آمادگی دفاع سایبری

ارائه دهنده : خالق گرجی

فهرست مطالب

تعاریف

تمرین/رزمایش سایبری:

- عبارت است از مجموعه اتفاقات طرح ریزی شده به منظور ایجاد و ارتقاء توانمندیها و آمادگی‌ها و ارزیابی آنها در یک سازمان که به منظور پیشگیری از حملات سایبری،کشف و کاهش تاثیرات و واکنش به آن، اجرا می‌شود.
- یک رویداد برنامه‌ریزی شده که طی آن یک سازمان یک اختلال سایبری را برای توسعه یا آزمایش قابلیت هایی مانند جلوگیری ، شناسایی ، کاهش ، پاسخ یا بهبودی از اختلال شبیه سازی می کند.[1]
- از تمرین‌های سایبر برای شبیه سازی محیط های حادثه سایبر برای ارزیابی دانش و مهارت پرسنل امنیت اطلاعات استفاده می شود. استفاده از تمرین سایبر برای ارزیابی آمادگی جامعه در برابر بحران سایبری و حوادث مهم زیرساخت اطلاعاتی گسترش یافته است.

1. *Source: NICCS™ Portal Cybersecurity Lexicon, National Initiative for Cybersecurity Careers and Studies (https://niccs.us-cert.gov/glossary) as of 11 November 2015*
2. **A Cyber Exercise Post Assessment: Adoption of the Kirkpatrick Model**: Arniyati Ahmad, Christopher Johnson, Timothy Storer

اهداف اجرای تمرین/رزمایش سایبری

- آزمودن میزان آمادگی خودی در برابر تهدیدات و حملات
- استخراج نقاط ضعف و قوت در برابر تهدیدات
- استخراج آسیب‌پذیری‌های موجود در سامانه‌های عملیاتی
- آموزش متخصصین سایبری
- ایجاد فرصتی جهت بکارگیری تجربیات
- ایجاد زیرساخت‌های فنی
- افزایش سطح همکاری بین تیم‌های شرکت کننده در برابر رخدادها و حوادث سایبری

برخی برنامه ها و سازمان‌های مهم برگزار کننده تمرین سایبری در دنیا

- Locked Shields,

بزرگترین ، پیچیده ترین پیشرفته‌ترین تمرین دفاع سایبری است که توسط مرکز تعالی دفاع سایبری مشارکتی ناتو “CCD COE در " تالین" پایتخت "استونی" برگزار می‌شود. این تمرین سایبری در سال ۲۰۱۷ با حضور بیش از ۹۰۰ متخصص امنیت سایبری از سراسر جهان و و تیم‌های مدافع سایبری ۲۰ کشور برگزار شد. در این تمرین که در آن بیش از ۳۰۰۰ سیستم مجازی درگیر بودند، بیش از ۲۵۰۰حمله به تیم های مدافع انجام شد. در این تمرین/مانور سیستم های شبکه هوشمند ، سیستم های سوخت رسانی هوا به هوا و سیستم های کنترل هواپیماهای بدون سرنشین در سال ۲۰۱۷ به محیط تمرین و مانور سایبری اضافه شدند.

برخی برنامه ها و سازمان‌های مهم برگزار کننده تمرین سایبری در دنیا

- Cyber Coalition

ائتلاف سایبری یک تمرین جمعی بین اعضای ناتو است که جنبه رقابتی ندارد و برای حل مشکلات و تمرین انجام وظایف مشخص ، برای رسیدن به یک هدف خاص کار می کنند.

ائتلاف سایبری سه هدف اساسی را دنبال می کند:

- برای **تعامل بین ناتو** ، متحدان و شرکا برای بهبود همکاری در حوزه فضای مجازی با مکانیزم های موجود
- **افزایش توانایی اتحاد** در انجام عملیات فضای مجازی برای نهادهای نظامی و غیرنظامی با استفاده از **توسعه آگاهی وضعیتی** ، به **اشتراک گذاری اطلاعات** فضای مجازی و **مدیریت حوادث** سایبری ،
- شناسایی ضعف توانایی ، جهت احصاء نیازهای آموزشی.

