# آکادمی لیان

LIAN ACADEMY


E-LEARNING

برای ارتباط با گروه آموزشی لیان
و دسترسی به شبکه‌های اجتماعی
QR کد روبرو را اسکن کنید

# LIAN ACADEMY



CONTENTS

CONTENTS



# لیان در یک نگاه

پیشرفت فناوری اطلاعات برای شرکت‌ها و سازمان‌ها در حوزه‌های گوناگون مزایای بسیاری را به همراه داشته است؛ مجموعه‌های فعال در صنایع مختلف با بهره‌گیری از فناوری‌های دیجیتال می‌توانند بهره‌وری، انعطاف‌پذیری و توان رقابتی خود را به‌طور قابل ملاحظه‌ای افزایش دهند و تداوم کسب‌وکار و پیشرفت بلندمدت خود را تضمین کنند. با این وجود، سازمان‌ها در به‌کارگیری فناوری‌های ارتباطی و اطلاعاتی، با دو چالش جدی روبه‌رو هستند: تامین امنیت اطلاعات، و کمبود شدید نیروی ماهر – به‌ویژه در حوزه امنیت. از آن‌جایی که در بسیاری از سازمان‌ها، کارکنان ناآگاه ضعیف‌ترین حلقه امنیت هستند، آکادمی لیان با بهره‌گیری از تجربه خود در پیاده‌سازی تجهیزات و فناوری‌های IT و امنیت اطلاعات و تامین امنیت مجموعه‌های مختلف، امکان آموزش کارکنان سازمان‌ها را به وجود آورده تا این چالش را کم‌رنگ‌تر کند. آکادمی لیان هم‌چنین با برگزاری جدیدترین و معتبرترین دوره‌های امنیت، شبکه و برنامه‌نویسی، امکان ارائه آموزش‌های تخصصی به افراد علاقه‌مند به حوزه IT و امنیت را فراهم کرده تا ضمن پرکردن شکاف مهارتی موجود، پلی برای ورود به بازار کار به وجود بیاورد.

LIANGROUP

# سخنی با شما دانشجویان

آموزش و یادگیری یکی از ابتدایی‌ترین گام‌ها برای به‌دست آوردن تخصص است. اولین گام شما به عنوان یک دانشجوی علاقه‌مند برای ورود به دنیای تکنولوژی و به‌خصوص حوزه‌های «شبکه، امنیت سایبری و برنامه‌نویسی» نیز یادگیری مباحث تئوری و عملی مرتبط با حوزه مورد نظر شماست. به همین دلیل، شرکت‌ها و موسسات بسیاری در سراسر دنیا به تدوین و طراحی محتواهای آموزشی و دوره‌های مقدماتی تا پیشرفته مشغول هستند. آکادمی لیان نیز با تکیه بر دانش و تجربه کارشناسان و اساتید خود، و هم‌چنین با استفاده از محتوای استانداردی که از سوی موسسات برتر جهان ارائه شده، اقدام به برگزاری دوره‌های آموزشی نموده است. این دوره‌ها در سه بخش «شبکه»، «امنیت سایبری» و «برنامه‌نویسی» دسته‌بندی شده و هرکدام دارای زیرمجموعه‌های گسترده‌ای هستند. گروه لیان در برگزاری دوره‌های خود، از تجربه‌ی بالای خود در پیاده‌سازی زیرساخت‌های IT به‌ویژه امنیت سایبری استفاده کرده تا مسیری مطمئن برای ورود به بازار کار برای شما فراهم کند.

تجربه و سابقه‌ی درخشان اساتید لیان در فضای امنیت و IT کشور، داشتن تاییده از مراجع معتبری مانند «افتا» و هم‌چنین تدریس سرفصل‌های ارائه‌شده از سوی موسسات خوش‌نامی مانند SANS و EC-Council، تاییدی بر کیفیت بالای دوره‌های این مجموعه است.

**تا تخصص راه زیادی در پیش نیست، با ما همراه شوید!**


# دوره‌های پیش‌نیاز

برای کار در دنیای فناوری و به‌خصوص IT و امنیت، تسلط به مباحث پایه و مقدماتی اهمیت بالایی دارد. این مباحث شامل آشنایی عمومی و بنیادی با کامپیوتر و شبکه‌های کامپیوتری است. یکی از بهترین راه‌ها برای کسب این دانش پایه، شرکت در دوره‌های موسسه کامپتیاست. شش دوره‌ی این موسسه شامل A+ (آشنایی با مفاهیم اولیه سخت‌افزار، شبکه و سیستم‌های کامپیوتری)، Network+ (آشنایی با استانداردها و پروتکل‌های شبکه)، Linux+ (آشنایی اولیه با سیستم‌عامل پرطرفدار لینوکس)، Security+ (آشنایی با مفاهیم اصلی و ابتدایی امنیت)، Server+ (آشنایی با نحوه کار سرورها) و Storage+ (آشنایی با سیستم‌های ذخیره‌سازی)، زیربنای بسیار قدرتمندی را برای شروع کار در دنیای IT و امنیت تشکیل می‌دهند. آکادمی لیان اقدام به برگزاری این شش دوره را در قالب دوره جامع CompTIA کرده تا دانشجویان بتوانند در یک دوره فشرده و جامع، تمام دانش پایه برای شروع مسیر شغلی خود در دنیای IT را به دست آورند.

# دوره‌های مایکروسافت

غیرممکن است که در دنیای IT فعالیت کنید، و با کمپانی بزرگ مایکروسافت آشنا نباشید! مایکروسافت صرفا سازنده سیستم‌عامل ویندوز نیست و محصولات بسیار زیاد این شرکت بزرگ، امروزه در سراسر جهان مورد استفاده قرار می‌گیرند. محصولاتی نظیر خانواده Office، ویندوز سرور و... که هرکدام با امکانات متنوع و قدرتمند خود، بخشی از نیازهای سازمان‌ها را برآورده می‌کنند. به همین خاطر است که سازمان‌های کوچک و بزرگ بسیاری در سراسر جهان، زیرساخت شبکه و سیستم‌های اطلاعاتی خود را با استفاده از محصولات شرکت مایکروسافت بنا کرده‌اند. شرکت مایکروسافت، دوره‌های آموزشی مختلفی را متناسب با محصولات خود طراحی و ارائه کرده است تا کارشناسان شبکه بتوانند بر طراحی و اجرا و هم‌چنین نگهداری و به‌روزرسانی چنین زیرساخت‌هایی مسلط شوند. آکادمی لیان با نظر به این موضوع، دو دوره معتبر MCSA Window Server 2016 و هم‌چنین دوره پیشرفته‌تر MCSE Window Server 2019 را برگزار کرده و هم‌چنین آمادگی برگزاری دوره‌های پیشرفته‌تر (مانند دوره‌های Azure) را در صورت درخواست سازمان‌ها دارد.

# دوره‌های سیسکو

CISCO

CISCO

برای طراحی و پیاده‌سازی همه‌ی شبکه‌های سازمانی دو رکن اصلی لازم است:
۱- تجهیزات سخت‌افزاری و نرم‌افزاری ۲- نیروی متخصص

کمپانی سیسکو (Cisco) یکی از معتبرترین کمپانی‌های تامین‌کننده تجهیزات شبکه است. به خاطر تنوع و گسترش بالای محصولات سیسکو در سازمان‌های کوچک و بزرگ دنیا، دوره‌هایی توسط همین شرکت تدوین شده تا کارشناسان شبکه بتوانند کار با تجهیزات و بسترهای این شرکت به طور کامل بیاموزند و شما می‌توانید با گذراندن این دوره‌ها و دریافت گواهینامه‌های معتبر این شرکت، در سراسر دنیا با عنوان «کارشناس شبکه سیسکو» فعالیت کنید. سیسکو به دلیل ارائه تجهیزات فیزیکی بسیار متنوع و خدمات بسیار گسترده، سرفصل‌های زیادی را دوره‌های مقدماتی تا پیشرفته در حوزه‌های مختلف ارائه کرده است. هرچه دانش شما در زمینه پیکربندی، پیاده‌سازی، عیب‌یابی و مدیریت تجهیزات سیسکو بالاتر باشد و یا تجربه کاری بیشتری در این زمینه داشته باشید، شبکه قدرتمندتر و کارآمدتری خواهید ساخت.

CISCO

می‌توان دوره‌های شبکه سیسکو را به سه سطح کلی دستیار (Associate)، کارشناس (Professional) و متخصص (Expert) تقسیم‌بندی کرد. اولین دوره از موسسه سیسکو که دانشجویان می‌توانند پس از گذراندن دوره‌های پیش‌نیاز برای گذراندن آن اقدام کنند، دوره CCNA است. در این دوره دانشجویان با مفاهیم و مبانی شبکه، پیکربندی، پیاده‌سازی و اجرا، مدیریت و عیب‌یابی تجهیزات و محصولات سیسکو آشنا می‌شوند. در دوره CCNA به شما آموزش داده می‌شود که چگونه دسترسی به شبکه را فراهم کرده و اتصال و سرویس‌های IP را پیاده‌سازی کنید؛ ضمن این که در دوره CCNA به طور مختصر به مبانی امنیت شبکه و هم‌چنین اتوماسیون پرداخته خواهد شد. در سطح بعدی یعنی سطح Professional، مدرک CCNP قرار دارد. این مدرک پنج دسته‌بندی در حوزه‌های مختلف دارد که برای دریافت هر مدرک، دانشجویان باید ابتدا یک آزمون اصلی (Core) را گذرانده و سپس با انتخاب یکی از سه تا شش آزمون تخصصی هر حوزه (آزمون Concentration) و گذراندن آن، مدرک خود را دریافت کنند.

