
LianGroup


DATA PROTECTION

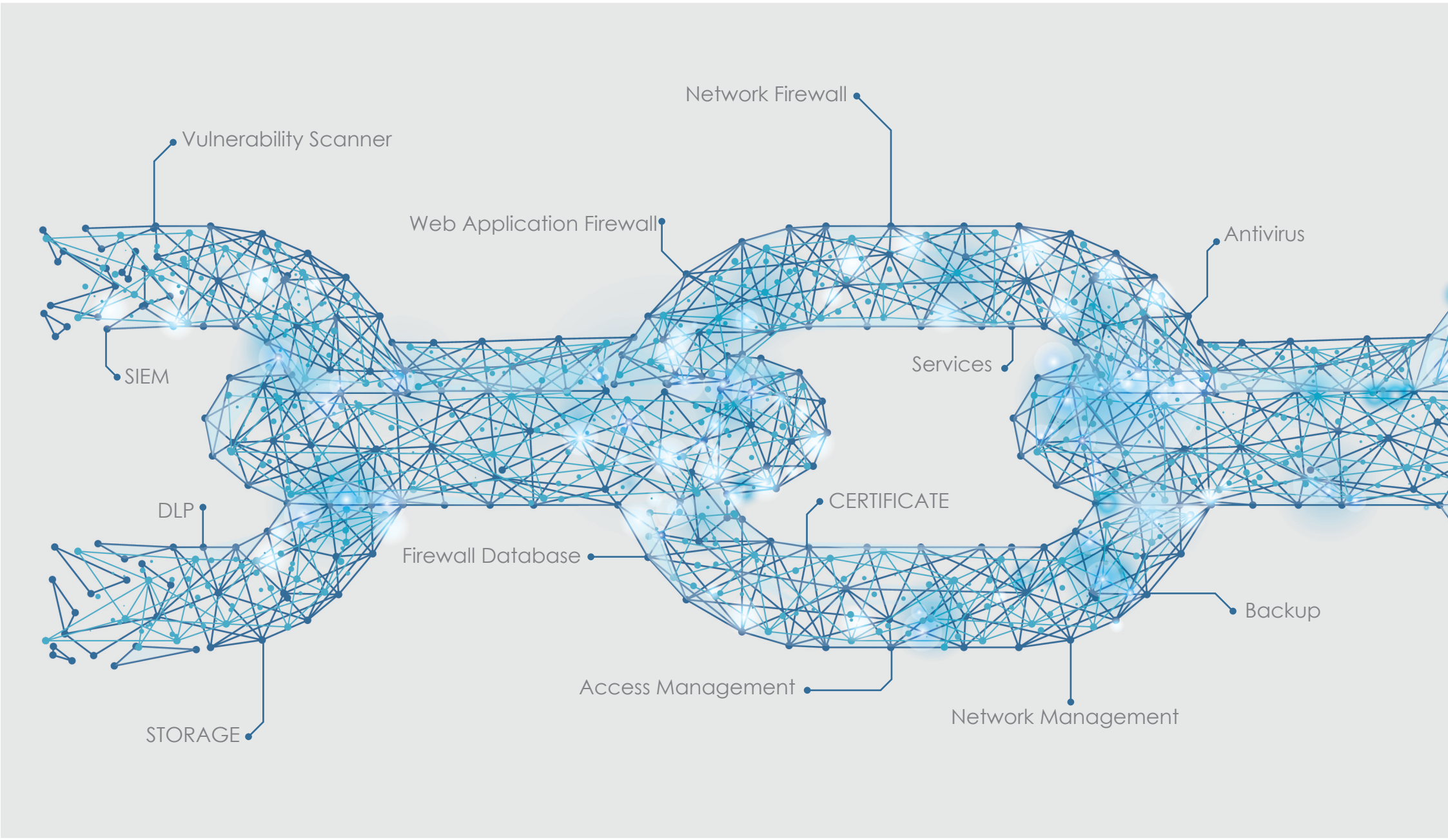
شرکت مهرنا رایانه لیان در سال ۱۳۹۲ تاسیس و فعالیت خود را در زمینه ارائه خدمات موردنیاز مشتریان در بخش انفورماتیک شاخه امنیت سایبری و زیرمجموعه های مرتبط آغاز کرد. با رشد روزافزون وابستگی ما به تجهیزات رایانه‌ای و ارتباطات اینترنتی، نیاز به ایمن‌سازی دربرابر حملات سایبری و مقابله با هرگونه رخدادهایی که امنیت شبکه‌های رایانه‌ای و داده‌های سازمان را به خطر می‌اندازد بیش‌ازپیش خودنمایی می‌کند.

این شرکت با تکیه بر توانمندی کارشناسان با تجربه خود و همچنین با استفاده از منابع و شرکت‌های همکار، چه درداخل و چه در خارج از کشور، سعی کرده است نیازمندی مشتریان را هم در زمینه تامین تجهیزات امنیت سایبری و هم در زمینه ارائه خدمات آموزشی به کارکنان و مدیران رده‌های مختلف سازمانی تامین و ساختار امنیتی‌شان را مستحکم‌تر و غیرقابل نفوذتر کند.

خدمات، محصولات و راهکارهای ارائه شده در این شرکت بطور کامل لایه‌های مختلف شبکه سازمانی، چه در بخش وب اپلیکیشن و چه در بخش شبکه را پوشش داده و با ارائه دوره‌های آموزشی به کاربران این واحدها، زنجیره دفاعی مناسبی در برابر انواع حملات و آسیب‌پذیری‌ها ایجاد می‌کند.

# SECURITY

**خدمات امنیت:** در بحث ایجاد تبادل در فضای سایبری، امنیت اطلاعات حرف اول را می‌زند. زیرا در دنیای دیجیتال امروزی، داده‌ها با ارزش‌ترین دارایی‌های هر سازمان هستند. شرکت لیان سعی بر آن دارد با ارائه برترین فن‌آوری‌های امنیت سایبری چه به‌صورت نرم‌افزاری و چه سخت‌افزاری به سازمان‌ها کمک کند هرچه بیشتر و بهتر از این دارایی‌های ارزشمند خود مراقبت کنند. تجهیزات، محصولات و خدماتی که توسط شرکت لیان با استانداردهای جهانی در اختیار سازمان‌ها قرار می‌گیرد مانند آنتی‌ویروس‌ها، فایروال‌ها و ذخیره‌سازهای اطلاعات، ازجمله تجهیزاتی هستند که باید در بسترشبکه هر سازمانی نصب و راه‌اندازی شوند تا ایمن‌سازی در تمام لایه‌های شبکه تامین گردد. همچنین با رشد و توسعه هرسازمان، نرم‌افزارهایی در قالب مدیریت‌دسترسی اطلاعات، مانیتورینگ شبکه، تست‌نفوذ شبکه، بکاپ‌گیری از اطلاعات و خدمات مربوط به گواهینامه‌های تاییدیه امنیتی و... به سازمان‌ها ارائه خواهند شد.