این ائتلاف سایبر همه ساله توسط ناتو سازماندهی می شود. این یک رویداد سه روزه است و مشارکت اعضای ناتو و کشورهای متحد است.

برخی برنامه ها و سازمان‌های برگزار کننده تمرین سایبری در دنیا

- Cyber Europe

این برنامه توسط ENISA[1] (آژانس اتحادیه اروپا برای شبکه و امنیت اطلاعات) ، هر دو سال یکبار برای اعضای اتحادیه اروپا برگزار می شود. بر خلاف تمرین های مستقر در ارتش مانند Lock Shields و ائتلاف سایبر ، این تمرین توسط یک مقام غیرنظامی برگزار می شود. این رزمایش که در سال ۲۰۱۶ برگزار شد ، شامل ۲۸ کشور عضو اتحادیه اروپا و ۲ کشور عضو " اتحادیه تجارت آزاد اروپا" (EFTA)[2] بود ، گرچه این کشورها عضو اتحادیه اروپا نیستند.

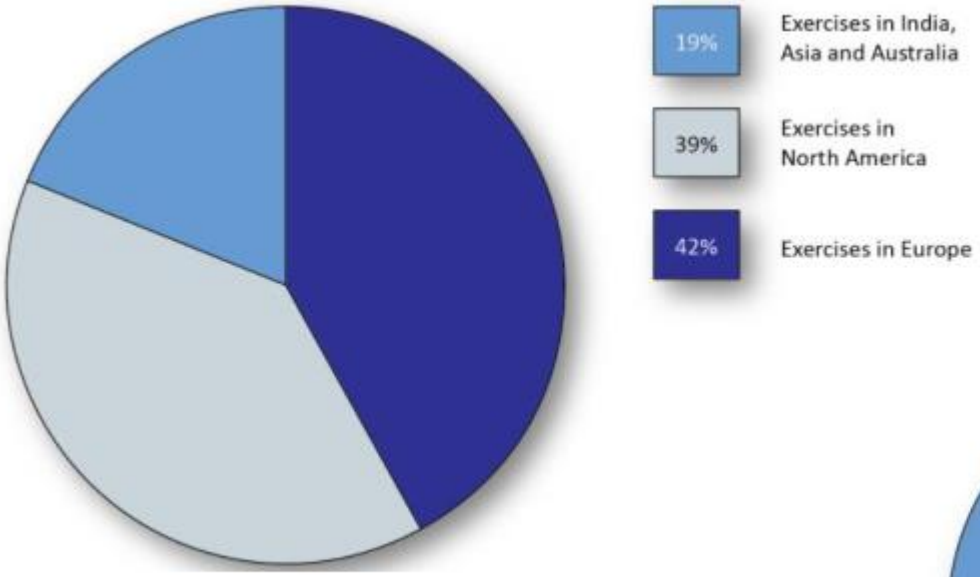
- Cyber Defence Exercise(CDX)

یک رقابت سالانه است که توسط اداره تضمین اطلاعات متعلق به آژانس امنیت ملی ایالات متحده برگزار و پشتیبانی می‌شود و تعدادی ازکارشناسان موسسات آموزشی را برای طراحی ، پیاده سازی و دفاع از یک شبکه رایانه ای در برابر حمله رقابت می‌کنند. NSA شبکه تمرینی را ایجاد می کند و زیرساخت های امتیازدهی را فراهم می‌نماید و به عنوان داور مسابقه عمل می کند و یک تیم قرمز را با هدف به خطر انداختنِ محرمانگی، صحت و در دسترس بودن شبکه های رقبا ، آماده کرده و به کار می‌گیرد.شرکت کنندگان در این تمرین به شرح زیر هستند.

