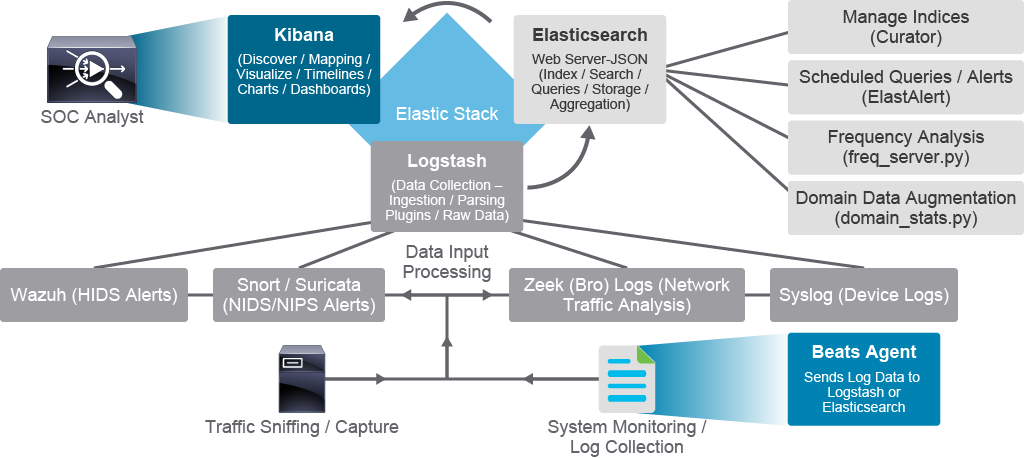
* جمع وتحليل بيانات الأمان من مصادر متعددة
* الكشف عن الأنشطة المشبوهة
* الاستجابة للحوادث بسرعة وفعالية

#### أهم الأدوات في بيئة الـSOC

| **🧩 الأداة** | **📝 الوظيفة الأساسية** | **🎯 المميزات والاستخدامات الرئيسية** |
| --- | --- | --- |
| *IT Service Management (ITSM) – مثل ServiceNow* | إدارة وتتبع الحوادث (Incidents) عبر تذاكر تحتوي على الأجهزة المتأثرة، الإجراءات المتخذة، والموظفين المشاركين. | - لوحة تحكم لإدارة جميع الحوادث  - تعتمد على بيانات التنبيهات (Alert Data)  - تسهّل تسليم التذاكر بين المحللين (Tier 1 و Tier 2) |
| *Security Information and Event Management (SIEM) – مثل Splunk Enterprise* | تجميع (Aggregation) وتحليل (Correlation) كميات ضخمة من البيانات من مصادر مثل الجدران النارية (Firewalls) وأنظمة IDS/IPS ونقاط النهاية (Endpoints). | - إنشاء تنبيهات عند اكتشاف أنشطة مشبوهة  - تسهيل البحث وإنشاء التقارير  - دعم الذكاء الاصطناعي والتعلم الآلي لتحليل الأنماط  - التكامل مع أدوات Cisco عبر تطبيقات Splunk Apps |
| *Cisco SecureX* | منصة موحدة لإدارة وتنظيم الأمن (Security Orchestration & Automation). | - دمج أدوات Cisco الأمنية المختلفة في واجهة واحدة  - أتمتة الاستجابة للحوادث  - جمع معلومات من مصادر متعددة مثل Secure Endpoint و Talos Threat Intelligence |
| *Cisco Secure Network Analytics (Stealthwatch)* | تحليل تدفق البيانات (NetFlow/IPFIX) للكشف عن التهديدات مثل DDoS، APT، والهجمات الداخلية. | - يعتمد على التحليل السلوكي (Behavioral Analysis)  - يرصد اتصالات الشبكة المشبوهة  - يكشف عن البرمجيات الخبيثة غير المعروفة (Zero-day Malware) |
| *Cisco Secure Malware Analytics (Threat Grid)* | منصة تحليل البرمجيات الخبيثة (Malware Sandbox). | - تحليل الملفات المشبوهة سلوكيًا وثابتًا (Dynamic/Static Analysis)  - مقارنة العينات مع قاعدة بيانات عالمية  - مدمجة مع أدوات Cisco الأخرى |
| *Wireshark* | أداة تحليل بروتوكولات الشبكة (Network Protocol Analyzer). | - التقاط الحزم (Packet Capture) وتحليلها تفصيليًا  - مفيدة في التحقيقات الجنائية (Forensics) واستقصاء التهديدات (Threat Hunting) |
| *NetFlow Analyzer* | مراقبة حركة البيانات (Traffic Monitoring) عبر تدفقات الشبكة. | - تحديد إذا كان الجهاز المصاب يتصل بخادم تحكم (Command & Control Server)  - جمع بيانات الجلسات (Session Data) |
| *Security Onion* | منصة مفتوحة المصدر لمراقبة الشبكة وتحليل الحوادث. | - تحتوي على أدوات متعددة مثل Zeek, Snort, Suricata, ELSA, Wireshark  - وظائفها الأساسية:  1. التقاط الحزم بالكامل (Full Packet Capture)  2. كشف التسلل (IDS)  3. تحليل الأمان (Security Analysis)  4. إدارة السجلات (Log Management) |