Network Firewall
Vulnerability Scanner
Web Application Firewall
Antivirus
SIEM
Services
DLP
CERTIFICATE
Firewall Database
Backup
Access Management
Network Management
STORAGE

# Antivirus

فایل‌هایی وارد سیستم شما شده‌اند که نام‌های عجیبی دارند. سرعت کامپیوترهای شخصی یا سیستم‌های شبکه به شدت کاهش یافته است. کارکردن با چنین سیستم‌هایی به‌شدت برای‌تان سخت شده، پس می‌توان گفت که قطعاً سیستم شما آلوده به بدافزار شده است. هرسیستمی که به اینترنت متصل می‌شود، درگاه خروجی و ورودی داشته و یا به‌طور کلی با دستگاه‌های دیگر تبادل اطلاعات دارد، حتماً درخطر آلوده شدن به بدافزار قرار خواهد گرفت. پس آنتی‌ویروس‌ها عضو مهم و جدانشدنی سیستم‌های کامپیوتری هستند. حال اگر بر روی سیستم‌های شبکه یک سازمان آنتی‌ویروسی وجود نداشته باشد، در حقیقت اولین لایه دفاعی که وظیفه محافظت در برابر انواع بدافزارها را دارد، بر روی سیستم‌ها فعال نیست.

ESET، Kaspersky، F-Secure، Carbon Black و Symantec از جمله آنتی‌ویروس‌های قدرتمند موجود، برای مبارزه با ویروس‌های قوی هستند. برای انتخاب هرکدام از آن‌ها، نقاط قوت و نقاط ضعف‌شان را بشناسید تا انتخاب دقیق‌تری داشته باشید.

Carbon Black. KASPERSKY lab ESET F-Secure Symantec

# Network Firewall

تمامی سازمان‌ها بر بستر شبکه فعالیت می‌کنند و تمامی شبکه‌ها، دارای کاربران متعدد و دسترسی‌های مختلفی هستند. اگر بستر شبکه یک سازمان ایمن‌سازی نشده باشد، هرکسی می‌تواند از خارج یا داخل سازمان، به سیستم‌های موجود در آن‌جا دسترسی داشته باشد. ازآنجا که اطلاعات محرمانه یک سازمان بر روی بستر شبکه موجود هستند، پس دسترسی‌های غیرمجاز می‌تواند هزینه‌های جبران‌ناپذیری برای سازمان به‌همراه داشته باشد. فایروال‌های تحت شبکه، ما بین اطلاعات موجود در شبکه و افرادی که تقاضای دسترسی به آن‌ها را دارند قرار می‌گیرند. این فایروال‌ها هستند که تمام ترافیک رفت و برگشتی را کنترل کرده و از دسترسی‌های غیرمجاز جلوگیری می‌کنند. پس وجود یک فایروال شبکه (سخت‌افزار و نرم‌افزار) برای هر سازمانی به شدت ضروری‌ست.

ازجمله فایروال‌های تحت شبکه قوی می‌توان به Fortinet , PaloAlto , Juniper , Kerio Cisco Firepower , Sophos اشاره کرد. تمامی این فایروال‌ها ازسوی سازمان‌های بزرگ تایید شده‌اند و دارای ویژگی‌های مختلفی هستند که می‌تواند شما را در ایمن‌سازی شبکه سازمان موردنظرتان کمک کند.

cisco paloalto NETWORKS KerioControl JUNIPER NETWORKS FORTINET SOPHOS

# Web Application Firewall

فعالیت‌های مخرب تنها مخصوص شبکه‌ها نیستند بلکه یکی از اصلی‌ترین اهدافشان، وب‌سایت‌ها است. سالانه درصد زیادی از وب‌سایت‌های بزرگ و کوچک مورد حمله هکرها قرار می‌گیرند که بسیاری از آن‌ها به‌دلیل نداشتن دانش کافی و ابزارهای مناسب برای مقابله با این هکرها، مغلوب می‌شوند. WAF یا همان Web Application Firewall، وظیفه محافظت از وب‌سایت‌ها را به‌عهده دارد. این فایروال بدین‌صورت عمل می‌کند که ترافیک وارده به سمت وب‌سایت‌ها را مانیتور کرده و بخشی که مخرب است را فیلتر و مسدود می‌کند. درحقیقت اصل کار WAF بدین‌گونه است که کاربر درخواست خود را ارسال می‌کند (مثلاً جست‌وجوی نام یک سایت)، وب سرور درخواست کاربر را شناخته و محتوا را به کاربر ارسال می‌کند، سپس WAF در این بین به میان آمده و ترافیک مخرب را شناسایی و مسدود می‌کند. پس استفاده از نرم‌افزارهای WAF باعث جلوگیری از رسیدن ترافیک مخرب به وب‌سایت می‌شود. ازجمله فایروال‌های تحت وب قدرتمند می‌توان به Imperva, Barracuda, Sucuri, F5 , Fortiweb اشاره کرد.

imperva FORTINET f5 SUCURI Real People. Real Security. Barracuda

# Database Firewall

از آنجا که پایگاه‌های اطلاعاتی، محل نگهداری بیشتر اطلاعات سازمان‌ها هستند، بنابراین تامین امنیت این پایگاه‌ها نیز از اهمیت بالایی برخوردار است. اطلاعاتی که در دیتابیس‌های یک سازمان ذخیره می‌شوند، شامل اسناد و مدارکی هستند که با ازبین رفتن آن‌ها، سازمان متحمل هزینه‌ی زیادی خواهد شد. برای ایجاد امنیت چنین مراکز مهمی، استفاده از فایروال‌هایی که وظیفه تامین امنیت را برعهده می‌گیرند، بسیار اهمیت دارد. فایروال‌های سخت‌افزاری و نرم‌افزاری، با قرار گرفتن میان کاربران و محتوای ذخیره‌شده در دیتابیس، از دسترسی‌های غیرمجاز و نفوذ افراد غیرمجاز به دیتابیس جلوگیری می‌کنند. ازجمله محصولاتی که در زمینه فایروال‌های دیتابیس بسیار قدرتمند عمل کرده‌اند و سازمان‌های بسیاری را مشتری خود کرده‌اند می‌توان به McAfee و IBM Security Guardium اشاره کرد.

IBM

McAfee

# Network Management

هرشبکه‌ای که راه‌اندازی می‌شود، نیازمند یک مدیراجرایی یا همان Admin است. ادمین شبکه نیز برای حفظ و بهبود وضعیت شبکه، از ابزارهای QoS استفاده می‌کند. هدف از «مدیریت شبکه» دستیابی به شبکه بدون خطاست. امروزه در محیط‌های شبکه، ابزارهای مدیریت شبکه به‌گونه‌ای به‌کار گرفته می‌شوند تا از بروز هرگونه خطا در این محیط، جلوگیری شود. و یا این خطاها به‌سرعت از بستر شبکه حذف شوند. اما به‌طورکلی نرم‌افزارهای مدیریت شبکه به چهاردسته‌ی شناسایی خطا، مدیریت اجرایی، ارائه شبکه، حفظ QoS تقسیم می‌شوند.

با استفاده از چهاردسته نرم‌افزارهای اصلی مدیریت شبکه، اهداف زیر حاصل خواهند شد:

- شناسایی خطاها پیش از این‌که به کاربران شبکه آسیبی برسد
- بازگرداندن شبکه به وضعیت اصلی و بهبودیافته با استفاده از مدیریت اجرایی
- محاسبه تقاضای آینده براساس روند فعلی شبکه
- حفظ کیفیت خدمات موجود در شبکه (QoS) با گذشت زمان

ازجمله محصولات مدیریت شبکه می‌توان به ، SolarWinds ، ManageEngine PRTG و GFI اشاره کرد.

