جمهوری اسلامی ایران
وزارت تعاون، کار و رفاه اجتماعی

سازمان آموزش فنی و حرفه ای کشور

معاونت پژوهش، برنامه‌ریزی و سنجش مهارت

دفتر پژوهش، طرح و برنامه‌ریزی درسی

استاندارد آموزش شایستگی

پیاده سازی امنیت شبکه های مایکروسافت

Securing Windows Server 2016

(MSCE 70-744)

گروه شغلی

فناوری اطلاعات

کد ملی آموزش شایستگی

۱	۱	۴	۰	۰	۰	۰	۳	۵	۰	۳	۱	۱	۵	۳
نسخه	شناسه شایستگی			شناسه شغل			شناسه گروه			سطح مهارت	ISCO-08			

تاریخ تدوین استاندارد : ۹۹/۸/۱۲

نظارت بر تدوین محتوا و تصویب استاندارد : دفتر پژوهش، طرح و برنامه‌ریزی درسی

کد ملی شناسایی آموزش شایستگی : ۳۵۱۱۳۰۵۳۰۰۰۰۴۱۱

اعضاء کارگروه برنامه‌ریزی درسی :فناوری اطلاعات					
ردیف	نام و نام خانوادگی	آخرین مدرک تحصیلی	رشته تخصصی	شغل و سمت	سابقه کار
۱	علیرضا پزشکیان	کارشناسی	فناوری اطلاعات	مدیر و موسس آموزشگاه اُکسین، مدرس سیسکو، مایکروسافت، میکروتیک	۱۶ سال
۲	عباس پلاسی زاده	کارشناسی	نرم افزار	مدیر IT شرکت توزیع برق استان هرمزگان	۱۶ سال
۳	عاطفه حیدریان	کارشناسی	فناوری اطلاعات	مدرس آموزشگاه اُکسین	۱۰ سال
۴	سید مهدی تولایی زاده	کارشناس	نرم افزار	مدرس آموزشگاه اُکسین	۱۰سال
۵	اسماء کریمی	کارشناسی	مهندسی الکترونیک	مدیرکل فنی و حرفه ای استان هرمزگان	۱۴سال
۶	عصمت لشکری	کارشناسی ارشد	مدیریت آموزشی	کارشناس پژوهش	۱۰ سال
۷	محمدرضا کنجه مرادی	کارشناسیارشد	فناوری اطلاعات	دبیرکارگروه برنامه ریزی درسی فناوری اطلاعات	۱۲سال

آدرس: دفتر پژوهش، طرح و برنامه‌ریزی درسی

تهران، خیابان آزادی، نبش خیابان خوش جنوبی، سازمان آموزش فنی و حرفه‌ای کشور

دورنگار ٦٦٥٨٣٦٥٨

تلفن ٦٦٥٨٣٦٢٨

آدرس الکترونیکی : rpc@irantvto.ir

تعاریف :

استاندارد شغل :

مشخصات شایستگی‌ها و توانمندی‌های مورد نیاز برای عملکرد موثر در محیط کار را گویند در بعضی از موارد استاندارد حرفه‌ای نیز گفته می‌شود.

استاندارد آموزش :

نقشه‌ی یادگیری برای رسیدن به شایستگی‌های موجود در استاندارد شغل.

نام یک شغل :

به مجموعه‌ای از وظایف و توانمندی‌های خاص که از یک شخص در سطح مورد نظر انتظار می‌رود اطلاق می‌شود.

شرح شغل :

بیانیه‌ای شامل مهم‌ترین عناصر یک شغل از قبیل جایگاه یا عنوان شغل، کارها ارتباط شغل با مشاغل دیگر در یک حوزه شغلی، مسئولیت‌ها، شرایط کاری و استاندارد عملکرد مورد نیاز شغل.

طول دوره آموزش :

حداقل زمان و جلسات مورد نیاز برای رسیدن به یک استاندارد آموزشی.

ویژگی کارآموز ورودی :

حداقل شایستگی‌ها و توانایی‌هایی که از یک کارآموز در هنگام ورود به دوره آموزش انتظار می‌رود.

کارورزی:

کارورزی صرفا در مشاغلی است که بعد از آموزش نظری یا همگام با آن آموزش عملی به صورت محدود یا با ماکت صورت می‌گیرد و ضرورت دارد که در آن مشاغل خاص محیط واقعی برای مدتی تعریف شده تجربه شود.(مانند آموزش یک شایستگی که فرد در محل آموزش به صورت تئوریک با استفاده از عکس می‌آموزد و ضرورت دارد مدتی در یک مکان واقعی آموزش عملی ببیند و شامل بسیاری از مشاغل نمی‌گردد.)

ارزشیابی :

فرآیند جمع‌آوری شواهد و قضاوت در مورد آنکه یک شایستگی بدست آمده است یا خیر، که شامل سه بخش عملی، کتبی عملی و اخلاق حرفه‌ای خواهد بود.

صلاحیت حرفه‌ای مربیان :

حداقل توانمندی‌های آموزشی و حرفه‌ای که از مربیان دوره آموزش استاندارد انتظار می‌رود.

