الوحدة 10

تحليل التهديد

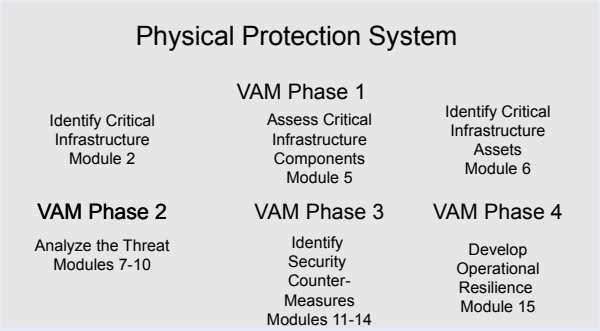
هدف الوحدة

- يتمكن المشاركون بنهاية هذه الوحدة من القيام بعمل بيان تحليل التهديد في نطاق البنية الأساسية الحرجة.

Module Objective

- By the end of this module, you will be able to create a threat analysis statement for critical infrastructure

نظام الحماية المادية



الغرض من تحليل التهديد

- جمع البيانات الخاصة بالتهديد
- تحديد مصادر البيانات
- إعداد البيان الخاص بتحليل التهديد
- تحقيق المتطلبات المتعلقة بتصميم نظام الحماية المادية

Purpose of the Threat Analysis

- Gather threat data
- Identify data sources
- Prepare threat analysis statement
- Establish physical protection system design requirements

بيان تحليل التهديد (1 من 2)

- التعرف على القدرات التهديدية المحتملة أو الموثوقة
- يمثل تقييم يقوم به مجموعة من الكوادر العليمة والمؤهلة باستخدام كافة المعلومات المتاحة.

Threat Analysis Statement (1 of 2)

- Identifies potential or credible threat capabilities
- Represents an assessment by informed and qualified people using available information

بيان تحليل التهديد (2 من 2)

- يساعد مصممي نظام الحماية المادية على تحديد المتطلبات الأساسية لنظام الأمن المادي بالبنية الأساسية الحرجة.
- المراجعة والتحديث كما تقتضي الضرورة

Threat Analysis Statement (2 of 2)

- Helps determine the basic requirements of a critical infrastructure's physical protection system
- Review and update as necessary

عينة من بيان تحليل التهديد لدراسة الحالة (1 من 3)

راجع

راجع النشرة10.1

- الغرض: هو فحص ومناقشة عينة بيان تحليل التهديد المستنبط من حالة دراسية بعينها
  - المدة: 30 دقيقة (20 دقيقة للقراءة؛ 10 دقائق للمناقشة)
  - تركيبة المجموعة: مجموعات كل طاولة
  - استخلاص المعلومات: نقاش يدور في إطار مجموعة كبيرة

Sample Threat Analysis Statement Case Study (1 of 3)	Refer To: Handout 10.1

- Purpose: to examine and discuss a sample threat analysis statement from a given case study
  - Duration: 30 minutes (20-reading; 10-discussion)
  - Group composition: table groups
  - Debrief: large-group discussion

عينة من بيان تحليل التهديد لدراسة الحالة (2 من 3)

راجع

راجع النشرة10.1

- المنشأة: معمل الطاقة النووية في بليندابا، جنوب أفريقيا
- تهديد محدد: إرهابي، تخريب إشعاعي
- تهديد موثوق: إرهابي، سرقة أو تمويه بتحويل مسار مواد نووية

Sample Threat Analysis Statement Case Study (2 of 3)	Refer To: Handout 10.1

- Facility: nuclear power plant in Pelindaba, South Africa
- Specific threat: terrorist, radiological sabotage
- Credible threat: terrorist, theft, or diversion of special nuclear material

عينة من بيان تحليل التهديد لدراسة الحالة (3 من 3)

راجع

راجع النشرة10.1

- ما هي المعلومات الحساسة التي لم يتم إدراجها في عينة تحليل التهديد؟
- ما هي بعض النقاط البارزة في بيان تحليل التهديد؟
- ما هي بعض جوانب الفشل في التدابير الأمنية المضادة؟

Sample Threat Analysis Statement Case Study (3 of 3)	Refer To: Handout 10.1

- What critical information was not included in the sample threat analysis?
- What were some of the significant points of the threat analysis statement?
- What were some of the security countermeasure failures?