PRTG NETWORK MONITOR

GFI®

solarwinds

ManageEngine

# Access Management

فرض کنید در یک سازمان بزرگ، سیستم‌های تمام کاربران به‌صورت شبکه به‌هم متصل‌اند. چه‌کسی می‌تواند کنترل تمام این سیستم‌ها را به‌دست بگیرد؟ هرکسی می‌تواند تا چه حد به فایل‌ها و اسناد موجود در شبکه دسترسی داشته باشد؟ و به‌طور کلی دسترسی‌های موجود بین کاربران و فایل‌های اشتراکی، تا چه حد عمومی است؟
تمام این سوالات می‌تواند به دست یک نفر که با نام ادمین (Admin) شناخته می‌شود، پاسخ داده شوند. ادمین یک شبکه می‌تواند با استفاده از نرم‌افزارهای مدیریتی موجود، برای هر کاربر به‌صورت مشخص، دسترسی خاصی ایجاد کند. نرم‌افزارهایی مانند Cyberark, Ping Identity, Okta, FortiAuthenticator, Arcon که در دسته نرم‌افزارهای Access Management قرار می‌گیرند، می‌توانند به ادمین شبکه در زمینه ایجاد دسترسی‌های خاص، بسیار کمک کنند.

okta FORTINET Ping Identity Arcon CYBERARK

# Vulnerability Scanner

متخصصان IT یا افراد عادی که از سیستم‌های کامپیوتری استفاده می‌کنند، حتماً می‌دانند که سیستم‌عامل‌ها و نرم‌افزارها دارای آسیب‌پذیری‌های امنیتی هستند. گاهی این آسیب‌پذیری‌ها را می‌شناسیم و از پیش برای برطرف کردن آن‌ها اقدام می‌کنیم. گاهی نیز اصلاً از وجود آن‌ها بی‌خبر بوده و یا قادر به پیدا کردن‌شان نیستیم. دقیقاً همین نقطه است که نرم‌افزارهایی باعنوان Vulnerability Scanner به میان خواهند آمد. تست نفوذ یا همان Penetration Test از جمله لزومات هر شبکه، وب‌سایت و اپلیکیشن‌های موبایلی است که با بستر اینترنت تبادل اطلاعات دارند. پس برای ایجاد امنیت چنین بسترهایی، نیازمند نرم‌افزارهایی هستیم تا پیش از آن‌که ازطریق آسیب‌پذیری‌های موجود، ازسوی هکرها مورد حمله قرار بگیریم، آن آسیب‌پذیری را برطرف کنیم. اسکنرهایی مانند Netsparker ، Nessus ، Burp Suite ، Acunetix و Metasploit Pro می‌توانند آسیب‌پذیری‌های موجود بر روی شبکه و وب را با عملکرد بسیار قوی، شناسایی کنند.

گروه لیان با همکاری شرکت Appknox پلتفرمی به منظور اسکن آسیب پذیری های نرم افزارهای موبایلی اعم از Android و iOS به مشتریان خود ارائه می دهد.

netsparker RAPID7 METAPRO acunetix BURPSUITE appknox Nessus

# DLP

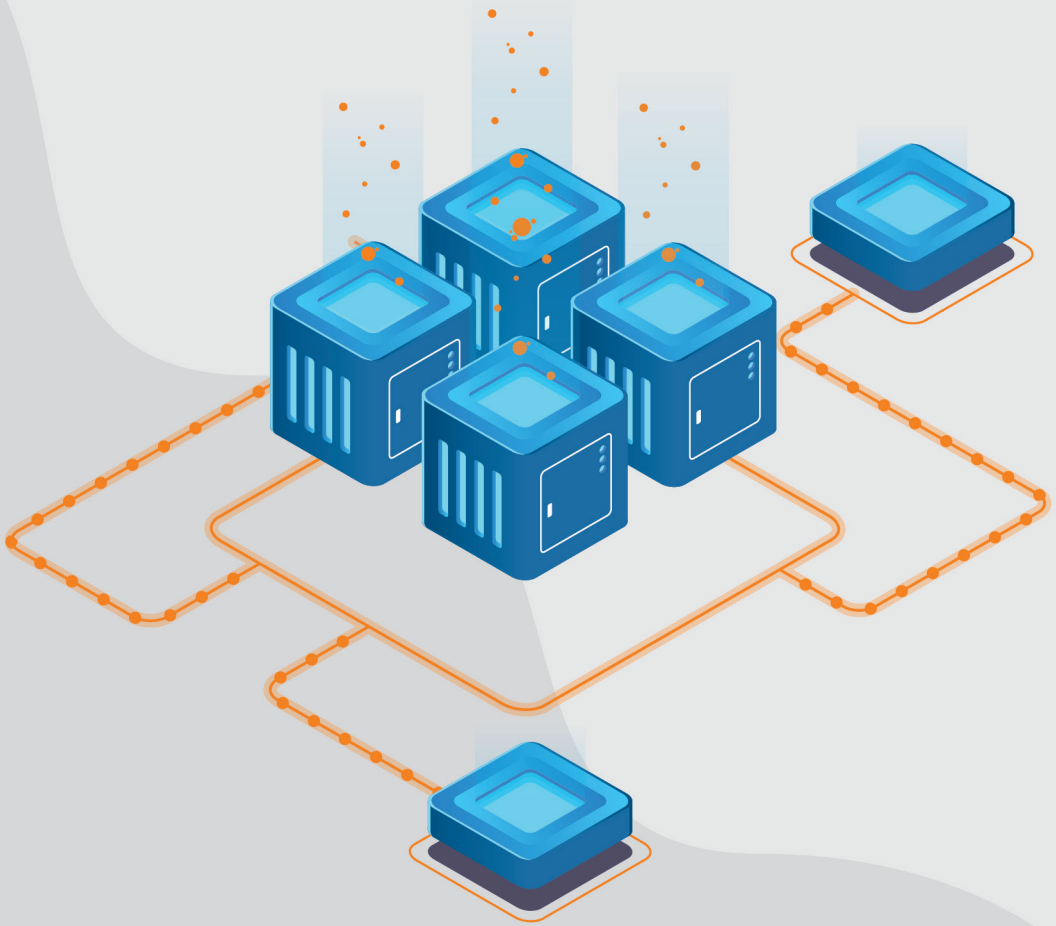
بسیاری از افراد به‌طور ناخواسته، اطلاعاتی از سیستم خود را به دست افراد سودجو می‌سپارند. گاهی با یک کلیک ساده بر روی یک لینک، اطلاعات حساسی از سیستم‌ها به بیرون نشت پیدا خواهند کرد که می‌توانند خطرهای بسیاری را برای صاحبان آن به‌وجود آورند. این نشت اطلاعات را Data Leak می‌نامند.

استراتژی‌ای که برای جلوگیری از نشت اطلاعات حساس و بحرانی به بیرون از سیستم یا شبکه درنظر گرفته می‌شود، DLP یا همان Data Leak Prevention نامیده می‌شود. نرم‌افزارهای قدرتمندی در راستای به‌کارگیری این استراتژی ایجاد شده است که می‌توان با استفاده از آن‌ها، تمام دسترسی‌ها و ارسال اطلاعات به خارج از شبکه را کنترل کرد. این استراتژی برای سازمان‌هایی که دارای چندین سیستم و کاربر در بستر یک شبکه هستند، بسیار مهم و ضروری خواهد بود. چراکه هرکدام از این کاربران می‌توانند با یک اشتباه ساده، تمامی اطلاعات موجود بر روی شبکه را در اختیار هکرها قرار دهند.