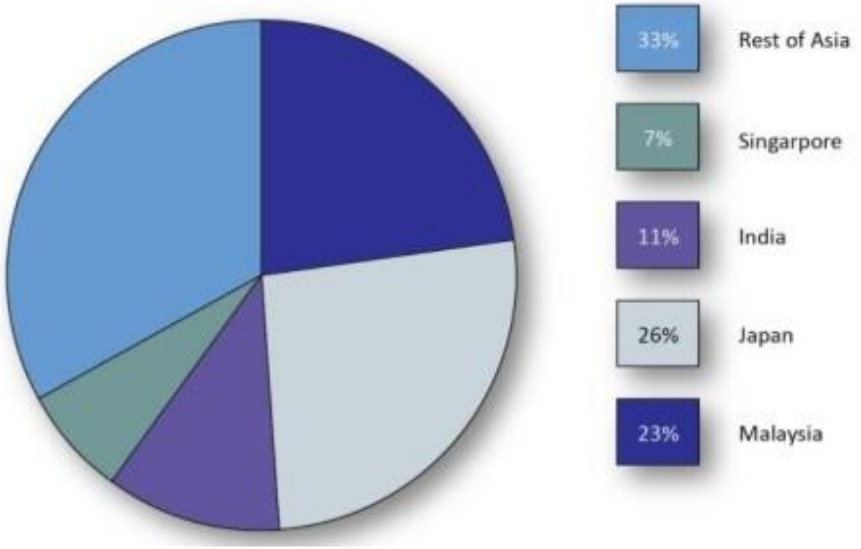
- United States Merchant Marine Academy
- United States Military Academy
- Air Force Institute of Technology
- Royal Military College of Canada

1. *European Union Agency for Network and Information Security*
2. *European Free Trade Association*

آمار تمرین‌های سایبری در دنیا



Cyber Defence Exercises (Worldwide Distribution)



Cyber Defence Exercises (Asia Distribution)

دسته بندی انواع تمرین‌های دفاع سایبری

Cyber Defence ExercisesTaxonomy

دسته بندی تمرین‌های دفاع سایبری

رزمایش مبتنی بر مذاکره

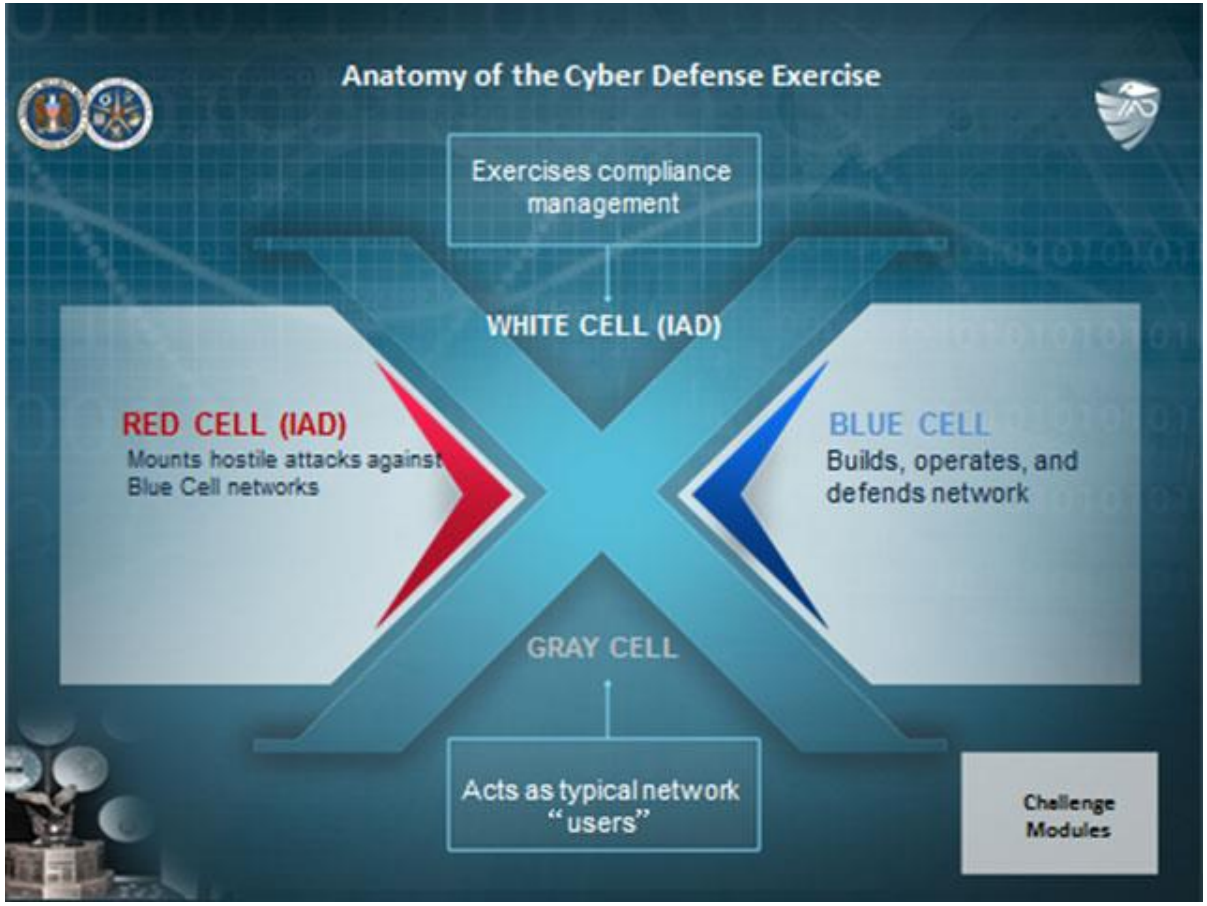
- در این نوع رزمایش، اعضای تیم‌های رزمایش درخصوص اهداف رزمایش و نحوه آمادگی تجهیزات و تیم‌های عمل کننده به بحث و بررسی و تحلیل وضعیت می‌پردازند. و با تهیه یک یا چند سناریو و انجام هماهنگیهای گروهی و سازمانی،اقدامات متناسب با آن را بررسی کرده و میزان آمادگی در برابر حوادث سایبری مورد ارزیابی قرار می‌گیرد.
- سمینار آموزشی
- کارگاه آموزشی
- دورمیزی
- بازی رزمایش (رزمایش شبیه‌سازی شده)