التهديدات المحتملة من الخصوم

- يغطي هذا القسم ما يلي:
  - فئات الخصوم
  - التصرفات المحتملة للخصم
  - دوافع الخصم
  - تكتيكات الخصم
  - قدرات ومحدوديات الخصم

Potential Adversary Threats

- This section will cover:
  - Adversary categories
  - Potential actions of an adversary
  - Adversary motivations
  - Adversary tactics
  - Adversary capabilities and limitations

فئات الخصوم (1 من 2)

- العناصر الداخلية -- الأفراد الذين لديهم تصريح بالنفاذ
- العناصر الخارجية -- الأفراد الذين ليس لديهم تصريح بالنفاذ
- العناصر الداخلية تعمل بالتواطؤ مع العناصر الخارجية

Adversary Categories (1 of 2)

- Insiders — individuals with authorized access
- Outsiders — individuals without authorized access
- Insiders working together with an outsider

فئات الخصوم (2 من 2)

- الإرهابيون
- المجرمون
- الموظفون الغاضبون
- النشطاء
- المختلّون عقلياً

Adversary Categories (2 of 2)

- Terrorists
- Criminals
- Discontented employees
- Activists
- Mentally ill persons

العناصر الداخلية

- أخطر الخصوم بسبب:
  - المعرفة
  - الدخول
  - الفرصة
  - الدافع
- تتضمن:
  - الموظفين والمتعاقدين
  - الباعة والزوار

Insiders

- Most dangerous adversary because of:
  - Knowledge
  - Access
  - Opportunity
  - Motivation
- Includes:
  - Employees and contractors
  - Vendors and visitors

دراسة حالة إطلاق النار في ساحة واشنطن البحرية (1 من 2)

راجع

راجع النشرة10.2

- الغرض: تعريف التهديد المتضمن في دراسة الحالة
  - المدة: 10 دقائق (5 دقائق دراسات الحالة؛ 5 دقائق لاستخلاص المعلومات)
  - تركيبة المجموعة: مجموعات كل طاولة
  - استخلاص المعلومات: نقاش يدور في إطار مجموعة كبيرة

Washington Navy Yard Shooting Case Study (1 of 2)

Refer To:

Handout 10.2

- Purpose: to identify the threat involved in the case study
  - Duration: 10 minutes (5-case study; 5-discussion)
  - Group composition: table groups
  - Debrief: large-group discussion

دراسة حالة إطلاق النار في ساحة واشنطن البحرية (2 من 2)

Washington Navy Yard
Shooting Case Study (2 of 2)

العناصر الإرهابية

- الخصائص:
  - تحركهم الدوافع السياسية أو الأهداف الإجتماعية
  - القيام بعمليات المراقبة المعادية
  - التخطيط للقتل لتحقيق الأهداف
  - استخدام متفجرات، أو أسلحة أوتوماتيكية، أو كلتيهما.
  - الإستعداد للمخاطرة بالوقوع في يد السلطات أو الإصابة أو الوفاة
  - استهداف البنية الأساسية الحرجة

Terrorists

- Characteristics:
  - Are motivated by political or social objectives
  - Conduct hostile surveillance
  - Plan to kill to achieve goals
  - Use explosives, automatic weapons, or both
  - Will risk capture, injury, or death
  - Target critical infrastructure

العناصر الإجرامية

- عادة ما تحركهم دوافع الربح المادي
- تطوير شبكات مالية لتمويل النشاطات الإرهابية
- السعي لتجنب الرصد والوقوع في يد السلطة

Criminals

- Often motivated by financial gain
- Develop financial networks to fund terrorist activity
- Seek to avoid either capture or detection

الموظفون الغاضبون (1 من 2)

- الإحساس بسوء المعاملة من المدير أو الخلافات مع زملاء العمل
- قد يقوم الموظفون الساخطون بتعطيل سير العمل الروتيني عن طريق السلوك العدواني، والسرقة، والتخريب واستخدام العنف.
- ربما يتعرضون لخطر الإنكشاف وإلقاء القبض عليهم.