CISCO CERTIFIED CCNP

CISCO CERTIFIED CCNA

CISCO

اولین دسته‌بندی مدرک CCNP، دسته‌بندی Enterprise است که بر پیاده‌سازی و مدیریت شبکه‌های سازمانی تمرکز داشته و با آزمون اصلی ENCOR شناخته می‌شود. دومین دسته‌بندی، مدرک Collaboration با آزمون اصلی CLCOR است که توانایی کارشناسان در پیاده‌سازی زیرساخت ارتباطی مورد نیاز سازمان‌ها را اثبات می‌کند. CCNP Data Center دسته‌بندی بعدی است که برای کارشناسان پیاده‌سازی و مدیریت دیتاسنتر طراحی شده و آزمون مرکزی آن، آزمون DCCOR است. مدرک CCNP Security، توانایی کارشناسان در تامین امنیت روترها، سوییچ‌ها و دستگاه‌های شبکه و هم‌چنین پیکربندی و پیاده‌سازی فایروال و سرویس VPN سیسکو را نشان می‌دهد و آزمون اصلی آن آزمون SCOR است. آخرین دسته‌بندی، CCNP Service Provider با آزمون اصلی SPCOR است که مخصوص کارشناسان پیاده‌سازی زیرساخت شبکه‌ی IP در سطح شرکت‌های سرویس‌دهنده (مانند اپراتورهای تلفن همراه) است. در سطح بعدی مدارک سیسکو یعنی سطح متخصص (Expert)، به مدارک CCIE می‌رسیم که دسته‌بندی‌هایی مشابه مدرک CCNP دارد، با این تفاوت که CCIE Enterprise به دو دسته زیرساخت و وایرلس تقسیم می‌شود و به همین خاطر این مدرک مجموعا شش دسته‌بندی دارد. دسته‌بندی‌های مدرک CCIE هم دارای یک آزمون مرکزی (Core) هستند که با آزمون‌های CCNP یکسان است ولی به جای آزمون‌های تخصصی، داوطلبان دریافت این مدرک باید در هر دسته‌بندی آزمون عملی (Lab) مرتبطی را بگذرانند که توانایی عملی آن‌ها را در پیاده‌سازی و اجرای مفاهیم آموخته‌شده نشان می‌دهد.


# دوره‌های میکروتیک

میکروتیک یک شرکت بزرگ سازنده تجهیزات شبکه است که محصولات آن، امروزه در سراسر دنیا توسط سازمان‌های بسیاری استفاده می‌شوند. میکروتیک نیز همانند برندهای معتبر دیگر در حوزه تجهیزات شبکه، سرفصل‌ها و دوره‌های آموزشی مخصوص تجهیزات خودش را طراحی و ارائه کرده است. افرادی که در این دوره‌ها شرکت می‌کنند، می‌توانند کار پیاده‌سازی، اجرا، تعمیر و نگهداری و مدیریت تجهیزات میکروتیک در سازمان‌های کوچک و بزرگ را برعهده گیرند. آکادمی لیان نیز اقدام به برگزاری دوره‌های این شرکت مانند MTCNA (کارشناس شبکه)، MTCRE (مهندس روتینگ)، MTCWE (مهندس وایرلس)، MTCTCE (مهندس کنترل ترافیک)، MTCSE (مهندس امنیت) و MTCSWE (مهندسی سوییچینگ) کرده تا دانشجویان بتوانند با دریافت آموزش‌های تخصصی، به بازار کار میکروتیک وارد شوند. البته لازم به ذکر است که پرطرفدارترین دوره‌های این شرکت دوره‌های MTCNA و MTCSE هستند که به ترتیب مباحث شبکه و امنیت را پوشش می‌دهند.

MikroTik MTCNA

MikroTik MTCTCE

# دوره‌های مجازی‌سازی

مجازی‌سازی فرایندی است که طی آن نسخه‌ی مجازی (مبتنی بر نرم‌افزار) از یک سیستم ایجاد می‌شود. این روش موثرترین راه برای کاهش هزینه‌های زیرساخت فناوری اطلاعات، ضمن افزایش بازدهی و چابکی (سرعت انطباق با شرایط جدید) برای کسب‌وکارهای کوچک تا بزرگ است. امروزه استفاده از زیرساخت مجازی در اکثر شبکه‌ها رواج دارد. پیاده‌سازی، مدیریت و نگهداری یک بستر مجازی، نیازمند آموزش‌های مقدماتی و پیشرفته است. به همین منظور موسسات معتبر، دوره‌هایی را طراحی و ارائه کرده‌اند که در هرکدام از آن‌ها، شما به‌طور تخصصی نحوه پیاده‌سازی و استفاده از محصولات مجازی‌ساز رایج در دنیا را فرا خواهید گرفت. بسترهایی نظیر VMware، Citrix و Hyper-V که شما با استفاده از آن‌ها می‌توانید زیرساخت‌هایی با قابلیت مقیاس‌پذیری و تحمل خرابی بسیار بالا در سازمان‌های بزرگ و کوچک ایجاد کنید. با شرکت در دوره‌های آکادمی لیان می‌توانید پیاده‌سازی و مدیریت این سه بستر پرطرفدار را به طور کامل فرابگیرید و برای ایجاد زیرساخت مجازی در شبکه‌های سازمانی آماده شوید.

# LINUX

# دوره‌های لینوکس

در حال حاضر سیستم‌عامل لینوکس، پرطرفدارترین سیستم‌عامل در زیرساخت‌های IT سازمانی به شمار می‌رود. انعطاف‌پذیری و بهینگی بسیار بالای این سیستم‌عامل در کنار دریایی از ابزارها و اپلیکیشن‌های متن باز، باعث شده بسیاری از سازمان‌ها برای پیاده‌سازی زیرساخت دیجیتال و سرویس‌های خود، این سیستم‌عامل را انتخاب کنند. یکی دیگر از دلایل محبوبیت این سیستم‌عامل، امکان پیکربندی و شخصی‌سازی عمیق و گسترده است که مزیت‌های فراوانی را برای سیستم‌های مختلف، به‌خصوص سیستم‌های مورد استفاده در زیرساخت IT مانند سرورها به همراه دارد. تمام این ویژگی‌ها به همراه امنیت بسیار بالا در مقایسه با سیستم‌عامل‌های پرطرفدار دیگر باعث شده که تسلط بر لینوکس، هم برای کارشناسان شبکه و هم کارشناسان امنیت مهارتی مهم محسوب شود. از این رو آکادمی لیان اقدام به برگزاری معتبرترین و جدیدترین دوره‌های لینوکس کرده تا دانشجویان بتوانند مهارت‌های خود در پیاده‌سازی و مدیریت سیستم‌ها و زیرساخت‌های لینوکسی را بهبود و توسعه دهند.

# LINUX

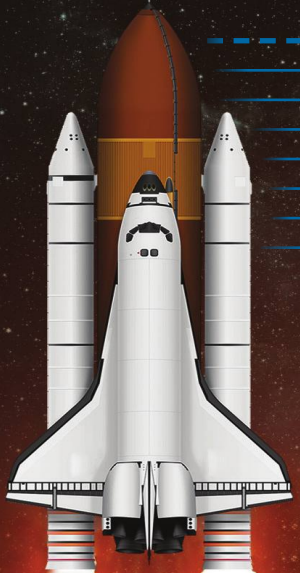
موسسه LPI یکی از معتبرترین موسسات جهانی در زمینه‌ی آموزش لینوکس است که با برگزاری آزمون‌های بین‌المللی، مدارک تخصصی لینوکس را در سطوح مختلف به متقاضیان اعطا می‌کند. سه مدرک پرطرفدار این موسسه، مدارک LPIC هستند که در سه سطح ارائه شده‌اند. مدرک LPIC-1 تحت عنوان «ادمین لینوکس» یک مدرک سطح جونیور است که توانایی فرد در نصب و راه‌اندازی یک سیستم کاری لینوکسی، حفظ و نگهداری سیستم از طریق خط فرمان و پیکربندی یک شبکه‌ی ساده را نشان می‌دهد. این مدرک پیش‌نیازی ندارد و داوطلبان برای دریافت آن می‌توانند دو آزمون ۱۰۱-۴۰۰ و ۱۰۲-۴۰۰ را بگذرانند. مدرک بعدی مدرک LPIC-2 تحت عنوان «مهندس لینوکس» است؛ این مدرک برای کارشناسانی طراحی شده که توانایی مدیریت شبکه‌های کوچک تا متوسط متشکل از سیستم‌های لینوکسی و غیرلینوکسی را دارند. داوطلبان برای دریافت این مدرک علاوه بر داشتن مدرک LPIC-1، باید دو آزمون ۲۰۱-۴۵۰ و ۲۰۲-۴۵۰ را بگذرانند. سطح سوم یعنی مدرک LPIC-3 با عنوان «متخصص لینوکس در سطح سازمانی» داری سه زیرشاخه اصلی با آزمون‌های مجزاست.

اولین زیرشاخه LPIC-3، زیرشاخه Mixed Environment است که بر مهارت کارشناسان در پیاده‌سازی و پیکربندی OpenLDAP و هم‌چنین مدیریت پیشرفته‌ی Samba تمرکز دارد. متقاضیان دریافت این مدرک باید آزمون ۳۰۰-۱۰۰ موسسه LPI را بگذرانند. زیرشاخه‌ی دوم، زیرشاخه‌ی Security است که مباحثی مانند کنترل‌های دسترسی و رمزنگاری و هم‌چنین امنیت اپلیکیشن، عملیات و شبکه را شامل می‌شود و با گذراندن آزمون ۳۰۳-۲۰۰ می‌توان آن را دریافت کرد. در نهایت زیرشاخه‌ی Virtualization and HA به مجازی‌سازی، لودبالانسینگ، مدیریت کلاسترها و کلاسترهای ذخیره‌سازی می‌پردازد. افرادی که آزمون ۳۰۴-۲۰۰ را بگذرانند موفق به دریافت این مدرک خواهند شد. لازم به ذکر است که برای دریافت هر سه مدرک LPIC-3، داشتن مدرک LPIC-2 ضروری است. یکی دیگر از موسسات معتبر در زمینه لینوکس، موسسه ردهت (Red Hat) است که توزیع لینوکسی آن یعنی RHEL، در سازمان‌ها و زیرساخت‌های فراوانی مورد استفاده قرار گرفته است. این موسسه نیز مدارکی مانند RHCSA (ادمین سیستم ردهت) و RHCE (مهندس ردهت) عرضه کرده تا کارشناسان بتوانند با دریافت آن‌ها توانایی خود را در پیاده‌سازی، پیکربندی و مدیریت زیرساخت مبتنی بر ردهت در مقیاس سازمانی نشان دهند.