شایستگی :

توانایی انجام کار در محیط‌ها و شرایط گوناگون به طور موثر و کارا برابر استاندارد.

دانش :

حداقل مجموعه‌ای از معلومات نظری و توانمندی‌های ذهنی لازم برای رسیدن به یک شایستگی یا توانایی که می‌تواند شامل علوم پایه(ریاضی، فیزیک، شیمی، زیست شناسی)، تکنولوژی و زبان فنی باشد.

مهارت :

حداقل هماهنگی بین ذهن و جسم برای رسیدن به یک توانمندی یا شایستگی. معمولاً به مهارت‌های عملی ارجاع می‌شود.

نگرش :

مجموعه‌ای از رفتارهای عاطفی که برای شایستگی در یک کار مورد نیاز است و شامل مهارت‌های غیر فنی و اخلاق حرفه‌ای می‌باشد.

ایمنی :

مواردی است که عدم یا انجام ندادن صحیح آن موجب بروز حوادث و خطرات در محیط کار می‌شود.

توجهات زیست محیطی :

ملاحظاتی است که در هر شغل باید رعایت و عمل شود که کمترین آسیب به محیط زیست وارد گردد.

نام استاندارد آموزش شایستگی:
پیاده سازی امنیت شبکه های مایکروسافت(MCSE 70-744) **Securing Windows Server 2016**
شرح استاندارد آموزش شایستگی :
پیاده سازی امنیت شبکه های مایکروسافت یکی از شایستگی های حوزه فناوری اطلاعات میباشد که شامل کارهای پیاده سازی راه حل های امن سازی سرور، ایمن سازی ساختار مجازی سازی شده، ایجاد ساختار شبکه امن، مدیریت هویت های ویژه (PRIVILEGE IDENTITLES)، پیاده سازی راه حل های شناسایی تهدید و ایمن سازی برای عملیات کاری خاص می باشد.
ویژگی‌های کارآموز ورودی :
حداقل میزان تحصیلات : دیپلم کامپیوتر **حداقل توانایی جسمی و ذهنی : داشتن سلامت کامل جسمی و ذهنی** **مهارت‌های پیش‌نیاز : پیاده سازی شبکه های مایکروسافت (MCSE Identity in Windows Server 2016 (۷۴۲-۷۰ با کد۳۵۱۱۳۰۵۳۰۰۰۰۳۸۱**
طول دوره آموزش :
طول دوره آموزش: ٦٥ ساعت **زمان آموزش نظری: ۲۷ ساعت** **زمان آموزش عملی: ۳۸ ساعت** **زمان کارورزی: ---** **زمان پروژه: ---**
بودجه‌بندی ارزشیابی(به درصد)
-کتبی:۳۰٪ **-عملی:٦۰٪** **-اخلاق حرفه ای:۱۰٪**
صلاحیت‌های حرفه‌ای مربیان :
لیسانس مهندسی کامپیوتر یا فناوری اطلاعات با حداقل ۳ سال سابقه کار مرتبط در شبکه های سیسکو

*** تعریف دقیق استاندارد(اصطلاحی) :**

این استاندارد شامل پیاده سازی راه حل های امن سازی سرور، ایمن سازی ساختار مجازی سازی شده، ایجاد ساختار شبکه امن، مدیریت هویت های ویژه (PRIVILEGE IDENTITLES)، پیاده سازی راه حل های شناسایی تهدید و ایجاد امنیت برای عملیات کاری خاص می باشد.

*** اصطلاح انگلیسی استاندارد(اصطلاحات مشابه جهانی) :**

MSCE: Microsoft Solution Certified Expert

*** مهم‌ترین استانداردها و رشته‌های مرتبط با این استاندارد :**

-تکنسین تجهیزات شبکه‌های کوچک

-تکنسین عمومی شبکه‌های کامپیوتری

-تکنسین عمومی امنیت شبکه‌های کامپیوتری

-تکنسین شبکه‌های کامپیوتری بی‌سیم

*** جایگاه استاندارد شغلی از جهت آسیب‌شناسی و سطح سختی کار :**

الف : جزو مشاغل عادی و کم آسیب ☐ طبق سند و مرجع .....

ب : جزو مشاغل نسبتاً سخت ☐ طبق سند و مرجع .....

ج : جزو مشاغل سخت و زیان آور ☐ طبق سند و مرجع .....