ازجمله نرم‌افزارهای DLP موجود می‌توان به Endpoint Protector ، Symantec Forcepoint وSecure Tower اشاره کرد. شما می‌توانید با مطالعه نقاط قوت و ضعف هرکدام از آن‌ها، نرم‌افزار مناسب شبکه خود را انتخاب کنید.

SecureTower™ Symantec ENDPOINT PROTECTOR FORCEPOINT

# SIEM



اگر با سیستم‌هایی که به‌صورت شبکه درآمده‌اند و بر روی سرور مرکزی فعال شده‌اند کار کرده باشید، حتماً می‌دانید که تمام فعالیت‌های کاربران موجود در آن شبکه، درجایی ثبت می‌شوند. تمامی اتصال‌ها، دسترسی‌ها، اسناد و مدارک بازبینی شده و... . این ثبت فعالیت‌ها در قالب یک سری فایل با نام Log، بر روی سرور اصلی ذخیره خواهند شد. بسته به تعداد کاربران و میزان فعالیت‌های آن‌ها، گاهی این Logها آن‌قدر زیاد هستند که نمی‌توان تک‌تک آن‌ها را به‌صورت جداگانه بررسی نمود. اما می‌دانیم که بررسی این لاگ‌ها به‌منظور شناسایی نقاط ضعف شبکه، بسیار مهم خواهند بود. دراینجا پای نرم‌افزارهای SIEM به‌میان می‌آید.

Security Information and Event Management شاخه‌ای از نرم‌افزارهای مدیریتی است که به مدیران شبکه، برای بررسی لاگ‌های موجود کمک می‌کند. نرم‌افزارهایی نظیر IBM QRadar، Splunk و ArcSight تمام Logهای موجود را بررسی کرده و مشکلات موجود، اتفاقات مخرب، دسترسی‌های غیرمجاز و... را به ادمین شبکه اطلاع می‌دهند. اگر نیازمند یک شبکه ایمن هستید، استفاده از نرم‌افزارهای SIEM می‌تواند به شما در این زمینه بسیار کمک کند.

FORTINET splunk> RAPID7 INSIGHTIDR IBM QRadar ArcSight

# STORAGE

در گذشته سازمان‌ها دارای اسناد و مدارک بسیاری بودند که در بخش‌های بزرگ و زیرزمینی به نام بایگانی، از آن‌ها نگهداری می‌شد. بایگانی‌هایی که گاهاً سال‌ها از اسناد کاغذی نگهداری می‌کردند. گم‌شدن اطلاعات، ازبین رفتن آن‌ها، دسته‌بندی‌های اشتباه و... ازجمله اتفاقات بسیار رایج در سازمان‌های بزرگ و بایگانی‌های آن‌ها بود.

اما به‌مرور به‌جای چنین بایگانی‌هایی، شبکه‌ها به‌وجود آمدند. شبکه‌هایی که تبادل اطلاعات را بسیار آسان‌تر و ذخیره‌سازی آن‌ها را مرتب‌تر از همیشه کرده‌اند. اما برای این‌که اطلاعات بسیار زیادی که در بستر شبکه تبادل می‌شوند و بسیاری اطلاعات دیگر که نیازمند بایگانی شدن دارند را نگهداری کنیم، به چه فضایی احتیاج داریم؟ اینجاست که نیاز به Storageها بیش‌ازپیش احساس می‌شود.

Storage سخت‌افزاری قدرتمند است که فضای کاملاً مناسب و ایمنی را برای ذخیره‌سازی اطلاعات ایجاد می‌کند. از جمله Storageهای معروف می‌توان به ، Quantum، EMC Thecus و Qnap اشاره کرد که هرکدام نقاط قوت و ضعف خودشان را دارند.

QNAP EMC² Thecus® Quantum

# Backup

بایگانی‌ها مکانی هستند که اسناد و مدارک یک سازمان در آن نگهداری می‌شود. پیش‌ازاین بایگانی‌ها در معرض خطراتی مثل آتش‌سوزی، پوسیدگی اسناد و... بودند. اما امروزه با ذخیره‌سازی اطلاعات، اسناد، مدارک و... در فضاهای ذخیره‌ساز (Storage) خطرات دیگری سیستم‌های یک سازمان را تهدید می‌کند. خطراتی از قبیل حملات سایبری، پاک‌شدن اطلاعات (سهوی یا عمدی)، دسترسی‌های غیرمجاز و...

هرسازمانی که سیستم‌های شبکه و فضای ذخیره‌ساز دارد، حتماً در معرض چنین خطراتی قرار می‌گیرد. اما راه‌حل آن چیست؟ پیشگیرانه‌ترین راه‌حل برای سازمان‌های بزرگ و کوچک، استفاده از تهیه نسخه پشتیبان است. نرم‌افزارهای Backup می‌توانند از تمامی اطلاعات شما نسخه پشتیبانی را تهیه کنند تا در آینده، پس از به‌وجود آمدن هریک از خطرات بالا، بتوانید همه‌ی آن اطلاعات را بازگردانی (Recovery) کنید.

بهترین‌های موجود در زمینه Backupگیری، نرم‌افزارهای Microsoft Backup، Acronis، Veritas و Veeam هستند. قدرت بسیار بالای این دو نرم‌افزار در زمینه بکآپ‌گیری و بازگردانی اطلاعات، می‌تواند حتی به سازمان‌های بزرگ با فضای ذخیره اطلاعات وسیع نیز کمک کند.

Acronis VEEAM Microsoft VERITAS

SIEM

# سامانه مدیریت رخداد بومی

اطمینان از ایمن‌بودن سرمایه‌های اطلاعاتی و تجهیزات زیرساختی کشور گذشته از ابعاد گسترده امنیت‌ملی، کلیدی برای فرصت‌های بی‌شمار تجاری و غیرتجاری جدید اینترنتی است. آنچه مسلم است، چالش امنیتی کشور عدم دسترسی به فناوری و یا عدم وجود محصولات امنیتی نیست. بلکه سیاست‌گذاری، فرهنگ‌سازی، استفاده مناسب از منابع موجود و نیز انطباق آن‌ها با نیازهای منحصربه‌فرد شبکه و فضای دیجیتالی کشور است.

مرکز عملیات امنیتی (SOC) یک ساختارعملکرد امنیت سایبری متمرکز در سازمان است که از افراد، فرآیندها و فناوری برای پویش و شناسایی مداوم وضعیت امنیتی سازمان استفاده می‌کند. و این‌کار با کشف، تجزیه و تحلیل و پاسخ به حوادث امنیت سایبری انجام می‌شود.

سیستم SIEM لیان، برای مدیریت عملیات مراکز SOC و به جهت تجزیه و تحلیل بلادرنگ داده‌های امنیتی برای مقابله با تهدیدهای داخلی و خارجی تولیدشده است. همچنین وظیفه این سیستم جمع‌آوری، ذخیره‌سازی، تحلیل و گزارش روی داده‌های ابزارها، نرم‌افزارها و برنامه‌های کاربردی سازمان‌ها است که با هدف پاسخ به حوادث، پیگیری قانونی و تنظیم مجدد قوانین تطبیقی انجام می‌شود.

