جمهوری اسلامی ایران
ریاست جمهوری
مرکز مدیریت راهبردی افتا

معرفی دوره های آموزشی افتا

مهر ۹۶

سطح محرمانگی:عادی


بسم الله الرحمن الرحيم

مشخصات سند:

عنوان سند	معرفی دوره‌های آموزشی افتا
شناسه سند	SET-۰۰۰۱-۰۱
ویرایش	ششم
تاریخ آخرین تغییرات	۱۳۹۶/۰۷/۱۵
سطح محرمانگی	سطح محرمانگی:عادی
مخاطبان	شرکت‌های دارای پروانه فعالیت آموزش افتا

فهرست مطالب

۱- مقدمه

باتوجه به توسعه روزافزون فناوری اطلاعات در ابعاد سازمانی و در راستای نیاز کشور به تربیت متخصصین امنیت اطلاعات مرکز مدیریت راهبردی افتا اقدام به تدوین مستندی به منظور معرفی دوره‌های آموزشی افتا نموده است. این سند که بخشی از نظام آموزش افتا می‌باشد، با محوریت دامنه تحت پوشش «نظام ارزیابی محصولات فتا و خدمات افتا» و در گام نخست، با اولویت تمرکز بر نیازمندی‌های کشور در ارائه خدمات امنیتی افتا تدوین شده‌است. از این‌رو دوره‌های آموزشی معرفی شده در این سند براساس حوزه‌های مرتبط با دسته‌بندی خدمات افتا ارائه‌شده‌اند و شناسنامه معرفی هر دوره شامل هدف دوره، سرفصل مطالب و مرجع، نحوه ارائه، و پیش‌نیاز دانشی لازم برای هر دوره مشخص شود.

این سند با مشارکت سازمان فناوری اطلاعات و ارتباطات ایران و شرکت‌های باتیس کیان ارتباط، شبکه علمی غرب آسیا، امن گستر پیام پرداز، و علی الخصوص مشارکت فعال شرکت‌های سماتک، موسسه فناوری اطلاعات و ارتباطات نیس، کهکشان نور، کاربرد سیستم سدید، و کاریار ارقام بازبینی و تکمیل شده است.

شایان ذکر است که با هدف پوشش دوره‌های جدید و متناسب با نیازهای روز کشور، این سند در بازه‌های زمانی یک ساله بازبینی و اصلاح خواهد شد.

۲- دوره‌های عمومی امنیت

آموزش‌هایی در این دسته قرار می‌گیرند که در راستای آشنایی عمومی با مبحث امنیت اطلاعات و سیستم‌های اطلاعاتی تدوین شده‌اند و زیرساخت علمی لازم برای ورود به حوزه‌های تخصصی امنیت را فراهم آورند. کارشناسان حوزه‌های مختلف امنیت باید تسلط لازم بر روی مباحث این دوره‌ها را داشته باشند.

۲-۱- دوره آشنایی با اصول و مفاهیم امنیت اطلاعات (۱)

جدول ۱: شناسنامه دوره اصول و مفاهیم امنیت اطلاعات (۱)

هدف دوره	آشنایی با اصول و مفاهیم امنیت اطلاعات و سیستم‌ها
مخاطبان	کلیه کارشناسان حوزه امنیت فناوری اطلاعات
سرفصل مطالب	• مفاهیم عمومی امنیت • شناسایی ریسک‌های بالقوه • زیرساخت و ارتباطات • مانیتورینگ و خطایابی شبکه • امن‌سازی شبکه و محیط (امنیت کاربرد، داده و میزبان) • آشنایی با تروجان‌ها، درب‌های پشتی، روت‌کیت‌ها، ویروس‌ها و کرم‌ها و همچنین نحوه پاکسازی و مقابله با آنها • امن‌سازی سیستم‌عامل • امن‌سازی تبادلات آنلاین • تهدیدات مهندسی اجتماعی و راهکارهای مقابله • امنیت اطلاعات و الزامات قانونی • مقدمات، روش‌ها و استانداردهای رمزنگاری • سیاست‌ها و روال‌های امنیتی • راهبری امنیت • آشنایی با دیواره‌های آتش و پیکربندی امنیتی آنها • آشنایی با نحوه تنظیم گزارش‌های وقایع، خطاها و مستندات امنیتی در سازمان
نحوه ارائه دوره	تئوری
پیش‌نیاز	این دوره پیش‌نیاز در حوزه امنیت اطلاعات ندارد، اما آشنایی با مفاهیم عمومی کامپیوتر، سیستم و شبکه لازم است.
مراجع	SANS ۳۰۱
مدت زمان دوره	۴۰ ساعت

۲-۲-دوره آشنایی با اصول و مفاهیم امنیت اطلاعات (۲)

جدول ۲: شناسنامه دوره اصول و مفاهیم امنیت اطلاعات (۲)

هدف دوره	آشنایی با اصول و مفاهیم امنیت اطلاعات و سیستم‌ها
مخاطبان	کلیه کارشناسان حوزه امنیت فناوری اطلاعات
سرفصل مطالب	• مفاهیم شبکه و مجازی سازی • پروتکلهای پایه شبکه • مفاهیم تضمین اطلاعات • سیاست‌ها و روال‌های امنیتی • طرح تداوم کسب و کار • کنترل دسترسی • مدیریت کلمه عبور • پاسخ به رخداد • روشها و استراتژی‌های حمله • پویش آسیب پذیری • امنیت وب • دیوار آتش • تله عسل • حفاظت در سطح سیستم کاربری • تشخیص و جلوگیری از نفوذ مبتنی بر شبکه • رمزنگاری • کنترل‌های امنیتی حیاتی • ارزیابی و ممیزی امنیتی • امنیت ویندوز • امنیت لینوکس
نحوه ارائه دوره	تئوری
پیش‌نیاز	دوره اصول و مفاهیم امنیتی (۱)
مراجع	SANS ۴۰۱
مدت زمان دوره	۴۰ ساعت

۳- دوره‌های مدیریت امنیت

این دسته دوره‌های شامل دوره‌های آموزشی لازم برای استقرار سیستم مدیریت امنیت اطلاعات و نیز دوره‌های تخصصی لازم برای مدیران امنیت فناوری اطلاعات تدوین گردیده است.