د : نیاز به استعلام از وزارت کار ■

استاندارد آموزش شایستگی

- کارها

ردیف	عناوین	ساعت آموزش		
		نظری	عملی	جمع
۱	پیاده سازی راه حل های امن سازی سرور	۵	۷	۱۲
۲	ایمن سازی ساختار مجازی سازی شده	۴	۶	۱۰
۳	ایجاد ساختار شبکه امن	۴	۶	۱۰
۴	مدیریت هویت های ویژه (PRIVILEGE IDENTITLES)	۵	۷	۱۲
۵	پیاده سازی راه حل های شناسایی تهدید	۴	۷	۱۱
۶	ایمن سازی برای عملیات کاری خاص	۴	۶	۱۰
	جمع ساعات	**۲۷**	**۳۸**	**٦٥**

عنوان : پیاده سازی راه حل های امن سازی سرور	زمان آموزش			
	نظری	عملی	جمع	
	۵	۷	۱۲	
دانش، مهارت، نگرش، ایمنی توجهات زیست محیطی مرتبط				**تجهیزات، ابزار، مواد مصرفی و منابع آموزشی**
دانش :				وایت برد ماژیک دیتا پروژکتور رایانه Patch Cord Layer2Switch Cisco Layer3Switch Cisco Cisco Router Internet Public IP Address
– مراحل اجرای فناوری Network Unlock				
– بازیابی رمز عبور				
– بازیابی رمز عبور با استفاده از AD DS				
- بازیابی خودکار (self-service)				
–مدیریت سیستم فایل رمزنگاری شده (EFS-Encrypted File System)				
– برنامه های بازیابی داده				
– نصب و پیکربندی سرویس WSUS				
- نصب سرویس WSUS				
- ایجاد گروههای رایانه ها و پیکربندی به روزرسانی خودکار (Automatic Update)				
- مدیریت به روزرسانی ها با استفاده از WSUS				
- اشکال یابی در پیکربندی و اجرای سرویس دهنده WSUS				
- مدیریت Windows Defender در سیستم عامل ویندوز سرور ۲۰۱۶				
- انواع قراردادها در AppLocker				
– کنترل و آزمایش قراردادهای AppLocker				
- فعال سازی Control Flow Guard				
- اجزا و پیش نیازهای فناوری Device Guard				
- ایجاد آیین نامه های قراردادی Code Integrity				

عنوان : پیاده سازی راه حل های امن سازی سرور	زمان آموزش			
	نظری	عملی	جمع	

دانش، مهارت، نگرش، ایمنی توجهات زیست محیطی مرتبط				**تجهیزات، ابزار، مواد مصرفی و منابع آموزشی**
دانش:				
- تعیین نیازها برای استفاده از فناوری Credential Guard				
- نیازهای سیستم برای استفاده از فناوری Credential Guard				
- عملکرد فناوری Credential Guard				
- نقاط ضعف فناوری Credential Guard				
- ایجاد و درون ریزی Security Baselines				
- Import کردن Baseline ها و مقایسه آنها				
- Local GPO				
- سنجش فراگیری				
- پاسخ های سنجش فراگیری				
مهارت :				
-پیکربندی رمزنگاری دیسک و فایل				
-کار با سخت افزار و firmware مورد نیاز برای Secure Boot و عملیات کلیدی رمزنگاری				
-پیکربندی UEFI و Secure Boot و TPM				
-فعال سازی BitLockerبرای استفاده در Secure Boot به همراه کنترل مشمولیت BCD				
پیاده سازی BitLocker Drive Encryption (BDE)				
-پیکربندی BitLocker بااستفاده و یا بدون استفاده از TPM				
-پیاده سازی فناوری BitLockerدر دیسکهای CSV وSAN				

عنوان : پیاده سازی راه حل های امن سازی سرور	زمان آموزش			
	نظری	عملی	جمع	
دانش، مهارت، نگرش، ایمنی توجهات زیست محیطی مرتبط				**تجهیزات، ابزار، مواد مصرفی و منابع آموزشی**
مهارت:				
-پیکربندیNetwork Unlock				
-پیاده سازیBitlocker Recovery Processes				
-پیاده سازی راه حل های ارتقا و به روزسانی سرور				
-پیکربندی گزارش در WSUS				
-پیاده سازی فناوری BitLocker در ماشین های مجازی Hyper-V				
-پیاده سازی محافظ های بدافزار				
-پیاده سازی راه حل های ضد بدافزار با استفاده از Windows Defender				
-پیاده سازی جست و جوی بدافزار توسط Windows Defender از طریق خط فرمان پاورشل				
-پیکربندی Windows Defender همراه با WSUS و Windows Update				
صدور مجوز به روزرسانیWindows Defender با استفاده از سرویس WSUS				
-پیکربندیWindows Defender از طریق Group Policy				
-پیاده سازی قراردادهای AppLocker				
-پیاده سازی یگ آیین نامه در ابزار AppLocker				
-پیاده سازی Control Flow Guard				
-پیاده سازی آیین نامه های Device Guard				
-پیاده سازی اجرای Device Guard				