در این نوع رزمایش، تمامی اجزای رزمایش یا بخشی از آن در یک محیط شبیه‌سازی می‌شود و سپس با مشارکت تیم‌های شرکت کننده، رزمایش اجرا می‌شود.

رزمایش عملیاتی

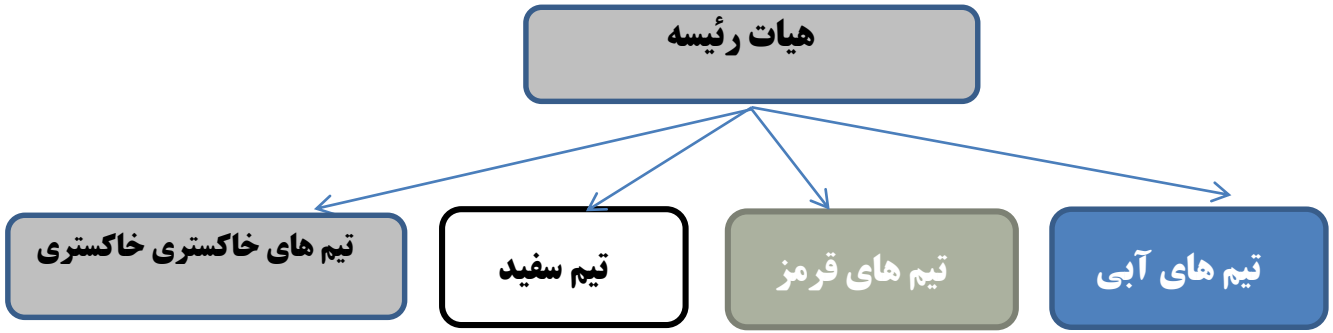
- در این روش تیم‌های شرکت‌کننده در رزمایش در محیط‌های واقعی مطابق با اصول و سناریو تهیه شده و رزمایش انجام می‌دهند.
- شبیه سازی با اقدام اجرایی تیم آبی
- عملیاتی محدود
- عملیاتی کامل