کارشناسان استقرار سیستم مدیریت امنیت اطلاعات به دسته‌های زیر تقسیم بندی می‌شوند:

- کارشناس استقرار سیستم مدیریت امنیت اطلاعات
- کارشناس مدیریت مخاطرات
- مدیر استقرار سیستم مدیریت امنیت اطلاعات
- ممیز و سرممیز سیستم مدیریت امنیت اطلاعات

کارشناس استقرار سیستم مدیریت امنیت اطلاعات می‌تواند به ترتیب از دوره‌های زیر استفاده نماید:

۱. دوره آشنایی با اصول و مفاهیم و تشریح الزامات سیستم مدیریت امنیت اطلاعات
۲. دوره پیاده‌سازی کنترل‌های فنی استاندارد مدیریت امنیت اطلاعات

کارشناس مدیریت مخاطرات می‌تواند به ترتیب از دوره‌های زیر استفاده نماید:

۱. دوره آشنایی با اصول و مفاهیم و تشریح الزامات سیستم مدیریت امنیت اطلاعات
۲. آشنایی با مفاهیم مدیریت مخاطرات

مدیر استقرار سیستم مدیریت امنیت اطلاعات می‌تواند به ترتیب از دوره‌های زیر استفاده نماید:

۱. دوره آشنایی با اصول و مفاهیم و تشریح الزامات سیستم مدیریت امنیت اطلاعات
۲. دوره طرح ریزی و استقرار سیستم مدیریت امنیت اطلاعات
۳. دوره اندازه‌گیری اثربخشی سیستم مدیریت امنیت اطلاعات
۴. دوره سرممیزی مدیریت امنیت اطلاعات

ممیز و سرممیز سیستم مدیریت امنیت اطلاعات می‌توانند به ترتیب از دوره‌های زیر استفاده نماید:

۱. دوره آشنایی با اصول و مفاهیم و تشریح الزامات سیستم مدیریت امنیت اطلاعات
۲. دوره طرح ریزی و استقرار سیستم مدیریت امنیت اطلاعات
۳. دوره سرممیزی مدیریت امنیت اطلاعات

ضمن آنکه پیشنهاد می‌گردد که ممیز و سرممیز بر مباحث دوره‌های " آشنایی با مفاهیم مدیریت مخاطرات" و " پیاده‌سازی کنترل‌های فنی استاندارد مدیریت امنیت اطلاعات" و " اندازه‌گیری اثربخشی سیستم مدیریت امنیت اطلاعات" اشراف داشته باشد.

مدیران امنیت فناوری اطلاعات می‌توانند به ترتیب از دوره‌های زیر استفاده نمایند:

۱- دوره کارشناس امنیت سیستم‌های اطلاعاتی

۲- دوره مدیر امنیت اطلاعات

۳-۱-دوره آشنایی با اصول و مفاهیم و تشریح الزامات سیستم مدیریت امنیت اطلاعات

جدول ۳: شناسنامه دوره آشنایی با اصول و مفاهیم و تشریح لزامات سیستم مدیریت امنیت اطلاعات

هدف دوره	آشنایی با اصول و مفاهیم و تشریح الزامات سیستم مدیریت امنیت اطلاعات
مخاطبین دوره	کارشناسان استقرار سیستم مدیریت امنیت اطلاعات
سرفصل مطالب	• معرفی انواع مشکلات و نقض‌های امنیتی رایج در سازمان‌ها • آشنایی با مفاهیم کلی اطلاعات و نقش آن به‌عنوان بخشی از سرمایه‌ها و دارایی‌های سازمانی • لزوم حفاظت از دارایی‌های اطلاعاتی • آشنایی با مفهوم مخاطرات و آسیب‌پذیری‌ها • آشنایی با گام‌های پیاده‌سازی سیستم مدیریت امنیت اطلاعات • سیاست‌های امنیتی • سازماندهی امنیت اطلاعات فیزیکی و مجازی • مدیریت تجهیزات • امنیت فیزیکی و پیرامونی • مدیریت ارتباطات و عملیات • کنترل دسترسی ها • کسب، بهبود و نگهداری سیستم اطلاعات • مدیریت حوادث امنیتی • مدیریت مستمر کسب و کار
نحوه ارائه دوره	تئوری
پیش‌نیاز	دوره آشنایی با اصول و مفاهیم امنیت اطلاعات (۱)
مراجع	PECB ISO 27001:2013 foundation
مدت زمان دوره	۱۶ساعت