#### مكونات Security Onion بالتفصيل

| **🧠 المكون** | **💡 الوظيفة** |
| --- | --- |
| ***Snort / Suricata*** | كشف ومنع التسلل (NIDS/NIPS) عبر تحليل الحزم وإنشاء تنبيهات. |
| ***Zeek (Bro)*** | تحليل البروتوكولات وسلوك الشبكة لتحديد الأنشطة غير الطبيعية. |
| ***ELSA*** | نظام لإدارة واستعلام السجلات (Logs) بسرعة وكفاءة عالية. |
| ***Wazuh (OSSEC)*** | نظام كشف التسلل على مستوى الأجهزة المضيفة (HIDS). |
| ***Sguil / Squert*** | واجهات لتحليل وتنظيم التنبيهات والأحداث الأمنية بشكل مرئي. |
| ***NetworkMiner / Wireshark / CapME*** | أدوات تحليل حزم وتدفقات الشبكة (Packet & Flow Analysis). |
| ***Elastic Stack (ELK)*** | الجيل الجديد من Security Onion ويشمل: Elasticsearch (فهرسة وتحليل) Logstash (إدخال وتحليل البيانات) Kibana (عرض مرئي وتحليلي). |



#### أدوات اختبار الاختراق (Penetration Testing Tools)

* Kali Linux: نظام يحتوي على مجموعة من أدوات اختبار الاختراق.
* Metasploit Framework: لاختبار الثغرات واستغلالها.
* Armitage: واجهة رسومية لاستغلال الثغرات وتنفيذ الهجمات التجريبية.
* SET (Social Engineer Toolkit): أداة لهجمات الهندسة الاجتماعية.

الاختلاف بين:

* Vulnerability Assessment → تحديد الثغرات فقط.
* Penetration Testing → استغلال الثغرات فعليًا لاختبار الحماية.

— — — — — — — — — — — — — — — —

### الجهات الداخلية (Internal Stakeholders)

| **🏢 الجهة الداخلية (Internal Stakeholder)** | **💎 الأصول أو الأصول المؤسسية (Corporate Assets)** | **🎯 الدور الأساسي (Role)** | **🤝 العلاقة مع مركز العمليات الأمنية (Relationship with SOC)** |
| --- | --- | --- | --- |
| **فريق الإدارة التنفيذية (Executive Management Team / C-Level Exec)** | جميع الأصول (All Assets) | إدارة الاستجابة للحوادث (Incident Response Administration) | تنسيق الاستجابة للحوادث بين الأقسام، تسهيل التواصل بين الفرق، العمل مع الـSOC لضمان استمرارية الأعمال وتقليل التأثير السلبي. |
| **مدير فريق الاستجابة للحوادث (Incident Response Team Manager)** | غير قابل للتطبيق (Not Applicable) | ضمان التنفيذ الصحيح لأنشطة الاستجابة للحوادث | التنسيق بين الأطراف المعنية، تمثيل حلقة الوصل بين الـSOC والأقسام الأخرى، ضمان توفر الموارد والمهارات اللازمة في الفريق. |
| **القائد الفني للاستجابة للحوادث (Incident Response Technical Lead)** | غير قابل للتطبيق | ضمان الدقة التقنية في تنفيذ أنشطة الاستجابة | التعاون مع الـSOC لضمان الدقة التقنية في تحليل وتطبيق الإجراءات أثناء الحوادث. |
| **الموارد البشرية (Human Resources - HR)** | معلومات الهوية الشخصية (PII)، المعلومات الصحية المحمية (PHI)، المعلومات الحساسة الشخصية (PSI) | التدريب على الأمن السيبراني، التواصل الداخلي، الإجراءات التأديبية | التعاون مع الـSOC للحفاظ على الامتثال الأمني في حالات فقدان البيانات، وتدريب الموظفين على الوعي الأمني، وتنفيذ الإجراءات التأديبية المناسبة. |
| **قسم تكنولوجيا المعلومات (Information Technology / Network Security Engineer)** | البنية التحتية للشبكة (Network Infrastructure) | إدارة الشبكات وتأمين بيئة الإنتاج | إدارة بنية الـSOC التحتية، تزويد الـSOC بمؤشرات الشبكة، ضمان استمرارية الأعمال، وتحسين الوضع الأمني العام. |
| **قسم الحوكمة والمخاطر والامتثال (Governance, Risk, and Compliance - GRC)** | الملكية الفكرية والأصول عالية القيمة (Intellectual Property / Crown Jewels) | مواءمة أهداف العمل مع متطلبات الأمان والامتثال | التعاون مع الـSOC للحفاظ على الوضع الأمني للأصول المؤسسية وضمان الامتثال للمتطلبات التنظيمية. |
| **المستشار القانوني (Legal Counsel)** | نزاهة المؤسسة والإجراءات القانونية | ضمان الامتثال القانوني أثناء الاستجابة للحوادث | العمل مع الـSOC لجمع الأدلة الرقمية، تفسير القوانين واللوائح، وضمان صلاحية الأدلة في الإجراءات القضائية. |
| **العلاقات العامة والإعلام (Public Relations Affairs and Media Relations)** | الصورة العامة للمؤسسة (Public Image) | إدارة العلاقات العامة أثناء الحوادث | التعاون مع الـSOC لتقديم بيانات رسمية عن الحوادث الأمنية، وضمان التواصل الدقيق مع وسائل الإعلام. |
| **مكتب المساعدة (Help Desk)** | غير قابل للتطبيق | نقطة الاتصال الأولى للاستجابة للحوادث | استلام البلاغات الأولية، جمع البيانات المبدئية، إخطار فرق الاستجابة، تحديث الأطراف المتأثرة، وتطبيق التصحيحات بعد الحادث. |

— — — — — — — — — — — — — — — —

### أصحاب المصلحة الخارجيون (External Stakeholders)

عند وقوع حادث أمني سيبراني، تحتاج المنظمة للتواصل مع عدة جهات خارجية تُعرف باسم أصحاب المصلحة الخارجيين.