این سیستم، با ایجاد یک چتر امنیتی روی کلیه تجهیزات و نرم‌افزارهای سازمان، تمامی رخدادها را دریافت کرده و به‌صورت بلادرنگ آن‌ها را نرمال‌سازی می‌کند. جهت تشخیص رخدادهای به‌هم پیوسته‌ی غیرمعمول، آن‌ها را به موتور تحلیل‌گر ارسال می‌کند. موتور تحلیل‌گر لیان با کمک پایگاه دانش قوی، به‌صورت بلادرنگ فعالیت‌های مشکوک را تشخیص داده و پس از اولویت‌بندی و تشخیص میزان ریسک، بلافاصله آن‌ها را گزارش می‌کند. از ویژگی‌های سیستم SIEM لیان، ارتباط بی‌واسطه با سیستم Service Desk لیان می‌باشد که حوادث را ریشه‌یابی کرده و اقدامات موقت ضروری و در ادامه، حل دائمی مشکل را انجام می‌دهد.

# Services

«خدمات» امروزه یکی از اصول موفقیت هر کسب‌وکاری به‌شمار می‌رود. در زمینه سیستم‌های شبکه و امنیت آن نیز خدماتی وجود دارد که باید از متخصصان آن درخواست کرد. اگر به شبکه شما نفوذ شده باشد، اطلاعاتی از آن به بیرون نشت پیدا کرده باشد، دسترسی‌های غیرمجاز رخ‌داده باشد و...، حتماً باید از متخصصان آن درخواست کنید تا چگونگی انجام این اتفاقات و راه‌حل‌های موجود برای جلوگیری از آن‌ها را به شما ارائه کنند. کلیه‌ی خدمات تست نفوذ، خدمات فارنزیک، خدمات مشاوره امنیت، خدمات NOC، خدمات SOC و خدمات ISMS می‌توانند امنیت لازم برای سیستم‌های شما را فراهم کنند. امنیتی که باعث می‌شود سیستم‌های شما ایمن‌سازی شده و در اختیار کارکنان‌تان قرار گیرند.

FORENSICS | PENTEST | CONSULTANT | ISMS | SOC / NOC

# TRAINING

**آموزش:** طبق تحقیقات انجام شده توسط کارشناسان حوزه امنیت سایبری، بیشترین آسیب‌های ایجاده شده در سازمان‌ها، به‌دلیل فقدان دانش کافی در زمینه تهدیدات موجود در فضای سایبری و ناتوانی در مدیریت بحران‌های پیش‌رو می‌باشد. نتایج این تحقیقات نشان می‌دهد که ضعیف‌ترین زنجیره‌ی دفاعی یک سازمان، می‌تواند کارکنان ناآگاه آن باشد که علی‌رغم استفاده سازمان از بهترین فن‌آوری‌های امنیت سایبری همچنان آسیب‌های خطرناکی متوجه سازمان می‌شود.

یکی دیگر از اهداف اصلی شرکت لیان، افزایش آگاهی و دانش کارکنان سازمان (مدیریت ارشد مدیریت میانی و کارکنان عادی) نسبت به خطرات موجود در زمینه فضای سایبری است. سازمان‌ها و کسب و کارها علاوه‌بر نیاز به مدیرشبکه و مدیرامنیت‌شبکه به کارکنانی نیاز دارند که مفاهیم اصلی امنیت سایبری و اقدامات ضروری در مقابل حملات و آسیب‌پذیری‌های سایبری را آموزش دیده و بطور روزمره در تمامی تعاملات خود بکار بندند. این آموزش‌ها در سه بخش شبکه، امنیت و برنامه‌نویسی از پایه تا پیشرفته متناسب با نیاز هر سازمان قابل ارائه و سفارشی‌سازی می‌باشد.

برای بهینه‌سازی و استفاده تجهیزاتی که در سازمان بکارگرفته می‌شوند، آموزش مداوم کاربران این تجهیزات ضروری است. همچنین با رشد بی‌حد و مرز تهدیدات سایبری و سوءاستفاده‌کنندگان از فضای سایبری، ضرورت به‌روزرسانی اطلاعات و دانش کاربران در این زمینه برای تمامی سطوح سازمان بیش‌از پیش احساس می‌شود. برای حصول این مهم، شرکت لیان با ارائه دوره‌ها و کارگاه‌های آموزشی، کارکنان سازمان را از تهدیدات موجود آگاه کرده و با انتقال دانش وتجربه متخصصان خود به کارکنان سازمان‌ها، محیطی ایمن را فراهم می‌سازد. دوره‌های قابل برگزاری در شرکت لیان به‌صورت کارگاه‌های ترکیبی عملی و تئوری و همچنین دوره‌های سازمانی، ارائه و مدارک مربوطه صادر می‌گردد.

شرکت لیان با تکیه‌بر دانش کارشناسان و اساتید خود، دوره‌های آموزشی خود را در قالب سه بخش، دراختیار دانش‌پذیران خود قرار داده است. دوره‌های «شبکه»، «امنیت شبکه» و «برنامه‌نویسی» سه شاخه‌ای هستند که گذراندن دوره‌های زیرمجموعه‌ی آن‌ها برای فعالان فضای سایبری نیاز است.

تمرکز دوره‌های شرکت لیان بر روی «امنیت شبکه» است اما به‌دلیل آن‌که بعضاً دوره‌های شبکه و برنامه‌نویسی نیز به‌عنوان پیش‌نیاز دوره‌های امنیت شبکه قرار می‌گیرند، برگزاری آن‌ها نیز در دستورکار شرکت لیان قرار گرفته است.

اساتید این دوره‌ها ازسوی سازمان‌های معتبر همانند «افتا» تایید شده‌اند و سطح علمی آن‌ها نیز ازسوی شرکت لیان تایید شده است. سرفصل تمامی دوره‌ها نیز از موسسات معتبری همچون EC Council و SANS گرفته شده و تمامی مباحث به‌طور کامل تدریس می‌شوند.

سازمان‌هایی که دارای تیم‌های IT قدرتمند هستند، حتماً بر تکمیل دانش کارکنان خود (از کارکنان مبتدی تا کارشناسان IT) تاکید زیادی داشته و به‌دنبال دوره‌های مفید در این زمینه خواهند بود.

به‌طور کلی سازمان‌ها باید در ساختار فنی IT خود، دو تیم قرمز و آبی داشته باشند. تیم آبی وظیفه دفاع از شبکه و سیستم‌های سازمان دربرابر تهدیدات خارجی را برعهده دارد. تیم قرمز نیز وظیفه تست شبکه و آسیب‌پذیری‌های آن (ازطریق حملات داخلی و کنترل‌شده در سازمان) را برعهده دارد. کارشناسانی که در این تیم‌ها مستقر می‌شوند باید دوره‌های مربوط به امنیت شبکه و متقابلاً پیش‌ازآن، دوره‌های مربوط به شبکه و برنامه‌نویسی را بگذرانند. شرکت لیان در راستای تحقق هدف ایجاد محیطی امن برای اطلاعات سازمان‌ها، آماده برگزاری تمامی دوره‌های مذکور برای افراد و سازمان‌های علاقمند می‌باشد.

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 به‌منظور 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.

دوره‌هایی که توسط افتا تدوین شده‌اند در قالب پنج دسته جای گرفته‌اند:

### 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.

### دوره‌های مدیریت امنیت

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

### دوره‌های آزمون و ارزیابی

این دوره‌ها جهت آموزش کارشناسان حوزه آزمون و ارزیابی در نظر گرفته شده است.

### دوره‌های پایش و تحلیل امنیت

این دوره‌ها جهت آموزش کارشناسان حوزه پایش و تحلیل امنیت در نظر گرفته شده است.

### دوره‌های امن‌سازی زیرساخت‌ها، سرویس‌ها و سامانه‌ها

این دوره‌ها جهت آموزش کارشناسان حوزه امن‌سازی زیرساخت‌ها، سرویس‌ها و سامانه‌ها در نظر گرفته شده است.