۳-۲- دوره طرح ریزی و استقرار سیستم مدیریت امنیت اطلاعات

جدول ۴: شناسنامه دوره طرح ریزی و استقرار پیاده‌سازی مدیریت امنیت اطلاعات

هدف دوره	آشنایی با فرایندها و کنترل‌های غیرفنی استاندارد ISO ۲۷۰۰۱
مخاطبین	کارشناسان استقرار سیستم مدیریت امنیت اطلاعات
سرفصل مطالب	• معرفی اصول، مفاهیم و الزامات سیستم مدیریت امنیت اطلاعات • آشنایی با مفهوم فرآیند و دیدگاه فرآیندگرا و چرخه PDCA • معرفی و تشریح فازهای پروژه پیاده سازی ISMS • نحوه آنالیز شکاف (Gap Analysis) سازمان کارفرما و شناخت اولیه • تهیه و تدوین خط مشی امنیت اطلاعات • انتخاب متدولوژی شناسایی و مدیریت مخاطرات امنیت اطلاعات • چگونگی شناسائی ریسک‌های سازمانی • نحوه برخورد و مقابله با مخاطرات • تشریح کنترل‌ها و اهداف کنترلی پیوست الف ISO ۲۷۰۰۱ • تهیه طرح پروژه پیاده سازی سیستم مدیریت امنیت اطلاعات • نحوه تدوین و طراحی روش‌های اجرایی و مستندات مورد نیاز • تهیه برنامه آموزش و آگاهی رسانی امنیتی • مدیریت حوادث امنیتی و مدیریت تداوم کسب و کار (BCM) • شاخص‌های امنیتی پایش و اندازه گیری اثربخشی کنترلهای ISMS • مروری بر گام‌های پیاده سازی ISMS طبق ISO ۲۷۰۰۳
نحوه ارائه دوره	تئوری- عملی
پیش‌نیاز	دوره آشنایی با اصول و مفاهیم و تشریح الزامات سیستم مدیریت امنیت اطلاعات
مراجع	PECB ISO ۲۷۰۰۱:۲۰۱۳ Lead Implementer
مدت زمان دوره	۴۰ ساعت

۳-۳-دوره پیاده‌سازی کنترل‌های فنی استاندارد سیستم مدیریت امنیت اطلاعات

جدول ۵: شناسنامه دوره پیاده‌سازی کنترل‌های فنی سیستم مدیریت امنیت اطلاعات۲۷۰۰۱

هدف دوره	آشنایی با فرایندها و کنترل‌های فنی استاندارد ISO۲۷۰۰۱
مخاطبین دوره	کارشناسان استقرار سیستم مدیریت امنیت اطلاعات
سرفصل مطالب	• کنترل‌های امنیت فیزیکی و محیطی • کنترل‌های مدیریت ارتباطات و عملیات • کنترل‌های مدیریت دسترسی • کنترل‌های توسعه و نگهداری سیستم • کنترل‌های مدیریت حوادث • کنترل‌های مدیریت تداوم کسب و کار • کنترل‌های انطباق با الزامات قانونی
نحوه ارائه دوره	تئوری- عملی
پیش‌نیاز	دوره آشنایی با اصول و مفاهیم و تشریح الزامات سیستم مدیریت امنیت اطلاعات
مراجع	SANS ۵۶۶
مدت زمان دوره	۴۰ ساعت

۳-۴-آشنایی با مدیریت مخاطرات

جدول ۶: شناسنامه دوره آشنایی با مفاهیم مدیریت مخاطرات

هدف دوره	شناسایی، ارزیابی و مدیریت مخاطرات
مخاطبین	کارشناسان استقرار سیستم مدیریت امنیت اطلاعات
سرفصل مطالب	• مقدمه‌ای بر مخاطرات و مدیریت مخاطرات • مروری بر مدل‌های موجود در مورد مخاطرات و مدیریت آن • مروری بر تعیین جایگاه افراد در پروژه و جایگاه مدیریت مخاطرات در پروژه • تخصیص مخاطرات و چگونگی انجام آن در قراردادها • فرایندهای مدیریت مخاطرات • مبانی آنالیز کیفی و کمی مخاطرات • مبانی کنترل و مدیریت مخاطرات • آشنایی با روش‌های شناسایی و مدیریت دارایی‌ها • آشنایی با آسیب‌پذیری‌ها و تهدیدات امنیتی دارایی‌ها • آشنایی با روش‌های ارزیابی مخاطرات امنیت اطلاعات • آشنایی با روش‌های شناسایی و تعیین احتمال وقوع تهدیدات • آشنایی با روش‌های مدیریت مخاطرات سایبری • آشنایی با روش‌های اتخاذ کنترل‌های امنیتی • مفاهیم و ابزارهای پیشرفته مدیریت امنیت • مدیریت مخاطرات کسب و کار • بدست آوردن متدولوژی‌های مختلف بررسی و شناسایی مخاطرات • آنالیز کیفی و کمی پیشرفته مخاطرات • شناخت نقش سرمایه سازمان و خطرات مرتبط با آن • توسعه و طراحی و اجرای ابزارهای مورد نیاز برای شناسایی و اندازه‌گیری • آشنایی و بررسی متدولوژی شناسایی و مدیریت دارایی‌ها • نحوه انتخاب و تعیین متدلوژی مناسب ارزیابی مخاطرات امنیت اطلاعات
نحوه ارائه دوره	تئوری
پیش‌نیاز	دوره آشنایی با اصول و مفاهیم و تشریح الزامات سیستم مدیریت امنیت اطلاعات
مراجع	PECB Lead Risk Manager
مدت زمان دوره	۲۴ ساعت