هذه الجهات قد تكون هيئات حكومية، مزودي خدمات، أو وسائل إعلام، ويكون التواصل من خلال شخص محدد يُعرف باسم Point of Contact (POC)، وغالبًا يُعيّن بديل له أيضًا.

### أبرز أصحاب المصلحة الخارجيين:

1. الجهات الحكومية (Federal Agencies):

مثل FedRAMP، ويجب الإبلاغ عن أي خرق أمني وفق القوانين مثل HIPAA.

التواصل يتم عبر US-CERT، الجهة المسؤولة عن جمع وتحليل تقارير الحوادث.

1. جهات إنفاذ القانون (Law Enforcement):

مثل FBI وSBI والشرطة المحلية، للتحقيق في الجرائم السيبرانية ومتابعة الأدلة.

1. مزودو الخدمات السحابية والإنترنت (Cloud Providers & ISPs):

يساعدون في تتبع مصدر الهجوم أو منع الهجمات (blocking attacks).

1. الإعلام والعلاقات العامة (Media & Public Affairs):

يتم التواصل معهم فقط من خلال POC مخوّل رسميًا لتجنب تسرب المعلومات الحساسة.

يشارك قسم العلاقات العامة والقانوني في صياغة ما يمكن نشره للعامة.

1. مزودو البرمجيات (Software Vendors):

يُتواصل معهم لمعرفة تفاصيل الثغرات الأمنية أو الهجمات الجديدة التي تؤثر على برامجهم.

— — — — — — — — — — — — — — — —

### تجميع البيانات الأمنية (Security Data Aggregation)

يُعد نظام (SIEM - Security Information and Event Management) من الأنظمة التي تُستخدم في أغلب المؤسسات لمراقبة وتحليل التنبيهات الأمنية بشكل لحظي (real-time).

يقوم هذا النظام بـ جمع (collecting)، فرز (sorting)، معالجة (processing)، تخزين (storing)، وإبلاغ (reporting) التنبيهات الأمنية إلى محللي الأمن (Security Analysts).

#### الهدف من (SIEM):

* تسريع اكتشاف التهديدات (Threat Detection) واحتوائها (Containment).
* ربط أدوات الأمان المختلفة (Security Tools Integration) داخل المؤسسة في نظام واحد متكامل.
* توفير رؤية شاملة (Single Pane of Glass) لحالة الأمن داخل المؤسسة.

#### مثال عملي:

إذا أُصيب حاسوب موظف (Employee Laptop) ببرمجية خبيثة (Malware)، فسيحاول الانتشار داخل الشبكة.

أنظمة الحماية (Security Controls) سترسل إشعارات إلى نظام (SIEM) الذي يقوم بدوره بـ ربط وتحليل الأحداث (Event Correlation) لتحديد:

* الجهاز المصاب الأصلي (Original Infected System)
* الأجهزة المستهدفة (Targeted Systems)

ثم يتم عزل الجهاز المصاب (Isolation) حتى إزالة البرمجية الخبيثة.

#### أمثلة على أنظمة (SIEM):

* مفتوحة المصدر (Open Source): نظام OpenSOC
* خاصة بالشركات (Vendor-Specific): نظام Splunk (قد يحتوي على مكونات مفتوحة المصدر أيضًا)

تُظهر لوحة التحكم (Dashboard) في **Splunk**:

* الحالة الأمنية للمؤسسة (Security Posture)
* عدد الأحداث المهمة (Notable Events)
* تقارير آنية (Real-time Reports) وتاريخية (Historical Reports) لتقييم الأداء الأمني على مدى شهور

#### الوظائف الرئيسية لنظام (SIEM):

1. جمع السجلات (Log Collection): من جميع الأنظمة والأجهزة داخل المؤسسة.
2. توحيد السجلات (Log Normalization): تحويل السجلات المختلفة إلى نموذج بيانات موحد (Common Data Model).
3. ربط الأحداث (Event & Log Correlation): لتسريع اكتشاف الهجمات والتعامل معها.
4. دمج السجلات المكررة (Duplicate Consolidation): لتقليل حجم البيانات التي يتم تحليلها.
5. إنشاء التقارير (Reporting & Compliance): لتلبية متطلبات الامتثال التنظيمي (Regulatory Compliance).

