معرفی دوره آموزشی

عنوان دوره:

فارسی: **راهبردهای امن‌سازی زیرساخت‌های حیاتی کشور**

انگلیسی: **Infra Security**

درباره دوره:

همزمان با گسترش روز افزون فناوری‌های نوین در زیرساخت‌های حیاتی و منابع کلیدی کشورمان، مباحث مربوط به امنیت آنها نیز در عین وجود کارایی، از اهمیت بسیار بالایی برخوردار است چرا که هرگونه آسیب جدی به این زیرساخت‌های حساس می‌تواند لطمات جبران‌ناپذیری را برای آن سازمان‌ها و همچنین شمار زیادی از شهروندان دربرداشته باشد.

در این دوره آموزشی، مخاطبان ضمن آشنایی کامل با زیرساخت‌های حیاتی و تجهیزات امنیتی مورد استفاده در آنها با راهکارهای امن‌سازی و تأمین امنیت در زیرساخت‌های حیاتی، مطابق با استانداردهای بین‌المللی و بهترین تجربه‌های جهانی آشنا شده و می‌توانند طرح‌های جامع امنیتی را که دربرگیرنده نیازهای اصلی زیرساخت‌های حیاتی در کشورمان است، در این مراکز کلیدی، اجرا و پیاده‌سازی کنند.

اهداف دوره:

۱- آشنایی با زیرساخت‌های حیاتی و تجهیزات امنیتی مورد استفاده در آنها

۲- آشنایی با بهترین تجربه‌های جهانی در حوزه امن‌سازی زیرساخت‌های حیاتی

۳- آشنایی با استانداردها و چارچوب‌های امن‌سازی زیرساخت‌های حیاتی

۴- آشنایی با متدولوژی‌های کاهش ریسک در زیرساخت‌های حیاتی

۵- آشنایی با استراتژی‌های لایه‌ای و رویکردهای دفاع در عمق، جهت امن‌سازی زیرساخت‌های حیاتی

۶- آشنایی با راهکارهای جامع امن‌سازی در زیرساخت‌های حیاتی کشورهای مورد بررسی

۷- آشنایی با راهبردهای امن‌سازی زیرساخت‌های حیاتی در کشورمان

۸- تحلیل نیازمندی‌های امنیتی زیرساخت‌های حیاتی کشورمان

۹- آشنایی با چگونگی تدوین نقشه راه امنیتی در زیرساخت‌های حیاتی کشورمان

۱۰- آشنایی با راهکارهای جامع امن‌سازی سیستم‌های کنترل صنعتی مورد استفاده در زیرساخت‌های حیاتی

۱۱- آشنایی با چالش‌های امن‌سازی زیرساخت‌های حیاتی در ایران و راهکارهای برطرف‌سازی آنها

۱۲- چگونگی پیاده‌سازی راهکارهای جامع امنیتی در زیرساخت‌های حیاتی کشورمان

مخاطبان دوره:

- ✓ مدیران و مسئولان زیرساخت‌های حیاتی
- ✓ مدیران و کارشناسان فناوری اطلاعات و امنیت زیرساخت‌های حیاتی
- ✓ مدیران و کارشناسان حراست زیرساخت‌های حیاتی
- ✓ مدیران و کارشناسان فناوری اطلاعات و امنیت شبکه‌های صنعتی
- ✓ مدیران و کارشناسان امنیت و فناوری اطلاعات
- ✓ مشاوران امنیت اطلاعات زیرساخت‌های حیاتی
- ✓ سایر علاقمندان به مباحث امنیت اطلاعات

مدت زمان دوره:

۱۶ ساعت (۲ روز)

محتویات دوره:

۱. سازمان‌های حیاتی و غیرحیاتی

- آیا می‌توان میان سازمان‌های حیاتی و غیرحیاتی، تمایز قایل شد؟
- تعاریف زیرساخت حیاتی
- مهمترین جنبه‌های امنیتی سازمان‌های حیاتی
- رویکرد شبکه‌ای به زیرساخت‌های حیاتی
- متدولوژی های شناسایی و طبقه‌بندی زیرساخت‌های حیاتی