۳-۵-دوره اندازه‌گیری اثربخشی سیستم مدیریت امنیت اطلاعات

جدول ۷: شناسنامه دوره اندازه گیری اثربخشی سیستم مدیریت امنیت اطلاعات

هدف دوره	آشنایی با نحوه اندازه گیری، تعیین شاخص ها، تحلیل داده‌ها و گزارش دهی اثربخشی امنیت اطلاعات
مخاطبین	کارشناسان استقرار سیستم مدیریت امنیت اطلاعات
سرفصل مطالب	• مروری بر مفاهیم سیستم مدیریت امنیت اطلاعات (ISMS) • معرفی استاندارد ISO ۲۷۰۰۴ بعنوان استانداردی جهت اندازه گیری اثربخشی ISMS • اهداف اندازه گیری امنیت اطلاعات • مزایای اندازه گیری اثربخشی امنیت در سازمان • گام‌های فرآیند اندازه گیری امنیت • برنامه اندازه گیری امنیت اطلاعات • فاکتورهای مؤثر در موفقیت برنامه اندازه گیری امنیت اطلاعات • مدل اندازه گیری امنیت اطلاعات • انواع معیارها و مشخصه‌های اندازه گیری • گزارش دهی نتایج اندازه گیری • ارزیابی و بهبود برنامه اندازه گیری امنیت اطلاعات
نحوه ارائه دوره	تئوری
پیش‌نیاز	دوره طرح ریزی و استقرار پیاده‌سازی مدیریت امنیت اطلاعات
مراجع	Measurement of Information Security (ISO/IEC ۲۷۰۰۴)
مدت زمان دوره	۱۶ ساعت

۳-۶-دوره سرممیزی سیستم مدیریت امنیت اطلاعات

جدول ۸: شناسنامه دوره سرممیزی سیستم مدیریت امنیت اطلاعات

هدف دوره	آشنایی با اصول و ضوابط ممیزی شخص ثالث و سازمان
مخاطبین	کارشناسان استقرار سیستم مدیریت امنیت اطلاعات
سرفصل مطالب	• آموزش مفاهیم و الزامات سیستم مدیریت امنیت اطلاعات • مروری بر کنترلهای امنیتی و اهداف کنترلی ISO/IEC ۲۷۰۰۱ • آشنایی با نحوه تعیین صلاحیت، ارزیابی و انتخاب ممیزان داخلی و خارجی • مروری بر مفاهیم سرممیزی مدیریت امنیت اطلاعات • آشنایی با مخاطرات و مخاطرات‌های سازمان • اجرا و هدایت تیم ممیزی ، جمع آوری اطلاعات • جمع بندی اطلاعات ، یافته‌ها ، شناخت موارد عدم انطباق و نگرش به ریشه های عدم انطباق‌ها • تهیه چک لیست ممیزی • ثبت و طبقه بندی عدم انطباق‌ها • فرایند گزارش‌دهی عدم انطباق‌ها • پیگیری عدم انطباقها و اقدامات اصلاحی • بهره‌گیری از رویکردهای روانشناختی در ممیزی مرحله دوم • برنامه ریزی برای ممیزی داخلی و خارجی • نحوه بررسی و سنجش ارزیابان و ممیزان • نحوه ارزیابی ممیزان و کارشناسان انجام ممیزی سازمان • فرایند ارائه گواهینامه • آشنایی با روال و ضوابط بین المللی ممیزی شخص ثالث واستانداردهای راهنما ISO ۱۷۰۲۱
نحوه ارائه دوره	تئوری- عملی
پیش‌نیاز	دوره طرح ریزی و استقرار پیاده‌سازی مدیریت امنیت اطلاعات
مراجع	PECB ISO 27001:2013 Lead auditor
مدت زمان دوره	۴۰ ساعت

۳-۷-دوره کارشناس امنیت سیستم‌های اطلاعاتی

جدول ۹: شناسنامه دوره کارشناس امنیت سیستم‌های اطلاعاتی

هدف دوره	کسب مهارت در شناسایی و تحلیل مخاطرات، تکنیک‌های کنترل دسترسی و حفاظت از اطلاعات
مخاطبین	مدیران ارشد ، مدیران امنیت، شبکه و فناوری اطلاعات, مدیران حراست سازمانها
سرفصل مطالب	مدل ISO، پروتکل‌ها، امنیت شبکه و زیر ساخت شبکه امنیت ارتباطات و کنترل دسترسی حملات و پایش مفاهیم و مبانی مدیریت امنیت ارزش دارایی‌ها، سیاست‌ها و نقش‌ها امنیت داده‌ها و نرم افزارهای کاربردی کدهای مخرب و حمله به نرم افزارهای کاربردی رمزنگاری و الگوریتم‌های کلید خصوصی و زیر ساخت کلید عمومی و نرم افزارهای رمزنگاری مبانی طراحی رایانه ای و مبانی مدل‌های امنیتی مدیریت اجرایی و ممیزی و پایش برنامه ریزی استمرار کسب و کار برنامه ریزی برای مقابله با حوادث غیر مترقبه قوانین و پی جویی و حوادث و اصول اخلاقی امنیت فیزیکی
نحوه ارائه دوره	تئوری
پیش‌نیاز	دوره اصول و مفاهیم امنیت اطلاعات (۲)
مراجع	Official (ISC)²® Guide to the CISSP® CBK® ,Fourth Edition.
مدت زمان دوره	۴۰ ساعت

