# دورات الاستخبارات التدريبية لدى Treadstone 71

## شهادة مهنية استخبارات الفضاء الإلكتروني

تتبع دورة شهادة مهنية استخبارات الفضاء الإلكتروني الخطوط العريضة المذكورة فيما بعد وتتبع النمط المعتاد من طرق التدريس التي تبدأ بمحاضرات ثم تجارب عملية ثم محاضرات ثم تجارب عملية طوال فترة الدورة. نقوم بتقسيم الفصل إلى فرق من أجل أداء عمليات بحث عن استخبارات المصادر المفتوحة (جمع البيانات وتنظيمها وتحليلها والكتابة التحليلية وكتابة ملخصات موجزة داخل الفصل) للعديد من حالات الدراسة التي تتضمن الجمع السلبي للمعلومات عن الأهداف النشطة. كما أن هناك العديد من التدريبات العملية الأخرى على مدار الدورة. نحن نتبع دورة حياة تقليدية للاستخبارات مع مناهج متكررة باستخدام المحتوى المبني على معايير العمليات الأمنية. نحن نركز بالفعل على من يقومون بالتهديد وعلى الحملات وعلى الاستخبارات التكتيكية والإستراتيجية. يعتمد البحث على مجموعات نشطة من الأعداء (من خلال الجمع السلبي) ومن خلال معلومات مأخوذة مباشرة من العناوين الرئيسية. نقوم بعرض مواد الدورة من خلال تطبيق Amazon Kindle App كما نوفر للطلاب إمكانية الدخول على شبكات خاصة افتراضية كما نوفر لهم كتابين على الأقل. يستخدم الطلاب أيضاً Dropbox في الوصول إلى المواد الأخرى للدورة الدراسية ومشاركة بيانات حالات الدراسة الأخرى. كما ننصح باستخدام تطبيق Slack داخل الفصل في التواصل.

**معايير العمليات الأمنية**

- مدرسة شيرمان كنت للتحليل الاستخباراتي
- مهنية وكالة الاستخبارات المركزية
- مهنية وكالة الأمن الوطني
- طرق الاستخبارات العسكرية
- توجيهات العمليات الأمنية
- المواد الأكاديمية (جامعة ميرسي هيرست / كلية يوتيكا)
- ترتكز على الخبرة العملية على أرض الواقع و15 عام من عمليات استخبارات الفضاء الإلكتروني

وقد قمنا بتدريس هذه الدورة وتنقيحها على مدار ما يقرب من 10 سنوات وبدأنا على مستوى درجة الماجستير الجامعية عبر الإنترنت. ومنذ ذلك الوقت قمنا بتدريب المئات في المجال والذين صعدوا وترقوا في مناصب مهمة. نحن لا نمنح درجة الدبلوم كما لا نقوم بتدريس العديد من الدورات الدراسية الأخرى المختلفة. نحن نركز فقط على الاستخبارات.

**شرح تفصيلي لبرنامج شهادة مهنية استخبارات الفضاء الإلكتروني (قابل للتعديل)**

CYBINT1 – إخفاء الهوية وإعداد الشخص لمرحلة إخفاء الهوية، طرق وأساليب جمع المعلومات، التخطيط لجمع المعلومات، PIRs، أدوات جمع واستهداف المعلومات. التكيف مع احتياجات طريقة الملاحقة والاكتشاف، الروابط معCSIRT ، TTPs، IoCs، استخبارات التهديدات، استخبارات المصادر المفتوحة، استخبارات جميع المصادر، قاموس معياري، وتصنيف المعلومات

CYBINT2 – المؤسسات، الإنتاج، أساليب التحليل المنظم، أسلوب الخداع والإنكار لدى العدو، استخدام الأساليب، أنواع الأدلة، إدارة الإنتاج، التفكير الحرج، معايير القياس، استمارات وقوالب تلقي المعلومات

CYBINT3 – أنماط طرق التحليل، تفكيك المعلومات، إعادة تجميع المعلومات، طرق دمج المعلومات، حالات دراسة في التحليل، الانحياز المعرفي، مصداقية وموثوقية المصادر، مستويات الثقة، تحليل الافتراضات الأخرى، تشريح الأدلة، سيناريوهات التحليل، الانتقال إلى مرحلة الملاحقة والاكتشاف، CSIRT، TTPs، IoCs، المنهج الاستقرائي / الاستدلالي / المعتمد على التخمين، التوجهات التاريخية، وتحليل الحملات، الاستخبارات من أجل تطويع المؤسسات

CYBINT4 – 4 حالات دراسة، التعرف على عملائك، التعرف على أصحاب المصلحة، التحليل، أوامر وتعليمات القيادة، نظرة عامة على ترتيب الأدلة، الكتابة التحليلية، BLUF، AIMS، أنواع التقارير، تخطيط خطوط الإنتاج / ترتيب التقارير بأرقام مسلسلة، نشر الأخبار، عرض حالات الدراسة، محاضرات، تجارب عملية، تدريب عملي، تدريبات داخل الفصل، العروض التقديمية للطلاب، منتجات تحليلية، القوالب، مواد الدورة.