Discontented Employees (1 of 2)

- Perceived mistreatment by boss or disagreements with coworkers
- May disrupt known routines with aggressive behavior, theft, sabotage, or force
- May risk capture or detection
- May use fear and intimidation
- May be an insider or an outsider with insider information

الموظفون الغاضبون (2 من 2)

- عادة ما يستخدمون الخوف والترهيب
- وقد يكون الموظف المستاء عنصرا داخليا أو خارجيا وله وسيلة نفاذ للمعلومات الداخلية

Discontented Employees (2 of 2)

- May use fear and intimidation
- May be an insider or an outsider with insider information

النشطاء

- معارضة البرامج البيئية، والسياسية والإقتصادية
- استخدام تكتيكات عنيفة أو غير عنيفة في المواجهة المباشرة
- احتمال محاولة الإلتفاف حول العوائق (السياجات والأسوار)
- قد تتضمن عناصر داخلية أو خارجية

Activists

- Oppose ecological, political, and economic programs
- May use violent or nonviolent tactics for direct confrontation
- May attempt to defeat barriers (fences and walls)
- May be insider or outsider

المختلّون عقلياً(1 من 2)

- تاريخ أو سجل جنائي ينطوي على خلل عقلي أو عنف من جانب افراد العائلة
- علاقة معرفة مع أعضاء منظمة إرهابية
- سلوك ظاهر تحت تأثير الكحول أو المخدرات أو سائر العقاقير

Mentally Ill Persons (1 of 2)

- Known criminal with mental illness history or family history of violence
- Known member of a terrorist organization
- Appearance of being under the influence of alcohol or other drugs

المختلّون عقلياً(2 من 2)

- مرض عقلي غير واضح التشخيص بدون أعراض ظاهرة
- قد تتضمن عناصر داخلية أو خارجية

Mentally Ill Persons (2 of 2)

- Undiagnosed mental illness with no outward signs
- May be insider or outsider

سؤال للمناقشة

- ما هي بعض الأمثلة حول الإضرار بأصول البنية الأساسية الحرجة من جانب العناصر الإرهابية أو الإجرامية أو الموظفين الساخطين أو المتخلفين عقلياً في بلدك؟

Discussion Question

- What are some examples of damage to critical infrastructure assets caused by terrorists, criminals, discontented employees, or mentally ill persons in your country?

التصرفات المحتملة للخصم (1 من 2)

- النظر في أنماط الجرائم والهجمات الإرهابية التي تدخل في دائرة اهتمام تلك الفئات المختلفة من الخصوم وخصوصا التي يستطيعون ارتكابها
- تحديد أي من تلك الأفعال تشكل تهديدا حقيقيا على موقع معين
- دراسة الأمثلة والتوجهات التاريخية

Potential Actions of an Adversary (1 of 2)

- Consider the types of crimes and terrorist attacks these various adversaries are interested in and capable of carrying out
- Determine which of these acts pose a credible threat to the specific site
- Study historical examples and trends

التصرفات المحتملة للخصم (2 من 2)

- التخريب -- التدمير المتعمد الخبيث أو التسلل لإلحاق الضرر
- السرقة -- الحيازة غير المشروعة للممتلكات، والمعدات، أو المعلومات
- تحويل مسار المواد -- نقل أو تحريك غير مشروع
- سائر أعمال العنف -- ضد الأصول الحرجة للأفراد

Potential Actions of an Adversary (2 of 2)

- Sabotage — deliberate and malicious destruction or intrusion
- Theft — unlawful possession of property, equipment, or information
- Diversion of materials — unlawful movement or transfer
- Other violent acts — against critical people assets

دوافع الخصم

- سياسية
- فلسفية
- اجتماعية
- اقتصادية
- شخصية

Adversary Motivations

- Political
- Philosophical
- Social
- Economic
- Personal

التكتيكات الإرهابية (1من 2)

- يتضمن تحليل التهديد جزئيا فحص التكتيكات التي ينتهجها كل خصم محتمل.
- وقد تشمل التكتيكات العناصر التالية بصفة منفردة أو معا:
  - الخلسة -- القيام بالمهمة دون رصد أو مراقبة

Terrorist Tactics (1 of 2)

- Part of the threat analysis involves examining the tactics of each potential adversary
- Tactics may include or be a combination of:
  - Stealth — perform a task undetected

التكتيكات الإرهابية (2 من 2)

- القوة -- الدخول عن طريق استخدام العنف
- الخداع -- تقديم معلومات مزيفة لتحقيق الدخول
- المساعدة على تحسين تصميم نظام الحماية المادية

Terrorist Tactics (2 of 2)

- Force — gain access through the use of violence
- Deceit — provide false information to gain access
- Help enhance the design of the physical protection system