DevOps

# دنیای دوآپس

جایگاه شغلی DevOps با این هدف به وجود آمد که شکاف بین تیم‌های توسعه محصول و تیم‌های عملیات IT را ازبین ببرد. پرشدن این شکاف باعث افزایش تعامل بین این دو تیم و بالا رفتن سرعت فرایند توسعه و استقرار پیوسته‌ی اپلیکیشن می‌شود. در حقیقت دوآپس مجموعه‌ای از روش‌ها، فرایندها و ابزارهایی است که باعث یکپارچگی و چابکی فرایند توسعه تا استقرار محصول می‌شود. یک مهندس دوآپس باید بتواند توسعه‌دهندگان محصول و مهندسان اجرایی در بخش عملیات IT را به شکلی نظام‌مند درکنار یکدیگر قرار دهد و در واقع پلی بین تیم برنامه‌نویسی و تیم نگهداری از زیرساخت IT به وجود آورده و امکان یکپارچه‌سازی پیوسته و استقرار پیوسته محصولات (CI/CD) فراهم کند. به همین خاطر علاوه بر آشنایی با فرایند برنامه‌نویسی و توسعه اپلیکیشن و هم‌چنین شناخت نسبت به سیستم‌ها و زیرساخت IT، مهندس دوآپس باید توانایی اتوماسیون فرایند تست و استقرار محصول، تسلط به زیرساخت‌های ابری، مهارت در استفاده از بسترهای نسخه‌بندی (Versioning)، توانایی استفاده از ابزارهای مختلف ایجاد پکیج و ارکستراسیون و مهارت پیاده‌سازی و به‌کارگیری سیستم‌های مانیتورینگ را نیز داشته باشد.



با توجه به تقاضای بالا نسبت به مهندسان دوآپس و پیچیدگی‌های مسیر آموزشی این حوزه، آکادمی لیان دوره‌های جامع دوآپس خود را در سه سطح مختلف و تحت نظر مهندسان باتجربه دوآپس تدوین کرده تا دانشجویان بتوانند مهارت‌های کلیدی لازم برای ورود به دنیای دوآپس را در مسیری مشخص فرابگیرند. سطح اول دوره دوآپس شامل مهارت‌های ادمین سیستم، دوره‌های LPIC-1 و LPIC-2 جهت تسلط به مدیریت و پیکربندی زیرساخت‌های لینوکسی، دوره اسکریپت‌نویسی به زبان Bash برای انجام اتوماسیون و هم‌چنین مدیریت و نگهداری سیستم‌های لینوکسی، و دوره آموزش پیاده‌سازی و استفاده از سیستم مانیتورینگ متن باز پرطرفدار و قدرتمند Zabbix است. در دوره دوآپس سطح ۲ دانشجویان استفاده از بستر پرطرفدار Docker برای ساخت پکیج‌ها (یا اصطلاحا کانتینرهای) نرم‌افزاری را می‌آموزند که در ساده‌سازی استقرار محصول و مدیریت زیرساخت نقش به‌شدت موثری دارد. علاوه بر این، در این دوره دانشجویان استفاده از نرم‌افزار مانیتورینگ قدرتمند Prometheus و هم‌چنین بستر معروف Git برای نسخه‌بندی اپلیکیشن‌ها را فرامی‌گیرند.

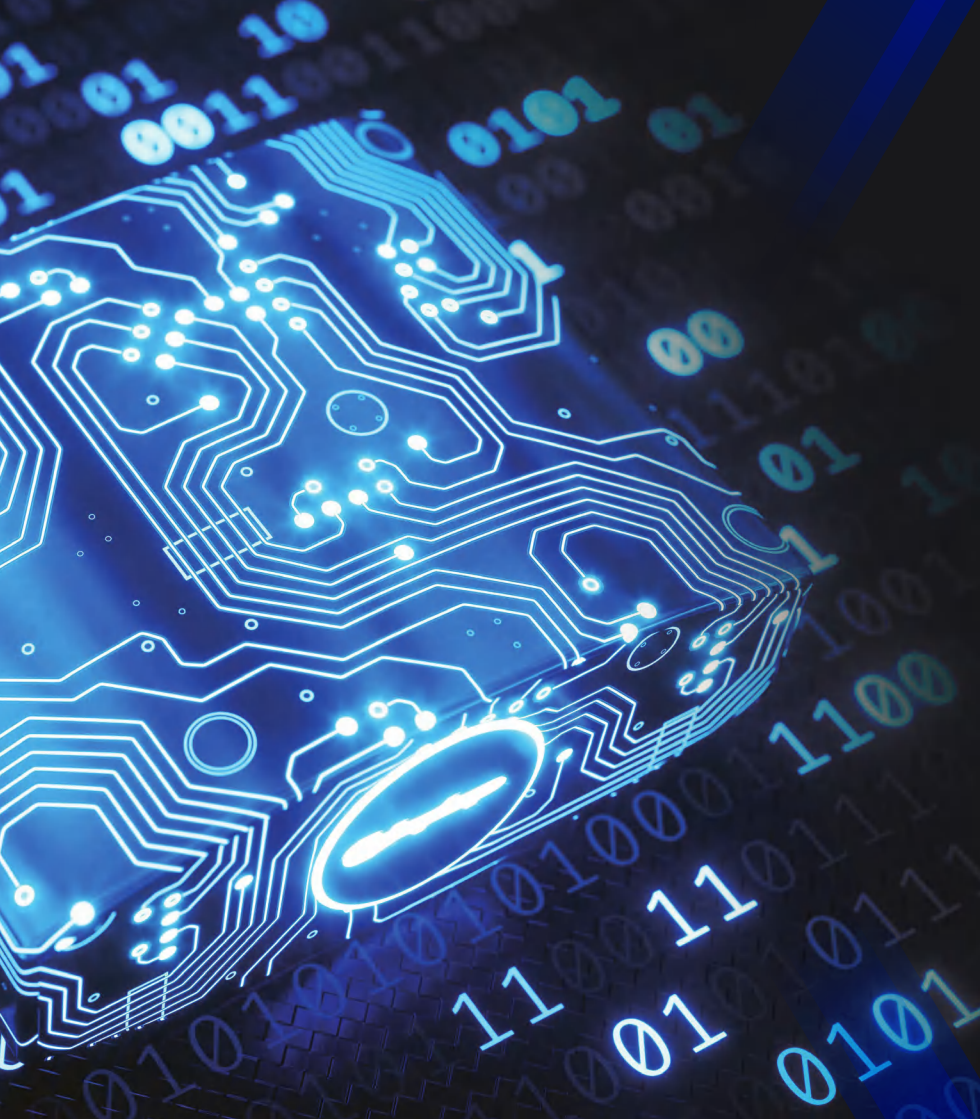
در ادامه‌ی دوره سطح دو، دانشجویان استفاده از سرور Jenkins را جهت اتوماسیون فرایند تست، پیکربندی و استقرار اپلیکیشن‌ها و ایجاد یک خط لوله‌ی CI/CD می‌آموزند. در انتهای این سطح نیز به ابزار قدرتمند Ansible پرداخته‌می‌شود. این ابزار با اتوماسیون عملیات IT، امکان تهیه‌ی منابع برای استقرار اپلیکیشن‌ها و پیاده‌سازی مفهوم «زیرساخت به‌عنوان کد» (IaC) را به وجود آورده و چرخه‌ی CI/CD را تکمیل می‌کند. در دوره‌ی سطح سه دوآپس، به مباحث پیشرفته‌تر برای کار در محیط‌های بزرگ‌مقیاس پرداخته خواهد شد. در ابتدای این دوره، دانشجویان استفاده از سیستم قدرتمند Kubernetes را برای ارکستراسیون پکیج‌ها و کانتینرهای نرم‌افزاری می‌آموزند که در تحقق مقیاس‌پذیری نقش بسیار مهمی دارد. در ادامه این دوره نیز زیرشاخه‌های امنیت و HA از دوره LPIC-3 آموزش داده می‌شوند تا دانشجویان بتوانند محیط‌هایی امن و قابل اطمینان برای توسعه و استقرار اپلیکیشن‌ها به وجود بیاورند. البته لازم به ذکر است که در هر سه سطح ممکن است به صلاحدید اساتید و با توجه به نیاز روز صنعت، سرفصل‌هایی اضافه شده یا تغییر کنند.


x = "Welcome to the Mirror."
y = 0
while y <= len(x):
os.system("clear")
print(x[:y])
time.sleep(0.2)
y = y+1
time.sleep(2)
x = "You will stay here for as long as you can, you may
forfeit when you would like to."
y = 0
while y <= len(x):
os.system("clear")
print(x[:y])
time.sleep(0.2)
y = y+1
time.sleep(2)
x = "Please stand here, and stare into the mirror."
y = 0
while y <= len(x):
os.system("clear")
print(x[:y])
time.sleep(0.2)
y = y+1
time.sleep(2)
x = "This is you in the mirror:"

# پایتون با گرایش‌های مختلف

پایتون یک زبان برنامه‌نویسی همه‌منظوره، قدرتمند و تطبیق‌پذیر است. پایتون یکی از زبان‌های برنامه‌نویسی محبوب بین توسعه‌دهندگان، کارشناسان علم داده، مهندسان نرم‌افزار و حتی هکرهاست. دلیل این محبوبیت این زبان علاوه بر تطبیق‌پذیری، انعطاف‌پذیری و شی‌گرا بودن آن، وجود کتابخانه‌ها و ماژول‌های فراوان و قدرتمند و فریم‌ورک‌های گوناگون است که ابزارهای فراوانی را در اختیار کاربران پایتون قرار می‌دهند. همین مزایای برجسته است که باعث شده در دنیای علم و فناوری، پایتون به انتخاب اول بسیاری از حوزه‌ها تبدیل شود. امروزه پایتون زبان اصلی حوزه‌های هوش مصنوعی، یادگیری ماشین و علم داده تبدیل شده و بسیاری از اپلیکیشن‌ها و نرم‌افزارها نیز با این زبان توسعه داده می‌شوند. علاوه بر این، این زبان در برنامه‌نویسی بک‌اند (فریم‌ورک django) و حتی فرانت‌اند نیز محبوبیت فراوانی یافته است. در چند سال اخیر نیز کاربرد پایتون در دنیای فناوری اطلاعات رشد بسیار چشم‌گیری داشته و بخش اعظمی از مهندسان شبکه و کارشناسان امنیت و به‌خصوص تست نفوذ، برای انجام اتوماسیون و ایجاد ابزارها و ماژول‌های مورد نظر خود، این زبان را به عنوان انتخاب اول خود برگزیده‌اند.

