Cybersecurity Operations

ما هو مركز عمليات الأمن(SOC) ؟

ببساطة، يمكن تشبيه مركز عمليات الأمن بالحارس الذي يعمل على مدار 24 ساعة لحماية المؤسسة. إنه مكان مركزي داخل الشركة، مهمته الأساسية هي مراقبة الشبكة والبنية التحتية الرقمية بالكامل. سواء كانت الشبكة داخلية، أو شبكة الخوادم ومراكز البيانات(Data Center) ، أو حتى حركة المرور من وإلى الإنترنت، فإن فريق الـ SOC يقوم بتحليل كل هذا لضمان أمنه.

مهمتهم هي التأكد من أن البيانات التي تدخل وتخرج من المؤسسة آمنة، ولا تحتوي على أي شيء ضار(Malicious) ، ولا تسرب معلومات حساسة عن المؤسسة.

مركز العمليات الأمنية (SOC): هو مركز قيادة لمراقبة أنظمة المعلومات التي تستخدمها المؤسسة لبنيتها التحتية لتكنولوجيا المعلومات، قد يشمل ذلك كل شيء بدءًا من مواقع الويب الخاصة بالعمل وقواعد البيانات والخوادم والتطبيقات والشبكات وأجهزة سطح المكتب ومراكز البيانات ومجموعة متنوعة من نقاط النهاية .

يراقب إعداد الأمن السيبراني SOC كل عنصر من عناصر البنية التحتية ، ويقيم حالتها الحالية ، بما في ذلك التهديدات المحتملة والحالية ، ويستجيب للتهديدات. كما تضع SOC أيضًا إجراءات وبروتوكولات لأمن المعلومات مصممة لمنع التهديدات المستقبلية.

Soc

كمثال توضيحي تُظهر الصورة هنا نموذج مركز العمليات الأمنية (SOC) الخاص بشركة IBM .

يتميّز مركز العمليات الأمنية (SOC)عادةً بوجود شاشات كبيرة في المنتصف، بحيث يتمكّن جميع الأفراد الجالسين من رؤيتها بوضوح. وتُعرض على هذه الشاشات بيانات مشتركة بين جميع أعضاء الفريق.

بعد ذلك، يُلاحظ أن تنظيم المكان يتم على شكل صفوف أو مستويات متتالية؛ حيث يوجد أفراد في الصف الأول، وآخرون في الصف الثاني، ثم الثالث، وهكذا. وغالبًا ما يكون لكل صف نفس الوصف الوظيفي (Job Description) والمهام (Tasks)التي يقوم بها الأفراد ضمن هذا المستوى.

مصادر البيانات:(Data Sources)

تشمل مجموعة واسعة من الأنظمة والأجهزة التي تُعدّ أساسًا لعمليات المراقبة والتحليل داخل مراكز العمليات الأمنية (SOC).تتنوّع هذه المصادر لتغطي مختلف طبقات البنية التحتية التقنية في المؤسسة، وتشمل ما يلي:

1. **جدران الحماية :(Firewalls)** تعمل على مراقبة حركة المرور الشبكية والتحكم فيها وفقاً لسياسات الأمان المحددة مسبقاً، وتولّد سجلات تحتوي على معلومات حول محاولات الوصول المصرح بها وغير المصرح بها.
2. **قواعد البيانات :(Databases)** تُعدّ من أهم مصادر البيانات الحساسة، إذ تُسجّل العمليات المتعلقة بالوصول إلى البيانات وتعديلها، مما يساعد في اكتشاف الأنشطة المشبوهة أو محاولات الاختراق.
3. **نقاط النهاية :(Endpoints)** وتشمل أجهزة الحواسيب المكتبية والمحمولة وأجهزة المستخدمين النهائيين. تُنتج هذه النقاط سجلات لأنشطة المستخدمين وتحديثات النظام، وهي عنصر حيوي في كشف البرمجيات الخبيثة والهجمات المستهدفة.
4. **خوادم الويب :(Web Servers)** تُسجّل طلبات المستخدمين وأنشطة الوصول إلى التطبيقات والمواقع، وتوفّر بيانات مهمة حول محاولات الهجمات مثل الحقن (SQL Injection) أو هجمات الحرمان من الخدمة.(DDoS)
5. **خوادم الملفات :(File Servers)** تحتوي على سجلات تتعلق بعمليات إنشاء الملفات أو تعديلها أو حذفها، وتُستخدم لمراقبة سلوك المستخدمين وحماية البيانات الحساسة من التسريب أو الوصول غير المصرح به.
6. **خوادم الإدارة :(Management Servers)** تتعامل مع إدارة الأنظمة وتوزيع السياسات الأمنية، وتوفّر سجلات توضح من قام بتغيير إعدادات النظام أو تطبيق سياسات جديدة.
7. **أجهزة التوجيه :(Routers)** تقوم بتوجيه حركة المرور داخل الشبكة وخارجها، وتُنتج بيانات عن الاتصالات، وعناوين المصدر والوجهة، وأنواع البروتوكولات المستخدمة.
8. **أنظمة منع التسلل :(IPS)** تعمل على تحليل حركة المرور في الزمن الحقيقي للتعرف على الأنشطة الضارة ومنعها فورًا قبل أن تُلحق الضرر بالنظام.
9. **أنظمة كشف التسلل :(IDS)** تُستخدم لاكتشاف الأنشطة المشبوهة أو الأنماط غير الطبيعية في الشبكة، وتُرسل تنبيهات إلى مركز العمليات الأمنية لاتخاذ الإجراءات المناسبة.

كل هذه الأجهزة والأنظمة تُولّد كميات ضخمة من البيانات، التي تُجمّع وتُحلّل داخل مركز العمليات الأمنية (SOC) بهدف الكشف المبكر عن التهديدات، وتحسين مستوى الحماية، وضمان سلامة البنية التحتية الرقمية للمؤسسة.

معالجة البيانات في مركز عمليات الأمن

تواجه الشبكات تحديًا بسبب الكم الهائل من البيانات من مصادر متنوعة فكيف يتم التعامل مع كل تلك السجلات.

- **خطوات معالجة البيانات**:

1. **الجمع (Collect):** تُجمع كل البيانات.
2. **التطبيع (Normalize):** تُحوّل البيانات المجمعة إلى شكل قابل للفهم.
3. **الفهرسة (Index) :**تُفهرس البيانات بناءً على نوعها.
4. **صيانة قاعدة البيانات (Maintain Database):** تُصان قاعدة بيانات للمساعدة في ربط الأحداث.
5. **الربط (Correlate):** تُربط الأحداث معًا، حيث تصل أحداث متعددة إلى مركز عمليات الأمن.
6. **مراقبة لوحات المعلومات (Monitor Dashboards) :**يراقب محلل مركز عمليات الأمن لوحات المعلومات التي تعرض هذه البيانات المترابطة والمُطبّعة. يجب على المحلل قراءة وفهم التنبيهات على هذه اللوحات.

7. التنبيه، الإبلاغ، الاستعلام، الأرشفة، سير العمل (Alerting, Reporting, Querying, Archiving, Workflow) :

كل هذه الأنشطة جزء من عملية لوحة المعلومات. يحتاج محللو مركز عمليات الأمن إلى تدريب لفهم لوحات المعلومات من مختلف أدوات ومنتجات الأمن.

مستويات العمل داخل مركز العمليات الأمنية (SOC) ودورة حياة الحوادث الأمنية

تتوزع مهام العمل داخل مركز العمليات الأمنية (SOC) على عدة مستويات، يشار إليها عادةً بالمصطلحات Tier 1، Tier 2، Tier 3. لا يُكتفى بتسمية الشخص بأنه مهندس أمن (SOC Engineer) فقط، بل يجب تحديد المستوى الذي يعمل فيه داخل منظومة الـ SOC. هذا التقسيم يهدف إلى توزيع المهام وفقًا للخبرة والمسؤوليات، بحيث تتكامل الجهود لتحقيق الاستجابة المثلى للحوادث الأمنية.