۳-۸-دوره مدیر امنیت اطلاعات

جدول ۱۰: شناسنامه دوره مدیر امنیت اطلاعات

هدف دوره	**توانمندسازی مدیران ارشدو روسای امنیت سایبری**
مخاطبین	مدیر امنیت اطلاعات، مدیر فناوری اطلاعات، راهبر مدیریت ریسک
سرفصل مطالب	• حکمرانی امنیت اطلاعات (خط‌مشی‌ها ، قوانین و مقررات و انطباق با الزامات و آئین‌نامه‌های اجرایی) • کنترلهای سیستم مدیریت امنیت اطلاعات و مدیریت بر فرآیند ممیزی امنیت اطلاعات • مدیریت در حوزه پروژه‌ها و عملیات مرتبط با امنیت اطلاعات(پروژه ها، فناوری‌ها و عملیات اجرایی) • شایستگیهای محوری در امنیت اطلاعات • برنامه ریزی استراتژیک و مدیریت مالی
نحوه ارائه دوره	تئوری
پیش‌نیاز	دوره کارشناس امنیت سیستم‌های اطلاعاتی
مراجع	Eccouncil CCISO
مدت زمان دوره	۴۰ ساعت

۴- دوره‌های آزمون و ارزیابی

این دوره‌ها جهت آموزش کارشناسان حوزه آزمون و ارزیابی در نظر گرفته شده است. کارشناسان حوزه آزمون و ارزیابی بر اساس تخصص به دسته‌های زیر تقسیم بندی می‌شوند:

- کارشناس تست نفوذ شبکه و زیرساخت
- کارشناس تست نفوذ وب
- کارشناس تست نفوذ موبایل
- کارشناسان تست نفوذ شبکه‌های بی سیم

کارشناسان تست نفوذ شبکه و زیرساخت می‌توانند به ترتیب از دوره‌های زیر استفاده نمایند:

۱- دوره مقدماتی نفوذ و مقابله در فضای سایبری
۲- دوره نفوذ و مقابله در شبکه
۳- دوره پایتون و اکسپلویت نویسی برای تست نفوذ

کارشناسان تست نفوذ وب می‌توانند به ترتیب از دوره‌های زیر استفاده نمایند:

۱- دوره مقدماتی نفوذ و مقابله در فضای سایبری
۲- دوره مقدماتی تست نفوذ برنامه‌های کاربردی تحت وب
۳- دوره پیشرفته تست نفوذ برنامه‌های کاربردی تحت وب

کارشناسان تست نفوذ موبایل می‌توانند به ترتیب از دوره‌های زیر استفاده نمایند:

۱- دوره مقدماتی نفوذ و مقابله در فضای سایبری
۲- دوره مقدماتی تست نفوذ موبایل

کارشناسان تست نفوذ شبکه‌های بی سیم می‌توانند به ترتیب از دوره‌های زیر استفاده نمایند:

۱- دوره مقدماتی نفوذ و مقابله در فضای سایبری
۲- دوره نفوذ و مقابله در شبکه‌های بی سیم

۴-۱-دوره مقدماتی نفوذ و مقابله در فضای سایبری

جدول ۱۱: شناسنامه دوره مقدماتی نفوذ و مقابله در فضای سایبری

هدف دوره	کسب توانایی کشف آسیب‌پذیری‌های سیستم، شبکه و سامانه‌ها و مدیریت رخدادها
مخاطبین	کلیه کارشناسان حوزه آزمون و ارزیابی
سرفصل مطالب	Incident handling step-by-step Computer and network hack exploits Hacker tools workshop
نحوه ارائه دوره	تئوری- عملی
پیش‌نیاز	دوره‌های آشنایی با اصول و مفاهیم امنیتی (۱و۲)
مراجع	SANS SEC ۵۰۴
مدت زمان دوره	۴۰ ساعت

۴-۲- دوره نفوذ و مقابله در شبکه

جدول ۱۲: دوره نفوذ و مقابله در شبکه

هدف دوره	کسب توانایی کشف آسیب‌پذیری‌های شبکه
مخاطبین	کارشناسان تست نفوذ شبکه و زیرساخت
سرفصل مطالب	Comprehensive Pen Test Planning, Scoping and Recon In-depth Scanning Exploiting Post-Exploitation Password Attack Wireless and web apps Pen Testing
نحوه ارائه دوره	تئوری-عملی
پیش‌نیاز	دوره مقدماتی نفوذ و مقابله در فضای سایبری
مراجع	SANS ۵۶۰
مدت زمان دوره	۴۰ ساعت

۴-۳-دوره مقدماتی تست نفوذ برنامه‌های کاربردی تحت وب

جدول ۱۳: شناسنامه دوره مقدماتی تست نفوذ برنامه‌های کاربردی تحت وب

هدف دوره	آشنایی با مباحث مقدماتی تست نفوذ برنامه‌های کاربردی تحت وب
	کارشناسان تست نفوذ وب
سرفصل مطالب	آشنایی با اصول جمع آوری اطلاعات آشنایی با انواع تست‌های شناسایی اعلام و احراز هویت تحت وب آشنایی با صول Injection آشنایی با Java Script و XSS آشنایی با CSRF ، Logical Flow
نحوه ارائه دوره	تئوری-عملی
پیش‌نیاز	دوره مقدماتی نفوذ و مقابله در فضای سایبری
مراجع	SANS-۵۴۲
مدت زمان دوره	۴۰ ساعت

