IT Professional Training Center

SANS SEC401: Security Essentials Bootcamp Style

(آشنایی با مفاهیم ضروری امنیت)

خلاصه دوره: با افزایش تهدیدات پیشرفته ، هدف قرار گرفتن سازمان ها توسط هکر ها و مهاجمان سایبری اجتناب ناپذیر است. دفاع در برابر این حملات یک چالش مداوم است. برای موفقیت ، سازمان ها باید بدانند که در امنیت سایبری چه عواملی موثر است. آنچه موثر بوده و همیشه موثر خواهد بود رویکرد های مبتی بر ریسک است (Risk-Based Approach). قبل از اینکه سازمان شما کوچکترین هزینه ای را برای امنیت سایبری خرج کند باید به سوالات زیر پاسخ داده شود:

۱. ریسک چیست؟
۲. آیا بالاترین خطر در اولویت پیشگیری است؟
۳. مقرون به صرفه ترین روش برای کاهش خطر چیست؟

در این دوره شما با مؤثرترین مراحل برای جلوگیری از حملات و شناسایی مهاجمین آشنا خواهید شد. تمرکز اصلی دوره SEC401 بر فراهم آوردن مهارت و تکنیک های ضروری امنیت اطلاعات مورد نیاز شما است تا بتوانید اطلاعات و دارایی های سازمان خود را امن نگه داشته و از آن ها محافظت کنید. تکنیک های عملی که در این دوره گفته خواهد شد به شما در جلوگیری از حملات و شناسایی مهاجمان کمک بسیاری خواهد کرد.

آیا SANS SEC401 دوره مناسبی برای شماست؟

سوالات زیر را از خودتان بپرسید:

- آیا اطلاع دارید که چرا برخی از شرکت ها و سازمان ها دائما به خطر می افتند و برخی دیگر نه؟
- اگر سیستم آسیب پذیری در شبکه شما وجود داشته باشد ، آیا اطمینان دارید که میتوانید آن را پیدا کنید؟
- آیا کارایی و عملکرد درست هر دیوایس و تکنولوژی امنیتی را میدانید و مطمئن هستید که آنها به درستی کانفیگ (Config) شده اند؟
- آیا معیار های امنیتی مناسب برای هدایت تصمیمات امنیتی تنظیم و به مدیران شما ابلاغ شده است؟

دوره SANS SEC401 دانش امنیتی لازم به همراه آزمایشگاه های عملی برای پاسخگویی به این سوالات را در محیط کارتان را فراهم میکند.

در کل سازمان ها هدف قرار میگیرند و به آنها حمله میشود. امروزه ، بیش از هر زمان دیگری ، تشخیص به موقع حمله و پاسخ به آن بسیار مهم است. هنگامی که یک حمله موفقیت آمیز باشد ، به سازمان ما خسارت وارد خواهد شد. در آینده ای نزدیک این نکته به موضوع اصلی در امنیت اطلاعات تبدیل خواهد شد: "چقدر سریع میتوان یک هکر را شناسایی و در برابر آن اقدام کرد؟"

"شما نمیتوانید از آنچه که نمیدانید محافظت کنید."

طول دوره: "۴۰ ساعت

پیشنیاز: SANS SEC301: Introduction to Cyber Security

اهداف دوره:

در انتهای این دوره دانشجویان موارد زیر را یاد خواهند گرفت:

- یک دستورالعمل مناسب برای توسعه معیار های امنیتی در شرکت یا سازمان خود فراهم کنند.
- خطرات و ریسک های موجود را برای ایجاد یک نقشه راه امنیتی مناسب تجزیه و تحلیل کنند.
- برای حل مشکلات امنیتی در محل کارشان ، نکات و راهکار های مناسب تنظیم کنند.

- چرا برخی از سازمان ها در محافظت خود از حملات برنده میشود و برخی دیگر بازنده؟ و از همه مهمتر ، چگونه در سمت برنده باشیم؟
- زمینه های اصلی امنیت و چگونگی ایجاد یک برنامه امنیتی بر اساس شناسایی (Detection) ، واکنش (Response) و جلوگیری (Prevention) را درک کنند.