عنوان : پیاده سازی راه حل های امن سازی سرور	زمان آموزش			
	نظری	عملی	جمع	
دانش، مهارت، نگرش، ایمنی توجهات زیست محیطی مرتبط				**تجهیزات، ابزار، مواد مصرفی و منابع آموزشی**
مهارت:				
-پیاده سازی حفاظت از اطلاعات هویتی				
-پیکربندیCredential Guard				
-پیکربندیCredential Guard با استفاده از WMI و دستورات خط فرمان				
-پیاده سازی فناوری NTLM blocking				
-پیکربندی حد نصاب های امنیت				
-پیاده سازی نصب و پیکربندی فناوری SCM				
-پیاده سازی نصب نرم افزار SCM v4.0				
-پیکربندیSCM v4.0 و مشاهده Baselines				
-پیاده سازی آیین نامه های امنیتی برای سرورهای موجود در دامنه و سرورهای مستقل				
نگرش : -رعایت اخلاق حرفه ای به همراه ایجاد تخصص برای ایجاد و حفظ امنیت				
ایمنی و بهداشت : - رعایت استانداردهای حفاظت و ایمنی در کار				
توجهات زیست محیطی : - رعایت مقررات و ضوابط مرتبط با حفظ محیط زیست				

عنوان : ایمن سازی ساختار مجازی سازی شده	زمان آموزش			
	نظری	عملی	جمع	
	۴	۶	۱۰	
دانش، مهارت، نگرش، ایمنی توجهات زیست محیطی مرتبط				**تجهیزات، ابزار، مواد مصرفی و منابع آموزشی**
دانش :				وایت برد ماژیک دیتا پروژکتور رایانه Patch Cord Layer2Switch Cisco Layer3Switch Cisco Cisco Router Internet Public IP Address
- آماده سازی گره های HGS در کلاستر				
- انتخاب روش تایید امضا و هویت (Attestation)				
- نکاتی در مورد گواهی امضا TPM-trusted				
- انتقال ماشین های مجازی به میزبان های محافظت شده دیگر				
- آزمایش میزبان محافظت شده				
- انتقال ماشین مجازی دارای محافظ به میزبان محافظت شده دیگر و رفع اشکال میزبان های محافظت شده				
- تعیین نیازمندی ها و موراد کاربرد استفاده از ماشین های مجازی محافظ دار				
- مفهوم Virtualization-based security				
- دسترسی راهبر عملیاتی				
- ایجاد ماشین مجازی محافظ دار با استفاده از Hyper-V				
- مزایای یک مدیر فابریک				
- ایجاد ماشین مجازی محافظ دار بدون استفاده از SCVMM				
- ایجاد فایل محافظت شده (PDK)				
-نظارت بر نصب ماشین مجازی محافظت شده بر روی میزبان محافظ				
- فعال سازی و پیکربندی فناوری vTPM				
-محیط کار ایزوله شده (IUM-Isolated User Mode)				
- فعال سازی فناوری vTPM در ماشین مجازی Hyper-V				
- رمز نگاری و اجرا				

عنوان : ایمن سازی ساختار مجازی سازی شده	زمان آموزش			
	نظری	عملی	جمع	
دانش، مهارت، نگرش، ایمنی توجهات زیست محیطی مرتبط				**تجهیزات، ابزار، مواد مصرفی و منابع آموزشی**
دانش:				
- تعیین نیازها و موارد کاربرد استفاده از ماشین های مجازی رمزنگاری شده				
- بازیابی ماشین مجازی محافظ دار				
- مراحل بازیابی				
مهارت :				
-پیاده سازی راه حل Guarded Fabric				
-نصب و پیکربندی Host Guardian Service(HGS)				
- پیکربندی و نصب سرویس HGS بر روی سرور مورد نظر				
- پیکربندی سرور HGS				
- پیکربندی گواهی امضا تایید راهبریا TPM-trusted				
-پیکربندی و راه اندازی سرور HGS				
-پیکربندی فناوری Key Protection با استفاده از HGS				
-پیکربندی میزبان محافظت شده				
-پیاده سازی ماشین های مجازی محافظ دار با پشتیبانی از رمزنگاری				
-پیاده سازی ماشین مجازی رمزنگاری شده				
نگرش : -کار گروهی،اخلاق حرفه ای،رعایت استانداردهای حرفه ای، خلاقیت ونوآوری				
ایمنی و بهداشت : - رعایت استانداردهای حفاظت و ایمنی در کار				

عنوان : ایمن سازی ساختار مجازی سازی شده	زمان آموزش			
	نظری	عملی	جمع	
دانش، مهارت، نگرش، ایمنی توجهات زیست محیطی مرتبط				**تجهیزات، ابزار، مواد مصرفی و منابع آموزشی**
توجهات زیست محیطی : -رعایت مقررات و ضوابط مرتبط با حفظ محیط زیست				