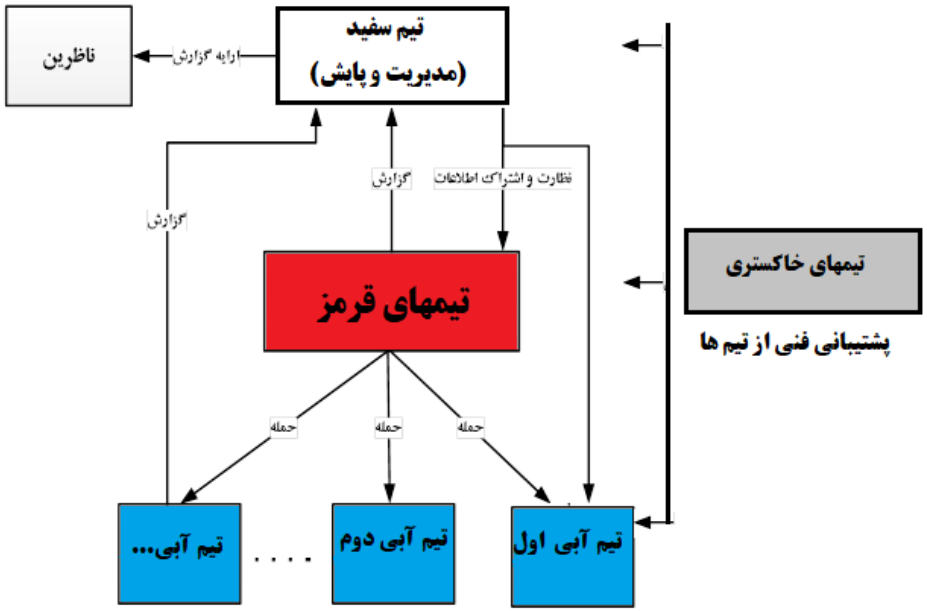
ساختار و سازمان تمرین سایبری



Cyber Defense Exercise (CDX)
In US

ساختار و سازمان تمرین سایبری





ساختار و سازمان تمرین سایبری

- هیئت رئیسه
  - هدایت و راهبری رزمایش
  - تصویب زمان شروع و پایان رزمایش.
  - تصویب و ابلاغ سناریوی رزمایش.
  - سیاست‌گذاری و تعیین رویکرد رزمایش.
  - تحلیل گزارشات پایانی و ابلاغ نتایج و دستاوردهای رزمایش پس از برگزاری آن.
  - دریافت گزارشات از تیم سفید و بررسی آن و کنترل چهارچوب اجرای رزمایش مطابق با سناریوی ابلاغی
- *تیم سفید*
  - تهیه و تدوین سناریو رزمایش و اخذ تاییدیه از هیئت رئیسه
  - کنترل نحوه اجرای رزمایش (تعیین زمان شروع، پایان و تقدم و تاخر انجام وظایف تیم ها)
  - رصد و پایش اقدامات تیم‌های آبی و قرمز
  - تهیه چک لیست برابر سناریو رزمایش با کمک تیم های شرکت کننده
  - ارزیابی اقدامات تیم های آبی و قرمز
  - تجزیه و تحلیل و تهیه گزارش اقدامات تیم‌ها
  - تهیه گزارش ارزیابی نهایی رزمایش و ارائه به هیئت رئیسه
  - نظارت بر آماده‌سازی زیرساختهای مورد نیاز جهت انجام رزمایش توسط زیرساخت مربوطه

- **تیم‌های آبی**

تیم‌های آبی مخاطبان اصلی مانور هستند. این تیم‌ها باید در زمان اجرای مانور به مجموعه‌ای از وظایف عمل کند. وظایف کلی این تیم عبارتند از:

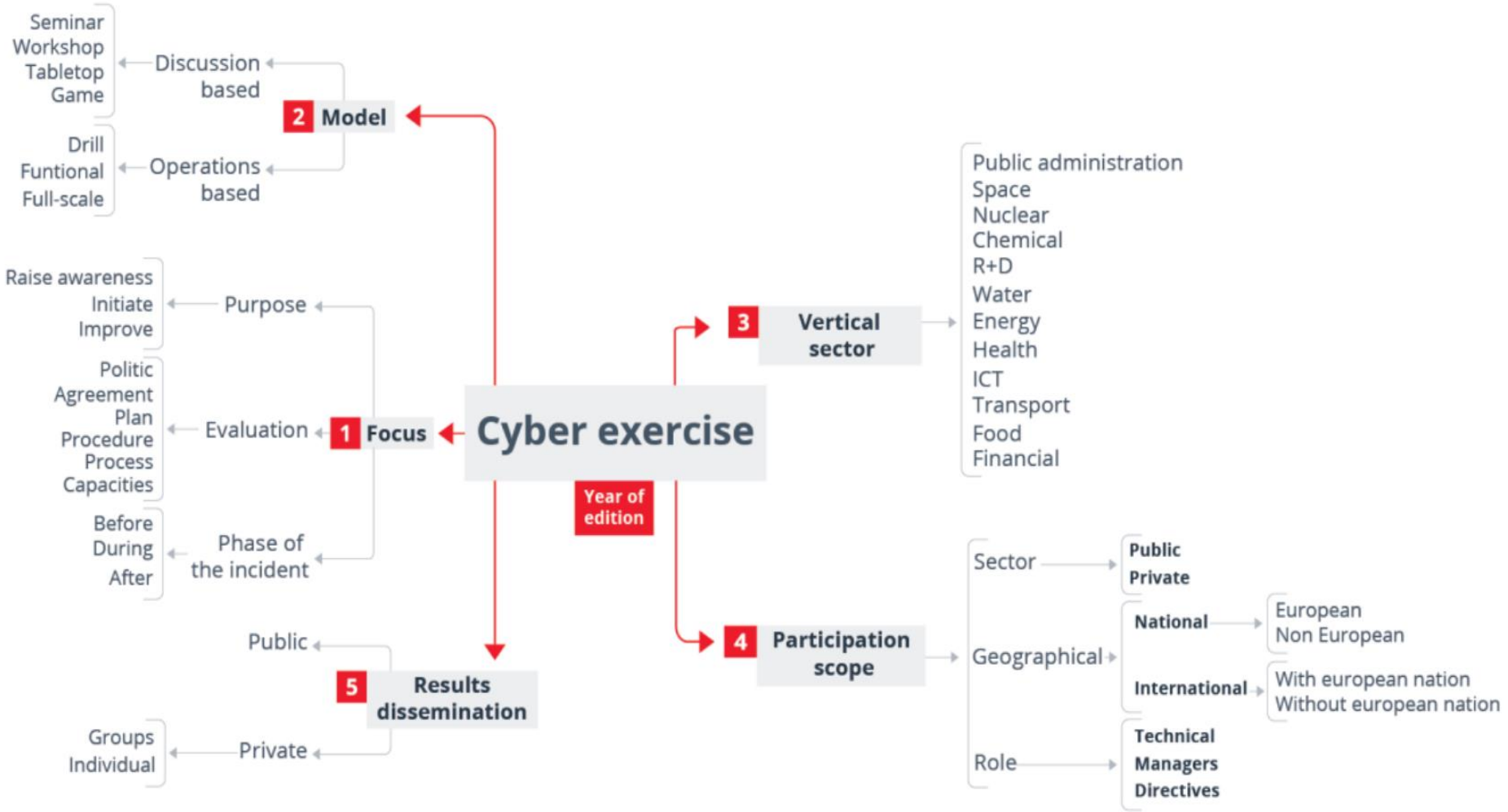
- تضمین امنیت سیستم‌های ناامن و دفاع در مقابل حملات تیم قرمز
- مصون‌سازی، امن‌سازی و پایدارسازی سیستم‌ها
- شناسایی حوادث رخ داده در ارایه گزارش از هر یک از آن‌ها
- ارایه گزارشی از مجموعه عملکرد گروه آبی به تیم سفید