#### 

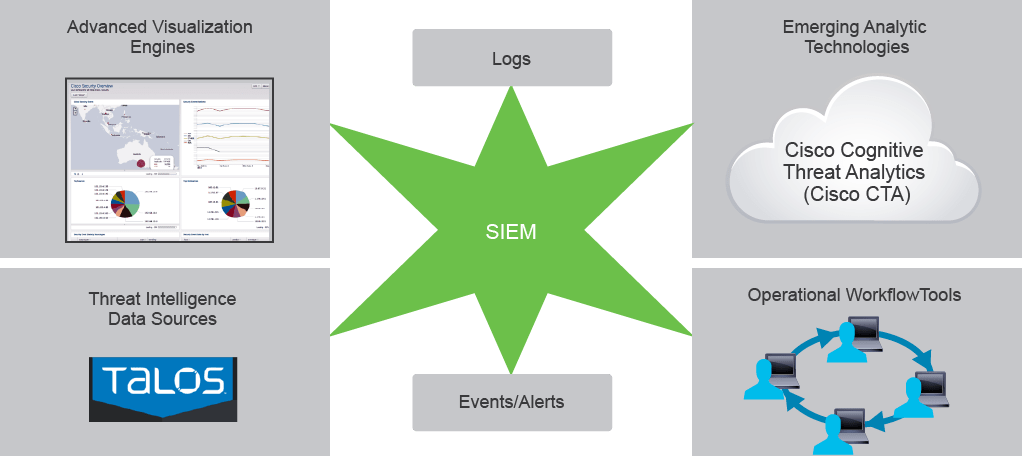
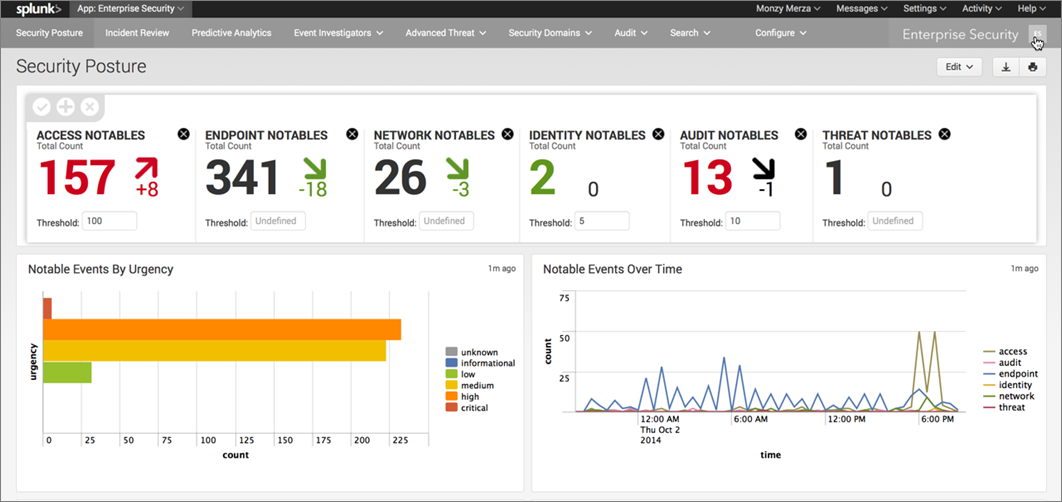
#### ملاحظات حول تنفيذ النظام (Deployment):

نظام (SIEM) ليس جاهزًا للتثبيت والاستخدام مباشرة (Not Plug-and-Play)،

بل يتطلب تخطيطًا دقيقًا (Proper Planning) يشمل:

* نطاق المشروع (Scope)
* المتطلبات التجارية (Business Requirements)
* المواصفات التقنية (Engineering Specifications)

كما يجب التأكد من أن قدرة التخزين (Storage Capacity) والأداء (Performance) كافيان لمعالجة كمية البيانات وحجم السجلات ضمن المدة المطلوبة (Search Time Range).



— — — — — — — — — — — — — — — —

### زمن الاكتشاف (Time to Detection - TTD)

يشير (Time to Detection - TTD) إلى المدة الزمنية بين حدوث نشاط ضار (Malicious Event) في النظام بعد تجاوزه لجميع تقنيات الحماية، وحتى اكتشاف التهديد (Threat Detection) المرتبط بذلك النشاط.

يُعرف أيضًا باسم زمن البقاء (Dwell Time).

#### أهمية المؤشر:

* كلما طال زمن الاكتشاف، زادت فرصة المهاجمين (Threat Actors) في تنفيذ أنشطة التجسس (Surveillance) وسرقة البيانات الحساسة (Sensitive Data).
* وفقًا لتقرير الأمن لعام 2016، فإن زمن الاكتشاف في معظم المؤسسات يتراوح بين 100 إلى 200 يوم، وهو وقت غير مقبول في ظل تطور البرمجيات الخبيثة السريع.

#### الإحصاءات (وفقًا لـ Ponemon Institute):

* في القطاع المالي (Financial Services): متوسط الاكتشاف هو 98 يومًا.
* في قطاع التجزئة (Retail): متوسط الاكتشاف هو 197 يومًا.
* رغم ذلك، 58% من العاملين في المالية و71% في التجزئة غير متفائلين بتحسن هذه النتائج قريبًا.

#### تقليل زمن الاكتشاف:

لتقليل (TTD)، يجب تعزيز الرؤية الأمنية الشاملة (End-to-End Visibility) عبر الشبكة باستخدام:

* الأشخاص (People)
* العمليات (Processes)
* التقنيات (Technologies)

مثال على ذلك:

نظام (Cisco SISAS) الذي يستطيع تقليل زمن الاكتشاف من أيام إلى ساعات باستخدام استراتيجيات مثل

* عملية الاستجابة للحوادث (Incident Response Process)
* الحماية المتقدمة من البرمجيات الخبيثة (Advanced Malware Protection)

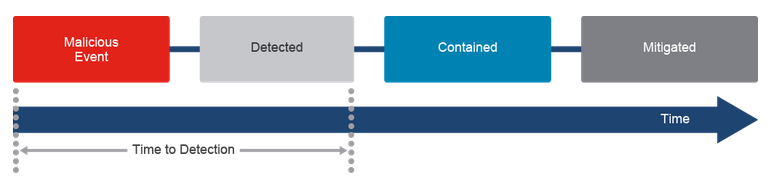
#### العلاقة مع مراحل الاستجابة للحوادث (Incident Response Phases):

بعد مرحلة الاكتشاف (Detection Phase)، تأتي:

1. مرحلة الاحتواء (Containment Phase)
2. مرحلة التخفيف (Mitigation Phase)

كما توجد مؤشرات أخرى لقياس كفاءة مركز العمليات الأمنية (SOC Effectiveness Metrics) مثل:

* زمن الاحتواء (Time to Containment)
* زمن التخفيف (Time to Mitigation)



فعالية اكتشاف الضوابط الأمنية (Security Controls Detection Effectiveness)

وجود ضوابط أمنية فعّالة تعمل قبل وأثناء وبعد الهجوم يساعد في تقليل وقت الاكتشاف (TTD) للهجمات أو الأنشطة الخبيثة.