قدرات ومحدوديات الخصم

- تحديد متطلبات أداء النظام
- تعريف التهديد بشكل أوضح
- تضمين الإعتبارات الخاصة كالتالي:
  - الأفراد
  - المعرفة، والمهارات والخبرات
  - نوع وكمية الأسلحة
  - الأدوات والمعدات
  - النقل

Adversary Capabilities and Limitations

- Determine system performance requirements
- Define threat more clearly
- Include specific considerations of:
  - Personnel
  - Knowledge, skills, and experience
  - Types and quantity of weapons
  - Tools and equipment
  - Transportation

لحظة التعليم الإسترجاعي

- لماذا من المهم تحليل التهديد؟
- ما هي الأنواع المختلفة لتهديدات الخصم؟

TeachBack Moment

- Why is it important to analyze the threat?
- What are the different types of adversary threats?

مصادر معلومات تتعلق بتهديدات محتملة (1 من 4)

- تساعد المعلومات في تحديد التهديد:
  - أصول البنية الأساسية الحرجة المستهدفة
  - هدف الخصم

Information Sources on Potential Threat (1 of 3)

- Threat information helps define the threat:
  - The targeted critical infrastructure asset
  - Adversary's objective

مصادر معلومات تتعلق بتهديدات محتملة (2 من 4)

- الاتصال بمنظمات يمكن أن تقدم معلومات
- تتضمن مصادر المعلومات عن التهديد:
  - تقارير وكالات تطبيق القانون
  - تقارير الإستخبارات الخاصة بالدول المجاورة
  - تقارير البيانات الخاصة بالتهديد القومي (الذي يتعرض له الوطن)

Information Sources on Potential Threat (2 of 4)

- Communication with organizations that can provide information
- Sources of threat information include:
  - Law enforcement reports
  - In-country intelligence reports
  - National threat data reports

مصادر معلومات تتعلق بتهديدات محتملة (3 من 4)

- الجيش ووكالات إنفاذ القانون
- وكالات الاستخبارات الدولية
- تقارير الحوادث بالموقع
- تقارير عن الأنشطة الإجرامية أو الإرهابية بالمنطقة

Information Sources on Potential Threat (3 of 4)

- Military and law enforcement agencies
- International intelligence agencies
- Site incident reports
- Reports of criminal or terrorist activities in the area

مصادر معلومات تتعلق بتهديدات محتملة (4 من 4)

- قوائم بيانات الإتصال الخاصة بأنشطة تطبيق القانون
- عدد وأنواع الأفراد المتواجدين في المنشأة
- أية معلومات متوافرة عن التهديد

Information Sources on Potential Threat (4 of 4)

- Contact lists for law enforcement activities
- Number and types of personnel at the facility
- Any available threat information

أسئلة المناقشة

- ما هي سائر الإقتراحات بخصوص مصادر المعلومات المتعلقة بالتهديدات المحتملة في بلادكم؟
- ما هي أنواع المصادر المماثلة من الإحصائيات التي لدى حكومتكم عن الأنشطة الإرهابية؟

Discussion Questions

- What are other suggestions for sources of information about potential threats in your country?
- What types of similar sources of statistics on terrorist activities does your government have?

تنظيم معلومات التهديد

- قوالب معلوماتية تساعد في تسهيل عملية اتخاذ القرارات الحرجة:
  - ما هي التهديدات الواجب إدراجها في نطاق التهديد؟
  - ماهو مدى فعالية نظام الحماية المادية القائم لدينا؟
- إدراج أنماط الخصوم، من العناصر الداخلية والخارجية معاً، في بيان تحليل التهديد

Organizing Threat Information

- Formats information to help facilitate the critical decision-making process:
  - Which threats should be included in the threat spectrum?
  - What is the effectiveness of the existing physical protection system?
- Includes both types of adversaries, insider and outsider, in the threat analysis statement

عوائق التفكير التحليلي (1 من 2)

راجع

الكتيب10.1

- يساعد الوعي بالعوائق الشائعة على تحقيق ما يلي:
  - تفادي الأخطاء الحساسة التي يمكن أن تؤثر سلبا على حماية الأصول الحيوية للبنية الأساسية الحرجة
  - تسهيل عملية الفكر التحليلي بشأن نظام الحماية المادية

Barriers to Analytical Thinking (1 of 2)

Refer To:
Workbook 10.1

- An awareness of common barriers will help:
  - Avoid critical mistakes that could negatively affect critical infrastructure protection
  - Facilitate the analytical thought process relating to the physical protection system