- **تیم قرمز**

تیم قرمز نقش مهاجم و یا مختل کننده در زیرساخت را دارد از نمایندگان و تیم‌های تحت کنترل و مدیریت دستگاه‌های مرتبط تمرین/رزمایش می‌باشند که عهده دار وظایف زیر هستند:

- تیم قرمز سعی در نفوذ، اختلال و یا از کاراندازی سیستم‌ها را بر عهده دارد.
- حمله به نقاط آسیب‌پذیر سیستم‌های تحت حفاظت تیم آبی
- گردآوری اطلاعات مورد نیاز در مورد هدف‌های مورد نظر و تصویب شده.
- تعیین فرایندهای هجوم به تیم آبی و تعیین روش‌های نفوذ.
- ارایه گزارشی از مجموعه عملکردهای گروه به تیم سفید
- تهیه و تدوین سناریوی تهاجم

Cyber Exercise Taxonomy



Cyber Defence Exercises (CDX)
Planning, Execution, Evaluation

- سه فاز اصلی تمرین دفاع سایبری
- طراحی (planning)
- اجرا(Execution)
- ارزیابی (Evalution)

Cyber Defence Exercises (CDX)
Planning

1. فاز طراحی (Planning)

- تعیین موجودیتها Determination of Objectives
- فرآیند طراحی (Planning Process)

Planning Process

تعیین موجودیتها Determination of Objectives

- تعیین هدف و خروجی

فرآیند برنامه ریزی با تعیین هدف تمرین و نتیجه مطلوب آن شروع می‌شود. بدون اهداف صریح، برنامه ریزان نمی توانند تمرین معناداری را طراحی کنند. این اهداف به شرکت کنندگان اجازه می دهد تا به طور واضح سناریوها را در عمل پیکربندی کنند تا مشخص کنند که آیا آنها مهارت های لازم را در یک محیط سایبری در برابر تهدیدات سایبری دارند یا خیر.

تعیین موجودیتها *Determination of Objectives*

- ***تعیین هدف و خروجی***

- تعریف اهداف رزمایش، نقطه شروع برای طراحی رزمایش‌های امنیتی سایبری است. در واقع تمام مراحل طراحی رزمایش، به اهداف انتخاب شده بستگی دارد و آنها را تحت تاثیر قرار می گیرند. اهداف یک رزمایش امنیتی سایبری را بسته به نوع آموزش امنیتی انجام شده، می‌توان به دو دسته اصلی تقسیم کرد: امنیت تهاجمی (PT) یا امنیت دفاعی(SA)
- آموزش امنیت دفاعی، شرکت‌کنندگان را برای سمت مدیر امنیت آماده می‌کند. هدف اصلی آنها آماده سازی و خبره نمودن کارشناسان جهت تنظیم و مدیریت تجهیزات امنیتی مختلف است. بهترین مثال برای این نوع آموزش عملی، سالانه "تمرینات دفاع سایبری" است که توسط آکادمی نظامی ایالات متحده در وست پوینت برگزار می شود.

تعیین موجودیتها *Determination of Objectives*

- **تعیین هدف و خروجی**

از سوی دیگر، آموزش امنیت تهاجمی یک روش موثر برای یادگیری امنیت اطلاعات است،این نوع آموزش‌ها شرکت کنندگان را برای کار عمومی تست نفوذ آماده می کند و به شیوه ای پیشگیرانه به آنها کمک می‌کند تا به مانند دشمن فکر کنند.

از دیگر موارد مهم که می توان به عنوان اهداف رزمایش مطرح کرد عبارتند از:

- ارزیابی میزان آمادگی،پایداری، کارایی و تداوم کارکرد زیرساخت‌های ضروریِ وابسته به شبکه ملی اطلاعات در برابر انواع حملات سایبری.
- ارزیابی میزان آمادگی و تداوم کارکرد زیرساخت‌های نظیر ارتباطات، پولی و مالی، حمل و نقل، انرژی، شهری و سلامت در برابر انواع حملات سایبری.