۲. آشنایی با سازمان‌های حیاتی و منابع کلیدی

- طبقه‌بندی ۱۸ گانه زیرساخت‌های حیاتی
- حوزه‌های موجود در هر گروه از زیرساخت‌های حیاتی
- سازمان‌ها و نهادهای مسئول حفاظت از هر گروه از زیرساخت‌های حیاتی

۳. زیرساخت‌های مهم فناوری اطلاعات در سازمان‌های حیاتی

- دلایل اهمیت ویژه به فناوری اطلاعات در زیرساخت‌های حیاتی
- نقش فناوری اطلاعات در تولیدات و خدمات زیرساخت‌های حیاتی
- لزوم توجه به امنیت فناوری اطلاعات در زیرساخت‌های حیاتی
- زیربخش‌های مهم فناوری اطلاعات در زیرساخت‌های حیاتی

۴. آشنایی با مفاهیم امنیت اطلاعات

- اجزای اصلی امنیت اطلاعات
- عناصر و مؤلفه‌های کلیدی امنیت اطلاعات

۵. اصطلاح‌ها و واژگان امنیت اطلاعات

۶. چرا امنیت اطلاعات در سازمان‌های حیاتی مهم است؟

- جایگاه حفاظت از اطلاعات در بقای سازمان‌های حیاتی
- تهدیدها و مخاطرات متوجه زیرساخت‌های حیاتی
- روش‌های پاسخگویی به رخدادهای امنیتی در زیرساخت‌های حیاتی
- بردار تکامل حملات به سازمان‌های حیاتی در طول زمان
- سازوکارهای نفوذ به سازمان‌های حیاتی
- انواع بدافزارهای مشاهده شده در سازمان‌های حیاتی

۷. ضرورت توجه به امنیت اطلاعات در سازمان‌های حیاتی

- نحوه گزارش رخدادهای امنیتی در زیرساخت‌های حیاتی
- چگونگی تشخیص تهدیدات در زیرساخت‌های حیاتی
- زمان‌های لازم برای تشخیص تهدیدات در زیرساخت‌های حیاتی
- نقش دارایی‌های لیست نشده در بروز تهدیدات در زیرساخت‌های حیاتی
- نواحی خطر متوجه زیرساخت‌های حیاتی
- عوامل تأثیرگذار بر امنیت در زیرساخت‌های حیاتی

۸. ارتباط زیرساخت‌های حیاتی با فضای سایبر

۹. تاریخچه حملات سایبری به سازمان‌های حیاتی

- حمله به سیستم کنترل فاضلاب Maroochy
- حمله به سیستم‌های اسکادای زیرساخت‌های حیاتی آمریکا
- حمله استاکس‌نت
- حمله سایبری خاموشی آمریکایی

۱۰. نمونه‌هایی از حمله سایبری به سازمان‌های حیاتی

۱۱. آشنایی با انواع حملات در سازمان‌های حیاتی

- مفاهیم و تعاریف حمله سایبری
- اکسپلویت‌ها و سوءاستفاده از آسیب‌پذیری‌های سیستم
- حملات قابل انجام در زیرساخت‌های حیاتی

۱۲. بررسی انواع حملات سازمانی در سازمان‌های حیاتی

- حملات داخلی و حملات بیرونی به زیرساخت‌های حیاتی
- اهداف و تأثیر حملات داخلی و بیرونی به زیرساخت‌های حیاتی
- دیگر حملات شایع به زیرساخت‌های حیاتی