جميع قرارات أو استجابات أنظمة الحماية تُصنف ضمن أربع فئات رئيسية:

1. سلبية كاذبة (False Negative)
   * لم يكتشف النظام نشاطًا خبيثًا فعلاً.
   * هذا أخطر نوع من الأخطاء ويجب تقليله قدر الإمكان، حتى لو أدى إلى زيادة الإيجابيات الكاذبة.
2. إيجابية كاذبة (False Positive)
   * النظام استجاب لنشاط غير خبيث (عادي).
   * كثرة الإيجابيات الكاذبة تُرهق محللي مركز العمليات الأمنية (SOC) لأنها تتطلب تحقيقات غير ضرورية.
3. سلبية حقيقية (True Negative)
   * النظام لم يتخذ أي إجراء لأن النشاط كان طبيعيًا فعلاً.
   * هذا يمثل العمل الأمثل والطبيعي للنظام.
4. إيجابية حقيقية (True Positive)
   * النظام استجاب لنشاط خبيث فعلي.
   * هذا أيضًا يمثل العمل الأمثل والطبيعي للنظام.

**النتيجة الأساسية**

يجب أن يهدف النظام الأمني الفعّال إلى:

* زيادة الإيجابيات الحقيقية (True Positives)
* تقليل السلبيات الكاذبة (False Negatives) بأعلى أولوية
* تخفيض الإيجابيات الكاذبة (False Positives) عبر الضبط والتحسين المستمر

— — — — — — — — — — — — — — — —

### قياسات مركز العمليات الأمنية (SOC Metrics)

في العصر الحالي، تنفق الشركات أكثر من 100 مليار دولار سنويًا على الأمن السيبراني من أدوات وعمليات وأفراد، ومع ذلك هذا لا يضمن دائمًا الحماية الكاملة.

ولذلك، فإن فعالية مركز العمليات الأمنية (SOC) تعتمد على ثلاثة عناصر أساسية:

1. السرعة (Speed)

تساعد على الكشف والاستجابة بسرعة، مما يقلل من متوسط زمن الاستجابة للحوادث.

1. الدقة (Accuracy)

تتطلب مراقبة وتحليل مستمرين وجمع بيانات دقيقة مثل التقاط الحزم الكاملة (Full Packet Capture) للكشف عن أي نقاط ضعف خفية.

1. التركيز (Focus)

يعني تقليل الإيجابيات الكاذبة (False Positives) لضمان أن الجهود تُوجَّه نحو التهديدات الحقيقية فقط.

#### أهمية القياسات (Metrics) في الـ SOC

القياسات هي مجموعة من المؤشرات الكمية تُستخدم لتقييم أداء المركز خلال فترة زمنية معينة.

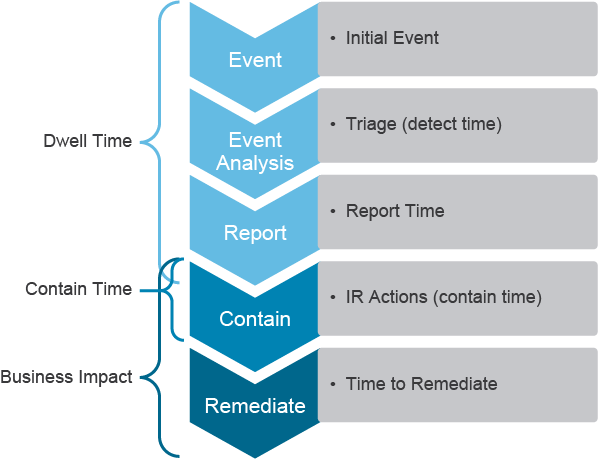
وهي أساسية لأنها تساعد القيادة على اتخاذ قرارات مبنية على البيانات والحقائق وليس العواطف.

القياسات الجيدة يجب أن تكون:

* محددة (Specific)
* قابلة للقياس (Measurable)
* قابلة للتحقيق (Attainable)
* ذات صلة (Relevant)
* وفي الوقت المناسب (Timely)

#### أهم القياسات المستخدمة في الـ SOC

من الأمثلة على المقاييس الأساسية لقياس فعالية المركز:

* متوسط وقت الاكتشاف (Mean Time To Detect - MTTD) بعد حدوث الحادثة.
* متوسط وقت الاحتواء (Mean Time To Contain) بعد اكتشافها.
* متوسط وقت التخفيف أو المعالجة (Mean Time To Mitigate) بعد احتوائها.
* عدد الحوادث المكتشفة والمحتواة والمخففة.
* عدد الهجمات من نوع يوم الصفر (Zero-Day Attacks) التي تم اكتشافها.
* معدل الإيجابيات الكاذبة مقابل الإيجابيات الحقيقية.
* عدد القواعد أو “السيناريوهات” الجديدة المضافة إلى دليل التشغيل (Playbook).
* تكاليف تشغيل مركز العمليات الأمنية.

### مفاهيم نظام إدارة سير العمل في مركز العمليات الأمنية (SOC WMS Concepts)

#### ما هو نظام إدارة سير العمل (Workflow Management System - WMS)؟

هو برنامج يُستخدم لتتبع الأحداث الأمنية (Security Events) من مرحلة الكشف (Detection) إلى الاستجابة (Response) ثم الاحتواء والتخفيف (Mitigation) وصولًا إلى إغلاق التذكرة (Ticket Closure).

يهدف WMS إلى تنظيم وأتمتة (Orchestrate & Automate) عمليات الاستجابة للحوادث الأمنية داخل مركز العمليات الأمنية (SOC).