عنوان : ایجاد ساختار شبکه امن	زمان آموزش			
	نظری	عملی	جمع	
	۴	۶	۱۰	
دانش ، مهارت ، نگرش ، ایمنی توجهات زیست محیطی مرتبط				**تجهیزات ، ابزار ، مواد مصرفی و منابع آموزشی**
دانش :				وایت برد ماژیک دیتا پروژکتور رایانه Patch Cord Layer2Switch Cisco Layer3Switch Cisco Cisco Router Internet Public IP Address
-مفهوم The Windows Firewall Control Panel				
- فایروال ویندوز به همراه کنسول Advanced Security				
- زمایش قانون ترافیک ورودی (Inbound rule) پیش فرض				
- ایجاد آیین نامه کنترل ترافیک ورودی جدید Inbound (rule)				
- برون ریزی (Export) پیکربندی فایروال				
- مشاهده فهرست و برون ریزی آیین نامه ها با استفاده از دستور پاورشل netsh				
- import تنظیمات آیین نامه ها				
- انواع آیین نامه های ارتباط امن با استفاده از IPsec				
- تعریف آیین نامه امنیت ارتباط با استفاده از Group Policy				
- تعریف آیین نامه امنیت ارتباط در IPsec Console				
- تعریف آیین نامه امنیت ارتباط با استفاده از خط فرمان پاورشل				
- آیین نامه های تنظیم شده برای لایه کاربرد				
- تعیین نیازها و سناریوهای مربوط به پیاده سازی Microsoft Azure،SDN، Distributed Firewall				
- استفاده از فناوری Azure SDN در شبکه داخلی سازمان				
- سرویس Network Controller				
- آیین نامه های Distributed Firewall و گروه های امنیتی شبکه				
- zure Stack و مالیکت چندگانه				

عنوان : ایجاد ساختار شبکه امن	زمان آموزش			
	نظری	عملی	جمع	
دانش ، مهارت ، نگرش ، ایمنی توجهات زیست محیطی مرتبط				**تجهیزات ، ابزار ، مواد مصرفی و منابع آموزشی**
دانش:				
- لیست کنترل دسترسی در Datacenter Firewall				
- مجازی سازی شده Hyper-V				
-مفهوم SMB3.0				
- Pre-authentication integrity				
- ارتقای کارآیی رمزنگاری (EncryptionPerformance improvements)				
- مفهوم Cluster dialect fencing				
-فعال سازی رمزنگاری پروتکل SMB در فضاهای ذخیره سازی اشتراکی (SMB Shares)				
-ترافیک امن DNS با استفاده از DNSSEC و آیین نامه های DNS				
-مبانی DNSSEC				
-Name Resolution Policy Table(NRPT)				
-آیین نامه های DNS				
- اطلاعات در پاسخ های DNS				
مهارت :				
-پیکربندی فایروال ویندوز				
- پیکربندی فایروال ویدوز با استفاده از AdvancedSecurity				
-پیکربندی و پیاده سازی پروفایل های مکانی شبکه با استفاده از Group Policy				

عنوان : ایجاد ساختار شبکه امن	زمان آموزش			
	نظری	عملی	جمع	
دانش ، مهارت ، نگرش ، ایمنی توجهات زیست محیطی مرتبط				**تجهیزات ، ابزار ، مواد مصرفی و منابع آموزشی**
مهارت:				
- پیکربندی آیین نامه های ارتباطی امن با استفاده از Group Policy کنسول رابط گرافیکی وIPsec و امنیت سرور				
-پیکربندی پیش فرض های IPsec				
-پیکربندی فایروال ویندوز برای مجوز اجرا و یا مسدودسازی نرم افزار				
-پیکربندی استثناهای تایید هویت شده در فایروال				
-پیاده سازی فایروال نرم افزاری تعریف شده گسترده				
-پیاده سازی ترافیک امن شبکه				
-پیکربندی ورود به سرور SMB و غیرفعال کردنSMB 1.0				
-پیکربندی ورود به سرور (SMB signing)SMB				
-پیاده سازی سریع DNSSEC				
-نصب و پیکربندی (MMA) Microsoft Message Analyzer برای آنالیز ترافیک شبکه				
نگرش : -کار گروهی،اخلاق حرفه ای -رعایت استانداردهای حرفه ای -خلاقیت ونوآوری				
ایمنی و بهداشت : - رعایت استانداردهای حفاظت و ایمنی در کار				
توجهات زیست محیطی : -رعایت مقررات و ضوابط مرتبط با حفظ محیط زیست				

عنوان : مدیریت هویت های ویژه (PRIVILEGE IDENTITIES)	زمان آموزش			
	نظری	عملی	جمع	
	۵	۷	۱۲	

دانش ، مهارت ، نگرش ، ایمنی توجهات زیست محیطی مرتبط				**تجهیزات ، ابزار ، مواد مصرفی و منابع آموزشی**
دانش :				وایت برد ماژیک دیتا پروژکتور رایانه Patch Cord Layer2Switch Cisco Layer3Switch Cisco Cisco Router Internet Public IP Address
- لایه های راهبری اکتیو دایرکتوری				
- اعتماد میان فارست ها				
- توصیه های کاربردی در معماری ESAE				
- تشخیص موارد کاربرد و نیازهای مربوط به پیاده سازی اصل منبع تمیز در معماری اکتیو دایرکتوری				
- وابستگی های قابل انتقال				
- سخت افزار تمیز برای سخت افزار سیستم				
- منبع تمیز برای فایل های نصب				
- منبع تمیز برای ساختار راهبری				
- ایجاد یک فارست راهبری (bastion) جدید در محیط اکتیو دایرکتوری موجود با استفاده از MIM				
- ایجاد یک PAM مطمئن				
- ایجاد کپی از حسابهای کاری (Shadow principles)				
- درخواست سطح دسترسی ویژه با استفاده از پورتال وب MIM				
- تعیین نیازها و موراد کاربرد برای راه حل های PAM				
- نیازهای سخت افزاری و نرم افزاری				
- قابلیت دسترسی دائمی (High Availability)				
- ایجاد نقش در سرویس PAM				
- مشحص کردن آیین نامه های مبتنی بر زمان				
- مدیریت دسترسی نقش ها				
- نقش PAM در پاورشل ویندوز				