دوره آموزش پایتون آکادمی لیان با این هدف طراحی شده که دانشجویان بتوانند با شرکت در یک دوره جامع و بدون نیاز به هیچ‌گونه پیش‌زمینه در برنامه‌نویسی یا IT، به طور کامل و گام‌به‌گام از سطح مقدماتی تا پیشرفته به استفاده از زبان پایتون مسلط شوند. علاوه بر این، دو دوره «پایتون برای شبکه» و «پایتون برای بلک‌هت» دانشجویان را برای اتوماسیون شبکه با استفاده از پایتون، و همچنین اسکریپت‌نویسی و ایجاد ابزارهای تست نفوذ کاملا آماده می‌کنند.



# حوزه‌های امنیت

سرعت بالای رشد فناوری اطلاعات و گسترش روزافزون زیرساخت‌های دیجیتال در تمام صنایع، باعث شده امنیت اطلاعات به چالشی کلیدی تبدیل شود. یکی از اصلی‌ترین معضلات سازمان‌ها در حفاظت از دارایی‌های دیجیتال خود، کمبود شدید نیروی کار ماهر در حوزه امنیت سایبری است که باعث شده تقاضای شدیدی برای کارشناسان امنیت به وجود بیاید. به همین علت است که آکادمی لیان تمرکز اصلی خود را بر برگزاری دوره‌های معتبر جهانی امنیت از موسساتی مانند ISACA، (ISC)2، EC-Council، SANS، Offensive-Security و موسسات آموزشی معتبر دیگر قرار داده تا بتواند با آموزش کارشناسان ماهر امنیت اطلاعات تحت نظر متخصصان باسابقه و شناخته‌شده صنعت امنیت کشور، به حل چالش کمبود نیروی کار در این حوزه کمک کند. امنیت سایبری را می‌توان به سه زیرشاخه اصلی «امنیت دفاعی»، «امنیت تهاجمی» (یا تست نفوذ) و «پاسخ به حادثه، جرم‌شناسی دیجیتال و تحلیل بدافزار» تقسیم‌بندی کرد. هر کدام از این شاخه‌ها نیز به زیرمجموعه‌های جزئی‌تری تقسیم می‌شوند که در مجموع حوزه‌های کاری امنیت سایبری را تشکیل می‌دهند.

در هر زیرشاخه از امنیت سایبری، دوره‌های فراوان و متنوعی وجود دارد که هرکدام مباحث مختلفی از امنیت را پوشش می‌دهد، ولی برای هر کسی که قصد ورود به دنیای امنیت را دارد، گذراندن دو دوره‌ی پیش‌نیاز ضروری است. دوره اول دوره CEH از موسسه EC-Council است که شاید معروف‌ترین دوره در حوزه امنیت و تست نفوذ به شمار رود؛ این دوره دانشجویان را با مفاهیم پایه‌ای مثل انواع آسیب‌پذیری‌ها و حملات سایبری در سطوح مختلف حمله آشنا می‌کند. دوره دوم، دوره PWK از موسسه Offensive Security است که تکنیک‌ها و رویکردهای مختلف تست نفوذ را به دانشجویان می‌آموزد و آزمون مدرک OSCP بر اساس آن طراحی شده است. این دو دوره در ترکیب با یکدیگر، دانشجویان را به طور کامل با ادبیات دنیای امنیت آشنا کرده و آن‌ها را برای گذراندن دوره‌های پیشرفته‌تر آماده می‌کنند. آکادمی لیان با بهره‌گیری از تجربه خود در زمینه آموزش و هم‌چنین در زمینه ارائه خدمات امنیت، اقدام به برگزاری دوره‌های معتبر جهانی در کنار دوره‌های با سرفصل اختصاصی کرده که هم افراد علاقه‌مند به کار در دنیای امنیت، و هم سازمان‌ها برای آموزش کادر امنیت سایبری خود، می‌توانند از آن‌ها استفاده کنند.

# CYBER SECURITY

# امنیت شبکه

امنیت شبکه یکی از معروف‌ترین و پرطرفدارترین، و البته پرتقاضاترین زیرشاخه‌های امنیت دفاعی است. کارشناسان امنیت شبکه علاوه بر تسلط بر مفاهیم و استانداردهای امنیتی، باید شناخت کامل و دقیقی از فناوری‌های شبکه و زیرساخت‌های سازمانی داشته باشند. دوره‌های فراوانی در حوزه امنیت شبکه وجود دارند، اما یک نقطه شروع مناسب برای دوره‌های امنیت شبکه، دوره SEC401 موسسه SANS است که دانشجویان در آن با مبانی اولیه امنیت و حفاظت از اندپوینت‌ها، شبکه‌ها و فضاهای ابری آشنا می‌شوند. دوره SEC501 مبانی پیشرفته امنیت را شامل شده و شرکت‌کنندگان را برای تامین امنیت محیط‌های سازمانی آماده می‌کند. در ادامه دوره SEC440 قرار دارد که دانشجویان را با ۲۰ کنترل امنیتی حیاتی SANS آشنا می‌کند. این ۲۰ کنترل امنیتی به گونه‌ای طراحی شده‌اند که فرهنگ امنیت را در سازمان ارتقا داده و از بسیاری از حملات رایج جلوگیری کنند. در دوره SEC503 نیز دانشجویان با مبانی TCP/IP و بخش اعظمی از پروتکل‌های لایه اپلیکیشن آشنا می‌شوند تا بتوانند با بررسی ترافیک شبکه، نفوذهای امنیتی را شناسایی کنند. در دوره SEC487، به جمع‌آوری و تحلیل اطلاعات متن باز (OSINT) پرداخته می‌شود که ابزاری قدرتمند در دفاع از شبکه در برابر جدیدترین تهدیدات است.

NETWORK SECURITY

در دوره بعدی یعنی دوره SEC555، دانشجویان نحوه بهبود دادن راهکارهای لاگ‌گیری در سیستم‌های SIEM، و ریشه‌یابی دقیق‌تر لاگ‌های جمع‌آوری‌شده را می‌آموزند که در شبکه‌های متوسط تا بزرگ مهارتی ارزشمند محسوب می‌شود. دوره‌های بعدی دوره‌های پیشرفته‌تر هستند که برای کارشناسان امنیت با چند سال سابقه کار در صنعت امنیت طراحی شده‌اند. دوره SEC530 طراحی و مهندسی معماری امنیت را با تمرکز بر بهره‌گیری از زیرساخت موجود خواهند آموخت. شرکت‌کنندگان در دوره SEC566 پیاده‌سازی عملی و ممیزی ۲۰ کنترل حیاتی SANS را برای برآورده‌کردن بازه‌ی وسیعی از استانداردها و مقررات حوزه امنیت سایبری خواهند آموخت. در دوره SEC599 به تاکتیک‌های تیم بنفش و راهکارهای دفاعی موثر در برابر مراحل مختلف چرخه کشتار سایبری می‌پردازد و دانشجویان را برای متوقف‌کردن، شناسایی و پاسخ‌دادن فعال به مهاجمان آماده می‌کند. مهندسان امنیت شبکه پس از کسب تجربه کافی، می‌توانند در دوره ISMS شرکت کرده و خود را برای طراحی کامل سیستم‌های مدیریت امنیت اطلاعات در مقیاس بزرگ و مطابق با جدیدترین استانداردهای بین‌المللی امنیت آماده کنند. علاوه بر این، برای کارشناسانی که قصد طراحی یا ممیزی سیستم‌ها و زیرساخت امنیت در سازمان‌های مالی یا مجموعه‌های مرتبط را دارند، آشنایی با مجموعه مقررات PCI-DSS و نحوه تحقق آن‌ها مهارتی حیاتی محسوب می‌شود.

# مرکز عملیات امنیت (SOC)

مرکز عملیات امنیت یا Security Operation Center – که معمولا از نام اختصاری SOC برای آن استفاده می‌شود - واحدی مرکزی در یک سازمان است که با به‌کارگیری افراد، فرایندها و فناوری‌های گوناگون، به طور پیوسته وضعیت کلی امنیت یک سازمان را مانیتور کرده و بهبود می‌دهد و در عین حال از حوادث امنیتی جلوگیری می‌کند، این حوادث را شناسایی و تحلیل کرده و به آن‌ها پاسخ می‌دهد. واحد SOC در واقع مانند یک واحد فرماندهی مرکزی عمل کرده و داده‌های مختلف را از زیرساخت IT شامل شبکه‌ها، دستگاه‌ها، اپلیکیشن‌ها و سامانه‌های ذخیره‌سازی اطلاعات دریافت کرده و با یافتن روابط میان آن‌ها و شناسایی داده‌های مشکوک، رویدادهای امنیتی را تولید می‌کند. در قلب مرکز SOC، سیستم اطلاعات امنیت و مدیریت رویداد (SIEM) قرار دارد که چشم‌اندازی جامع از وضعیت امنیت اطلاعات سازمان در اختیار کارشناسان SOC قرار می‌دهد. این سیستم وظیفه دارد داده‌های امنیتی را جمع‌آوری کند، این داده‌ها را با پروفایل‌های تعریف‌شده توسط ادمین SIEM تطابق دهد، روابط بین این داده‌ها با یکدیگر و با اطلاعات زمینه‌ای (مانند زمان، الگوی فعالیت، مکان جغرافیایی و ...) را به دست آورد و هشدارهای امنیتی معنی‌داری را با توجه به این روابط تولید کند.