في حالات الدراسة استخدم جميع الطرق والأساليب والأدوات المشار إليها في مواد الدورة. حالات الدراسة مستقاة بشكل مباشر من العناوين الرئيسية ما يوفر للطلاب خبرة على أرض الواقع داخل الفصل.

هذه الدورة تتبع المعايير التعليمية للرابطة الدولية للاستخبارات في التدريبات الأساسية على التحليل الاستخباراتي:

أولاً مقدمة عن الاستخبارات
ثانياً التفكير الحرج
ثالثاً الكتابة التحليلية
رابعاً التفكير الإبداعي
خامساً الإيجاز التحليلي
سادساً أساليب التحليل الهيكلية
سابعاً المشاكل التحليلية
ثامناً تخطيط الأدلة
تاسعاً حالات دراسة

**أولاً مقدمة عن الاستخبارات**

A. دورة الاستخبارات: ناقش دورة أو عملية الاستخبارات وكيفية ارتباط عناصرها مع بعضها البعض.
B. نظرة عامة على قطاع الاستخبارات: اكتب وصفاً لقطاع الاستخبارات الذي تعمل فيه الوكالة وأدوار كل مشارك.
C. تصنيف الاستخبارات: استخدم الطرق المناسبة في التصنيف وتمييز مختلف الوثائق.

**ثانياً التفكير الحرج**

A. تعريف التفكير الحرج: اشرح ما هو التفكير الحرج وسبب أهميته للتحليل الاستخباراتي وعمليات حل المشاكل.
B. العناصر الثمانية للتفكير: استخدم نموذج بول وإلدر (أو أي نموذج معروف فى التفكير الحرج) باستخدام العناصر الثمانية للتفكير الحرج (أو الهيكل التنظيمي المرتبط به) من أجل التقييم الحرج للتقييمات المكتوبة.
C. المعايير الفكرية: أشرح المعايير الفكرية لبول وإلدر (أو أي مجموعة معايير فكرية أخرى) وكيفية استخدامها في التحليل الاستخباراتي.

**ثالثا: الكتابة التحليلية**

*ملحوظة: بالإشارة إلى المعايير يمكن أن تكون هذه المعايير بديلة للمعايير المطبقة بناءً على إرادة الجماهير.*

A. نظرة عامة على المنتجات: تعرَّف على مزايا منتجات IC الفعالة.

B. معايير المهنية: اربط بين المعايير المهنية التحليلية وبين الكتابة الواضحة.

C. معايير استقاء المصادر: تدرب على طريقة الكتابة بما يتوافق مع معايير استقاء المصادر.

D. كتابة البيانات المعلنة: اشرح طريقة كتابة البيانات المعلنة.

E. تدريبات عملية: راجع مهارات التفكير الحرج وتدرَّب عليها بكتابة وثائق استخباراتية مناسبة.

**خامساً التفكير الحرج**

A. استثارة الأفكار: وسع نظرتها للبدائل.

B. إعادة النظر: تحدى افتراضاتهم وأوهامهم المعرفية.

C. التفكير الجانبي: وفر بدائل أنماط التفكير.

D. الفرق الصديقة: فكر من وجهة نظر الخصم.

E. تدريبات عملية داخل الفصل: وفر لأصحاب المصلحة/القيادة الخيار من خلال عرض الأهداف / التحليل الذي يمكن الدفاع عنه وساعدهم على التقييم الحرج للاستخبارات / المعلومات.

**رابعاً الإيجاز التحليلي**

**1.** قواعد الإيجاز: اشرح قواعد الإيجاز.

2. صياغة الإيجاز: صغ إيجازاً بناءً على هذه القواعد
3. تدريب: استعرض تقرير موجز حول موضوع استخباراتي – ثم استعرض النتائج التحليلية شفوياً بطريقة عملية.

