ملخص اللقاء الأول – يوم في حياة موظف مركز العمليات السيبرانية وتثبيت نظام Security Onion

تنويه:

إن هذا الملف وضع لتسهيل عملية وصولك لمرفقات اللقاء ولن يغنيك عن المحتوى الوارد فيه.

هذا اللقاء سيكون كل يوم أربعاء عند الساعة السابعة والنصف مساءً وقد يتم تحديث المواعيد دوريًا لذلك عليك متابعتنا على الديسكورد.

https://twitter.com/MAlajab/status/1287489064069992449?s=20

الاجندة:

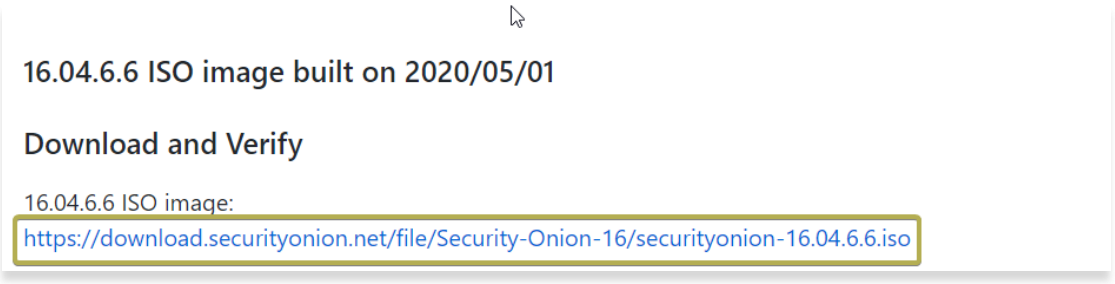
1- نظرة تعريفية على ماهية المهام التي يقوم بها محلل مركز العمليات السيبرانية المستوى الأول (SOC analyst L1) حسب تصنيف الاطار الوظيفي الصادر من الهيئة الوطنية للأمن السيبراني "سيوف".
2- مواقع تساعدك في عملية التحليل اليومي.
3- تثبيت نظام رصد ومراقبة التهديدات وتستطيع تثبيته في المنزل أو العمل كمختبر للتجارب.
4- التحديات اليومية التي تواجه محلل التهديدات السيبرانية.

تحميل نظام Security Onion

قم بالتحميل من خلال هذا الرابط.

https://github.com/Security-Onion-Solutions/security-onion/blob/master/Verify_ISO.md

ثم قم باختيار:



تابع هنا للتثبيت إذا كنت تستخدم vmware:

https://youtu.be/d9MgjPw1_bU?t=466

هنا إذا كنت تستخدم VirtualBox:

https://www.youtube.com/watch?v=jRoQUVY-2Ic

أو من هنا:

https://www.youtube.com/watch?v=YUEMjWk6dvk

بالبداية ماهو موظف المستوى الأول (SOC analyst L1) في مركز العمليات السيبرانية؟

بحسب تصنيف الهيئة الوطنية للأمن السيبراني فالمسمى هو "محلل معلومات التهديدات السيبرانية".

الوصف:

جمع معلومات عن التهديدات السيبرانية من مصادر مختلفة وتحليلها لتكوين فهم وإدراك عميقين للتهديدات السيبرانية، وخطط المخترقين، والأساليب والإجراءات المتبعة، لاستنباط وتوثيق مؤشرات من شأنها مساعدة المنظمات في الكشف عن الحوادث السيبرانية والتنبؤ بها، وحماية الـُنظم والشبكات من التهديدات السيبرانية.

سوف تعمل ضمن إدارة التهديدات Threat Monitoring .

من يستطيع العمل هناك؟

كل من لديه شهادة جامعية في مجال الحاسب ويملك المتطلبات الأساسية لشغل هذا المنصب.

ماهي المهام التي يقوم بها؟

اقرأ هنا :

https://github.com/Malajab/incyber/blob/master/SOC/level-1.md#Soc-level-1

من الأمور المهم ذكرها هو مدى أهمية وعي موظفي مركز العمليات المستوى الأول فكلما كان الرصد سريع جنّبك المشاكل وتبعاتها. لذلك إن كنت تعمل في هذا الخط الدفاعي الأمامي فلديك ضغط كبير يجب أن تكون متفهم له. ونجاحك موثر كثيرًا في نجاح المنظمة.