عوائق التفكير التحليلي (2 من 2)

راجع

الكتيب10.1

- التركيز على الحقائق وليس الآراء الشخصية
- استخدام عمليات التفكير التحليلي للتغلب على العوائق

Barriers to Analytical Thinking (2 of 2)

Refer To:
Workbook 10.1

- Focus on facts not personal opinions
- Use analytical thinking processes to overcome barriers

أسئلة المناقشة

- من واقع خبراتك الخاصة، ما هي أنماط العوائق التي تعترض تفكيرك التحليلي؟
- ما هي الاجراءات التي ستتخذها لمنع أو تفادي تلك العوائق؟

Discussion Questions

- In your experience, which types of barriers to analytical thinking have you encountered?
- What actions could you take to prevent or avoid these barriers?

المحصلات البديلة وأساليب التفكير

راجع

الكتيب10.1

- مناصرة الرأي المقابل
- تحليل الفريق أ أو الفريق ب
- تحليل الفريق الآخر
- تحليل "ماذا لو؟"
- العواقب ذات الإحتماليات المرتفعة وتحليل الإحتمالات المنخفضة
- التفكير من الخارج للداخل
- الألعاب والمحاكاة

Alternative Outcome Thinking Techniques	Refer To: Workbook 10.1
▪ Advocating the opposite view ▪ Team A or Team B analysis ▪ Other team analysis ▪ “What if?” analysis ▪ High consequence and low probability analysis ▪ Outside-in-thinking ▪ Gaming and simulation	

ورقة العمل الخاصة بمعلومات تهديد العناصر الداخلية

- الشروع في تحليل التهديد بالنظر في التهديدات الداخلية المحتملة الفريدة التي تفرضها العناصر الداخلية في منشآت البنية الأساسية الحرجة
- تصنيف وتنظيم معلومات التهديد الداخلي في ورقة العمل


Source: DOL.GOV

Insider Threat Information Worksheet

- Begin threat analysis by considering unique potential insider threats posed by insiders at the critical infrastructure facility
- Rate and organize the insider threat information on a worksheet

نشاط ورقة العمل الخاصة بمعلومات تهديد العناصر الداخلية

راجع


الكتيب 10.2

- الغرض: المساعدة في تنظيم المعلومات التي يتم جمعها عن التهديدات الداخلية
  - المدة: 15 دقيقة (5 دقائق للقراءة؛ 10 دقائق للمناقشة)
  - تركيبة المجموعة: مجموعات كل طاولة
  - استخلاص المعلومات: نقاش يدور في إطار مجموعة كبيرة

Insider Threat Information Worksheet Activity	Refer To: Workbook 10.2

- Purpose: to help organize gathered information about insider threats
  - Duration: 15 minutes (5-reading; 10-discussion)
  - Group composition: table groups
  - Debrief: large-group discussion

ورقة العمل الخاصة بمعلومات التهديد الخارجي

راجع

الكتيب 10.3

- يتم تنظيمها عن طريق تقييم التهديد المحتمل:
  - الإجراءات
  - الدوافع
  - التكتيكات
  - القدرات

Outsider Threat Information Worksheet	Refer To: Workbook 10.3

- Organized by an assessment of potential threat:
  - Actions
  - Motivations
  - Tactics
  - Capabilities

نشاط ورقة العمل الخاصة بالتهديد الخارجي

راجع


الكتيب10.3

- الغرض: المساعدة في تنظيم المعلومات التي يتم جمعها عن التهديدات الخارجية
  - المدة: 15 دقيقة (5 دقائق للقراءة؛ 10 دقائق لاستخلاص المعلومات)
  - تركيبة المجموعة: مجموعات كل طاولة
  - استخلاص المعلومات: نقاش يدور في إطار مجموعة كبيرة

Outsider Threat Worksheet Activity	Refer To: Workbook 10.3

- Purpose: to help organize gathered information about outsider threats
  - Duration: 15 minutes (5-reading; 10-debrief)
  - Group composition: table groups
  - Debrief: large-group discussion

تقييم احتمال وقوع هجوم (1 من 2)

راجع


الكتيب 10.4

- تحديد المعلومات عن كل إرهابي:
  - نمط التهديد
  - القدرة
  - التاريخ والنوايا
  - جاذبية الهدف

Estimating Likelihood of Attack (1 of 2)