في بعض الحالات يُطلق عليه أيضًا اسم SOAR (Security Orchestration, Automation and Response).

#### دور الـ WMS داخل بيئة الـ SOC

* يبدأ عمل الـ WMS بعد أن يحدد نظام الـ SIEM (Security Information and Event Management) الحادث الأمني.
* يقوم الـ WMS بتنسيق المهام بين أعضاء الفريق ومزامنة البيانات بين الأنظمة المختلفة.
* الهدف هو تحسين كفاءة المركز (SOC Efficiency) وتسريع الاستجابة للحوادث.

#### أنواع سير العمل (Workflow Types)

1. تتابعي (Sequential Workflow)
   * يسير بخطوات متتالية مثل المخطط الانسيابي (Flow Chart).
   * لا يمكن الرجوع إلى خطوة سابقة.
2. آلي بالحالات (State Machine Workflow)
   * ينتقل من حالة إلى أخرى، ويمكن العودة إلى حالة سابقة عند الحاجة.
   * أكثر تعقيدًا من التتابعي.
3. قائم على القواعد (Rules-driven Workflow)
   * يعتمد على سير العمل التتابعي، لكن القواعد (Rules) هي التي تحدد سير العملية.

#### الفرق بين WMS و SIEM

| **النظام** | **الدور الأساسي** |
| --- | --- |
| **SIEM** | جمع وتوحيد وتحليل السجلات (Logs) من مختلف الأجهزة لاكتشاف الحوادث. |
| **WMS (أو SOAR)** | تنفيذ عمليات الأتمتة بعد اكتشاف الحادث، مثل الاحتواء والمعالجة. |

باختصار: SIEM يكتشف الحوادث، وWMS يعالجها ويغلقها.

#### المهام القابلة للتكرار (Repeatable Tasks)

في بيئة الـ SOC الحقيقية، هناك مهام تتكرر بشكل دوري. يمكن للـ WMS أتمتتها لتوفير الوقت وتقليل الأخطاء البشرية.

ومن أبرز هذه المهام:

| **المهمة** | **الوصف** |
| --- | --- |
| جمع وتخصيب سجلات التدقيق (Audit Log Collection and Enrichment) | جمع السجلات من جميع الأجهزة وإضافة معلومات إضافية إليها ضمن نظام SIEM. |
| استعلام عن معلومات المستخدم (User Information Lookup) | استخراج تفاصيل المستخدم من Active Directory مثل القسم أو المسمى الوظيفي. |
| استعلام عن معلومات الجهاز (Device/IP Lookup) | استعلام من DNS أو قاعدة بيانات الأصول لمعرفة عنوان IP أو اسم الجهاز. |
| الإشعارات والتنبيهات (Notifications and Alerts) | توليد تنبيهات بناءً على شروط معينة في أنظمة الأمن. |
| استخبارات التهديدات (Threat Intelligence) | تحليل التهديدات باستخدام مصادر خارجية وفقًا لطبيعة عمل المنظمة وبياناتها. |
| إدارة التذاكر (Ticket Management) | إنشاء التذاكر ومتابعتها حتى الإغلاق الكامل. |
| الاتصالات والتصعيدات (Callouts and Escalations) | التواصل مع الأطراف المناسبة (مثل فرق أخرى أو السلطات) عند حدوث حادث مؤكد. |

#### الفائدة من أتمتة المهام

* تقليل الوقت اللازم لمعالجة الحوادث.
* زيادة الدقة والثبات في الإجراءات.
* تخفيف العبء على الموظفين الجدد أو المبتدئين.
* تمكين الإدارة من التركيز على الحوادث المعقدة التي تتطلب تدخلًا بشريًا.

— — — — — — — — — — — — — — — —

### مفهوم سير عمل الاستجابة للحوادث

الاستجابة للحوادث (Incident Response) هي عملية منظمة ومستمرة تهدف إلى التعامل مع الهجمات أو الأنشطة المشبوهة بطريقة منتظمة ومتناسقة داخل مركز العمليات الأمنية (SOC).

#### مراحل دورة حياة الاستجابة للحوادث

1. التحضير (Preparation):

تجهيز الأدوات، السياسات، والفِرق اللازمة قبل حدوث أي حادث.

1. الكشف والتحليل (Detection & Analysis):

اكتشاف النشاط غير الطبيعي وتحليل مدى خطورته.

1. الاحتواء والإزالة والتعافي (Containment, Eradication & Recovery):

منع انتشار الهجوم، إزالة مصدره، واستعادة الأنظمة إلى وضعها الطبيعي.

1. النشاط بعد الحادث (Post-Incident Activity):

مراجعة ما حدث واستخلاص الدروس لتحسين الأداء المستقبلي.

#### مراحل سير العمل داخل SOC

سير العمل عادةً يُقسَّم إلى ثلاث مراحل رئيسية:

1. الكشف (Detect):

ملاحظة أي نشاط غير طبيعي من خلال النظام أو المستخدمين.