**سادساً طرق التحليل الهيكلية**

1. تنظيم / مقارنة البيانات: فهم الحاجة إلى تنظيم البيانات بكفاءة من أجل تحليلها بالطريقة المناسبة.
2. طرق تطوير المشاكل / المعضلات:
    1. إعادة صياغة المشكلة: فهم كيفية إعادة صياغة المشكلة من أجل حل أكثر كفاءة للمشكلة.
    2. تقييم الدليل: اشرح كيف ومتى يتم تقييم الدليل وكفاءة المهارة في القيام بذلك.
    3. مراجعة الافتراضات: اشرح طبيعة الافتراضات وأثرها على اتخاذ القرار وسبب الحاجة إلى معرفتها والتحدث عنها بوضوح وعلانية.
    4. مراجعة مفهوم الإنكار والخداع: اشرح عناصر مفهوم الإنكار والخداع وأثرها على التحليل.
C. طرق وضع التصورات

1 – التحليل الربطي: اشرح طبيعة الارتباط وكيف أن تحليل هذه يمكن أن يوفر الدليل أو يقود إلى عمليات تآمرية.

2 – أنماط التحليل: فهم الأنماط التي يمكن أن توجد وكيف يمكن أن تساعد هذه الأنماط في تطوير مؤشرات ومحاذير وسبب ذلك.

3 – تحليل الإطار الزمني: وضح استخدام الأطر الزمنية كأداة تنظيمية.

4 – تحليل تدفق المنتجات: وضح كفاءة حركة تدفق هذه الأشياء بالنسبة للأنشطة السرية.

D. أساليب التحليل البديلة:

1 – ماذا لو؟: ناقش كيفية النظر إلى الأحداث غير المتوقعة والتي لها تأثير كبير.

2 – تحليل الافتراضات المغايرة: فهم القدرة على استخدام تحليل الافتراضات المغايرة كأداة تحليلية.

3 – الفريق الأول – ضد الفريق الثاني: اشرح كيف يمكن أن يكون استخدام فرق المحللين في استقصاء وجهات النظر المختلفة فعالاً عند النظر في البدائل.

4 – المناظرات السفسطائية: اشرح كيف يمكن استخدام المناظرات السفسطائية في الكشف عن البدائل التحليلية.

5 – تقييم المراحل قبل النهائية: قم بتقييم ما قد يحدث في المستقبل في حالة اكتشاف أن نتائجك غير صحيحة.

**سابعاً المشاكل التحليلية**

أ – الدمج بين جامع / محلل البيانات: اشرح دور جامعي البيانات؛ وكيفية إيجاد الثغرات في الأدلة والعمل مع جامعي البيانات من أجل سد الثغرات.

ب – قواعد البيانات التحليلية: اشرح قواعد البيانات التحليلية المتاحة وكيفية استخدامها.

ج – برامج الكمبيوتر التحليلية: اشرح برامج الكمبيوتر التحليلية المتاحة ووضح كيفية استخدامها.

د – الأخلاقيات في مجال الاستخبارات: اختبر الحاجة إلى السلوك الأخلاقي في مجال الاستخبارات.

هـ - النتائج والمصادر التحليلية: اشرح الطرق المختلفة التي يمكن أن تكون من خلالها النتائج التحليلية فعالة بما في ذلك المصادر المتاحة في المصدر المفتوح.

و – مشاركة العملاء: افهم أهمية معرفة عملائك ومعرفة احتياجاتهم.

ز – المخاطر التحليلية: اشرح أمثلة عن المخاطر التاريخية في التفكير التحليلي واقترح طرقاً لتجنبها.

**ثامناً تخطيط الأدلة**

A. يختبر الطلاب تخطيط الأدلة ويقومون بعمل رسوم بيانية "من مربعات وأسهم" للمنطق وخصوصاً لعمليات الجدال والمناظرات المعقدة. يوضح تخطيط الأدلة قدرة الطلاب على صياغة المنطق والإيمان به وشرحه للآخرين ومن ثم تعزيز عملية التفكير الحرج.
B. يستخدم الطلاب طرق الرسوم البيانية في تخطيط الأدلة من أجل توضيح بنية المنطق والحجة. هذه الطريقة مهمة للتفكير الحرج المتطور. فبدون تخطيط من الصعب أن تكون واضحاً بشأن بنية الدليل، وبدون هذا الوضوح عادةً ما تأتي الاستجابات الحرجة بنتائج عكسية.

1. إتقان فن تخطيط الأدلة يساعد الطلاب على تنمية مهارات التفكير الحرج والمنطق العام.
2. صياغة حجج قوية وواضحة ومرتبة جيداً.
3. توصيل منطقك للطلاب.
4. استخدام التخطيط في تقييم المنطق.
5. استخدام التخطيط في حل الخلافات بطريقة منطقية.
6. استخدام التخطيط في اتخاذ قرارات أفضل.