# SOC

واحد SOC معمولا شامل چهار سطح یا Tier است. سطح اول شامل تحلیل‌گران امنیتی کم‌تجربه‌ای است که بر رویدادهای امنیتی نظارت کرده و به دنبال فعالیت مشکوک می‌گردند. در صورتی که مورد مشکوکی یافت شد، این مورد به همراه اطلاعات جانبی به سطح ۲ ارجاع داده می‌شود، فرایندی که به آن تریاژ (یا اولویت‌بندی) گفته می‌شود. تحلیل‌گران سطح ۲ تحقیقات عمیق‌تری روی فعالیت مشکوک انجام داده و ماهیت تهدید و دامنه‌ی تاثیر آن روی زیرساخت سازمان را می‌سنجند. سطح ۳ از واحد SOC که به سطح «شکار تهدید» معروف است، باتجربه‌ترین تحلیل‌گران امنیت را در خود جای داده که پاسخ به حوادث پیچیده را بر عهده دارند و باقی وقت خود را صرف بررسی اطلاعات فارنزیک و تله‌متری می‌کنند تا تهدیدات احتمالی را بیابند که بسترهای شناسایی تهدید قادر به تشخیص آن‌ها نبوده‌اند. سطح ۴ نیز با بکارگیری تجربیات خود، وظیفه رهبری تیم SOC را بر عهده دارد. با توجه به افزایش به‌کارگیری واحد SOC در سازمان‌ها و نیاز شدید به تحلیل‌گران امنیت، آکادمی لیان دوره‌هایی را به طور ویژه جهت آموزش تحلیل‌گران واحد SOC تدوین کرده است. علاوه بر افراد علاقه‌مند به ورود به حوزه امنیت، سازمان‌ها نیز می‌توانند برای آموزش نیروهای IT خود و تشکیل واحد SOC با استفاده از ظرفیت‌های موجود، از این دوره‌ها بهره‌مند شوند.


CLOUD
SECURITY

# امنیت ابری

در سال‌های گذشته زیرساخت‌های ابری محبوبیت فراوانی میان سازمان‌ها و شرکت‌ها پیدا کرده‌اند. سرعت، مقیاس‌پذیری ، قابلیت اطمینان و دسترس‌پذیری بالای زیرساخت‌های ابری باعث شده امروزه بیش از ۹۰ درصد سازمان‌ها، شکلی از زیرساخت ابری را در تاسیسات فناوری اطلاعات خود به کار ببرند. این گسترش و رشد ناگهانی منابع ابری باعث شده سازمان‌ها نتوانند در حفظ امنیت این زیرساخت‌ها پابه‌پای پیشرفت‌ها و تغییرات پیش بیایند؛ به همین خاطر است که امروزه لبه‌ی ابری به یک سطح حمله ی جذاب برای مهاجمان و مجرمان سایبری تبدیل شده است. آکادمی لیان برای پر کردن این شکاف مهارتی، اقدام به برگزاری دوره‌های تخصصی امنیت ابری کرده که علاوه بر آموزش مفاهیم پایه فناوری‌ها و زیرساخت‌های ابری، نحوه‌ی ایمن‌سازی پیشرفته و موثر آن‌ها را نیز به دانشجویان می‌آموزند. دوره‌های امنیت ابری، بخشی مهم از مسیر آموزشی تمام مهندسان و معماران امنیت بوده و به‌خصوص برای سازمان‌هایی ایده‌آل هستند که قصد دارند با آموزش نیروهای داخلی، امنیت زیرساخت‌های ابری اضافه‌شده به دارایی‌های دیجیتال خود را در کمترین زمان ممکن تامین کنند.

دوره‌های فراوان و متنوعی برای یادگیری مبانی ابتدایی تا پیشرفته‌ی امنیت ابری وجود دارند، و از میان آن‌ها دوره SEC488 نقطه‌ی مناسبی برای شروع است. این دوره سرویس‌دهندگان ابری اصلی (آمازون، مایکروسافت، گوگل و...) را پوشش داده و شما را با زیرساخت‌های ابری آشنا می‌کند. در دوره SEC510 به طور اختصاصی به تامین امنیت زیرساخت‌های ابر عمومی (Public Cloud) پرداخته خواهد شد و در دوره SEC522 نیز دانشجویان به مبانی امنیت وب‌اپلیکیشن‌ها مسلط می‌شوند که برای بسیاری از سازمان‌ها اهمیتی حیاتی دارد. دوره SEC540 روی ایمن‌سازی محیط‌های ابری مدرن و دوآپس تمرکز می‌کند و دریچه‌ی ورود به حوزه نسبتا جدید DevSecOps است. در دوره SEC541 کارشناسان امنیت با پیاده‌سازی و مدیریت سیستم‌های مانیتورینگ امنیت زیرساخت ابری آشنا می‌شوند تا بتوانند تهدیدات سایبری در لبه ابری را به‌طور موثری شناسایی کنند. در دوره‌ی تخصصی و پیشرفته‌ی SEC584 نیز دانشجویان به طور خاص روی حفاظت از کانتینرهای نرم‌افزاری و Kubernetes تمرکز می‌کنند. در نهایت از آن‌جایی که کارشناس امنیت زیرساخت ابری باید توانایی انجام تست نفوذ و یافتن آسیب‌پذیری‌ها در این محیط را نیز داشته باشد، این مهارت‌ها در دوره SEC588 آموزش داده می‌شوند.

# امنیت سیستم‌های کنترل صنعتی (ICS)

در دنیای مدرن هیچ صنعتی از نوآوری‌ها و تحولات مدرن دور نمانده و حتی صنایع زیرساختی مانند نیروگاه‌ها و پست‌های انتقال و توزیع، شرکت‌های نفتی، پالایشگاه‌ها، کارخانه‌های تولیدی، تصفیه‌خانه‌ها و بسیاری صنایع دیگر، سال‌هاست به استفاده از تجهیزات دیجیتال روی آورده‌اند. سیستم‌هایی مانند سیستم SCADA و دیگر سیستم‌های فناوری عملیاتی (OT)، چندین دهه است که به مهندسان در مانیتورینگ، کنترل و مدیریت فرایندهای صنعتی کمک می‌کنند. این سیستم‌ها در کنار افزایش بهره‌وری و کاهش چشم‌گیر هزینه‌های عملیاتی، ضریب اطمینان عملیات‌ها را نیز به طور قابل توجهی افزایش می‌دهند. اما در حوزه سیستم‌های کنترل صنعتی هم مانند بسیاری حوزه‌های دیگر، تحولات دیجیتال علاوه بر مزایای فراوان خود، یک چالش جدی برای مجموعه‌ها به وجود آورده‌اند و این چالش، تامین امنیت سیستم‌هایی است که از طرفی در شبکه‌های کامپیوتری قرار داشته و نسبت به حملات سایبری آسیب‌پذیرند، و از طرف دیگر عملیات‌های بسیار حساسی را کنترل می‌کنند که اختلالی کوچک در آن‌ها می‌تواند خسارات و تبعات جدی و خطرناکی به دنبال داشته باشد.

حیاتی‌بودن و درجه اهمیت شبکه‌های کنترل صنعتی باعث شده به هدفی ارزشمند برای مهاجمان سایبری تبدیل شوند. به همین خاطر است که امروزه نیاز بالایی به کارشناسان امنیت ICS وجود دارد. از طرف دیگر برای ورود به این حوزه، داشتن دانش کافی نسبت به عملیات‌های صنعتی و سیستم‌های کنترل صنعتی و هم‌چنین آشنایی با عملیات‌های سازمان هدف، ضرورت دارد. به همین خاطر است که بسیاری از مجموعه‌ها مانند نیروگاه‌ها، شرکت‌های توزیع برق، پالایشگاه‌ها و شرکت‌های نفت و گاز ترجیح می‌دهند با آموزش نیروهای باتجربه خود این نیاز را برطرف کنند. به همین خاطر آکادمی لیان علاوه بر برگزاری دوره‌های جامع امنیت ICS برای علاقه‌مندان این حوزه، برنامه‌های آموزشی ویژه‌ای را نیز جهت مجموعه‌های متقاضی تدوین کرده است. در حال حاضر دوره ICS410 (آشنایی با مبانی امنیت ICS و SCADA)، دوره ICS515 (دفاع فعال و واکنش به حادثه ICS) و ICS612 (امنیت سایبری ICS در عمق)، از دوره‌های پرطرفداری هستند که موسسه SANS – که یکی از برترین موسسات آموزش امنیت در زمینه سیستم‌های کنترل صنعتی به شمار می‌رود – برای آموزش کارشناسان این حوزه ارائه کرده است و در آکادمی لیان نیاز با سرفصل‌های یکسانی تدریس می‌شوند.