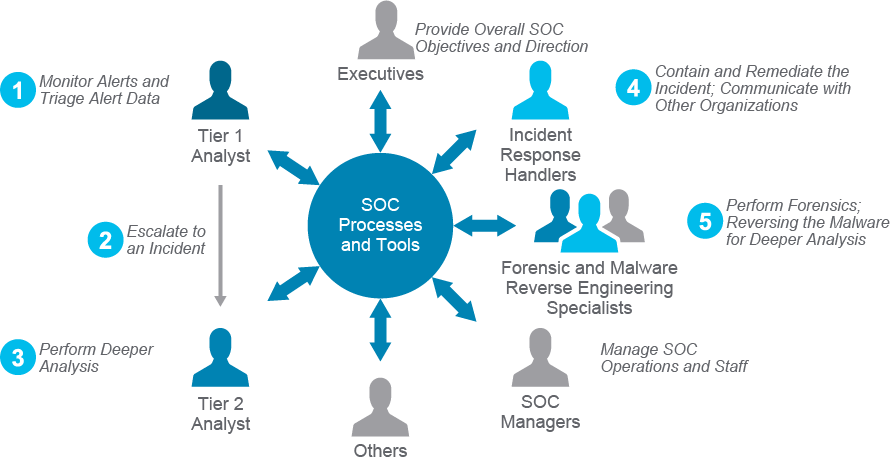
1. الفرز (Triage):

تقييم مدى أهمية الحادث وتحديد ما إذا كان يحتاج تدخلًا أو لا.

1. الاستجابة (Respond):

تحليل البيانات، اتخاذ الإجراءات، واحتواء التهديد.

* يمكن أن يبدأ الحادث إما عبر إبلاغ المستخدمين من خلال مركز المساعدة (Help Desk) أو عبر الكشف التلقائي بواسطة Playbook (أداة آلية).
* الهدف هو الحفاظ على التناسق في كل خطوة عبر أتمتة بعض المهام باستخدام WMS لتقليل الأخطاء اليدوية.

— — — — — — — — — — — — — — — —

### تكامل نظام إدارة سير العمل في مركز العمليات الأمنية (SOC WMS Integration)

#### كيف يعمل WMS داخل الـSOC

1. يتلقى التنبيهات (Alerts) من نظام SIEM، وهو النظام الذي يجمع ويحلل سجلات الأنشطة (logs) في الشبكة.
2. يرسل أوامر تلقائية إلى أجهزة الأمن (مثل الجدران النارية أو أنظمة الكشف عن الاختراق) لمعالجة التهديد أو احتوائه.
3. يُحدّث أنظمة أخرى مثل نظام التذاكر (Ticketing System) لتوثيق الخطوات والإجراءات.

بهذا الشكل، ينتقل الـSOC من حالة الضغط الزائد على المحللين إلى حالة أكثر تنظيمًا وفعالية بفضل الأتمتة.

#### فوائد استخدام WMS

* تقليل العبء على محللي SOC.
* تسريع عملية الاستجابة للحوادث.
* ضمان التناسق والموثوقية في الإجراءات.
* أتمتة التقارير والتنبيهات الدورية.
* تحسين التواصل بين الأدوات والأنظمة الأمنية المختلفة.

#### تكامل WMS مع أنظمة أخرى

عادة ما يتكامل الـWMS مع عدة أنظمة رئيسية داخل الـSOC:

| **النظام** | **الوظيفة** |
| --- | --- |
| **SIEM** | تزويد WMS بالتنبيهات والأحداث الأمنية. |
| **Ticketing System** | إنشاء أو تحديث التذاكر تلقائيًا لتوثيق الحوادث. |
| **Security Devices** | تنفيذ أوامر الاستجابة (مثل حظر عنوان IP أو إيقاف حساب). |
| **Threat Intelligence Sources (مثل TAXII)** | جلب معلومات عن التهديدات المعروفة لمساعدة WMS في اتخاذ قرارات ذكية. |

#### 

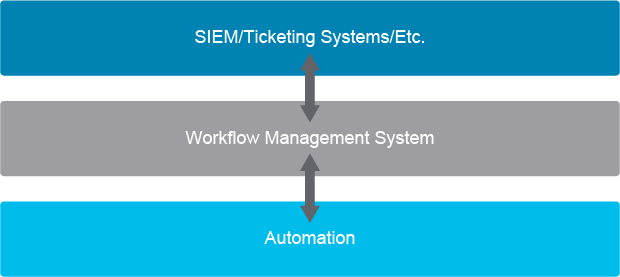
#### طرق التكامل بين WMS وباقي الأنظمة

هناك ثلاث طرق رئيسية للتكامل:

1. RESTful API
   * أكثر الطرق شيوعًا.
   * يستخدم HTTP requests (GET, POST, PUT, DELETE) للتفاعل بين الأنظمة.
   * مثال: يقوم WMS بتحديث حالة تذكرة في نظام التذاكر من خلال واجهة API.
2. Command-Line API
   * تنفيذ أوامر مباشرة من سطر الأوامر.
   * يُستخدم عادة في الاستعلامات السريعة أو الأوامر الفورية.
   * مثال: استعلام من WMS إلى SIEM لمعرفة حالة تهديد معين.
3. TAXII (Trusted Automated Exchange of Indicator Information)
   * آلية مفتوحة المصدر لتبادل معلومات التهديدات السيبرانية بشكل آلي.
   * تساعد WMS على اكتشاف التهديدات بناءً على مؤشرات (Indicators of Compromise) ومشاركتها مع أنظمة أخرى.

#### أمثلة على العمليات التي يمكن لـWMS إدارتها

* إدارة الحوادث الأمنية (Incident Management)
* إدارة الثغرات (Vulnerability Management)
* الصيد والاستخبارات التهديدية (Threat Hunting)
* مراقبة الشبكة والكشف عن التهديدات (Network Security Monitoring)
* الالتزام بالحوكمة والسياسات الأمنية (Governance & Compliance)
* الأمن الفيزيائي ومراقبة التهديدات المادية



### مثال على أتمتة سير العمل في مركز العمليات الأمنية (SOC Workflow Automation Example)

في الوقت الحالي، أصبحت الأتمتة (Automation) عنصرًا أساسيًا في مراكز العمليات الأمنية (Security Operations Center - SOC).