عنوان : مدیریت هویت های ویژه (PRIVILEGE IDENTITIES)	زمان آموزش نظری	عملی	جمع	
دانش ، مهارت ، نگرش ، ایمنی توجهات زیست محیطی مرتبط				**تجهیزات ، ابزار ، مواد مصرفی و منابع آموزشی**
دانش:				
- فعال سازی فناوری JEA بر روی ویندوز سرور ۲۰۱۶				
- مراحل در یک نشست JEA				
- اجزای JEA				
- ارتباط با سرور برای راهبری از یک نقطه کاربری JEA				
- مشاهده رخدادها				
- پروفایل های سخت افزار PAW				
- پروفایل سخت افزار PAW				
- ایجاد محدودیت ورود راهبران				
- فعال سازی فناوری Remote Credential Guard				
- نصب ابزارهای مدیریت LAPS				
- تغییر در اکتیو دایرکتوری				
- ایمن سازی رمزهای عبور محلی بااستفاده از LAPS				
- تغییر نام حساب کاری				
مهارت :				
-پیاده سازی دامنه های راهبری با قابلیت ENHANCED Security Administrative Environment				
-پیاده سازی Just-In-Time Administration				
-پیکربندی ارتباط مطمئن بین فارست محافظ (bastion) و فارست عملیاتی				
-تست ارتباط سرور DNS				
-پیکربندی پورتال وب سرویس MIM				

عنوان : مدیریت هویت های ویژه (PRIVILEGE IDENTITIES)	زمان آموزش نظری	عملی	جمع	
دانش ، مهارت ، نگرش ، ایمنی **توجهات زیست محیطی مرتبط**				**تجهیزات ، ابزار ، مواد** **مصرفی و منابع آموزشی**
مهارت:				
-پیکربندی آیین نامه های MIM				
-پیاده سازی حساب کاری راهبر از نوع Just-In-Time با استفاده از آیین نامه مبتنی بر زمان				
-پیاده سازی Just-Enough-Administration				
-ایجاد و پیکربندی فایل های session configuration				
-ایجاد و پیکربندی فایل role capability				
-پیکربندی نقطه کاربری JEA بر روی یک سرور با استفاده از DSC				
-پیاده سازی پیمانه DSC				
-پیاده سازی PAM و (Users Rights Assignments) URA				
-پیاده سازی فناوری PAW				
-پیکربندی آیین نامه های (User Rights Assignments) URA				
-پیکربندی User Rights Assignments				
-پیکربندی GPO مربوط به رایانه PWA				
-فعال سازی Remote Credential Guard				
-پیکربندی Remote Credential Guard				
-پیاده سازی راه حل های Local Administrator Password				
-نصب و پیکربندی ابزار LAPS				
-پیکربندی تنظیمات رمز عبور				

عنوان : مدیریت هویت های ویژه (PRIVILEGE IDENTITIES)	زمان آموزش			
	نظری	عملی	جمع	
دانش ، مهارت ، نگرش ، ایمنی توجهات زیست محیطی مرتبط				**تجهیزات ، ابزار ، مواد مصرفی و منابع آموزشی**
نگرش : -رعایت اخلاق حرفه ای به همراه ایجاد تخصص برای ایجاد و حفظ امنیت -خلاقیت ونوآوری				
ایمنی و بهداشت : - رعایت استانداردهای حفاظت و ایمنی در کار				
توجهات زیست محیطی : -رعایت مقررات و ضوابط مرتبط با حفظ محیط زیست				

عنوان : پیاده سازی راه حل های شناسایی تهدید	زمان آموزش			
	نظری	عملی	جمع	
	۴	۷	۱۱	

دانش ، مهارت ، نگرش ، ایمنی توجهات زیست محیطی مرتبط				**تجهیزات ، ابزار ، مواد مصرفی و منابع آموزشی**
دانش :				وایت برد ماژیک دیتا پروژکتور رایانه Patch Cord Layer2Switch Cisco Layer3Switch Cisco Cisco Router Internet Public IP Address
- تفاوت ها و موراد کاربرد استفاده از Advanced Auditing Policies ,Local Audit Policy				
- آیین نامه ی ممیزی محلی Local Audit Policies				
- اولیت ها در آیین نامه های ممیزی				
-ویرایش های سیستم عامل				
- ایجاد یک GPO جدید برای ممیزی				
- ممیزی Objects				
- ایجاد آیین نامه ممیزی با استفاده از عبارت توصیفی				
- تعیین مواردکاربرد ابزار ATA				
- جمع آوری اطلاعات اولیه و شناسایی هدف (Reconnaissance)				
-اطلاعات هویتی دستکاری شده (Compromised Credentials)				
- انتقال غیر مستقیم (Lateral movement)				
- ارتقای مجوز دسترسی (Privilege Escalation)				
- تسلط و نفوذ بر دامنه (Domain dominance)				
- تعیین نیازها برای اجرای ابزار ATA				
- ATA Center				
- ATA Gateways				
- Port mirroring				
- Event Forwarding				

