



## عناوین کارگاه‌های آموزشی سومین رویداد علمی - تخصصی امنیت شبکه‌های کنترل صنعتی

رویدادی همگام با آخرین روندها، استانداردها، متدولوژی‌ها، ابزارها و راهکارهای حل چالش‌های فناوری صنعت امنیت OT

شماره کارگاه	ساعت برگزاری	عنوان کارگاه آموزشی	ارائه‌کننده کارگاه	شرح مختصر کارگاه
<b>روز اول (سه‌شنبه - ۱۴۰۴/۱۱/۰۷)</b>				
۱	۰۸:۰۰ - ۱۲:۰۰	سنجش سطح بلوغ امنیتی و پیاده‌سازی استاندارد ۶۲۴۴۳	مهندس محمد مهدی واعظی نژاد	در این کارگاه آموزشی به بررسی استانداردها و به‌روشن‌های مطرح در حوزه امنیت زیرساخت‌های حیاتی صنعتی، به خصوص استانداردهای سری ۶۲۴۴۳ پرداخته خواهد شد. تشریح ساختار کنترلی و الزامات استاندارد ISA/IEC 62443-3-3، به همراه نحوه ارزیابی سطح بلوغ امنیتی فناوری عملیاتی (OT) شرکت و ارائه راهکار جهت دستیابی به سطح بلوغ مطلوب بر اساس این استاندارد مطرح بین‌المللی و الزامات بالادستی کشور، از جمله مباحث این کارگاه آموزشی می‌باشد. <b>مهارت عملی پس از پایان کارگاه:</b> فراگیران نحوه ارزیابی و تأمین امنیت یک شبکه صنعتی را بر اساس استانداردهای ۶۲۴۴۳ فرا گرفته و توانایی تدوین لیست پروژه‌های شرکت را جهت ارتقای سطح بلوغ امنیت سایبری صنعتی آن خواهند داشت.
۲	۱۳:۰۰ - ۱۷:۰۰	ارزیابی فنی و آزمون نفوذپذیری صنعتی	مهندس محسن خاشعی نژاد	در این کارگاه آموزشی در خصوص متدولوژی‌ها، ابزارها و نحوه انجام آزمون نفوذپذیری (پن‌تست) سامانه‌ها و تجهیزات پرکاربرد صنعتی بحث خواهد شد. ایجاد محیط شبیه‌سازی صنعتی، نصب نرم‌افزارها و ابزارهای رایج آزمون نفوذپذیری و انجام تست‌های متعدد بر روی سامانه HMI و تجهیزات صنعتی (PLC و RTU)، به همراه تشریح چگونگی برطرف‌سازی آسیب‌پذیری‌های شناسایی شده و امن‌سازی تجهیزات، از جمله مباحث این کارگاه آموزشی می‌باشد. <b>مهارت عملی پس از پایان کارگاه:</b> فراگیران نحوه نصب و کار با نرم‌افزارهای رایج ارزیابی فنی امنیتی را فرا گرفته و توانایی انجام آزمون نفوذپذیری بر روی تجهیزات و سامانه‌های کنترل صنعتی را در محیط امن شبیه‌سازی شده به همراه امن‌سازی آنها خواهند داشت.

روز دوم (چهارشنبه - ۱۴۰۴/۱۱/۰۸)

<p>در این کارگاه آموزشی در خصوص نحوه تدوین راهکارهای تداوم (BCP) سرویس‌های کلیدی زیرساخت‌های صنعتی و چگونگی بازیابی آنها (DRP) پس از وقوع فجایع و حملات سایبری بحث خواهد شد. نحوه انجام تحلیل اثر کسب‌وکار (BIA)، ارزیابی ریسک سرویس‌های حیاتی شرکت و تدوین طرح‌های عملیاتی تداوم و بازیابی از فاجعه برای چندین سرویس حیاتی، همراه با ارائه مثال‌های متعدد این حوزه، از جمله مباحث این کارگاه آموزشی می‌باشد.</p> <p><b>مهارت عملی پس از پایان کارگاه:</b> فراگیران توانایی تدوین طرح‌های تداوم (BCP) و بازیابی از فاجعه (DRP) را بر اساس نتایج ارزیابی ریسک، برای سرویس‌های کلیدی صنعتی شرکت خود خواهند داشت.</p>	<p>مهندس محمد مهدی واعظی نژاد</p>	<p>تداوم تولید و تاب‌آوری سایبری زیرساخت‌های حیاتی صنعتی</p>	<p>۰۸:۰۰ - ۱۲:۰۰</p>	<p>۳</p>
<p>در این کارگاه آموزشی در خصوص معماری امن شبکه صنعتی و ابزارهای مورد نیاز برای ایجاد یک شبکه ایمن بحث خواهد شد. طراحی امن شبکه صنعتی بر اساس مدل‌های مطرح این حوزه (همچون پوردو)، نحوه ایجاد بخش‌بندی شبکه صنعتی (iDMZ) و جداسازی شبکه با استفاده از فایروال و دیتا دیود، به همراه چگونگی سناریونویسی و پیکربندی یک نمونه فایروال صنعتی و نیز سامانه مدیریت رویدادها و اطلاعات امنیت صنعتی (ISIEM)، از جمله مباحث این کارگاه آموزشی می‌باشد.</p> <p><b>مهارت عملی پس از پایان کارگاه:</b> فراگیران، اصول معماری امن شبکه صنعتی را فرا گرفته و توانایی پیکربندی یک نمونه فایروال و سامانه SIEM مطرح صنعتی را خواهند داشت.</p>	<p>مهندس امیر رضا باقری</p>	<p>معماری امن شبکه صنعتی (OT)</p>	<p>۱۳:۰۰ - ۱۷:۰۰</p>	<p>۴</p>

توضیحات:

- ارائه‌کنندگان کارگاه‌های آموزشی از چهره‌های شاخص و مطرح آن حوزه هستند.
- در هر کارگاه آموزشی، تمرکز بر ارائه مباحث فنی و تجربیات عملی، علاوه بر مباحث تئوری آن حوزه است (حداقل ۷۵ درصد، ضریب فنی هر کارگاه می‌باشد).