- روش‌های جلوگیری و مقابله با حملات به زیرساخت‌های حیاتی

۱۳. آشنایی با انواع آسیب‌پذیری و نفوذ به سازمان‌های حیاتی

- مفاهیم آسیب‌پذیری
- عناصر تشکیل دهنده آسیب‌پذیری در سامانه‌های حیاتی
- ۴ روش اصلی برای نفوذ به سیستم‌های زیرساخت‌های حیاتی
- متدولوژی نفوذ به شبکه سامانه‌های حیاتی
- روش‌های جلوگیری از نفوذ به شبکه سامانه‌های حیاتی

۱۴. آشنایی با انواع آسیب‌پذیری و تهدیدات امنیتی سازمان‌ها

۱۵. دلایل توجه به امنیت سازمان‌های حیاتی

- نقش حساس سازمان‌های حیاتی در خدمات رسانی
- تهدیدات و حملات نوظهور در سازمان‌های حیاتی
- تأثیرات اقتصادی، فرهنگی و سیاسی
- پیامدهای ناشی از انتشار آسیب‌پذیری در زیرساخت‌های حیاتی
- ارزیابی عملکرد سازمان‌های حیاتی در شرایط بحرانی

۱۶. جنبه‌های امنیتی سازمان‌های حیاتی

- دسترسی غیرمجاز به نرم افزارهای کنترل کننده سیستم‌های کنترل صنعتی
- تأثیر کارمندان ناراضی در بروز تهدیدات داخلی
- مسایل مرتبط با امنیت ملی در حفاظت از زیرساخت‌های حیاتی

۱۷. مهمترین اولویت‌های نیازهای امنیتی سازمان‌های حیاتی

- ارتباطات اضطراری در زیرساخت‌های حیاتی
- ارزیابی خطر در زیرساخت‌های حیاتی

- آموزش اولین پاسخ دهندگان در زیرساخت‌های حیاتی
- امنیت سایبر در زیرساخت‌های حیاتی
- امنیت بیومتریک و هویت‌سنجی در زیرساخت‌های حیاتی

۱۸. مهمترین مخاطرات امنیتی سازمان‌های حیاتی و روش‌های جلوگیری از آنها

۱۹. مخاطرات امنیتی کارمندان سازمان‌های حیاتی از دیدگاه SANS

۲۰. ضرورت توجه به آموزش کارکنان برای گزارش حوادث امنیتی

۲۱. چرا سازمان‌های حیاتی در برابر مخاطرات امنیت اطلاعات آسیب‌پذیرند؟

۲۲. وظایف سازمان‌های حیاتی در مواجهه با مخاطرات امنیتی

- نحوه شناسایی مخاطرات و جمع‌آوری شواهد وقوع رخدادهای امنیتی
- اصول حاکم بر تدوین طرح تداوم خدمات سازمان‌های حیاتی
- برنامه‌های بازیابی از وضعیت خرابی در زیرساخت‌های حیاتی
- دارایی‌های حیاتی و دارایی‌های سایبری در زیرساخت‌های حیاتی

۲۳. پنج قدم مهم در مدیریت مخاطرات، بر اساس ISO/IEC 27005

۲۴. چالش‌های امنیتی فراروی سازمان‌های حیاتی

- آسیب‌پذیری‌های موجود در تجهیزات مورد استفاده سازمان‌های حیاتی
- مشکلات امنیتی معماری شبکه و سیستم‌های سازمان‌های حیاتی
- مشکلات امنیتی استفاده از بسترهای فناوری اطلاعات
- گزارش‌های مربوط به حملات و آسیب‌پذیری‌ها به زیرساخت‌های حیاتی
- تناسب بین کنترل‌های امنیتی و رخدادهای امنیت سایبری در زیرساخت‌های حیاتی
- پیاده‌سازی اقدامات جبرانی برای تهدیدهای جدید
- نقش زمان در پاسخ‌دهی به تهدیدات