عنوان : پیاده سازی راه حل های شناسایی تهدید	زمان آموزش			
	نظری	عملی	جمع	

دانش ، مهارت ، نگرش ، ایمنی توجهات زیست محیطی مرتبط				**تجهیزات ، ابزار ، مواد مصرفی و منابع آموزشی**
دانش:				
- ویـرایش فعالیـت هـای مشـکوک بـر روی Attack Time Line				
-راه حـل هـای شناسـایی تهدیـد بـا اسـتفاده از Operation Management Suite				
- موارد کاربرد و استفاد از OMS				
- فعال سازی عامل ها (Agents)				
- معرفی عملیات ممیزی و امنیتی قابل استفاده				
- بررسی ضد بدافزارها (Antimalware assessment)				
- امنیت و ممیزی (Security and Audit)				
- موراد کاربرد آنالیز رخدادها (log analytics)				
مهارت :				
-پیکربندی پیشرفته آیین نامه های ممیزی				
-پیاده سازی ممیزی بـا اسـتفاده از Auditpol.exe، Group Policy				
-پیاده سازی با Auditpol.exe				
-پیاده سازی ممیزی با استفاده از پاورشل ویندوز				
-پیکربندی آیین نامه ممیزی برای فعالیت PNP				
-پیکربنـــدی آیـــین نامـــه ممیـــزی Group Policy Membership				
-فعال سازی و پیکربندی ثبت رخدادها برای ماژول و مسدود کردن دستورات و ورود به پاورشل ویندوز				

عنوان : پیاده سازی راه حل های شناسایی تهدید	زمان آموزش			
	نظری	عملی	جمع	

دانش ، مهارت ، نگرش ، ایمنی توجهات زیست محیطی مرتبط				**تجهیزات ، ابزار ، مواد مصرفی و منابع آموزشی**
مهارت:				
-نصب و پیکربندی Microsoft Advanced Threat Analytics				
-نصب و پیکربندی ATA Gateway بر روی یک سرور اختصاصی				
-نصب ATA Center				
-نصب ATA Gateway				
-نصب و پیکربندی ATA Lightweight Gateway به طور مستقیم بر روی کنترل کننده دامنه				
-پیکربندی تنظیمات سرور ایمیل				
-پیکربندی تنظیمات سرور syslog				
-پیکربندی تنظیمات اعلان هشدار				
-پیاده سازسی OMS				
نگرش : -رعایت اخلاق حرفه ای به همراه ایجاد تخصص برای ایجاد و حفظ امنیت -خلاقیت ونوآوری				
ایمنی و بهداشت : - رعایت استانداردهای حفاظت و ایمنی در کار				
توجهات زیست محیطی : -رعایت مقررات و ضوابط مرتبط با حفظ محیط زیست				

عنوان : ایمن سازی برای عملیات کاری خاص	زمان آموزش			
	نظری	عملی	جمع	
	۴	۶	۱۰	
دانش ، مهارت ، نگرش ، ایمنی توجهات زیست محیطی مرتبط				**تجهیزات ، ابزار ، مواد مصرفی و منابع آموزشی**
دانش :				وایت برد ماژیک دیتا پروژکتور رایانه Patch Cord Layer2Switch Cisco Layer3Switch Cisco Cisco Router Internet Public IP Address
– ساختار امن برای سرویس های عملیاتی و محیط توسعه نرم افزار				
– موارد کاربرد پشتیبانی ازسرورهای عملیاتی وتوسعه نانوسرور				
– پیوستن به دامنه				
– ورود به نانو سرور				
– آشنایی برقراری ارتباط با نانو سرور از طریق خط فرمان پاورشل				
– موراد کاربرد و پیش نیازهای استفاده از محفظه های ویندوز و محفظه های Hyper-V				
– دو نوع استفاده از محفظه ها				
– ویندوز سرور ۲۰۱۶ و داکر (Docker)				
– ایجاد الگوهای quotas				
– ایجاد Quotas				
– اجزای DAC				
– ایجاد انواه درخواست کننده (Claim types)				
– علاج دریافت پیام عدم دسترسی(access-denied)				
مهارت :				
– نصب و پیکربندی نانو سرور				
–پیاده سازی دیسک سخت مجازی نانو سرور				
– پیکربندی و ایجاد نانو سرور در ماشین مجازی				