الغرض منها هو تسريع الاستجابة للحوادث الأمنية وتقليل الأعمال اليدوية المتكررة، مما يسمح للمحللين بالتركيز على المهام التي تحتاج إلى تفكير بشري وتحليل دقيق.

#### ما المقصود بأتمتة سير العمل (Workflow Automation)؟

هي عملية استخدام أدوات وتقنيات لتنفيذ إجراءات متكررة تلقائيًا دون تدخل بشري مباشر.

وتشمل الأتمتة في SOC عمليات مثل:

* تسجيل الدخول إلى عدة أجهزة وتنفيذ أوامر محددة.
* جمع سجلات (Logs) وتحميلها في نظام التذاكر (Ticketing System).
* استعلام عن المستخدمين، عناوين IP، أو السمعة (Reputation Score) من مصادر استخبارات التهديدات (Threat Intelligence).

الهدف من الأتمتة هو تقليل الوقت والجهد في تنفيذ المهام المتكررة وتحسين سرعة الاستجابة.

#### فوائد الأتمتة داخل الـSOC

| **الفائدة** | **التوضيح** |
| --- | --- |
| ⏱️ تسريع الاستجابة | اكتشاف واحتواء التهديدات بشكل أسرع. |
| 🤖 تقليل الأعمال اليدوية | النظام يقوم بالمهام الروتينية، مما يوفر وقت المحللين. |
| 🔁 العمل المتسق | تنفيذ نفس الإجراءات بنفس الطريقة دائمًا، مما يقلل الأخطاء البشرية. |
| 💡 تحسين الكفاءة | التركيز على القضايا التي تحتاج تحليل وتفكير بشري. |
| 💰 توفير الوقت والتكلفة | تقليل الجهد البشري والمهام المتكررة. |

#### تسلسل سير العمل (Workflow Example)

1. يتلقى الـSOC تنبيه (Alert) من نظام SIEM يشير إلى نشاط مشبوه (مثلاً: مستخدم اتصل بعنوان IP ذو سمعة سيئة).
2. المحلل من المستوى الأول (Tier 1 SOC Analyst) يبدأ التحقيق:
   * يتم فتح تذكرة (Case) في نظام التذاكر تلقائيًا.
   * الـWMS يجلب تلقائيًا تفاصيل المستخدم من Active Directory (الاسم، البريد الإلكتروني، الموقع، المدير...).
   * يجلب عنوان الجهاز وIP من DHCP أو الشبكة.
   * يستعلم عن الـIP في منصة Threat Intelligence لجلب سمعة التهديد (Threat Reputation).
   * يجمع تقارير الوكيل Proxy وحزم الشبكة Packet Captures ويضيفها للتذكرة.

كل هذه الخطوات تحدث بشكل آلي قبل أن يبدأ المحلل البشري التدخل.

بعدها يقوم المحلل بمراجعة البيانات وتحديد مدى خطورة التهديد، ثم:

* إما إغلاق التذكرة. أو رفعها للمستوى الثاني (Tier 2) للمزيد من التحقيق.

#### أدوار محللي الـSOC حسب المستوى

| **المستوى** | **المهام الرئيسية** |
| --- | --- |
| Tier 1 | فتح التذاكر، جمع معلومات المستخدم، مراجعة التقارير الأولية، تحديد الأولوية. |
| Tier 2 | تحليل أعمق: مراجعة حزم الشبكة، تحديد ما إذا تم استغلال ثغرة، جمع مؤشرات اختراق (IoCs)، تنفيذ العزل (Containment). |
| Tier 3 (Forensics & Incident Handler) | معالجة الأجهزة المصابة (Reimage)، استخراج مؤشرات جديدة، تحديث قاعدة بيانات التهديدات، إغلاق التذكرة. |
| الإدارة (Management) | تحليل الأداء: الوقت اللازم للاكتشاف، الاحتواء، الحل، والإغلاق. |

#### الفرق بين الأتمتة (Automation) والتنظيم (Orchestration)

* Automation: تنفيذ إجراءات محددة تلقائيًا (مثل جلب التقارير أو تنفيذ أوامر).
* Orchestration: تنسيق عدة عمليات آلية معًا لإنشاء سير عمل متكامل (Workflow).

#### أمثلة على أدوات (WMS / SOAR) المستخدمة في أتمتة الـSOC

| **الأداة** | **الميزة البارزة** |
| --- | --- |
| Cisco SecureX | تنسيق وأتمتة العمليات الأمنية بالكامل. |
| Cisco CloudCenter Action Orchestrator | إنشاء سير العمل بسهولة عبر واجهة سحب وإفلات. |
| CyberSponse | إدارة الاستجابة للحوادث الأمنية (IR). |
| IBM Resilient Systems | مرونة في التكامل مع أدوات متعددة. |
| Proofpoint Threat Response | ربط الاستجابة بالتحليلات البريدية والتهديدات. |
| Swimlane | منصة SOAR شاملة تدعم التكامل مع مختلف الأنظمة. |

#### مثال تطبيقي (Use Case)

في بيئة تستخدم Cisco SecureX مع Secure Network Analytics وSecure Endpoint:

1. يتم اكتشاف جهاز خبيث أو نشاط مشبوه من خلال التنبيهات.
2. يقوم الـWorkflow تلقائيًا بـ:
   * تحديد الجهاز المصاب.
   * عزله (Isolate Endpoint).
   * حظر الملفات الخبيثة عبر Hash Blocking.
   * إرسال إشعارات إلى الفريق الأمني.

النتيجة:

كل هذه الخطوات كانت تُنفّذ يدويًا سابقًا، أما الآن فهي تتم تلقائيًا بالكامل، مما يجعل الاستجابة أسرع وأكثر دقة.