**تاسعاً حالات دراسة**

أ – 1 – 3 حالات دراسة لتحليل من المهارات المهنية في بيئة تحاكي أرض الواقع

ب – 1 – 3 حالات دراسة لاستعراض المهارات في بيئة تحاكي أرض الواقع.

## مهنية مكافحة التجسس في الفضاء الإلكتروني – العمليات الإعلامية

**الجزأين الأول والثاني**

توضح هذه الدورة للطالب المبادئ الأساسية والعمليات في مجال مكافحة التجسس في الفضاء الإلكتروني مع التركيز على مهام مكافحة التجسس في الفضاء الإلكتروني وعمليات مكافحة التجسس الدفاعية وعمليات مكافحة التجسس الهجومية ومكافحة التجسس المضاد لأن هذه المجالات تنطبق على المهنية التقليدية وكيف ستبرز في نطاق الفضاء الإلكتروني. من خلال البدء بعمليات مكافحة التجسس التقليدي والانتقال إلى مكافحة التجسس في الفضاء الإلكتروني سيزيد لدى الطلاب تقدير جهود جمع المعلومات واستكشاف المخاطر المحتملة والمشاكل الداخلية ومخاطر ومزايا مكافحة التجسس.

مع زيادة أهمية الحاجة الكلية للاستخبارات في التوقيتات المناسبة للأمم وللشركات أيضاً، سوف يستعرض الطلاب العناصر الأساسية التي تشكل دوائر الاستخبارات مع التركيز على كيفية استعراض هذه النقاط المحورية. كجزء من هذه الدورة سوف يتم استعراض الأهمية المتزايدة للتفكير الحرج وأيضاً سوف يتم الحديث باستفاضة عن التحليل خارج الصندوق من أجل تنمية مهارات التفكير الحرج لدى الطلاب.
مع زيادة تطور مجالات الفضاء الإلكتروني تزداد أهمية استخبارات الفضاء الإلكتروني ولهذا سوف تزداد حماية دوائرنا الاستخباراتية أيضاً، مع التركيز على الحاجة المتزايدة إلى ضمان عدم الكشف عن عملياتنا في منظور الفضاء الإلكتروني. مكافحة التجسس في الفضاء الإلكتروني وربما هي أحد أكثر الموضوعات المهمة والحيوية في صلب جهودنا لجمع المعلومات. سوف تغطي الدورة احتمالات عمليات مكافحة التجسس الدفاعية الفعالة أو الهجومية بشكل متعمق.

سوف تعتمد هذه الدورة بقوة على عمليات البحث الفردية والمناقشات الجماعية لاستكشاف عالم مكافحة التجسس في الفضاء الإلكتروني، والاستفادة من قدرات الطلاب على التفكير في حل الواجبات العملية وتحليلها بشكل مستقل داخل الفصل من خلال جلسات المناقشة الأسبوعية.
تركز هذه الدورة على الاستخبارات مفتوحة المصدر والأعداء مع إنشاء ملفات شخصية على الإنترنت للمساعدة في جمع البيانات واستخلاص المعلومات.
تختبر هذه الدورة التمهيدية جمع الاستخبارات مفتوحة المصدر وأيضاً مدى توافر وإتاحة أدوات الاستخبارات مفتوحة المصدر واستخداماتها.

سوف يتم الطلاب من فهم استخدامات طرق إخفاء الهوية فقط، والأسس التي يعتمد عليها تطوير الملفات الشخصية في الفضاء الإلكتروني، والانضمام إلى مواقع التواصل الاجتماعي وتطبيقاتها واستخداماتها، وكيف يمكن نشر هذه الطرق الحالية في مؤسساتهم للمساعدة في عمليات أمن الفضاء الإلكتروني، ودفاعهم ضد الأعداء والجمع السلبي للبيانات.
يحتاج إنشاء ملفات شخصية على الإنترنت إلى الصبر والوقت اللازم لتأسيس مصدر موثوق. تحدث الأنشطة الموازية من خلال ما ذكرناه سابقاً. تحافظ Treadstone 71 على استقلاليتها عن العملاء حسب الحاجة من أجل الحفاظ على سرية الطرق والعمليات.

يمكن أن يعيد Sitreps والاستخبارات الحالية توجيه الأنشطة. الهدف هو إنشاء برنامج لاستخبارات الفضاء الإلكتروني والاستخبارات مفتوحة المصدر التي تخلق تياراً من البيانات للتحليل. تستغرق تيارات البيانات الوقت لكي تتطور وتتحول إلى روابط وتوجهات (trends) وميول وفي بعض الأحيان تتحول إلى تحليل قائم على التوقع والتنبؤ. الرغبة هي الانتقال من المنهج البوليسي إلى منهج وقائي مع التحول لكي يصبح منهج توقعي على نحو أشمل.