- وظایف سازمان‌های یاری‌رسان در هنگام بروز تهدیدات امنیتی به زیرساخت‌های حیاتی

۲۵. مهمترین مشکلات امنیتی سازمان‌های حیاتی

۲۶. امنیت سازمان‌های حیاتی در آمریکا

- وظایف رئیس جمورهای پیشین در امنیت زیرساخت‌های حیاتی ملی
- جایگاه کنگره ملی در امنیت زیرساخت‌های حیاتی
- نقش امنیت سایبر در امنیت ملی آمریکا
- اقدامات اوباما در حوزه امن‌سازی زیرساخت‌های حیاتی آمریکا
- نیروهای نظامی سایبری آمریکا جهت حفاظت از زیرساخت‌های حیاتی
- فعالیت‌های تهاجمی ارتش سایبری آمریکا به زیرساخت‌های حیاتی سایر کشورها

۲۷. بررسی قانون حفاظت از زیرساخت‌های حیاتی در آمریکا

- بررسی قانون بهبود امنیت سایبری زیرساخت‌های حیاتی
- نکات کلیدی در قانون حفاظت از زیرساخت‌های حیاتی آمریکا
- نحوه تعامل سازمان‌های دولتی و خصوصی برای اجرای این قانون
- سیاست‌های ایالات متحده آمریکا در حفاظت از زیرساخت‌های حیاتی
- استراتژی‌های امن‌سازی زیرساخت‌های حیاتی در این قانون
- مشکلات فنی و عملیاتی اجرای این قانون
- جایگاه متدولوژی در مدیریت تهدیدات سایبری به آمریکا

۲۸. چارچوب امنیت رایانه آمریکا در زیرساخت‌های حیاتی

۲۹. آشنایی با سیستم‌های مدیریت امنیت در زیرساخت‌های حیاتی

۳۰. استانداردهای امنیت سازمان‌های حیاتی

- استانداردهای ISO

- استانداردهای NIST
- استانداردهای IETF

۳۱. طرح‌ها و متدولوژی‌های کاهش ریسک در زیرساخت‌های حیاتی

- انواع مخاطرات امنیت اطلاعات مطرح در متدولوژی‌های مدیریت ریسک زیرساخت‌های حیاتی
- روش‌های مدیریت ریسک در زیرساخت‌های حیاتی
- انواع رویدادها و رخدادهای امنیتی در زیرساخت‌های حیاتی
- سناریوهای امنیتی مطرح در تعیین سطح مخاطرات دارایی‌های موجود در زیرساخت‌های حیاتی
- اصول مهم امنیت اطلاعات در تعیین سطح مخاطرات در زیرساخت‌های حیاتی
- سناریوهای ارزیابی ریسک در متدولوژی‌های مدیریت ریسک در زیرساخت‌های حیاتی
- روش‌های برخورد با ریسک در متدولوژی‌های مدیریت ریسک در زیرساخت‌های حیاتی
- فرایندهای اصلی مدیریت ریسک در متدولوژی‌های مدیریت ریسک در زیرساخت‌های حیاتی
- روش‌های پاسخ به ریسک در زیرساخت‌های حیاتی
- متدولوژی مدیریت ریسک در زیرساخت‌های حیاتی
- چارچوب‌های مطرح در حوزه مدیریت ریسک در زیرساخت‌های حیاتی

۳۲. فرایندهای بهبود امنیت در زیرساخت‌های حیاتی

۳۳. استراتژی‌ها و راهکارهای جامع امن‌سازی سازمان‌های حیاتی

- استراتژی‌ها و راهکارهای جامع NIST
- استراتژی‌های ملی چند کشور مورد مطالعه
- استراتژی‌ها و راهکارهای ایران در خصوص امن‌سازی زیرساخت‌های حیاتی
- بهترین تجربه‌های موجود در این حوزه

۳۴. سیاست‌های ابلاغی رهبری در حوزه امن‌سازی زیرساخت‌های حیاتی

۳۵. الزامات مرکز مدیریت راهبردی افتا در حوزه امن‌سازی سازمان‌های حیاتی

۳۶. راهبردهای امن‌سازی زیرساخت‌های حیاتی در اسناد بالادستی کشور

- سند افتا
- سند احکام فناوری اطلاعات در برنامه پنجم توسعه کشور
- سند نظام ملی پیشگیری و مقابله با حوادث رایانه‌ای کشور