أولاً: دورة حياة الحوادث الأمنية(Incident Lifecycle)

أي حادث أمني (Incident) يمر بعدة مراحل متتابعة تشكّل ما يُعرف بـ **دورة حياة الحوادث الأمنية (Incident Lifecycle)**، وتشمل المراحل التالية:

1. **التحضير :(Preparation)** وضع الخطط والسياسات والإجراءات المسبقة للتعامل مع الحوادث الأمنية.
2. **التعرف :(Identification)** الكشف عن الحادث الأمني من خلال مراقبة الأنشطة والتنبيهات.
3. **الاحتواء :(Containment)** عزل الحادث لمنع انتشاره أو تفاقمه.
4. **الإزالة :(Eradication)** التخلص من مصدر الهجوم أو البرمجيات الضارة المرتبطة به.
5. **الاستعادة :(Recovery)** إعادة الأنظمة المتأثرة إلى حالتها الطبيعية وضمان استقرارها.
6. **الدروس المستفادة :(Lessons Learned)** تحليل الحادث واستخلاص العبر لتحسين الإجراءات المستقبلية.

ثانياً: مستويات العمل داخل مركز العمليات الأمنية(SOC Tiers)

1-المستوى الأول(Tier 1 – SOC Analyst Level 1)

هو خط الدفاع الأول في مركز العمليات الأمنية، ويُعرف أحيانًا باسم SOC Analyst L1. يقوم العاملون في هذا المستوى باستلام البيانات القادمة من مختلف مصادر الشبكة Firewalls ، Routers، Switches، Endpoints، Proxy Servers وتحليلها مبدئيًا.

- **المهام الأساسية:**
  - مراقبة التنبيهات الصادرة من الأنظمة الأمنية.
  - فرز البيانات وتحديد ما يُحتمل أن يكون حادثًا أمنيًا حقيقيًا.
  - تصنيف التنبيهات إلى طبيعية (Benign) أو مشبوهة.(Suspicious)
  - تحويل الحوادث المحتملة إلى المستوى الثاني لمزيد من التحقيق.

يطلق على هذه العملية **الفرز الأولي(Triage)** ، وهي المرحلة التي يتم فيها تمييز التنبيهات الجادة من بين الكم الكبير من البيانات.

2- المستوى الثاني(Tier 2 – Incident Responder / SOC Analyst Level 2)

يُعرف العاملون في هذا المستوى باسم مستجيبي الحوادث(Incident Responders) ، وهم المسؤولون عن التحقيق (Investigation)في الحوادث التي تم تحويلها من المستوى الأول.

- **المهام الأساسية:**
  - إجراء تحليل متعمق للحوادث الأمنية باستخدام أدوات وتقنيات متقدمة.
  - التحقق من صحة الحادث وتحديد ما إذا كان حقيقيًا أم إنذارًا كاذبًا.(False Positive Alert)
  - تنفيذ إجراءات الاحتواء (Containment) والإزالة (Eradication) عند تأكيد الحادث.
  - التواصل مع الفرق الأخرى لتنسيق الاستجابة وتنفيذ الحلول التصحيحية.

يُعد هذا المستوى حجر الأساس في سلسلة الاستجابة الأمنية، إذ يحدد ما إذا كانت البيانات تتطلب تدخلًا مباشرًا أو لا.

3- المستوى الثالث(Tier 3 – Subject Matter Expert / Threat Hunter)

يُعرف هذا المستوى أيضًا باسم خبراء التهديدات (Threat Hunters) أو المتخصصين الفنيين

Subject Matter Experts يعمل هؤلاء بشكل دوري ومستمر على البحث والتحليل الاستباقي لاكتشاف التهديدات الجديدة وتحديث آليات الدفاع.

- **المهام الأساسية:**
  - تتبع أحدث الهجمات السيبرانية (Attacks) والبرمجيات الخبيثة المنتشرة عالميًا.
  - تطوير استراتيجيات جديدة للكشف المبكر عن التهديدات.
  - تحديث أدوات المراقبة وتحسين أنظمة الـ.SIEM
  - تقديم التوصيات التقنية لتقوية منظومة الأمن.

