

## معرفی دوره آموزشی

### عنوان دوره:

فارسی: امنیت سایبری سیستم‌های کنترل صنعتی

انگلیسی: ICS Cyber Security

### درباره دوره:

سیستم‌های کنترل صنعتی، سیستم‌هایی مبتنی بر رایانه هستند که برای کنترل فرایندهای صنعتی و عملکردهای فیزیکی استفاده می‌شوند. استفاده گسترده از این سیستم‌ها در زیرساخت‌ها و سامانه‌های حیاتی کشور، موجب شکل‌گیری نوع جدیدی از حملات سایبری به شبکه‌های بزرگ صنعتی کشورمان شده است که از نمونه‌های مشهور و شناخته شده آن در سال‌های اخیر می‌توان به استاکس‌نت اشاره کرد.

در این دوره آموزشی، ضمن بررسی چالش‌ها و مشکلات امنیتی سیستم‌های کنترل صنعتی، ارایه راهکارهای اجرایی برای کاهش مخاطرات امنیتی این سیستم‌ها، روش‌های امن‌سازی آنها بر اساس استانداردهای بین‌المللی، آشنایی با بهترین تجربه‌های جهانی در حوزه حفاظت از سیستم‌های کنترل صنعتی و همچنین بررسی الزامات ملی ایران در این خصوص، از دیگر موارد مطرح در این دوره است.

### اهداف دوره:

- ۱- آشنایی با راهکارهای امنیت سایبری سیستم‌های کنترل صنعتی
- ۲- آشنایی با چالش‌ها و مشکلات امنیتی در سیستم‌های کنترل صنعتی
- ۳- آشنایی با آسیب‌پذیری‌ها و مخاطرات امنیتی سیستم‌های کنترل صنعتی
- ۴- آشنایی با متدولوژی‌های مدیریت مخاطرات در سیستم‌های کنترل صنعتی
- ۵- آشنایی با مراکز مهم پژوهشی در رابطه با امنیت سیستم‌های کنترل صنعتی
- ۶- آشنایی با الزامات ملی کشورمان در حوزه امن‌سازی سیستم‌های کنترل صنعتی
- ۷- آشنایی با بهترین تجربه‌های جهانی در حوزه امن‌سازی سیستم‌های کنترل صنعتی
- ۸- آشنایی با استانداردهای بین‌المللی در خصوص امن‌سازی سیستم‌های کنترل صنعتی
- ۹- آشنایی با روش‌ها و سازوکارهای اجرایی فراهم‌آوری امنیت در سیستم‌های کنترل صنعتی

## مخاطبان دوره:

- ✓ مدیران، مسئولان و راهبران سیستم‌های کنترل صنعتی
- ✓ مدیران و کارشناسان فناوری اطلاعات و امنیت سیستم‌های کنترل صنعتی
- ✓ مدیران و کارشناسان فناوری اطلاعات و امنیت شبکه‌های صنعتی
- ✓ مدیران و کارشناسان حراست و پدافند غیرعامل سازمان‌های صنعتی
- ✓ مدیران و کارشناسان امنیت و فناوری اطلاعات
- ✓ مشاوران امنیت اطلاعات سیستم‌های کنترل صنعتی
- ✓ سایر علاقمندان به مباحث امنیت اطلاعات

## مدت زمان دوره:

۱۶ ساعت (۲ روز)

## محتویات دوره:

- ۱- آشنایی با سامانه‌های حیاتی و غیرحیاتی
- ۲- مشکلات و چالش‌های امنیتی سیستم‌های کنترل صنعتی
  - مفاهیم امنیتی سیستم‌های کنترل صنعتی
  - ضرورت توجه به امنیت سیستم‌های کنترل صنعتی
  - رخدادهای امنیتی سیستم‌های کنترل صنعتی
  - انواع بدافزارهای سیستم‌های کنترل صنعتی
  - آشنایی با آسیب‌پذیری‌های موجود در سیستم‌های کنترل صنعتی
  - آشنایی با آسیب‌پذیری‌های حیاتی در طراحی محصولات سیستم‌های کنترل صنعتی
    - آسیب‌پذیری آئورورا (Aurora)
    - آسیب‌پذیری بوریاس (Boreas)
  - نحوه شناسایی سیستم‌های کنترل صنعتی آسیب‌پذیر از طریق اینترنت
  - آشنایی با انواع تهدیدات و مخاطرات امنیتی در سیستم‌های کنترل صنعتی
  - بررسی انواع حملات سازمانی در شبکه‌های صنعتی
  - بررسی مشکلات امنیتی در معماری، سیستم کنترلی، تجهیزات و بستر ارتباطی شبکه‌های صنعتی