مكافحة التجسس في الفضاء الإلكتروني الجزء الأول – اختراق الفضاء الإلكتروني أو تنقيته، عمليات المعلومات، دعم المعلومات، دعم عمليات إستراتيجية المكافحة الوطنية للتجسس، قاموس وتصنيف قياسي، مكافحة التجسس القائمة على المهام، الجمع المضاد والتوقع، مفهوم الخداع والإنكار، مفهوم الخداع والإنكار المضاد، الفضاء الإلكتروني، الاستخبارات مفتوحة المصدر، طرق الجمع، الأدوات الخاصة، الأدوات المتخصصة، مواقع التواصل الاجتماعي والانضمام لها، طرق البحث على مواقع التواصل الاجتماعي، الطرق والأساليب، التوزيع الديموغرافي لمواقع التواصل الاجتماعي، تحديد متطلبات الأولويات الاستخباراتية، تحديد متطلبات المعلومات، استحواذ على الأهداف في الفضاء الإلكتروني واستغلالها، التحقق من الأهداف، التعرف على الحملات النشطة للأعداء، التعرف على النوايا والدوافع والأهداف والمتطلبات، الجمع السلبي للمعلومات، تطوير الحملات، استهداف المواقع، أساليب وطرق وإجراءات الانضمام للمواقع، نوايا وأهداف ودوافع ومتطلبات وأسباب الانضمام، دورات عملية، الاستثارة والحجب.

مكافحة التجسس في الفضاء الإلكتروني الجزء الثاني – المعرفة كنوع من الخداع، سيكولوجية المجتمع، الاختلافات الثقافية، التنوع، ونظرية هوفستد للأبعاد الثقافية، وعلم النفس الاجتماعي، ومفهوم التبادلية، والتجانس، والقبول المجتمعي، والاستحسان، والسلطة، والندرة، والعوامل الخمس الرئيسية للشخصية، وحرب المعلومات، والحروب النفسية في الفضاء الإلكتروني، وتحليل الأهداف والتلاعب بالرسائل كلما أمكن، وإنشاء ملفات شخصية، والتأسيس، والوقاية، والتوسع (بناءً على دراسة دورة الاستخبارات في الفضاء الإلكتروني)، وجمع البيانات، ودائرة تحديثات / تعديلات أو تحسينات Cyber CI، والتأليف للمدونات وكتابة مقالات من أجل التأثير، واستخدام مفاهيم وعبارات محددة.

مكافحة التجسس في الفضاء الإلكتروني الجزء الثالث – طبقة الملفات الشخصية في الفضاء الإلكتروني، إنشاء وتفعيل الملفات الشخصية، تطوير الملفات الشخصية في الفضاء الإلكتروني والحفاظ عليها، والأنماط الأولية للشخصية، وتطوير الملفات الحالية، وإنشاء ملفات جديدة، وتأسيس الحبكة الدرامية، وتلخيص القصة، وتغيير القصة والتحكم فيها، والعناق، وجمع وربط المعلومات والتوجهات والاتجاهات.

دورة التجسس في الفضاء الإلكتروني الجزء الرابع – الملفات الشخصية – الدوسيهات المستهدفة، تحليل الفجوات المستهدفة، تحديد المهمة لكي يمكن الربط بينها وبين الأهداف التنظيمية، وعمليات الجمع السرية للمعلومات، وعمليات الرصد، والرصد المضاد، وأنشطة الاستخبارات في الفضاء الإلكتروني، وتحليل وإنتاج أنشطة الاستخبارات في الفضاء الإلكتروني، وتحليل تقارير الاستخبارات في الفضاء الإلكتروني، ودعم الملخصات وتقييم المصدر وتقرير تحليل العمليات وتقييم الأصول وحزمة الدعم، وتقييم استخبارات في الفضاء الإلكتروني وحملات الاستخبارات في الفضاء الإلكتروني، والمهام وإدارة المهام، والعمليات التي تعتمد على التأثير أو إحداث أثر، والوظائف والخدمات.