Refer To: Workbook 10.4

- Determine information about each terrorist:
  - Threat type
  - Capability
  - History and intent
  - Target appeal (attractiveness)

تقييم احتمال وقوع هجوم (2 من 2)

راجع

الكتيب 10.4

- مقياس التصنيف:
  - منخفض جداً
  - منخفض
  - متوسط
  - مرتفع
  - مرتفع جداً
- المقياس الرقمي لتصنيف نمط التهديد 1 - 10 ، حيث يرمز رقم 10 إلى أقصى ارتفاع

Estimating Likelihood of Attack (2 of 2)	Refer To: Workbook 10.4

- Rating scale:
  - Very Low
  - Low
  - Medium
  - High
  - Very High
- Numerical scale to rate threat type: 1–10, with 10 being highest

نشاط ورقة العمل الخاصة بتقييم احتمال وقوع هجوم

راجع


الكتيب 10.4

- الغرض: تقديم مثال للمساعدة في تقييم احتمالات وقوع هجوم صادر عن تهديد تم تحديده
  - المدة: 25 دقيقة (20 دقيقة للنشاط، و 5 دقائق لاستخلاص المعلومات)
  - تركيبة المجموعة: مجموعات كل طاولة
  - استخلاص المعلومات: نقاش يدور في إطار مجموعة كبيرة

Estimating Likelihood of Attack Worksheet Activity	Refer To: Workbook 10.4

- Purpose: to provide an example to help you estimate the likelihood of attack of an identified threat
  - Duration: 25 minutes (20-activity; 5-debrief)
  - Group composition: table groups
  - Debrief: large-group discussion

خطوات إعداد بيان تحليل التهديد

راجع


الكتيب 10.5

1. مقارنة احتمالات الهجوم بالنسبة لكل نمط من أنماط التهديد
2. التعرف على أكثر أنماط التهديد بالنسبة لاحتمال حدوثها
3. إعداد بيان تحليل التهديد

Steps to Prepare Threat Analysis Statement	Refer To: Workbook 10.5
1. Compare the likelihood of attack for all threat types 2. Identify the most likely threat type 3. Prepare threat analysis statement	

إعداد نشاط بيان تحليل التهديد

راجع

- **الغرض: إعداد بيان تحليل التهديد في سيناريو معين**
  - **المدة: 15 دقيقة (10 دقائق للنشاط، و 5 دقائق لاستخلاص المعلومات)**
  - **تركيبة المجموعة: مجموعات كل طاولة**
  - **استخلاص المعلومات: نقاش يدور في إطار مجموعة كبيرة**

Preparing a Threat Analysis Statement Activity	Refer To: Workbook 10.5

- Purpose: to prepare a threat analysis statement using a given scenario
  - Duration: 15 minutes (10-activity; 5-debrief)
  - Group composition: table groups
  - Debrief: large-group discussion

مناقشة المشاركة المجتمعية وحقوق الإنسان

- ما هي أهمية اشراك المجتمع في تحديد أنواع التهديدات التي قد تكون قائمة بالفعل؟

Community Engagement
and Human Rights Discussion

- Why is it important to engage the community in determining the types of threats that may exist?

التمرين التفصيلي المقسّم، الجزء3
مبنى الوزارات الوطنية

راجع

دفتر الواجبات الجزء 3

- **الغرض: إعداد بيان تحليل التهديد**
  - **المدة: 60 دقيقة (45 دقيقة للتمرين؛ 15 دقيقة لاستخلاص المعلومات)**
  - **تركيبة المجموعة: مجموعات كل طاولة**
  - **استخلاص المعلومات: العروض والمناقشة**