# ICS

# مدیریت امنیت

برای حفاظت از یک سازمان، به چندین لایه‌ی دفاعی، تاسیسات و واحدهای مختلف و تعداد زیادی راهکار متنوع نیاز است. هر روزه لبه‌های جدیدی در شبکه‌ها و زیرساخت به وجود می‌آیند و لبه‌های قدیمی نیز دستخوش تحول می‌شوند و چشم‌انداز تهدیدات نیز دائما در حال گسترده‌ترشدن است. از طرف دیگر، تعیین اولویت‌ها در برنامه‌ی کلی امنیت سازمان با توجه به بودجه‌ی تخصیص‌یافته توسط سازمان و قوانین حوزه امنیت سایبری، وظیفه‌ای حساس و ظریف است که نیاز به تجربه و دانش فنی و مدیریتی بالایی دارد. خسارات و هزینه‌های مالی حوادث سایبری و تبعات آن‌ها چه از لحاظ حقوقی و چه از لحاظ واردشدن آسیب به وجهه‌ی مجموعه نیز روزبه‌روز بیشتر می‌شود. تمام این عوامل باعث شده سازمان‌ها در حوزه امنیت، به مدیرانی با توانایی تدوین یک استراتژی موثر و قدرتمند برای امنیت سایبری نیاز داشته باشند. بهترین جایی که سازمان‌ها می‌توانند مدیران خود را در آن بیابند، داخل خود سازمان است؛ مهندسان و معماران ارشد امنیت داخل سازمان که تجربه‌ای چندساله از کار در سازمان دارند، می‌توانند هم‌گام با بلوغ مجموعه، دانش و مهارت‌های خود را بیشتر کنند و در نهایت نیاز سازمان به مدیران امنیت باتجربه را برآورده کنند.

# SECURITY MANAGEMENT

کارشناسان امنیت می‌توانند با شرکت در دوره MGT512 اصول و مبانی مدیریت امنیت را فرا بگیرند. در دوره پیشرفته‌تر MGT516، مدیران امنیت آینده، مدیریت آسیب‌پذیری‌های امنیتی در سطح سازمان و زیرساخت ابری را فراخواهند گرفت. در دوره MGT520 متقاضیان به طور تخصصی روی طراحی و پیاده‌سازی امنیت ابری تمرکز خواهند کرد. یکی از دوره‌های مدیریتی مهم SANS، دوره MGT521 است که مدیران امنیت را برای ایجاد تحول در وضعیت امنیت سایبری سازمان و ایجاد فرهنگ امنیت آماده می‌کند. برای پیشرفت مطلوب فرایند مدیریت پروژه‌های IT، لازم است این پروژه‌ها به چند فرایند کوچک‌تر در دسته‌بندی‌های مختلف تقسیم شوند و پلی ارتباطی میان بخش مدیریت و بخش فنی سازمان ایجاد شود؛ مهارت‌هایی که مدیران در دوره MGT525 می‌آموزند. در نهایت نیز دوره MGT551، نحوه ایجاد، مدیریت و هدایت یک مرکز عملیات امنیت (SOC) را پوشش می‌دهد. غیر از موسسه SANS، موسسات معتبر دیگری نیز دوره‌های معتبری در زمینه مدیریت امنیت برگزار می‌کنند که دوره CISO از موسسه EC-Council و دوره CISSP از موسسه ISC(2) دو نمونه‌ی محبوب از آن‌ها هستند.

آکادمی لیان آمادگی برگزاری تمام دوره‌های مطرح مدیریت امنیت را هم برای کارشناسان امنیت علاقه‌مند به حوزه مدیریت، و هم برای کادر سازمان‌ها دارد.

# دوره‌های تست‌نفوذ شبکه

شبکه‌ها یکی از اصلی‌ترین و گسترده‌ترین بخش‌ها در هر زیرساخت IT هستند. تقریبا تمام دارایی‌های دیجیتال سازمان در لایه‌های مختلف، در یک یا چند شبکه قرار دارند و همین مساله، شبکه‌ها را به هدفی ارزشمند برای طیف گسترده و متنوعی از حملات سایبری تبدیل کرده است؛ از حملات منع سرویس (DoS) که صرفا با هدف خسارت‌زدن و ایجاد اختلال در عملیات‌های سازمانی انجام می‌شوند، تا حملاتی که به دنبال سرقت اطلاعات و حتی جاسوسی هستند. یکی از گام‌های حیاتی در تامین امنیت شبکه، یافتن آسیب‌پذیری‌ها و نقطه‌ضعف‌های آن از دید مهاجمان است و فرایند تست نفوذ، برای تحقق همین امر انجام می‌شود. برای ورود به حوزه تست نفوذ شبکه، ابتدا داشتن دانش پایه نسبت به دستگاه‌ها، سرویس‌ها و پروتکل‌های شبکه و پس از آن تسلط به مباحث بنیادی امنیت و تست نفوذ (دوره‌های CEH و PWK) ضروری است. پس از آن دوره‌های فراوانی از موسسات مختلف وجود دارند که دانشجویان را در مسیر تبدیل‌شدن به یک کارشناس حرفه‌ای تست نفوذ شبکه یاری می‌کنند، و دوره جامع تست نفوذ شبکه آکادمی لیان طی بیش از ۲۵۰ ساعت آموزش تخصصی، سرفصل‌های معتبرترین و پرطرفدارترین آن‌ها را پوشش می‌دهد. سرفصل‌های این دوره، یکی از بهینه‌ترین و سریع‌ترین مسیرهای آموزشی برای علاقه‌مندان به حوزه تست نفوذ شبکه است.

# NETWORK PENTEST

در دوره جامع تست نفوذ شبکه، دانشجویان ابتدا در دوره MSFU از موسسه Offensive Security استفاده از بستر قدرتمند متاسپلویت برای تست نفوذ شبکه را می‌آموزند. در ادامه و در دوره WiFu از همین موسسه، به طور کامل به حملات وایرلس پرداخته می‌شود. این دوره سرفصل‌های آزمون مدرک OSWP را پوشش می‌دهد. پس از آن دوره ECSA از موسسه EC-Council آموزش‌های دوره CEH را کامل می‌کند و توانایی تحلیل خروجی ابزارها و فناوری‌های تست نفوذ را به دانشجویان می‌دهد. دوره‌ی بعدی با عنوان LPT، پیشرفته‌ترین دوره تست نفوذ این موسسه است که شما را برای پیچیده‌ترین چالش‌های تست نفوذ در دنیای واقعی آماده می‌کند. پس از گذراندن این مراحل، دانشجویان برای دوره SEC560 از موسسه SANS آماده می‌شوند که به طور اختصاصی به تکنیک‌های حمله و نفوذ به شبکه می‌پردازد. در دوره SEC660 قوی‌ترین وکتورهای حمله و تکنیک‌های پیشرفته تست نفوذ در بستر شبکه را آموخته و با اکسپلویت‌نویسی آشنا می‌شوید. در نهایت دوره SEC760 به طور کامل به اکسپلویت‌نویسی پیشرفته اختصاص داده شده است که مهارتی ضروری برای تست نفوذ شبکه است. علاوه بر دوره‌های ذکرشده و با توجه به اهمیت پایتون در تست نفوذ، آکادمی لیان دوره پایتون برای بلک‌هت را نیز زیر نظر اساتید باسابقه تست نفوذ طراحی کرده تا دانشجویان بتوانند به استفاده از این زبان در فرایند تست نفوذ و طراحی ابزارهای تهاجمی مسلط شوند.

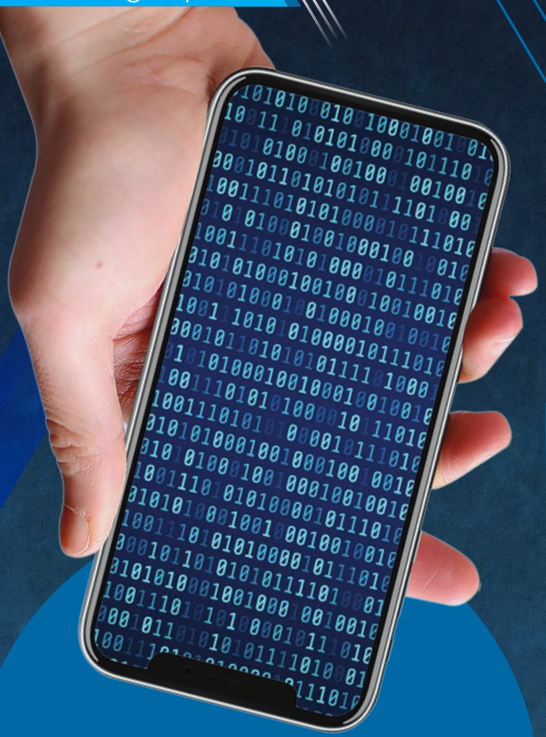
# دوره‌های تست نفوذ وب

امروزه کمترین سازمانی را می‌توان یافت که بخشی حیاتی از کسب‌وکار، خدمات یا عملیات‌های خود را به بستر اینترنت انتقال نداده باشد. بسیاری از وبسایت‌ها، وب‌اپلیکیشن‌ها و وب‌سرورها چنان کارکردهای حیاتی را بر عهده دارند که تداوم کسب‌وکار به آن‌ها وابسته است. علاوه بر اهمیت بنیادی و نقش کلیدی دارایی‌های تحت وب در عملیات‌های یک مجموعه، داده‌های خصوصی کاربران نیز توسط این سیستم‌ها و محصولات ذخیره یا منتقل می‌شود؛ این مساله باعث شده که دارایی‌های تحت وب از منظر حفظ حریم خصوصی و محرمانگی داده‌ها نیز اهمیت بالایی داشته باشند، چرا که سرقت یا از دست رفتن این اطلاعات می‌تواند تبعات حقوقی سنگینی را متوجه سازمان کند. ارزش بالا و اهمیت حیاتی دارایی‌های تحت وب، آن‌ها را به هدفی وسوسه‌انگیز برای مهاجمان و مجرمان سایبری تبدیل کرده است، زیرا در صورت نفوذ موفقیت‌آمیز به آن‌ها، امکان بهره‌برداری‌های مالی بسیار بیشتری خواهند داشت. به همین خاطر است که برای تعداد زیادی از سازمان‌ها، یافتن آسیب‌پذیری‌های وب پیش از مهاجمین، به یکی از اولویت‌های امنیتی تبدیل شده است که نتیجه‌ی آن، نیاز بالا به کارشناسان تست نفوذ وب و برنامه‌های گسترده‌ی باگ‌بانتی است.