دورة مكافحة التجسس في الفضاء الإلكتروني الجزء الخامس – التهديدات الداخلية لاستخبارات الفضاء الإلكتروني، التحريات، إعداد تقييم للوضع، إعداد الخطة، خطة الدعم، اختيار وساط الفضاء الإلكتروني، العمليات الأمنية على الإنترنت، وتطوير الإنتاج، الاختبارات الأولية – تحديد الأثر المحتمل على الجمهور المستهدف، إنتاج وتصنيف المواد، التنفيذ، الاختبارات اللاحقة بعد الدورة – تقييم ردود/استجابة الجمهور، الآراء والمقترحات، الوصايا العشر لمكافحة التجسس، البحث عن وتحليل طرق التأثير على الأعداء من مصادر معلومات مختلفة. العروض التقديمية للفرق / الأفراد.
محاضرة وتدريبات ودروس عملية وتدريبات داخل الفصل (وحالات دراسة واقعية)، وعروض الطلاب، والقوالب ومواد الدورة.

## الفضاء الإلكتروني السري والاستخبارات البشرية والاستخبارات مفتوحة المصدر التي تعتمد على الهدف

دورة الاستخبارات البشرية والاستخبارات مفتوحة المصدر في الفضاء الإلكتروني السري مصممة من أجل تزويد الطلاب بالتكتيكات والطرق والأساليب من أجل الحفاظ على إخفاء أثناء القيام بجمع المعلومات من الأعداء المستهدفين. فيما يلي توضيح غير شامل لما تغطيه هذه الدورة:
الاستخبارات مفتوحة المصدر
تعريف بالاستخبارات مفتوحة المصدر

فهم بروتوكولات فهرسة وتصنيف محركات البحث.
استراتيجيات وأدوات البحث المتطور على الويب العادي والويب العميق.
إخفاء المستندات الخاصة بالويب من محركات البحث واستعادة الصفحات التي تم حذفها من خوادم الويب.

البحث في المنتديات ومنديات النقاش الإلكترونية ومجموعات الأخبار والقوائم البريدية.
مقدمة عن البحث في الوسائط المتعددة، وسجلات الويب والبحث في مجتمع التدوين وشبكات التواصل الاجتماعي وقواعد بيانات موسوعات الإنترنت والخصوصية وإخفاء الهوية على الإنترنت.
أدوات تنسيق وتنظيم وترتيب الإنترنت
أساليب وطرق مكافحة التجسس في الاستخبارات مفتوحة المصدر التي تستخدمها العناصر الإجرامية.
خرائط مواقع الويب وطرق وأدوات أرشفتها.
مقدمة عن الاستخبارات مفتوحة المصدر وعمليات التحليل الاستخباراتي.
التخطيط الفعال لمشاريع الاستخبارات مفتوحة المصدر على الإنترنت.

فهم الاستخبارات مفتوحة المصدر

دورة الاستخبارات مفتوحة المصدر
أهداف جمع الاستخبارات مفتوحة المصدر
التوثيق الجيد
طرق التوثيق
أدوات التوثيق
وضع التصورات
تطبيقات كتابة الملاحظات
التوثيق
تطبيق / Hunchly
معالجة الكلمات
لقطات الشاشة
الخطوط الزمنية
تحديد ملف التهديدات الخاصة بك
العمليات الأمنية
الطرق التي قد تكشف ما تقوم به الاستخبارات مفتوحة المصدر
لاستهداف إعدادات منصة استخبارات مفتوحة المصدر
وسائط USB
خادم السحابة
الشبكات وبروتوكولات الشبكات الخاصة الافتراضية (VPNs)
متصفحات الويب
الامتدادات والإضافات المفيدة
الاستخبارات مفتوحة المصدر على الهواتف الجوالة
إدارة كلمات المرور
عادات البحث الفعالة
الاشتباك مع هدفك

Managing social media communities
Creating an inviting environment
Opinion Community
Creating and manipulating the buzz
Buzz campaign
Identifying fraudulent opinions
Measure what matters
Cast a wide net
Analyze the text
Establish links to performance metrics
Intelligence integration
Social Media demographics
Cyber Criminals
Methods of Social Media Research
Tools for Social Media Research – Collection and Discovery
Treadstone 71 Collection Toolkit
Social Media – People Searches
Basic Internet
Website Investigations
Social Media Investigations
Email, Phone, Address, People
Google Searching – Dorks
Discussion Forums
Search Operators
Google Guide
Quick Reference
Query Input
Understanding the Results
Search Tools
Services
Quick Reference
Media Image, Video & Document
Apps & Utilities
Targeted Social Media – Middle East / Iran

Government – Media
Google sites
Middle East Search
Privacy and Security Settings
Review and use of open source tools
Extensive list – examples / demonstration / use
Social Media – People Searches
Basic Internet
Website Investigations
Social Media Investigations
Email, Phone Address, People
Media – Image, Video, & Documents
Special Focus
Apps and Utilities
Google Hacks / Dorks
Advanced search techniques
People search
Addresses, phone numbers, user names, emails
Web page deconstruction
Backlinks
Website and user locations
Forums, discussion boards, newsgroups
Blogs and wikis
Open Source Data
Open Source Intelligence
Instant Messaging
Methods of secure communication
Monitoring for change
Google Plus
Google Hangouts
Chat Windows
Viber, Cyphr, Wicker, WhatsApp, Signal