- تعیین هدف/اهداف *Determination of Objectives*

Learning objective	Participant specialization: Security administrator (SA) or Penetration tester (PT)
- implement security configurations	SA
- monitor systems' activity	SA
- test / harden the administered system	SA
- security configuration fine tuning / improvement	SA
- incident handling / response	SA
- analyze logs and do forensics	SA
- hands-on experience with various attack tools	PT
- perform reconnaissance and gather information	PT
- perform scanning and enumeration	PT
- gain access	PT
- perform DDoS	PT
- escalate privileges	PT
- maintain access	PT
- cover tracks and place backdoors	PT
- write and test new tools	SA+PT
- understand the defense techniques according to the attack methods	SA+PT

Cyber Defence Exercises (CDX)

Planning

فرایند برنامه‌ریزی

Planning Process

ب. فرآیند برنامه ریزی

I برنامه ریزی اولیه(نشست/کنفرانس)

موضوعاتی مانند؛

- تعیین الزامات و شرایط،
- تعیین متغیرهای سناریو و پیش نویس پیشنهادات سناریو،
- جمع آوری اطلاعات مورد نیاز و توزیع وظایف بین برنامه ریزان اجرا،

تقریباً ۶، ۷ ماه قبل از تمرین انجام می شود.

ب. فرآیند برنامه ریزی

II برنامه ریزی میان مدت

بیش از موضوعاتی مانند؛

- تطبیق مشکلات لجستیکی و سازمانی مانند پرسنل، سناریو و زمان توسعه برنامه و الزامات اداری،
- بررسی، ارزیابی و نهایی کردن کلیه اسناد پیش نویس مورد استفاده در تمرین،
- بررسی و توسعه تزریقات قبل از مرحله برنامه ریزی نهایی،
- بررسی وظایف، شرایط و استانداردهای تعیین شده برای هدف تمرین،

تقریباً ۳، ۴ ماه قبل از تمرین انجام می شود.

- *ب. فرآیند برنامه ریزی*
- *III برنامه ریزی نهایی.*

کنفرانس برنامه ریزی نهایی آخرین جلسه برای بررسی فرآیندها و رویه های اجرایی است. پس از این جلسه، هیچ تغییر عمده ای نباید در طراحی یا پوشش تمرین یا اسناد پشتیبان آن ایجاد شود. تقریباً ۳، ۴ هفته قبل از تمرین انجام می شود.

- *ب. فرآیند برنامه ریزی*
- *IV تست-اجرا*

مرحله آماده سازی نهایی برای آزمایش و ارزیابی زیرساخت فنی رزمایش دفاع سایبری است. در اجرای آزمایشی، هدف این است که تمامی زیرساخت‌های مورد استفاده برای تمرین در محل انتخاب شده برای تمرین مستقر شوند و این زیرساخت‌ها به گونه‌ای آزمایش شوند که گویی روند تمرین به‌طور عادی کار می‌کند و مشکلات احتمالی قبل از تمرین مشاهده شود. شرکت تمامی تیم ها به جز تیم های آبی در مرحله آزمایشی انجام می شود. بدین ترتیب تمامی تیم ها این شانس را خواهند داشت که وضعیت نهایی و روند تمرین خود را قبل از شروع تمرین بررسی کنند. تست اجرا تقریبا یک هفته قبل از تمرین انجام می شود.

Cyber Defence Exercises (CDX)

Execution

- *A. Teams*
- *B. Scenario*
- *C. Scoring*
- *D. Monitoring*
- ……

Cyber Defence Exercises (CDX)
Evaluation

یکی از مهم ترین خروجی های رزمایش پدافند سایبری، گزارش After Actionاست.

جزئیات عملکرد تیم آبی پس از پایان تمرین

علاوه بر این سناریو و سناریوهای فرعی، تزریق، اهداف تمرین، شرکت‌کنندگان، امتیازدهی، زیرساخت‌های فنی، حملات تیم قرمز (سمت مشتری، وب، شبکه)، دفاع‌های تیم آبی، نقص در این دفاع‌ها، اشتباهات کلی، مشاهدات همه تیم‌ها و زیر تیم‌ها، توصیه‌ها و ارزیابی‌ها نیز پوشش داده شده است.