۴-۴-دوره پیشرفته تست نفوذ برنامه‌های کاربردی تحت وب

جدول ۱۴: شناسنامه دوره پیشرفته تست نفوذ برنامه‌های کاربردی تحت وب

هدف دوره	آشنایی با مباحث مقدماتی تست نفوذ برنامه‌های کاربردی تحت وب
مخاطبین	کارشناسان تست نفوذ وب
سرفصل مطالب	رمزگذاری برنامه‌های کاربردی وب برنامه‌های کاربردی موبایل و وب سرویس‌ها کشف و استفاده از برنامه‌های کاربردی خاص
نحوه ارائه دوره	تئوری-عملی
پیش‌نیاز	دوره مقدماتی تست نفوذ برنامه‌های کاربردی تحت وب
مراجع	SANS-۶۴۲
مدت زمان دوره	۴۰ ساعت

۴-۵-دوره مقدماتی تست نفوذ موبایل

جدول ۱۵: دوره مقدماتی تست نفوذ موبایل

هدف دوره	کسب توانایی ارزیابی سطح امنیتی برنامه‌های کاربردی و سیسم‌های عامل نهفته دستگاه‌های همراه
مخاطبین	کارشناسان تست نفوذ موبایل
سرفصل مطالب	معماری تجهیزات موبایل و تهدیدات رایج موبایل تحلیل برنامه‌های کاربردی و دسترسی به پلت‌فرم‌های موبایل مهندسی معکوس برنامه‌های کاربردی موبایل تست نفوذ دستگاه‌های موبایل
نحوه ارائه دوره	تئوری- عملی
پیش‌نیاز	دوره مقدماتی نفوذ و مقابله در فضای سایبری
مراجع	SANS-SEC۵۷۵
مدت زمان دوره	۴۰ ساعت

۴-۶-دوره نفوذ و مقابله در شبکه‌های بی‌سیم

جدول ۱۶: دوره نفوذ و مقابله در شبکه‌های بی سیم

هدف دوره	کسب توانایی نفوذ و مقاوم سازی در شبکه‌های بی سیم
مخاطبین	کارشناسان تست نفوذ شبکه‌های بی سیم
سرفصل مطالب	Wireless Data Collection and WiFi MAC Analysis Wireless Tools and Information Analysis Client, Crypto, and Enterprise Attacks Advanced WiFi Attack Techniques Bluetooth, DECT and ZigBee Attacks Wireless Security Strategies and Implementation
نحوه ارائه دوره	تئوری-عملی
پیش‌نیاز	دوره مقدماتی نفوذ و مقابله در فضای سایبری
مراجع	SANS ۶۱۷
مدت زمان دوره	۴۰ ساعت

۵- دوره‌های پایش و تحلیل امنیت

این دوره‌ها جهت آموزش کارشناسان حوزه پایش و تحلیل امنیت در نظر گرفته شده است. کارشناسان حوزه پایش و تحلیل امنیت بر اساس تخصص به دسته‌های زیر تقسیم بندی می‌شوند

- تحلیلگر امنیت اطلاعات
- پی جویی و کشف جرائم امنیت اطلاعات

کارشناسان تحلیلگر امنیت اطلاعات می‌توانند به ترتیب از دوره‌های زیر استفاده نمایند:

۱- دوره مفاهیم اولیه در پایش و تحلیل

۲- دوره تحلیل امنیت شبکه

۳- دوره پیشرفته تحلیل امنیت شبکه

۴- دوره مهندسی مجدد بدافزارها

کارشناسان پی جویی و کشف جرائم امنیت اطلاعات می‌توانند به ترتیب از دوره‌های زیر استفاده نمایند:

۱- دوره مقدماتی جرم‌شناسی رایانه‌ای

۲- دوره جرم‌شناسی رایانه‌ای

۳- دوره جرم‌شناسی پیشرفته دستگاه‌های موبایل

۴- دوره جرم‌شناسی پیشرفته حافظه

۵- دوره مهندسی مجدد بدافزارها

۵-۱-دوره مفاهیم اولیه در پایش و تحلیل

جدول ۱۷: شناسنامه دوره مفاهیم اولیه در پایش و تحلیل

هدف دوره	آشنایی با مفاهیم پایه در پایش و تحلیل
مخاطبین	کارشناسان تحلیلگر امنیت اطلاعات
سرفصل مطالب	Defensive Network Infrastructure Packet Analysis Pentest First Responder Malware Data Loss Prevention
نحوه ارائه دوره	تئوری-عملی
پیش‌نیاز	دوره اصول و مفاهیم امنیت اطلاعات (۲)
مراجع	SANS SEC۵۰۱
مدت زمان دوره	۴۰ ساعت

۵-۲- دوره تحلیل امنیت شبکه

جدول ۱۸: شناسنامه دوره تحلیل امنیت شبکه

هدف دوره	آشنایی با تحلیل رخدادها و تحلیل ترافیک
مخاطبین	کارشناسان تحلیلگر امنیت اطلاعات
سرفصل مطالب	TCP/IP for Intrusion Detection Network Traffic Analysis Using Tcpdump Intrusion Detection Snort Style Security Information Management and traffic Analysis
نحوه ارائه دوره	تئوری-عملی
پیش‌نیاز	دوره مفاهیم اولیه در پایش و تحلیل
مراجع	SANS-SEC ۵۰۳
مدت زمان دوره	۴۰ ساعت

۵-۳-دوره پیشرفته تحلیل امنیت شبکه

جدول ۱۹: شناسنامه دوره پیشرفته تحلیل امنیت شبکه

هدف دوره	آشنایی با مفاهیم پیشرفته در تحلیل ترافیک و رخدادها
مخاطبین	کارشناسان تحلیلگر امنیت اطلاعات
سرفصل مطالب	Off the Disk and Onto the Wire Core Protocols & Log Aggregation/Analysis NetFlow and File Access Protocols Commercial Tools, Wireless, and Full-Packet Hunting Encryption, Protocol Reversing, OPSEC, and Intel Network Forensics Capstone Challenge
نحوه ارائه دوره	تئوری-عملی
پیش‌نیاز	دوره تحلیل امنیت شبکه
مراجع	SANS-FOR ۵۷۲
مدت زمان دوره	۴۰ ساعت