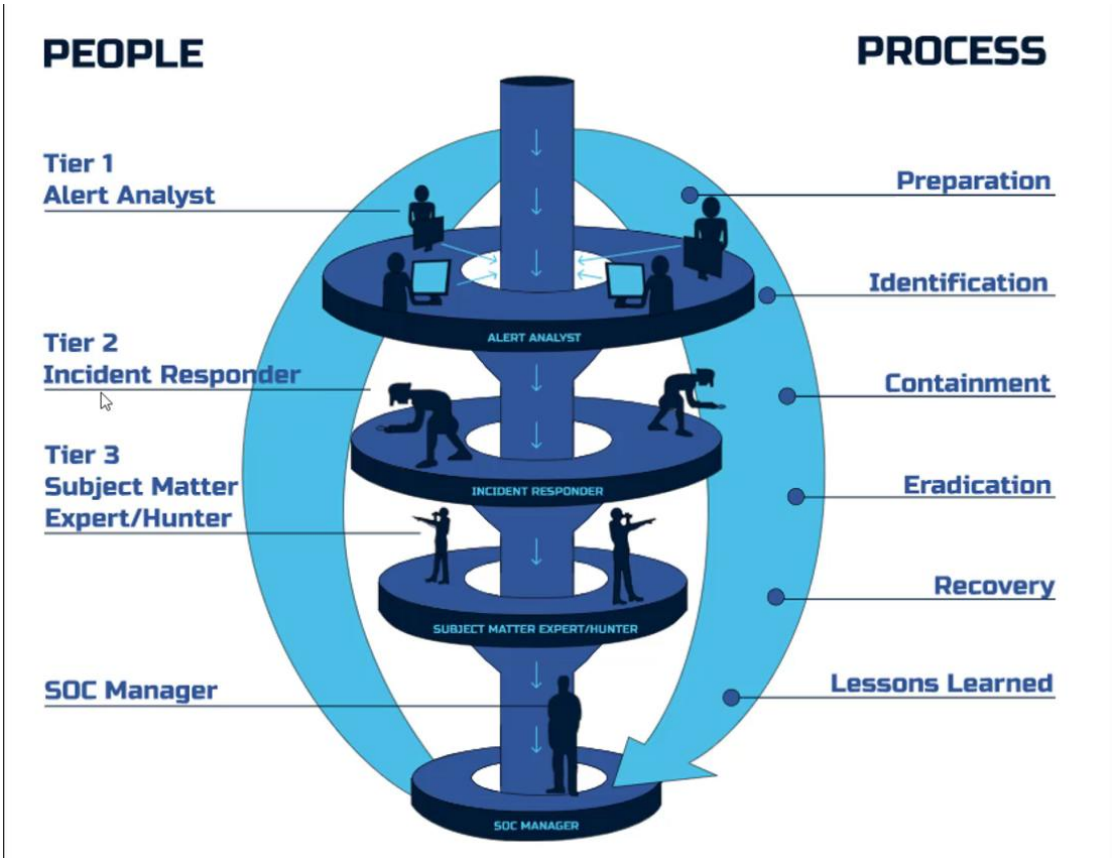
يُعتبر هذا المستوى الأكثر خبرة داخل مركز العمليات الأمنية، إذ يعتمد العاملون فيه على خبرة تراكمية من العمل في المستويين الأول والثاني.

4- الإدارة العليا لمركز العمليات الأمنية

في قمة الهيكل التنظيمي للـ SOC يوجد **مدير مركز العمليات الأمنية(SOC Manager)** ، وهو المسؤول عن:

- الإشراف على أداء الفرق المختلفة عبر المستويات الثلاثة.
- ضمان تنفيذ سياسات الأمن وفقًا للمعايير المؤسسية.
- التنسيق مع الإدارات الأخرى والاستجابة الفعّالة للحوادث.
- تطوير الخطط الاستراتيجية لتحسين أداء المركز.

Cybersecurity Operations



مستويات العمل داخل مركز العمليات الأمنية

إعداد: م /إسلام الشعراني