توانایی های دانشجویان پس از گذراندن دوره:

- تمامی مطالبی را که در این دوره یاد گرفتند مستقیما در محل کار خود استفاده کنند.
- طراحی و ایجاد ساختار شبکه با استفاده از VLAN ، NAC و 802.1x
- استفاده از ابزار های خط فرمان ویندوز (Windows Command Line) ، برای تحلیل سیستم های ویندوزی
- استفاده از ابزار های خط فرمان لینوکس و اسکریپت نویسی برای اجرای خودکار برخی از برنامه ها در جهت نظارت مستمر بر روی سیستم ها
- ایجاد یک سیاست تاثیر گذار و اجرایی برای سازمان ، چک لیست های امنیتی و معیار هایی برای آموزش و آگاهی
- با استفاده از ابزار های مختلف نقاط ضعف سیستم ها را شناسایی کرده و بعد از آن سیستم را برای ایمن تر بودن کانفیگ کنند.
- ایجاد یک نقشه کلی برای شبکه که در مقاوم سازی شبکه ، شناسایی سطح حملات و تعیین بهترین روش برای جلوگیری از آنها به ما کمک خواهد کرد.
- با استفاده از ابزار هایی مانند TCPDump و Wireshark ، ترافیک و پروتکل های مختلف را Sniff و آنالیز کنند.

مخاطبین دوره:

- متخصصان امنیتی (Security Professionals) که میخواهد خلا موجود در درک فنی امنیت اطلاعات را پر کنند.
- مدیرانی (IT Managers) که میخواهد امنیت اطلاعات را فراتر از اصطلاحات و مفاهیم ساده درک کنند.
- پرسنل عملیاتی (Operations Personnel) که برقراری امنیت وظیفه اصلی آنها نیست اما برای موثر بودن به درک امنیت نیاز دارند.
- مهندسان و سرپرستان فناوری اطلاعات (IT engineers and supervisors) که باید بدانند چگونه میتوانند یک شبکه قابل دفاع در برابر حملات ایجاد کنند.
- اَدمین هایی که مسئول نگهداری از سیستم هایی هستند که ممکن است توسط هکر ها هدف قرار گیرند.
- متخصصان جرایم دیجیتال ، جرم شناسی و دیجیتال فارنزیک (Digital Forensic) که به مبانی و اصول امنیتی احتیاج دارند تا بتوانند در کار خود تا حد ممکن موثر باشند.
- متخصصان تست نفوذ (Penetration testers)

"ã ⊣Mf"õ ℅b"D3 Û.

- SEC401.1: Network Security Essentials
  - An Introduction
  - Defensible Network Architecture
  - Protocols and Packet Analysis
  - Network Device Security
  - Virtualization and Cloud
  - Securing Wireless Networks
- SEC401.2: Defense-in-Depth
  - Defense-in-Depth
  - Identity and Access Management
  - Authentication and Password Security
  - CIS Controls
  - Data Loss Prevention
  - Security Plans and Risk Management
- SEC401.3: Vulnerability Management and Response
  - Vulnerability Assessments
  - Penetration Testing
  - Attacks and Malicious Software
  - Web Application Security
  - Security Operations and Log Management
  - Digital Forensics and Incident Response
- SEC401.4: Data Security Technologies
  - Cryptography
  - Cryptography Algorithms and Deployment
  - Applying Cryptography
  - Network Security Devices
  - Endpoint Security
- SEC401.5: Windows Security
  - Windows Security Infrastructure
  - Windows as a Service
  - Windows Access Controls
  - Enforcing Security Policy
  - Network Services and Cloud Computing
  - Automation, Auditing, and Forensics
- SEC401.6: Linux, Mac and Smartphone Security
  - Linux Fundamentals: Structure, Permissions, and Access Controls
  - Linux Security Enhancements and Infrastructure
  - Containerized Security
  - macOS Security
  - Mobile Device Security