۵-۴-دوره مقدماتی جرم‌شناسی رایانه‌ای[۱]

جدول ۲۰: شناسنامه دوره مقدماتی جرم‌شناسی رایانه‌ای

هدف دوره	شناسایی و کشف جرایم رایانه‌ای
مخاطبین	کارشناسان پی جویی و کشف جرائم امنیت اطلاعات
سرفصل مطالب	Windows Digital Forensics And Advanced Data Triage Core Windows Forensics Part I: Windows Registry Forensics And Analysis Core Windows Forensics Part II: Usb Devices And Shell Items Core Windows Forensics Part III: E-Mail, Key Additional Artifacts, And Event Logs Core Windows Forensics Part IV: Web Browser Forensics - Firefox, Internet Explorer, And Chrome Windows Forensic Challenge
نحوه ارائه دوره	تئوری-عملی
پیش‌نیاز	مقدماتی نفوذ و مقابله در فضای سایبری
مراجع	SANS-FOR ۴۰۸
مدت زمان دوره	۴۰ ساعت

[۱] CHFI

۵-۵- دوره تخصصی جرم‌شناسی رایانه‌ای

جدول ۲۱: شناسنامه دوره تخصصی جرم‌شناسی رایانه‌ای

هدف دوره	آشنایی با مفاهیم پیشرفته در جرم شناسی و تحلیل سیستم
مخاطبین	کارشناسان پی جویی و کشف جرائم امنیت اطلاعات
سرفصل مطالب	Advanced Incident Response & Threat Hunting Memory Forensics in Incident Response & Threat Hunting Intrusion Forensics Timeline Analysis Incident Response & Hunting Across the Enterprise | Advanced Adversary & Anti-Forensics Detection The APT Incident Response Challenge
نحوه ارائه دوره	تئوری- عملی
پیش‌نیاز	دوره مقدماتی جرم‌شناسی رایانه‌ای
مراجع	SANS-FOR۵۰۸
مدت زمان دوره	۴۰ ساعت

۵-۶- دوره آموزشی جرم‌شناسی پیشرفته دستگاه‌های موبایل

جدول ۲۲: شناسنامه دوره جرم‌شناسی پیشرفته دستگاه‌های موبایل

هدف دوره	جرم‌شناسی پیشرفته در تلفن‌های همراه
مخاطبین	کارشناسان پی جویی و کشف جرائم امنیت اطلاعات
سرفصل مطالب	Malware Forensics, Smartphone Overview, and SQLite Introduction Android Forensics Android Backups and iOS Device Forensics iOS Backups, Windows, and BlackBerry ۱۰ Forensics Third-Party Application and Knock-Off Forensics Smartphone Forensic Capstone Exercise
نحوه ارائه دوره	تئوری-عملی
پیش‌نیاز	دوره مقدماتی جرم‌شناسی رایانه‌ای
مراجع	SANS-FOR۵۸۵
مدت زمان دوره	۴۰ ساعت

۵-۷-دوره آموزشی جرم‌شناسی پیشرفته حافظه

جدول ۲۳: شناسنامه دوره جرم‌شناسی پیشرفته حافظه

هدف دوره	آشنایی با تحلیل محتوی حافظه
مخاطبین	کارشناسان پی جویی و کشف جرائم امنیت اطلاعات
سرفصل مطالب	Foundations in Memory Analysis and Acquisition Unstructured Analysis and Process Exploration Investigating the User via Memory Artifacts Internal Memory Structures Memory Analysis on Platforms Other than Windows Memory Analysis Challenges
نحوه ارائه دوره	تئوری- عملی
پیش‌نیاز	دوره پیشرفته جرم‌شناسی رایانه‌ای
مراجع	SANS-FOR۵۲۶
مدت زمان دوره	۴۰ ساعت

۵-۸-دوره مهندسی معکوس بدافزارها

جدول ۲۴: شناسنامه دوره مهندسی مجدد بدافزارها

هدف دوره	آشنایی با روش‌های مقابله با بدافزارها و آنالیز رفتار آنها
مخاطبین	کارشناسان پی جویی و کشف جرائم امنیت اطلاعات
سرفصل مطالب	Malware Analysis Fundamentals Reversing Malicious Code Malicious Web and Document Files In-Depth Malware Analysis Examining Self-Defending Malware Malware Analysis Tournament
نحوه ارائه دوره	تئوری-عملی
پیش‌نیاز	مقدماتی نفوذ و مقابله در فضای سایبری
مراجع	SANS-FOR۶۱۰
مدت زمان دوره	۴۰ ساعت

۶- دوره‌های امن سازی زیرساخت ها، سرویس‌ها و سامانه ها

این دوره‌ها جهت آموزش کارشناسان حوزه امن سازی زیرساخت ها، سرویس‌ها و سامانه‌ها در نظر گرفته شده است. کارشناسان حوزه امن سازی زیرساخت ها، سرویس‌ها و سامانه‌ها بر اساس تخصص به دسته‌های زیر تقسیم بندی می‌شوند:

- کارشناس امن سازی سیستم عامل
- کارشناس امن سازی زیرساخت
- کارشناس امن سازی نرم افزار

کارشناسان امن سازی سیستم عامل می‌توانند به ترتیب از دوره‌های زیر استفاده نمایند:

۱- دوره امن‌سازی ویندوز

۲- دوره امن‌سازی لینوکس/ یونیکس

کارشناسان امن سازی زیرساخت می‌توانند به ترتیب از دوره‌های زیر استفاده نمایند:

۱- دوره امن‌سازی ویندوز

۲- دوره امن‌سازی لینوکس/ یونیکس

۳- مجازی سازی و امنیت فضای ابر

کارشناسان امن سازی نرم افزار می‌توانند به ترتیب از دوره‌های زیر استفاده نمایند:

۱- دوره کد نویسی امن در طراحی وب

۲- دوره برنامه‌نویسی امن در جاوا

۳- دوره برنامه نویسی امن در .NET.