برای ورود به دنیای تست نفوذ وب، پس از کسب دانش پایه فناوری اطلاعات و گذراندن دوره‌های پیش‌نیاز امنیت، آشنایی با سه زبان PHP، جاوااسکریپت و SQL (البته بسیار کمتر از دانش مورد نیاز برای توسعه وب، و صرفا برای خواندن کد و نوشتن اکسپلویت) لازم است. پس از آن دانشجویان می‌توانند وارد دو دوره پیشرفته‌ی تست نفوذ وب موسسه SANS، یعنی SEC542 و SEC642 شوند. دوره SEC542 به صورت تخصصی روی تکنیک‌های تست نفوذ وب‌اپلیکیشن تمرکز می‌کند و دوره SEC642 تکنیک‌های پیشرفته تست نفوذ وب اپلیکیشن و اکسپلویت‌نویسی را به شما آموزش خواهد داد. پس از آن دانشجویان با پروژه OWASP، استانداردهای مرتبط با آن و لیست ۱۰ آسیب‌پذیری مهم تحت وب آشنا می‌شوند که دانشی مهم برای کارشناسان امنیت وب محسوب می‌شود. در نهایت دانشجویان با فراگیری کامل استاندارد PCI-DSS و الزامات آن، برای انجام تست نفوذ روی وب‌اپلیکیشن‌های دارای امکان پرداخت و قابلیت‌های مالی آماده می‌شوند. دوره جامع امنیت وب لیان تمام این مباحث را در کنار هم قرار داده و با بیش از ۲۰۰ ساعت آموزش، دانشجویان را برای شروع کار در حوزه تست نفوذ وب آماده می‌کند.

# تست‌نفوذ موبایل

بسیاری از سازمان‌ها برای بهبود خدمت‌رسانی و تجربه‌ی کاربری و هم‌چنین حفظ کاربران خود، بخشی از سرویس‌های خود را از طریق اپلیکیشن‌های موبایل ارائه می‌کنند. بسیاری از این اپلیکیشن‌ها با داده‌های حساس کاربران سر و کار دارند و در صورت وجود حفره‌های امنیتی در آن‌ها، این اطلاعات در معرض خطر جدی قرار می‌گیرند. در کنار داده‌های حساس، بخش اعظمی از اپلیکیشن‌های موبایل کارکردهای حساسی را نیز ارائه می‌کنند که در صورت سواستفاده‌ی مهاجمین، تبعات جدی برای کاربر به دنبال خواهند داشت که ممکن است مشکلات حقوقی جدی را متوجه سازمان کند. به همین دلیل است که یافتن آسیب‌پذیری‌های اپلیکیشن‌های موبایل برای سازمان‌ها اهمیت فراوانی پیدا کرده است. برای ورود به حوزه تست نفوذ موبایل، گام اول کسب دانش پایه و گذراندن دوره‌های پیش‌نیاز امنیت، و گام دوم یادگیری زبان‌های اصلی برنامه‌نویسی موبایل، یعنی جاوا و سوییفت است. پس از آن دانشجویان می‌توانند در دوره SEC۵۷۵ مهارت‌هایی مانند ارزیابی موثر امنیت دستگاه‌های موبایل، یافتن نقص‌های امنیتی در اپلیکیشن‌های موبایل و تست نفوذ دستگاه‌های موبایل را بیاموزند.



# MOBILE PENTEST

سرفصل‌های دوره جامع تست نفوذ موبایل آکادمی لیان علاوه بر زبان‌های برنامه‌نویسی موبایل، مباحث مطرح‌شده در دوره SEC575 را پوشش خواهد داد و دانشجویان را برای شروع کار به عنوان کارشناس تست نفوذ موبایل آماده می‌کند.

# پاسخ به حادثه، فارنزیک و تحلیل بدافزار

با وجود تمام تمهیدات امنیتی، رخدادن حوادث امنیتی کوچک و بزرگ در دارایی‌های دیجیتال ناگزیر است. هرچه سازمان بزرگ‌تر و زیرساخت دیجیتال آن گسترده‌تر باشد، تهدیدات و حوادث امنیتی نیز به تبع آن بیشتر خواهند شد. پس از رخدادن هر حادثه امنیتی، تیم پاسخ به حادثه یا Incident Response - که در بسیاری مواقع به اختصار به آن IR گفته می‌شود – وارد عمل می‌شود تا پس از ارزیابی اولیه از ماهیت و دامنه‌ی تاثیر حادثه، تا جای ممکن آن را محدود و عواقب آن را خنثی کرده و به طرف‌های ذی‌نفع اطلاع‌رسانی کند. عملیات فارنزیک نیز معمولا هم‌گام با فرایند پاسخ به حادثه آغاز می‌شود تا علاوه بر جمع‌آوری مدارک مورد نیاز جهت ارائه به مراجع قانونی، ریشه‌های حادثه شناسایی شده و در صورت امکان، گام‌های اولیه نیز در شناسایی مهاجمان احتمالی برداشته شوند. در فرایند تحلیل بدافزار که یکی از پیشرفته‌ترین حوزه‌های امنیت به شمار می‌رود، اکسپلویت‌ها و بدافزارهایی که در حملات سایبری علیه سازمان استفاده شده‌اند، مهندسی معکوس شده و نحوه‌ی کار آن‌ها مشخص می‌شود تا تیم امنیت بتواند خود را برای مقابله با آن‌ها در آینده آماده کند.

INCIDENT RESPONSE

حوزه پاسخ به حادثه، فارنزیک و تحلیل بدافزار، یکی از حوزه‌های پیشرفته و نسبتا پیچیده در امنیت سایبری محسوب می‌شود؛ افرادی که قصد ورود به این حوزه را دارند باید دانش و تجربه عملی قابل توجهی در زمینه شبکه‌ها و سیستم‌های کامپیوتری، سیستم‌عامل، مبانی سخت‌افزار و البته فناوری‌های امنیتی و هم‌چنین تست نفوذ داشته باشند. اولین دوره‌ای که برای ورود به این حوزه توصیه می‌شود، دوره SEC504 از موسسه SANS است که شما را با ابزارها و تکنیک‌های هکرها و اکسپلویت‌های مورد استفاده در حملات سایبری آشنا کرده و مبانی مدیریت حادثه را به شما می‌آموزد. در سرفصل‌های آموزشی این دوره، ابزارها و تکنیک‌های تهاجمی رایج ولی قدرتمندی پوشش داده خواهند شد که بیشترین کاربرد را در حملات سایبری دارند. پس از آن در دوره SEC503، یعنی دوره تشخیص نفوذ در عمق، دانش و دید عملی را برای دفاع از شبکه و یافتن نشانه‌های نفوذ با بررسی ترافیک شبکه به دست خواهید آورد. این دانش عملی، مباحثی مانند مدل TCP/IP و پروتکل‌های لایه اپلیکیشن مانند HTTP را شامل می‌شود که برای توانایی تحلیل ترافیک شبکه ضروری است.

# FORENSIC

دوره CHFI از موسسه EC-Council، یکی از مدارک محبوب و پرطرفدار فارنزیک است که تاییدیه موسسه استاندارد آمریکا (ANSI) را نیز دریافت کرده و جدیدترین و پیشرفته‌ترین ابزارها و تکنیک‌های فارنزیک را پوشش می‌دهد. این دوره‌ی جامع و آزمایشگاه‌محور، شما را برای انجام عملیات فارنزیک روی بازه‌ی گسترده‌ای از تجهیزات دیجیتال، فارغ از این که محصول کدام تولیدکننده باشند، آماده می‌کند. دوره‌های بعدی، دوره‌های تخصصی‌تر فارنزیک هستند که هر کدام روی حیطه‌ی خاصی متمرکز می‌شوند. دوره FOR500 به تحلیل فارنزیک ویندوز خواهد پرداخت و دانش جامع و عمیقی از جرم‌شناسی دیجیتال در این سیستم‌عامل به شما خواهد داد. در این دوره نحوه جمع‌آوری داده و دنبال‌کردن دقیق و جزئی فعالیت‌های کاربران را نیز می‌آموزید. دوره FOR508، دوره پیشرفته پاسخ به حادثه، شکار تهدید و فارنزیک دیجیتال است که تاکتیک‌ها و روندهایی را که در سال‌های اخیر در این حوزه توسعه داده شده‌اند پوشش می‌دهد.


MALWARE

در انواع حوادث سایبری، از نفوذ مهاجمان به دارایی‌ها و سرقت داده گرفته تا اقدامات خرابکارانه توسط کارکنان، شبکه دیدگاهی بی‌نظیر نسبت به حادثه به شما می‌دهد. دوره FOR572، یک دوره پیشرفته فارنزیک شبکه است که شما را برای شکار تهدیدات، تحلیل و پاسخ به حوادث آماده می‌کند. اطلاعات تهدید توان سازمان‌ها را در به‌روزرسانی و بهبود برنامه‌های تشخیص و پاسخ به حادثه چندین برابر کرده و آن‌ها را برای روبه‌رویی با حملات هدفمند آماده می‌کند؛ دوره FOR578 با این هدف طراحی شده که دانشجویان را برای استفاده از اطلاعات تهدید در پاسخ به حادثه آماده کند. دور FOR610 به طور تخصصی به مهندسی معکوس بدافزار، و ابزارها و تکنیک‌های تحلیل بدافزار می‌پردازد؛ کارشناسان امنیت با گذراندن این دوره، نحوه‌ی ارزیابی برنامه‌های مخربی را می‌آموزند که سیستم‌های ویندوزی را هدف قرار می‌دهند. از آن‌جایی که جمع‌آوری داده‌های فارنزیک از منابع ذخیره‌سازی مختلف مهارتی کلیدی در جرم‌شناسی دیجیتال به شمار می‌رود، دوره FOR498 به طور اختصاصی به استخراج و ذخیره داده از کامپیوترها، دستگاه‌های قابل حمل، شبکه‌ها و فضاهای ابری می‌پردازد.