شرکت لیان در راستای تحقق هدف ایجاد محیطی امن برای اطلاعات سازمان‌ها، که ازسوی سازمان افتا تبیین شده است، اقدام به برگزاری دوره‌های سازمانی کرده و آماده همکاری با تمامی سازمان‌ها و تیم‌های فنی آن‌ها می‌باشد.


یکی از مهم‌ترین مقوله‌ها در سطح یک سازمان، آموزش پرسنل عادی سازمان است. اما امروزه به‌نظر می‌رسد که پرسنل عادی، کمتر با مباحث امنیت IT درگیر هستند، در حالی که بیشترین خطرات از جانب همین افراد، متوجه شبکه و زیرساخت IT سازمان می‌باشد.

هر کاربر رایانه باید روش‌های محافظت از دارایی‌های اطلاعاتی خود و نحوه اتصال ایمن به سیستم‌های دیگر در شبکه را بداند. دوره آموزشی CSCU دانش امنیت اطلاعات و شبکه یک کاربر رایانه را در استفاده از منابع رایانه‌ای در داخل شبکه سازمان و یا حین اتصال به اینترنت، ارتقا می‌دهد. اخذ گواهینامه این دوره، گواهی می‌دهد که دارنده این مدرک، شایستگی و دانش استفاده‌از مهارت‌های شبکه‌های کامپیوتری را دارا بوده و مفاهیم ضروری امنیت IT را می‌داند. افراد با شرکت در دوره آموزشی CSCU، دانش و مهارت‌های لازم جهت حفاظت از اطلاعات خود را کسب خواهند نمود. نحوه طراحی این دوره به گونه‌ای انجام شده است که افراد شرکت‌کننده در آن، طی یک دوره آموزش تعاملی با کلیه تهدیدات موجود در زمینه امنیت اطلاعات اعماز تهدیدات مربوط به هویت افراد و کارت‌های اعتباری و همچنین رعایت مسائل امنیت فیزیکی آشنا خواهند شد. مهارت‌هایی که در این دوره به دانش‌پذیران آموخته خواهند شد، نه‌تنها در زمینه شناسایی این قبیل تهدیدات آن‌ها را یاری خواهد کرد، بلکه موجب کاهش موثر آن‌ها نیز می‌گردد. علاوه‌بر همه این مسائل، شرکت‌کنندگان در این دوره، آمادگی‌های لازم جهت شرکت در آزمون اخذ مدرک CSCU به شماره (۱۱۲-۱۲) متعلق به کمپانی EC-Council را نیز کسب خواهند نمود.

### سرفصل‌های این دوره:

- امنیت در سیستم‌عامل
- امنیت داده‌ها
- امنیت در اینترنت
- امنیت در شبکه
- سرقت هویت و مهندسی اجتماعی
- امنیت در تلفن همراه

به دلیل آن‌که هر روز به تعداد نفرات با استعداد و خرابکار، که سعی در سواستفاده از تکنولوژی اطلاعات دارند افزوده می‌شود، موفقیت استفاده‌از تکنولوژی اطلاعات، به پیشرفت هم‌زمان و موازی امنیت تکنولوژی اطلاعات بستگی دارد. برای مقابله با این افراد خرابکار یا در حقیقت هکر، مهم‌ترین امر کشف راه‌های نفوذ به شبکه و سپس به‌کارگیری روش‌های جلوگیری از آن می‌باشد. دوره CEH که مخفف Certified Ethical Hacker می‌باشد، یک دوره آموزشی هکر اخلاقی است که برای تمام افرادی که به‌طور حرفه‌ای در این زمینه فعالیت می‌کنند مورد نیاز است. این دوره توسط شرکت EC-Council ارائه می‌شود و از زمان شروع این دوره در سال ۲۰۰۳، دوره CEH انتخاب مطلق رشته امنیت اطلاعات در سراسر جهان بوده است. به‌طوری که این دوره به‌عنوان یک دوره پایه‌ای از سمت وزارت دفاع آمریکا انتخاب شده. دوره CEH دوره‌ای است که به‌خوبی می‌تواند نقاط آسیب‌پذیر را مورد بررسی قرار داده و همچنین ابزارهای تست این نقاط ضعف را نیز ارائه کند.

این دوره در بسیاری از سازمان‌ها به‌عنوان استاندارد استخدامی استفاده می‌شود و با داشتن این مدرک، افراد فرصت خوبی برای استخدام در سازمان‌هایی با رویکرد امنیتی خواهند داشت. همچنین بسیاری از سازمان‌ها نیز به‌منظور تقویت دانش اعضای واحد IT خود، از این دوره استفاده می‌کنند.

این دوره به‌طور کامل، نحوه اسکن، تست، هک و امنیت سیستم‌های هدف را به شرکت‌کنندگان خود آموزش خواهد داد و این افراد پنج مرحله زیر را برای تبدیل شدن به یک هکر اخلاق‌مدار، پشت‌سر خواهند گذاشت:

- Reconnaissance
- Gaining Access
- Enumeration
- Maintaining Access
- Covering Tracks


مدرک CISSP (گواهی متخصص امنیت سیستم‌های اطلاعاتی تاییدشده) یکی از معتبرترین مدارک بین‌المللی برای کارشناسان امنیت سایبری می‌باشد. این مدرک به‌طور مستقل و بدون در نظر گرفتن نوع سخت‌افزار و نرم‌افزار مورد استفاده در شرکت‌ها، ارزیابی و صادر می‌گردد و به‌عنوان یک عنصر کلیدی در انتخاب و استخدام کارشناسان امنیت سیستم‌های اطلاعاتی مورد استفاده قرار می‌گیرد. دارندگان این مدرک می‌توانند برای پست مدیریت امنیت سایبری سازمان‌های بزرگ و کوچک استخدام شوند و به‌طور کامل امنیت سایبری را در این سازمان‌ها مدیریت کنند.

CISSP گواهینامه‌ای مستقل از برند در حوزه امنیت اطلاعات است که توسط موسسه ISC2 معرفی و ارائه شده است. این گواهینامه برخلاف سایر گواهینامه‌های امنیتی، وابسته به محصولات هیچ برند خاصی نیست و می‌تواند به افراد متخصص امنیت، تبحر لازم را در طرح و پیاده‌سازی سیاست‌های کلان امنیتی اعطا نماید.

گواهینامه CISSP برای اشخاصی مناسب است که می‌خواهند مهارت‌های خود را در زمینه‌های مختلف امنیت شامل طراحی، مهندسی، پیاده‌سازی و مدیریت افزایش داده و امنیت سازمان خود را به‌عهده گیرند تا در نهایت بتوانند برای حملات پیچیده، آمادگی لازم را داشته باشند. این دوره عمق و وسعت دانش یك فرد را با تمرکز بر ۸ دامنه امنیت اطلاعات(Information Security) مورد ارزشیابی قرار می‌دهد.