۶-۱- دوره امن‌سازی ویندوز

جدول ۲۵: شناسنامه دوره امن‌سازی ویندوز

هدف دوره	آشنایی با مباحث مربوط به پیکربندی امن ویندوز و آموزش PowerShell
مخاطبین	کارشناسان امن سازی زیرساخت و سیستم عامل
سرفصل مطالب	PowerShell Automation and Security Continuous Secure Configuration Enforcement Windows Public Key Infrastructure and Smart Cards Administrative Compromise and Privilege Management

	Endpoint Protection and Pre-Forensics Defensible Networking and Blue Team WMI
نحوه ارائه دوره	تئوری-عملی
پیش‌نیاز	دوره آشنایی با اصول و مفاهیم امنیت اطلاعات (۲)
مراجع	SANS-SEC۵۰۵
مدت زمان دوره	۴۰ ساعت

۶-۲- دوره امن‌سازی لینوکس/ یونیکس

جدول ۲۶: شناسنامه دوره امن‌سازی لینوکس/ یونیکس

هدف دوره	آشنایی با پیکربندی امن سیستم عامل لینوکس
مخاطبین	کارشناسان امن سازی زیرساخت و سیستم عامل
سرفصل مطالب	Hardening Linux/Unix Systems, Part ۱ Hardening Linux/Unix Systems, Part ۲ Hardening Linux/Unix Systems, Part ۳ Application Security, Part ۱ Application Security, Part ۲ Digital Forensics for Linux/Unix
نحوه ارائه دوره	تئوری-عملی
پیش‌نیاز	دوره آشنایی با اصول و مفاهیم امنیت اطلاعات (۲)
مراجع	SANS- SEC۵۰۶
مدت زمان دوره	۴۰ ساعت

۶-۳-دوره مجازی سازی و امنیت فضای ابر

جدول ۲۷: شناسنامه دوره مجازی سازی و امنیت فضای ابر

هدف دوره	آشنایی با معماری فضای ابر و ریسک‌ها و مخاطرات فضای ابر
مخاطبین	کارشناسان امن سازی زیرساخت
سرفصل مطالب	Core Concepts of Virtualization Security Virtualization and Software-Defined Security Architecture and Design Virtualization Threats, Vulnerabilities, and Attacks Defending Virtualization and Software-Defined Technologies Virtualization Operations, Auditing, and Monitoring
نحوه ارائه دوره	تئوری- عملی
پیش‌نیاز	دوره آشنایی با اصول و مفاهیم امنیت اطلاعات (۲)
مراجع	SANS- SEC ۵۷۹
مدت زمان دوره	۴۰ ساعت

۶-۴-دوره آموزشی کد نویسی امن در طراحی وب

جدول ۲۸: شناسنامه دوره کد نویسی امن در طراحی وب

هدف دوره	کدنویسی امن در طراحی وب
مخاطبین	کارشناسان امن سازی نرم افزار
سرفصل مطالب	Web Basics and Authentication Security Web Application Common Vulnerabilities and Mitigations Proactive Defense and Operation Security AJAX and Web Services Security Cutting-Edge Web Security Capture and Defend the Flag Exercise
نحوه ارائه دوره	تئوری-عملی
پیش‌نیاز	دوره مقدماتی تست نفوذ برنامه‌های کاربردی تحت وب – آشنایی با مبانی برنامه نویسی وبرنامه نویسی وب
مراجع	SANS-DEV۵۲۲
مدت زمان دوره	۴۰ ساعت

۶-۵- دوره برنامه نویسی امن در جاوا

جدول ۲۹: شناسنامه دوره برنامه‌نویسی امن در جاوا

هدف دوره	آشنایی با برنامه‌نویسی امن در محیط جاوا
مخاطبین	کارشناسان امن سازی نرم افزار
سرفصل مطالب	Data Validation Authentication and Session Management Java Platform and API Security Secure Development Lifecycle
نحوه ارائه دوره	تئوری-عملی
پیش‌نیاز	دوره کد نویسی امن در طراحی وب
مراجع	SANS-DEV۵۴۱
مدت زمان دوره	۳۲ ساعت

۶-۶- دوره برنامه نویسی امن در .NET

جدول ۳۰: شناسنامه دوره برنامه نویسی امن در.NET

هدف دوره	شناخت آسیب‌پذیری‌های رایج هنگام طراحی وب سایت باNET. و امن‌سازی آن
مخاطبین	کارشناسان امن سازی نرم افزار
سرفصل مطالب	Data Validation Authentication & Session Management NET Framework Security Secure Software Development Lifecycle
نحوه ارائه دوره	تئوری-عملی
پیش‌نیاز	دوره کد نویسی امن در طراحی وب
مراجع	SANS-DEV۵۴۴
مدت زمان دوره	۳۲ ساعت