# MALWARE ANALYSIS

در دوره FOR518 دانشجویان نحوه پاسخ به حادثه و تحلیل فارنزیک دستگاه‌های دارای سیستم‌عامل Mac و iOS را می‌آموزند که امروزه در سازمان‌های زیادی رواج دارند. در طول این دوره، دانشجویان بر استخراج داده‌ی خام، تحلیل جزئی و عمیق داده‌ها و کسب بیشترین اطلاعات ممکن از دستگاه‌های مجهز به این دو سیستم‌عامل تمرکز خواهند کرد. در نهایت دوره FOR585 به صورت اختصاصی به تحلیل فارنزیک عمیق تلفن‌های هوشمند می‌پردازد. این دوره به طور مرتب به‌روزرسانی می‌شود تا جدیدترین بدافزارها، سیستم‌عامل‌های تلفن همراه، اپلیکیشن‌های جانبی و تکنیک‌های استخراج و رمزگذاری داده را پوشش دهد. آکادمی لیان با بهره‌گیری از اساتید باسابقه در حوزه پاسخ به حادثه، فارنزیک و تحلیل بدافزار، آمادگی برگزاری تمامی دوره‌های ذکرشده و دیگر دوره‌های معتبر و شناخته‌شده‌ی این حوزه را دارد. علاوه بر این، آکادمی لیان برنامه‌های آموزشی ویژه‌ای برای کارشناسان امنیت در سازمان‌ها تدارک دیده است که به مجموعه‌های مختلف کمک می‌کند تیم پاسخ به حادثه و فارنزیک خود را با استفاده از منابع انسانی موجود تشکیل دهند.

# تیم آبی، قرمز و بنفش

در دنیای امنیت امروز، سازمان‌هایی که به بلوغ کافی در امنیت رسیده باشند، تیم‌هایی تخصصی برای پوشش حوزه‌های مختلف امنیت در نظر گرفته‌اند. سه مورد از مهم‌ترین و شناخته‌شده‌ترین این تیم‌ها، تیم آبی (Blue Team)، تیم قرمز (Red Team) و تیم بنفش (Purple Team) هستند. تیم آبی که در سمت دفاعی امنیت فعالیت می‌کند، وظیفه دارد با در نظر گرفتن طرز فکر و تاکتیک‌های هکرها و مهاجمان سایبری، امنیت شبکه را ارزیابی و بازبینی کرده و بهبود دهد، و به صلاحدید خود از راهکارها و معماری‌های امنیتی در مکان‌های مختلف زیرساخت استفاده کند. وجود چنین تیمی شانس و میزان موفقیت حملات سایبری را به شدت کاهش داده و تاثیری چشم‌گیر در بهبود وضعیت کلی امنیت سازمان (Security Posture) دارد. در طرف دیگر، تیم قرمز قرار دارد که وظیفه انجام مانوورهای تست نفوذ، و یافتن مداوم نقاط آسیب‌پذیر در زیرساخت را بر عهده دارد. این تیم از کارشناسان با تجربه تست نفوذ تشکیل شده که بازه‌ی وسیعی از عملیات‌های تست نفوذ را بر عهده دارند و باید مهارت‌هایی متناسب با دارایی‌های دیجیتال خاص سازمان داشته باشند.

از آن‌جایی که تیم قرمز عضوی از مجموعه است، اختیارات و محدوده عملیاتی بسیار گسترده‌تری از کارشناسان تست نفوذ خارج از سازمان دارد. این تیم با توجه به نیازهای سازمان ممکن است مانورهای بسیار متنوعی از مهندسی اجتماعی گرفته تا بررسی امنیت فیزیکی زیرساخت انجام دهد که معمولا حساس‌تر از آن هستند که به تیم‌هایی از خارج سازمان سپرده شوند. از آن‌جایی که این محدوده‌ی عملیاتی گسترده باعث تقابل این تیم با تیم آبی می‌شود، وجود تیم سومی لازم است که حوزه اختیارات دو گروه را مشخص کرده و از تداخل آن‌ها با یکدیگر جلوگیری کند؛ در این جاست که تیم بنفش وارد عمل می‌شود. این تیم متشکل از افرادی است که هم در زمینه‌ی امنیت دفاعی و هم امنیت تهاجمی تخصص دارند. وظیفه‌ی تیم بنفش ایجاد هماهنگی بین دو تیم آبی و قرمز، و شاید مهم‌تر از آن تصمیم‌گیری در مواردی است که عملیات‌های یکی از این دو تیم باعث اختلال در عملیات‌های تیم دیگر شده و بین آن‌ها اختلاف نظر به وجود می‌آید. آموزش تیم‌های آبی، قرمز و بنفش نیاز به دانش و دید بالایی در مشاوره و پیاده‌سازی ساختارهای امنیت سازمانی دارد و آکادمی لیان از سابقه‌ی خود در حوزه امنیت سازمانی برای تدوین برنامه‌های آموزشی ویژه سازمان‌ها استفاده کرده است.



RED TEAM

PUR TEA

# دپارتمان امنیت لیان

در دنیای دیجیتال امروزی، داده‌ها ارزشمندترین دارایی‌های هر سازمان هستند، و به همین خاطر در حوزه ارتباطات و فناوری اطلاعات، امنیت سایبری به اولین اولویت تبدیل شده است. شرکت لیان با نظر به همین مساله و با ارائه و پیاده‌سازی به‌روزترین، قدرتمندترین و مورد اعتمادترین فناوری‌های امنیت سایبری در قالب محصولات و خدمات، به سازمان‌ها کمک میکند هرچه بیشتر و بهتر از این دارایی ارزشمند خود مراقبت کنند. سازمان‌ها فارغ از کوچک یا بزرگ بودن مقیاس آن‌ها، بدون شک دارای بسترهای مختلف اطلاعاتی نظیر زیرساخت شبکه، اینترنت، اپلیکیشن‌های تحت وب، بسترهای رصد نظیر SOC یا NOC و... هستند و شرکت امنیتی لیان آمادگی دارد در زمینه تهیه این تجهیزات و هم‌چنین پیاده‌سازی و نگهداری از آن‌ها، با بهره‌گیری از دانش و تخصص کارشناسان باسابقه و ظرفیت عملیاتی خود شما را یاری دهد.

اما هرکدام از بسترهای حوزه امنیت، برای پیاده‌سازی و اجرا نیازمند تجهیزات فیزیکی یا نرم‌افزاری هستند. این تجهیزات نیز حتماً باید با مشاوره از متخصصان این حوزه و همچنین توسط شرکت‌های معتبر خریداری و پیاده‌سازی شوند. تجهیزاتی که ممکن است قیمت بسیار بالایی داشته باشند و حتما نیازمند تهیه لایسنس‌های معتبر بین‌المللی هستند، باید ازطریق مسیرهای مطمئن و قابل اعتماد خریداری شوند. گروه امنیتی لیان این بستر را برای تمامی سازمان‌ها فراهم کرده تا تجهیزات معتبر در سراسر دنیا را با لایسنس‌های معتبر خریداری کرده و به نحو احسن بر زیرساخت‌های اطلاعاتی خود پیاده‌سازی کنند.

تجهیزاتی سخت‌افزاری یا نرم‌افزاری به‌دلیل پیچیدگی‌ها و تنظیمات خاص، همیشه نیازمند متخصصانی هستند که کار پیاده‌سازی، پیکربندی، تعمیر و نگهداری از آن‌ها را برعهده داشته باشند. پس خدمات حوزه امنیت، که توسط متخصصان این حوزه ارائه می‌شود، یکی از ضروری‌ترین نیازهای هر سازمان خواهد بود. خدماتی نظیر «مشاوره»، «تست نفوذ»، «ISMS»، «NOC»، «SOC»، «جرم‌شناسی» و... گروه امنیتی لیان با تکیه‌بر دانش متخصصان خود و همچنین سابقه همکاری با شرکت‌های معتبر خصوصی و دولتی، خدمات حوزه امنیت را نیز به تمام سازمان‌های موجود ارائه می‌کند.

# دپارتمان توسعه لیان

بسیاری از کسب‌وکارها و سازمان‌های امروزی، بخش قابل توجهی از خدمات خود را از طریق ابزارها و بسترهای دیجیتال در اختیار کاربران قرار می‌دهند. شرکت لیان با بهره‌گیری از تیم توسعه و برنامه‌نویسی متخصص و باتجربه خود، امکان تولید اپلیکیشن‌های تحت وب با سطح امنیت بسیار بالا و دارای استانداردها و گواهینامه‌های امنیتی معتبر را برای مجموعه‌های مختلف ایجاد کرده است. هم‌چنین واحد استارتاپ شرکت لیان، ظرفیت ایجاد و رشد استارتاپ‌های مختلف در زمینه شبکه، وب، امنیت و... را به وجود آورده و آماده‌ی خدمت‌رسانی به کارآفرینان و سازمان‌هایی است که قصد توسعه‌ی حوزه‌ی کاری خود را دارند. ما معتقدیم رشد شرکت لیان هم‌گام با رشد سازمان‌هایی است که در راه توسعه خود با مجموعه لیان همراه بوده‌اند. از همین رو مجموعه لیان تمامی امکانات و توان‌مندی خود را برای کمک به توسعه و رشد مشتریان و همکاران خود به‌کار بسته است.


TRAINING

02191004151
02191004151(5)
academy@liangroup.net
academy_lian
U.2, NO.42, ETEMADIYAN ST, FOROUTAN ST, AYATOLLAH KASHANI ST
2ND SADEGHIYEH SQUARE, TEHRAN, IRAN