**هشت دامنه امنیت اطلاعات شامل موارد زیر هستند:**

- امنیت و مدیریت ریسک (Security and Risk Management)
- امنیت دارایی (Asset Security)
- مهندسی امنیت (Security Enineering)
- امنیت شبکه و ارتباطات (Communication and Network Security)
- مدیریت دسترسی و هویت (Identity and Access Management)
- ارزیابی و تست امنیتی (Security Assessment and Testing)
- عملیات امنیت (Security Operations)
- امنیت توسعه نرم‌افزار (Software Development Security)

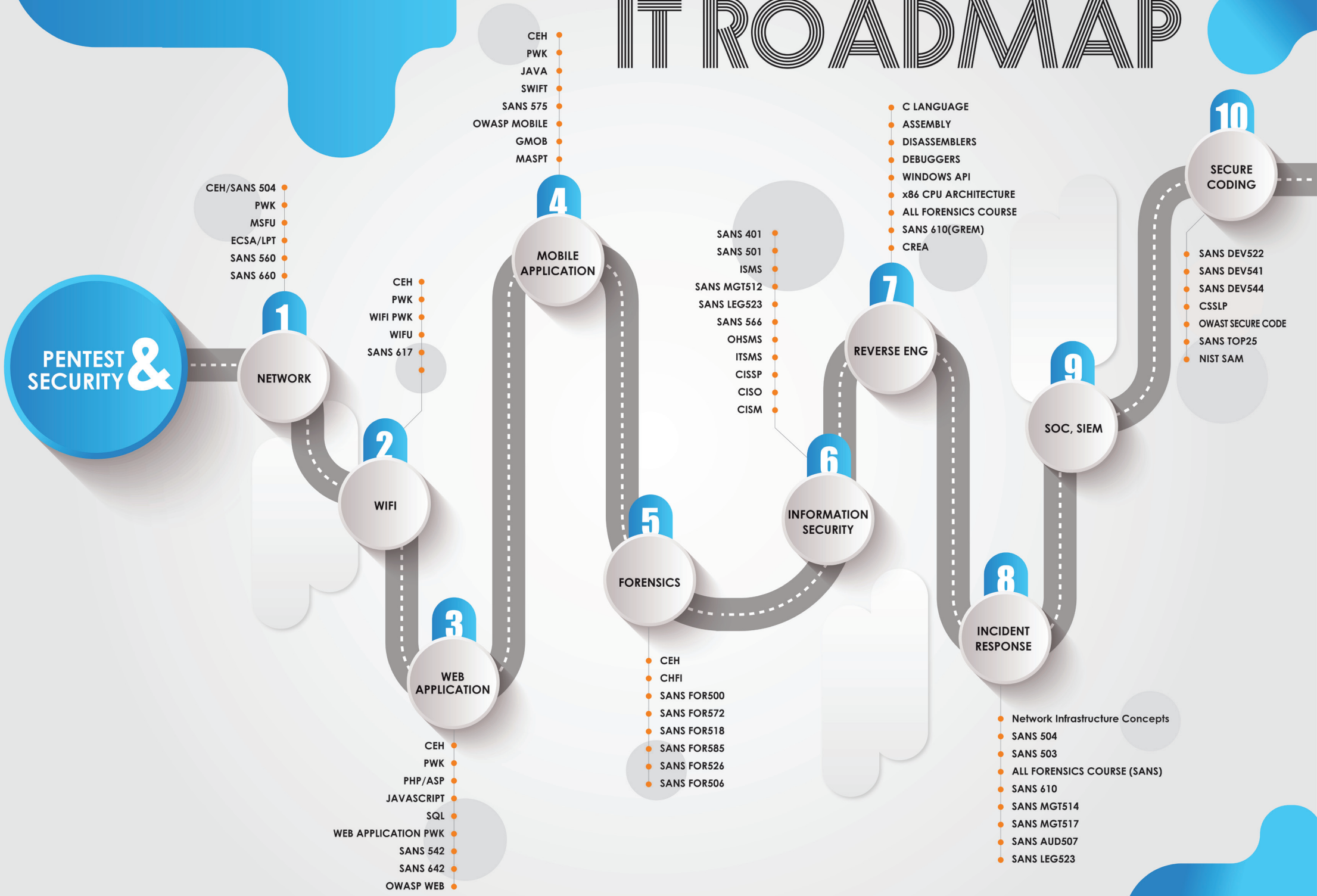
نفوذ و خرابکاری‌های موجود در سیستم‌های ارتباطی، هیچ‌گاه کهنه نخواهد شد و هر شبکه‌ای همیشه درمعرض این خطر خواهد بود. دوره CHFI یا Computer Hacking Forensics Investigatorکه توسط EC-COUNCIL ارائه شده، به‌منظور جلوگیری از این خرابکاری‌ها تبیین شده است. این دوره مخاطبان خود را آماده می‌سازد تا ردپای هکرهای موجود در شبکه را شناسایی کرده و پس‌از جمع‌آوری مدارک موجود، اقدامات لازم را انجام دهند.

در دوره CHFI که به معنی «بازرس قانونی جرایم رایانه‌ای» می‌باشد، مسیر هکرها تعقیب شده و مجرم اصلی شناسایی می‌شود. جرایم رایانه‌ای در سازمان‌ها و شرکت‌های کوچک و بزرگ همیشه اتفاق خواهند افتاد و تبعات آن‌ها نیز سواستفاده‌های بازرگانی و کلاهبرداری‌هایی‌ست که شاید جبران‌ناپذیر باشند. لذا سازمان‌ها برای جلوگیری از اتفاقات این‌چنینی، باید افرادی آموزش دیده و متخصص را به‌کار گیرند تا با انجام تحقیقات، آنالیز و بررسی تکنیک‌های ممکن، ردپای هکرهایی که اقدام به نفوذ می‌کنند را بدست آورند. در این دوره نیز مهارت‌هایی ازقبیل جمع‌آوری شواهد الکترونیکی در حملات سایبری، بررسی تمامی قسمت‌های کامپیوتر و شبکه و بازگردانی اطلاعات ازدست‌رفته و درنهایت ارائه مستندات به‌دست آمده به مراجع قانونی آموزش داده می‌شود.

سرفصل‌های این دوره پیشرفته، از مباحث تئوری درزمینه جرم‌شناسی سیستم‌های رایانه‌ای شروع شده و  تا آموزش‌های کامل مربوط به یک متخصص و بازرس ادامه خواهد داشت.