- بررسی چالش‌های امنیتی سیستم‌های کنترل صنعتی
  - معرفی روش‌های جلوگیری از تهدیدات امنیتی سیستم‌های کنترل صنعتی
  - بررسی رویکرد واکنشی به امنیت سایبری در سیستم‌های کنترل صنعتی
- ۳- تاریخچه حملات سایبری به سیستم‌های کنترل صنعتی
- ۴- استانداردهای امنیتی سیستم‌های کنترل صنعتی
- ISO
  - CPNI
  - NIST
  - NERC
  - DHS
  - DOE
  - ISA
- ۵- امنیت سیستم‌های کنترل صنعتی و زیرساخت‌های حیاتی در سایر کشورها (مطالعه موردی)
- ۶- بررسی امنیت در سیستم‌های کنترل صنعتی و سامانه‌های فناوری اطلاعات
- بررسی وصله‌های امنیتی در سیستم‌های کنترل صنعتی و سامانه‌های فناوری اطلاعات
  - بررسی پیچیدگی‌های سیستم‌های کنترل صنعتی نسبت به سامانه‌های فناوری اطلاعات
- ۷- امنیت سیستم‌های کنترل صنعتی
- فاکتورهای بروز آسیب‌پذیری در سیستم‌های کنترل صنعتی
  - مسایل امنیتی مربوط به ارتباط شبکه‌های کنترل فرایند سیستم‌های صنعتی با شبکه داخلی سازمان
  - مسایل امنیتی مربوط به طراحی، استقرار و بهره‌برداری از سیستم‌های کنترل صنعتی
  - مسایل امنیتی مربوط به پروتکل‌های اختصاصی سیستم‌های کنترل صنعتی
  - مسایل امنیتی مربوط به دسترسی‌های غیرمجاز به نرم افزارهای کنترل کننده سیستم‌های کنترل صنعتی
  - مسایل امنیتی مربوط به کارمندان ناراضی داخل سازمان
  - مسایل امنیتی مربوط به رسانه‌های ارتباطی سیستم‌های کنترل صنعتی (سیستم تلفن سوئیچ عمومی، ارتباطات بی‌سیم و اینترنت)
- ۸- الزامات مراکز بالادستی کشور در خصوص امن‌سازی سیستم‌های کنترل صنعتی
- ۹- بررسی متدولوژی‌های مدیریت مخاطرات سایبری سیستم‌های کنترل صنعتی
- ۱۰- روش‌های اجرایی فراهم‌آوری امنیت در سیستم‌های کنترل صنعتی
- نحوه تدوین خط‌مشی‌ها، روش‌های اجرایی و دستورالعمل‌های امنیتی
  - بررسی نقش مدیریت مخاطره در امن‌سازی سیستم‌های کنترل صنعتی
  - چگونگی وضع کنترل‌های امنیتی در سیستم‌های کنترل صنعتی
  - چگونگی ایمن‌سازی برنامه‌های سیستم کنترل صنعتی

- چگونگی امن‌سازی تجهیزات ارتباطی سیستم‌های کنترل صنعتی
  - چگونگی امن‌سازی محیط‌های ذخیره، پردازش و بازیابی اطلاعات سیستم‌های کنترل صنعتی
  - چگونگی طراحی ضمانت‌نامه‌های اجرایی مناسب در سیستم‌های کنترل صنعتی
  - چگونگی به کارگیری سیستم‌های اخطاردهی و گزارش نقص‌ها و نقص‌ها در سیستم‌های کنترل صنعتی
  - روش‌های احراز هویت در سیستم‌های کنترل صنعتی
  - آشنایی با سیستم‌ها و تجهیزات امنیتی سیستم‌های کنترل صنعتی
  - چگونگی سنجش اثربخشی کنترل‌های امنیتی سیستم‌های کنترل صنعتی
  - آموزش و آگاهی‌رسانی امنیتی در شبکه‌های صنعتی
  - نحوه امن‌سازی دسترسی‌های از راه دور به سیستم‌های کنترل صنعتی
  - امنیت فیزیکی و محیطی سیستم‌های کنترل صنعتی
  - نحوه تشکیل گروه‌های واکنش به رخدادها و حوادث امنیتی در شبکه‌های صنعتی
  - چگونگی تدوین طرح‌های تداوم کسب و کار و بازیابی از وضعیت خرابی در سیستم‌های کنترل صنعتی
  - آشنایی با معماری‌های امنیتی مرجع در امن‌سازی سیستم‌های کنترل صنعتی
  - نحوه برطرف‌سازی آسیب‌پذیری‌های امنیتی محصولات سیستم‌های کنترل صنعتی
  - آشنایی با نحوه تهیه و تدوین چک‌لیست‌های امنیتی سیستم‌های کنترل صنعتی
  - بررسی استراتژی‌های دفاع در عمق در امن‌سازی سیستم‌های کنترل صنعتی
- ۱۱- انجمن‌ها و مؤسسات پژوهشی در حوزه امن‌سازی سیستم‌های کنترل صنعتی

### ویژگی‌های دوره:

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