عنوان : ایمن سازی برای عملیات کاری خاص	زمان آموزش			
	نظری	عملی	جمع	
دانش ، مهارت ، نگرش ، ایمنی توجهات زیست محیطی مرتبط				**تجهیزات ، ابزار ، مواد مصرفی و منابع آموزشی**
مهارت:				
-پیکربندی IP آدرس نانو سرور				
-پیکربندی آیین نامه های فایروال				
-پیکربندی(WinRM)				
-پیاده سازی آیین نامه های امنیتی نانو سرور با استفاده از DSC(Desired Stare Configuration)				
-کامپایل کردن فایل پیکربندی DSC				
-انتشار پیکربندی های DSC				
-پیاده سازی فایل سرور امن با استفاده از (Dynamic Access DAC(Control				
-نصب سرویس File Server Resource (FSRM) Manager				
-پیکربندی فضای مجاز ذخیره سازی (quotas)				
-پیکربندی کنترل کننده های فایل (file screens)				
-پیکربندی گزارش های فضای ذخیره سازی				
-پیکربندی عملیات مدیریت فایل				
-پیکربندی File Classification Infrastructure				
-ایجاد Classification properties				
-ایجاد Classification rules				
-پیاده سازی Work Folders				
-نصب و سرویس Work Folders				
-کار با Work Folders Group				

عنوان : ایمن سازی برای عملیات کاری خاص	زمان آموزش			
	نظری	عملی	جمع	
دانش ، مهارت ، نگرش ، ایمنی توجهات زیست محیطی مرتبط				**تجهیزات ، ابزار ، مواد مصرفی و منابع آموزشی**
مهارت:				
-کار با فضای همگام سازی اشتراکی (Sync Shares)				
-پیکربندی کاربران سرویس Work Folders				
-پیکربندی کاربر و تجهیزات درخواست کننده				
-ایجاد و پیکربندی مشخصه های منابع و فهرست های آنها (Resource properties)				
-ایجاد و پیکربنید قوانین دسترسی و آیین نامه های آن (CAR) Central Access Rules				
-ایجاد و پیاده سازی آیین نامه های دسترسی متمرکز (CAP-Central Access Policies)				
-پیاده سازی تغییرات و استفاده از ایین نامه				
-پیکربندی ممیزی دسترسی به فایل				
نگرش : -رعایت اخلاق حرفه ای به همراه ایجاد تخصص برای ایجاد و حفظ امنیت،خلاقیت و نوآوری				
ایمنی و بهداشت : - رعایت استانداردهای حفاظت و ایمنی در کار				
توجهات زیست محیطی : -رعایت مقررات و ضوابط مرتبط با حفظ محیط زیست				

- برگه استاندارد تجهیزات

ردیف	نام	مشخصات فنی و دقیق	تعداد	توضیحات
۱	PC	Cpu:Corei3/Ram:4G/HDD:500/ODD	۱۵	
۲	Switch Layer2	WS-C2950-24TT-L	۵	
۳	Switch Layer 3	WS-C3750-24PS-S	۵	IP Base IOS
۴	Router	Cisco Router 2811	۵	IOS 15.0
۵	Server	HP G7-DL360	۱	
۶	Patch Panel	24Port	۵	
۷	Patch Cord	Cat6 UTP 5 Meter	۲۰	
۸	Patch Cord	Cat6 UTP 0.5 Meter	۶۰	
۹	Patch Cord	Cat6 UTP 1 Meter	۶۰	
۱۰	Patch Cord	Cat6 UTP 3 Meter	۶۰	
۱۱	Rollover	Cisco Console Cable	۱۶	
۱۲	Converter	RS232	۵	

توجه :

- تجهیزات به ازاء یک نفر و یک کارگاه به ظرفیت ۱۵ نفر محاسبه شود .

- برگه استاندارد مواد

ردیف	نام	مشخصات فنی و دقیق	تعداد	توضیحات
۱	ماژیک وایت برد	چهار رنگ آبی – قرمز – سبز – مشکی	۴	برای کارگاه
۲	دیتا پروژکتور	روشنایی حداقل ۲۵۰۰ انسی	۱	برای کارگاه
۳	وایت برد	۱۵۰ سانتیمتر در ۲۰۰ سانتیمتر	۱	برای کارگاه
۴	تستر شبکه	دیجیتال	۱	برای کارگاه

توجه :

- مواد به ازاء یک نفر و یک کارگاه به ظرفیت ۱۵ نفر محاسبه شود .

- برگه استاندارد ابزار

ردیف	نام	مشخصات فنی و دقیق	تعداد	توضیحات
۱	سیستم عامل ویندوز ۱۰	آخرین نسخه	۱۵	برای کارگاه
۲	نرم افزار Adobe Connect	آخرین نسخه	۱	برای کارگاه
۳	سرور	HP DL380 G7	۱	برای کارگاه
۴	سیستم عامل سرور ۲۰۱۶	آخرین ورژن	۱۵	برای کارگاه
۵	نرم افزار VM-Ware ESXi	۶,۰ به بالا	۱	برای کارگاه
۶	Hyper-V Server	آخرین ورژن	۱	برای کارگاه

توجه :

- ابزار به ازاء یک کارگاه به ظرفیت ۱۵ نفر محاسبه شود.