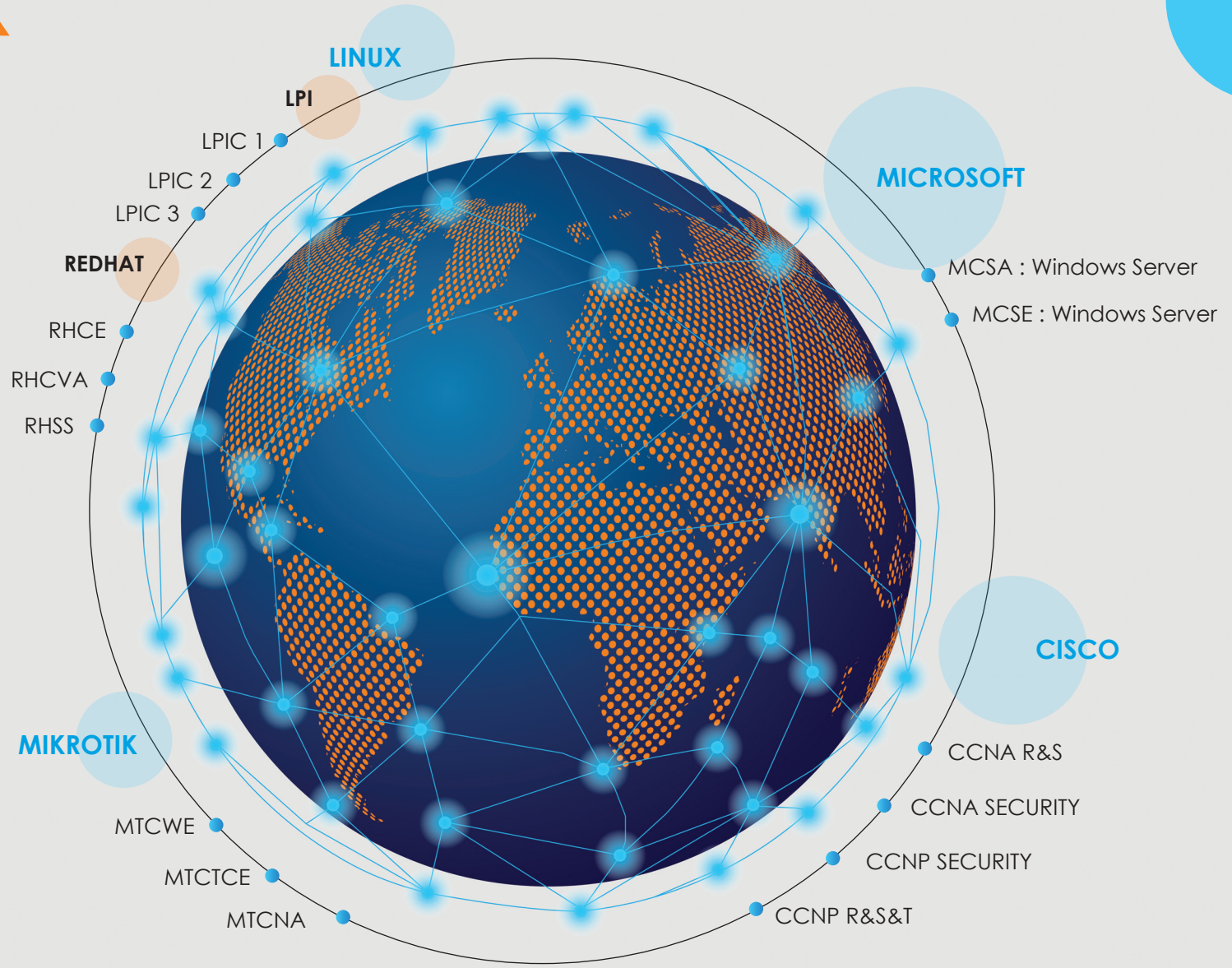
علاوه‌بر مدرک این دوره که می‌تواند زمینه‌ساز به‌دست آوردن بسیاری از مشاغل این حوزه باشد، شرکت‌کنندگان در این دوره می‌توانند پس‌از گذراندن این دوره، برای گرفتن گواهینامه بین‌المللی مربوطه از EC-COUNCIL نیز اقدام کنند.

# IT ROADMAP


PENTEST & SECURITY
1
NETWORK
CEH/SANS 504
PWK
MSFU
ECSA/LPT
SANS 560
SANS 660
2
WIFI
CEH
PWK
WIFI PWK
WIFU
SANS 617
3
WEB APPLICATION
CEH
PWK
PHP/ASP
JAVASCRIPT
SQL
WEB APPLICATION PWK
SANS 542
SANS 642
OWASP WEB
4
MOBILE APPLICATION
CEH
PWK
JAVA
SWIFT
SANS 575
OWASP MOBILE
GMOB
MASPT
5
FORENSICS
CEH
CHFI
SANS FOR500
SANS FOR572
SANS FOR518
SANS FOR585
SANS FOR526
SANS FOR506
6
INFORMATION SECURITY
SANS 401
SANS 501
ISMS
SANS MGT512
SANS LEG523
SANS 566
OHSMS
ITSMS
CISSP
CISO
CISM
7
REVERSE ENG
C LANGUAGE
ASSEMBLY
DISASSEMBLERS
DEBUGGERS
WINDOWS API
x86 CPU ARCHITECTURE
ALL FORENSICS COURSE
SANS 610(GREM)
CREA
8
INCIDENT RESPONSE
Network Infrastructure Concepts
SANS 504
SANS 503
ALL FORENSICS COURSE (SANS)
SANS 610
SANS MGT514
SANS MGT517
SANS AUD507
SANS LEG523
9
SOC, SIEM
10
SECURE CODING
SANS DEV522
SANS DEV541
SANS DEV544
CSSLP
OWAST SECURE CODE
SANS TOP25
NIST SAM

# IT ROADMAP
## PROGRAMMING

# IT ROADMAP
# NETWORK



# DEVELOPMENT

امروزه در دنیای فناوری اطلاعات، تولید ابزارهای متنوع برای ساده‌سازی و مدیریت بهتر کارها به‌شدت مورد علاقه کاربران است. شرکت لیان با استفاده از متخصصان و برنامه‌نویسان متخصص و متعهد، خدماتی در قالب تولید نرم‌افزارهای امنیتی تحت‌وب ارائه می‌کند. نرم‌افزارهایی که با تاییدیه‌های امنیتی استاندارد، در اختیار سازمان‌ها و شرکت‌هایی که دارای بستر وب هستند، قرار می‌گیرند. همچنین واحد استارت‌اپ شرکت لیان، به تولیداستارتاپ‌هایی در زمینه شبکه، وب، امنیت و... می‌پردازد که می‌تواند خدمات بسیار مفیدی را در اختیار مدیران سازمان‌ها و کارکنان آن‌ها قرار دهد.

ما معتقدیم رشد شرکت لیان همگام با رشد سازمان‌هایی که با ما همکاری می‌کنند همراه است. بنابراین شرکت لیان تمامی امکانات و توانمندی خود برای کمک به رشد و تعالی مشتریان و همکاران خود به‌کار می‌بندند تا بتوانیم دست در دست یکدیگر به اهداف عالی خود برسیم.

## برخی از مشتریان گروه لیان

بانک ملی ایران
پست بانک ایران
وزارت ورزش و جوانان
دیوان عدالت اداری
سازمان زندان ها
برق منطقه ای اصفهان
برق منطقه ای فارس
برق منطقه ای غرب
گروه مپنا
گمرک ایران

شرکت ساپکو
اداره کار و تعاون یاسوج
بیمه آسماری SOS
کارگزاری مفید
پارس تکنولوژی سداد
دانشگاه علوم پزشکی خوی
دانشگاه آزاد اروند
دانشگاه علوم پزشکی مراغه
دانشگاه علوم پزشکی خلخال
دانشگاه علامه محدث نوری
موسسه غیر انتفاعی کاوش
موسسه غیر انتفاعی رودکی
موسسه غیر انتفاعی پرندک
شرکت سرمایه گذاری صنایع مس افق کرمان
شرکت همگامان مس
شرکت فولاد آذربایجان
شرکت الکترونیک کارت دماوند
شرکت غرب استیل
شرکت تکتا
شرکت کربن سیمرغ
شرکت مبنا آسیا فرابر
شرکت صنایع پتروشیمی مسجد سلیمان
شرکت نیمروز
شرکت امن افزار نوین گستر
منطقه آزاد ارس
منطقه ویژه اقتصادی گرمسار
مجتمع طلای موته
انجمن حسابداری تهران


۰۲۱-۹۱۰۰٤۱۵۱

(۵) ۰۲۱-۹۱۰۰٤۱۵۱

contact@liangroup.net

فلکه دوم صادقیه، بلوار آیت الله کاشانی

خ نجف زاده فروتن، خ اعتمادیان، پلاک ٤۲، واحد ۲

liansec
itroadmap

lian_gpco