البيانات الحساسة
تطهير المنصة الخاصة بك

النظر إلى الاستخبارات مفتوحة المصدر كمنصة جمع استخباراتية

القواعد الأساسية للاستخبارات مفتوحة المصدر

الخصوصية على الإنترنت / أدوات إخفاء الهوية
طرق مكافحة التجسس التي تستخدمها العناصر الإجرامية
نظم قواعد البيانات على الإنترنت
منهجية وأدوات الأرشفة وطرق الحصول على صفحات الأرشيف والمعلومات السرية المخفية
طرق البحث المتطورة للمدونات وشبكات التواصل الاجتماعي
طرق تحديد المواقع الجغرافية
تقنية التعرف على الصور
تعزيز نقل الملفات كبيرة الحجم
أفضل الطرق للاستفادة من إمكانيات لقطات الشاشة
تحليل وتنظيم وإعداد التقارير المكتوبة

التخطيط لجمع وتحليل الاستخبارات مفتوحة المصدر

شرح نقاط القوة ونقاط الضعف في الاستخبارات مفتوحة المصدر.
الوكلاء والخصوصية – احمِ نفسك أولاً
مناهج البحث
طرق البحث الأساسية

طرق البحث المتطورة
الديب ويب (الإنترنت العميق) الجزء الأول – البحث عن الأشخاص
الديب ويب (الإنترنت العميق) الجزء الثاني – السجلات العامة
قواعد البيانات المدفوعة – أفضل النظم للاستخدام، الطرق فعالة التكاليف، المزايا والمساوئ
الديب ويب (الإنترنت العميق) الجزء الثالث – شبكات التواصل الاجتماعي، والمدونات والمنتديات ونصائح البحث في مواقع التواصل الاجتماعي
طرق استخدام مواقع التواصل الاجتماعي في تحرياتك
محركات وأدوات البحث الدولية
المواقع المتخصصة
الأخبار المباشرة – في الوقت الفعلي
المواقع التجارية
الدخول على النشرات الدورية
المصادر المفتوحة الأخرى
الأدوات والتنزيلات
التنظيم والتحليل والتلخيص وكتابة التقارير – اكتب نتائجك بسهولة في تقرير رسمي
تطبيقات وأمن الهواتف الذكية

تقييم الدور الذي تلعبه الاستخبارات مفتوحة المصدر في العملية الاستخباراتية.

جمع وإنتاج الاستخبارات مفتوحة المصدر.
التخطيط والتوجيه
متطلبات الجمع
ما الذي تجمعه؟
PIRs و SIRs
جمع البيانات
تحليل البيانات
إيجاد نتائج للعميل
الأدوات والأساليب
أطر العمل
الطرق
أوراق بيانات الاستخبارات مفتوحة المصدر لدى Treadstone 71
متصفحات الاستخبارات مفتوحة المصدر
Maltego و Spiderfoot، Paliscope، و Shodan ومتصفح الاستخبارات مفتوحة المصدر (OSINT Browser) و Buscador
مصادر الويب الأخرى في الاستخبارات مفتوحة المصدر
قاعدة بيانات Google dorks و Google Hacking
مواقع التواصل الاجتماعي
Facebook, LinkedIn, Twitter, Instagram, more
Facebook، و LinkedIn، و Twitter، و Instagram وأكثر
أدوات تحديد المواقع الجغرافية
البيانات الفوقية (Metadata)
هيئات الاستخبارات مفتوحة المصدر
تخطيط جمع الاستخبارات مفتوحة المصدر – أوامر وترتيب العمليات على الفضاء الإلكتروني

تدرب هذه الدورة الطلاب وتعلمهم كيفية تثبيت واستخدام تطبيقات Tor، Tails، Maltego، Oryon، Buscador، Spiderfoot، Paliscope، Paliscope، IACA بالإضافة إلى SkyProxy و I2P بشكل غير حصري. سوف يتعلم الطلاب كيفية تثبيت هذه الأدوات من أجهزة الفلاش لديهم ( flash drives) والهدف منها هوالمساعدة في طرق إخفاء الهوية. (ملحوظة: لا يعمل برنامج Tails على جميع أجهزة الكمبيوتر المحمولة ويواجه صعوبات مع أجهزة الكمبيوتر المحمول المخصصة للألعاب وأجهزة الكمبيوتر المحمول الجديدة وصعوبات في بعض الأحيان مع أجهزة Apple. أجهزة الكمبيوتر

المحمول البسيطة جداً هي المطلوبة لتثبيت برنامج Tails.). سوف نجعلك تتعرف بشكل أعمق على طريقة عمل Tor، Tails و I2P بالإضافة إلى بعض النصائح والطرق للحفاظ على الأمن التشغيلي.