خلال عملك في البداية سوف تواجه صعوبة التعامل مع التهديدات لذلك عليك الاطلاع على الكتيب الارشادي الذي يوضح كل تهديد وكيفية التعامل معه بالإضافة إلى الأساسيات التي لديك مثل أساسيات الشبكات وكيف تعمل؟ ماهي البروتوكولات؟ وماهي أنواعها؟ ماهو IP؟ TCP/UDP ؟ماهي الأنظمة؟ ماهو السيرفر؟ مالفرق بينه وبين workstation؟ ماذا نعني بـ active directory؟

حينما تبدأ بالعمل عليك التطبيق على جميع التهديدات التي ظهرت مسبقًا ولا تكتفي بذلك بل اقرأ دوريًا عن التهديدات التي تظهر وقم بتطوير نفسك في مجال اصطياد التهديدات.

كموظف في هذا القسم قد تواجه تهديدات ولاتعلم كيفية التعامل معها. هنالك مستودع معلوماتي ثري انصحك بالاطلاع عليه

https://github.com/hslatman/awesome-threat-intelligence

ولنظرة بسيطة عنه تابع:

https://youtu.be/d9MgjPw1_bU?t=1883

إذا كان هناك هجمة جديدة ولا أعلم كيف أتعامل معها؟

تابع هنا:

https://youtu.be/d9MgjPw1_bU?t=2090

مواقع ومصادر تفيدك في التحليل اليومي.

مصدر Awesome OSINT

وهو عبارة عن مصادر منسقة مفتوحة المصدر ويفيدك في تتبع المعلومات الاستخباراتية.

https://github.com/jivoi/awesome-osint

تابع هنا:

https://youtu.be/d9MgjPw1_bU?t=2536

موقع شودن - Shodan

هو محرك يقوم بعملية مسح للمنافذ المفتوحة على الانترنت. وتستطيع فحص أضرار IP والبحث المعمول عنه والثغرات المتواجدة فيه.

https://www.shodan.io/

تابع هنا:

https://youtu.be/d9MgjPw1_bU?t=2641

موقع - Threatcrowd

جيد لربط التهديدات التي تحصل لديك في المنظمة من خلال البحث بال IP

https://www.threatcrowd.org/

تابع هنا:

https://youtu.be/d9MgjPw1_bU?t=2681

موقع Open Threat Exchange

تستطيع بعد التسجيل فيه الحصول على تقارير ترفع لديهم.

https://cybersecurity.att.com/open-threat-exchange

تابع هنا:

https://youtu.be/d9MgjPw1_bU?t=2788

موقع Hybrid Analysis

لتحليل التهديدات الضارة.

https://www.hybrid-analysis.com/

أما إذا كنت تريد التطبيق أو تحليل برمجيات خبيثة تستطيع من خلال موقع malware traffic analysis

https://www.malware-traffic-analysis.net/

تابع هنا:

https://youtu.be/d9MgjPw1_bU?t=2995

موقع dnsdumpster

يقوم بعمل mapping domain وتستطيع من خلال استعراض الخارطة قراءة جميع الارتباطات.

https://dnsdumpster.com/

تابع هنا:

https://youtu.be/d9MgjPw1_bU?t=3204

موقع MXTOOLBOX

لكن يجدر بي التنبيه عن عدم تحميل الايميلات الحساسة الخاصة بالمنظمة إلا في حال عمل ترميز (decode) أو قم بتحميل cyberchef كاداة.

https://mxtoolbox.com/

تابع هنا:

https://youtu.be/d9MgjPw1_bU?t=3275

البدء بعمل التطبيق على نظام الرصد Security Onion

https://youtu.be/d9MgjPw1_bU?t=3769

تحميل Nessus

هي أداة تقوم بعمل اختبار اختراق للأنظمة لديك.

https://www.tenable.com/downloads/nessus?loginAttempted=true

لتشغيل الأداة اكتب هذا الأمر

```
/etc/init.d/nessusd start
```

اذهب للمتصفح وقم بلصق التالي:

[https://kali:8834/]

تابع هنا لكن العمل عليها سيكون فيما بعد:

https://youtu.be/d9MgjPw1_bU?t=4780

أخيرًا:

حينما تود تقديم تقرير يعرض الاحصائيات لديك فالطبع يجب أن تقوم بتقديمه بشكل احترافي (Kibana) تساعدك في ذلك. لن نتطرق كثيرًا إليها الآن فهي تحتاج لوقت أطول.

تابع هنا:

https://youtu.be/d9MgjPw1_bU?t=4870