Threaded Exercise Part 3 — National Ministries Building

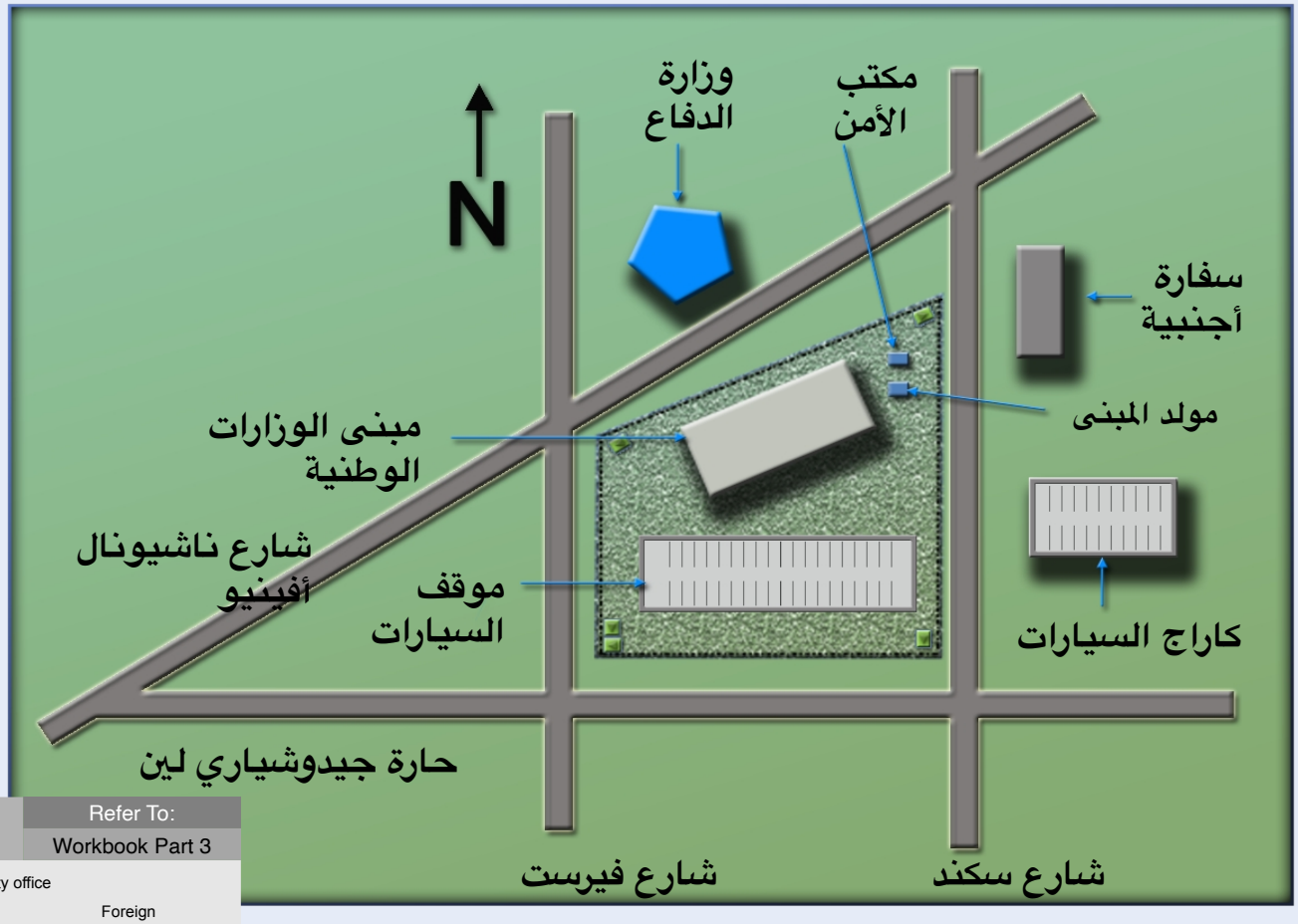
Refer To: Workbook Part 3

- Purpose: to prepare a threat analysis statement
  - Duration: 60 minutes (45-exercise; 15-debrief)
  - Group composition: table groups
  - Debrief: presentation and discussion

خريطة مجمّع مبنى الوزارات الوطنية

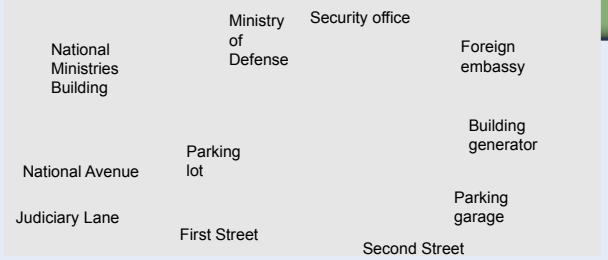
راجع

دفتر الواجبات الجزء 3



National Ministries Building Complex Map

Refer To: Workbook Part 3



ملخص الوحدة

- الغرض من تحليل التهديد
- التهديدات المحتملة من الخصوم
- مصادر معلومات تتعلق بتهديدات محتملة

Module Summary

- Purpose of the threat analysis
- Potential adversary threats
- Information sources on potential threat