سوف يُمد الطلاب بفلاشات (flash drives) وبها الأدوات اللازمة لاستخدامها مع أجهزة الكمبيوتر المحمولة الخاصة بهم. سوف يقوم الطلاب بعملية تثبيت الأدوات واستخدامها في حالات الدراسة الواقعية التي تستهدف أعداءً حقيقيين. (ملحوظة: سوف تظل جميع الأنشطة التي يتم القيام بها في إطار القانون). سوف يستخدم الطلاب الأدوات المتضمنة في المتصفحات ونظم التشغيل والتطبيقات من أجل الحصول على خبرة عملية.

تغطي المرحلة الثانية من التدريب استخبارات مواقع التواصل الاجتماعي مع التركيز على الاستحواذ على الأهداف واستغلالها. باستخدام مجموعة أدوات إخفاء الهوية، يمكن للطلاب عمل حالات دراسة من أجل جمع معلومات عن الأعداء بكفاءة. سوف يقوم الطلاب بإنشاء حسابات متعددة على مختلف منصات الويب وتطبيقات وسائل التواصل الاجتماعي والتطبيقات الأخرى المستخدمة في الاتصالات المشفرة أو مع إخفاء الهوية.

عمليات OPSEC المتطورة
تطوير الملفات الشخصية والحفاظ عليها
الحبكة الدرامية والشخصيات والتقلبات والمحاكاة
الاستحواذ على الهدف واستغلاله
الحملات
النوايا والدوافع والأهداف والمتطلبات
التحليل الثقافي الاجتماعي
APTs الحالية
مفاهيم الفرق الحمراء
الجمع السلبي للمعلومات
العمليات النفسية

تغطي المرحلة الثالثة من التدريب تطوير وإدارة الملفات الشخصية. سوف يُطلب من الطلاب إنشاء مجموعة من الملفات الشخصية بهويات مختلفة، وتطوير الشخصية والأبعاد (الدوافع والمنهجية والتقييم والغرض)، والحبكة الدرامية، ورسم الملخص، ودوافع ومحدودية القصة، وتقلبات القصة وإمكانية استخدامها ونطاقها والأدوات المستخدمة وطرق التفاعل مع الهويات الأخرى وإشراك شخصيات ثانوية وتنقيح الأهداف مع تطوير حملة من أجل اكتساب المصداقية لدى الشارع.

سوف تستعرض المرحلة الأخيرة من الدورة الدخول على الإنترنت المظلم (Darknet) وأدوات ومواقع الاستكشاف ومواقع الموسوعات والمواقع الأخرى الحالية المعروفة.

المرحلة الثانية

**وصف الدورة:**

تختبر هذه الدورة التمهيدية جمع الاستخبارات مفتوحة المصدر وأيضاً مدى توافر وإتاحة واستخدامات أدوات الاستخبارات مفتوحة المصدر. سوف يتمكن الطلاب من فهم استخدام طرق إخفاء الهوية فقط، والأساسيات وراء تطوير الملفات الشخصية على الإنترنت والانضمام لمختلف مواقع التواصل الاجتماعي وتطبيقاتها وكيف يمكن توظيف هذه الطرق الحديثة في مؤسساتهم للمساعدة في CYBER-OPSEC (العمليات الأمنية على الفضاء الإلكتروني)، ودفاعاتهم ضد الأعداء والجمع السلبي للمعلومات.

مواقع تلميع الأعداء والمنتديات وغرف الدردشة والمواقع الشخصية من أجل تجميع أجزاء المعلومات المستخدمة في الإضرار بالحكومات والمؤسسات التجارية. والتعرف على استخبارات الفضاء الإلكتروني، والاستخبارات مفتوحة المصدر والعمليات الأمنية في الفضاء الإلكتروني وكفاءة تسليح الطلاب بالأدوات لجمع نقاط المعلومات، وتحويل نقاط المعلومات هذه إلى استخبارات عملية كافية للتدخل تمنع مهاجمة الأهداف. سوف يتعلم الطلاب طرق إنشاء وإدارة الملفات الشخصية بالإضافة إلى الجمع السلبي للمعلومات التي تقود إلى المصداقية لدى الشارع.