۳۷. روش‌های اجرایی فراهم‌آوری امنیت در سازمان‌های حیاتی

۳۸. چگونگی پیاده‌سازی روش‌های اجرایی امنیتی در زیرساخت‌های حیاتی

۳۹. کنترل‌های حیاتی برای دفاع اثربخش سایبری در سازمان‌های حیاتی

۴۰. معماری‌های امنیتی و دفاع در عمق در زیرساخت‌های حیاتی

۴۱. استراتژی‌های امنیتی توافق‌نامه‌های شخص سوم در زیرساخت‌های حیاتی

۴۲. مستندسازی امنیتی در حوزه زیرساخت‌های حیاتی

- انواع سندهای امنیتی
- اصول کلی در مستندسازی امنیتی
- الزامات یک سند امنیتی
- سیستم کدگذاری سندهای امنیتی
- استانداردهای موجود در حوزه مستندسازی امنیتی

۴۳. امنیت سایبری در سازمان‌های حیاتی؛ جنگ و دفاع سایبری

۴۴. چند نکته مهم در امنیت اطلاعات سازمان‌های حیاتی

۴۵. امن‌سازی سیستم‌های کنترل صنعتی مورد استفاده در زیرساخت‌های حیاتی

۴۶. قوانین حقوقی در رابطه با امنیت زیرساخت‌های حیاتی در ایران

۴۷. انجمن‌ها و مؤسسات پژوهشی در حوزه امن‌سازی سازمان‌های حیاتی

۴۸. بررسی اسناد و راهنماهای امنیتی NIST

۴۹. آشنایی با فعالیت‌های DHS در حوزه مدل‌سازی امنیت میهن

۵۰. بهترین تجارب جهانی در رابطه با امن‌سازی سازمان‌های حیاتی ملی

۵۱. آشنایی با توانمندی‌های نظامی جمهوری اسلامی ایران در حوزه دفاع از سازمان‌های حیاتی

۵۲. مخفف واژگان و اصطلاحات مورد استفاده در زیرساخت‌های حیاتی

سایر مباحثی که در خلال برگزاری این دوره به آنها نیز پرداخته می‌شود، عبارتند از:

۱. امن‌سازی شبکه‌های هوشمند شهری در تأسیسات زیربنایی

۲. نحوه تدوین طرح‌های حفاظتی در زیرساخت‌های حیاتی و توسعه آنها

۳. چگونگی ایجاد ناحیه‌های حفاظت شده در شبکه‌های صنعتی و فناوری اطلاعات زیرساخت‌های حیاتی

۴. چگونگی تهیه چک‌لیست‌های امنیتی در زیرساخت‌های حیاتی

۵. مدیریت سیستم‌های امنیتی در زیرساخت‌های حیاتی

۶. نحوه سنجش اثربخشی طرح‌های امنیتی مورد استفاده در زیرساخت‌های حیاتی

۷. راهبری سرویس‌های منابع کلیدی از دیدگاه امنیتی

۸. الزامات امنیتی و قانونی در تمامی بخش‌های زیرساخت‌های حیاتی

۹. چگونگی تدوین خط‌مشی‌ها و فرایندهای امنیتی در زیرساخت‌های حیاتی

۱۰. آنالیز امنیتی سیستم‌های خاص در زیرساخت‌های حیاتی

۱۱. مانیتورینگ متمرکز در شبکه‌های هوشمند زیرساخت‌های حیاتی

ویژگی‌های دوره:

- ✓ امکان صدور گواهینامه معتبر حضور در دوره آموزشی
- ✓ برخورداری از ۱۰٪ تخفیف در صورت ثبت نام گروهی