بسمه تعالی

سرفصل

دوره مدیر ارشد امنیت CISO

بر اساس سرفصل های دوره های برتر جهانی:

ISSMP, CISM, CCISO, MIT university

ارایه دهنده: واحد مشاوره امنیت و حکمرانی شرکت پیشگامان فناوری اطلاعات هامون

www.haumoun.com

مرکز تماس از طریق واتس اپ و بله :۰۹۹۰۲۸۵۷۲۹۰

سرفصل ۱: Financial Management & Security Governance, Strategy

Reference:

CISM Domain 1 – CCISO Domain 1 – ISSMP Domain 1 – MIT Sloan "Cybersecurity for Managers"

زیرسرفصل‌ها:

- Alignment استراتژی امنیت با اهداف کلان سازمان
- بودجه‌ریزی امنیت، تحلیل CAPEX/OPEX و ROI امنیتی
- طراحی Security Governance Model در سطح هیئت‌مدیره
- سیستم شاخص‌گذاری امنیت (KPI/KRI)
- مدیریت ارزش، اولویت‌بندی و Portfolio امنیت

در این سرفصل، نقش CISO به‌عنوان یک مدیر اجرایی تشریح می‌شود؛ نه صرفاً یک مدیر فنی. امنیت اطلاعات یک سیستم حکمرانی است که باید با استراتژی سازمان یکپارچه باشد. بنابراین، CISO باید ساختار تصمیم‌گیری، نقش‌ها، مسئولیت‌ها و مدل ارتباط با هیئت‌مدیره را طراحی کند. این سرفصل بر توانایی تحلیل بودجه امنیت، مدیریت CAPEX/OPEX و مدل‌سازی بازگشت سرمایه امنیتی (ROSI) تأکید دارد تا CISO بتواند امنیت را به زبان مالی برای مدیرعامل و CFO قابل‌درک کند. موضوعاتی مانند مدیریت Portfolio امنیت و اولویت‌بندی سرمایه‌گذاری‌ها بر اساس ریسک پوشش داده می‌شود. مدیر امنیت باید بتواند امنیت را از یک «هزینه» به یک «مزیت رقابتی» تبدیل کند. نتیجه، توانمندسازی CISO برای ساخت و مدیریت یک Governance Model حرفه‌ای است.

سرفصل ۲: Supply Chain Security & Enterprise Risk Management

Reference:

CISM Domain 2 – CCISO Domain 3 – ISSMP Domain 1 – MIT Sloan "Managing Cyber Risk"

زیرسرفصل‌ها:

- تعریف Risk Appetite و Risk Tolerance
- مدیریت ریسک اشخاص ثالث و زنجیره تأمین (TPRM/SCRM)
- ریسک‌سنجی کمی و مالی‌سازی ریسک (Quantification)
- برخورد با ریسک و تحلیل Residual Risk
- فرآیند ATO و نقش CISO در پذیرش رسمی ریسک

مدیریت ریسک قلب تصمیم‌گیری امنیت است. CISO باید بتواند Risk Appetite و سطح تحمل ریسک را با مدیران تنظیم و در مدل‌های تصمیم‌گیری پیاده‌سازی کند. این فصل نشان می‌دهد که زنجیره تأمین و اشخاص ثالث یکی از مهم‌ترین بردارهای حمله هستند؛ بنابراین طراحی یک برنامه کامل TPRM شامل ارزیابی، مانیتورینگ و کنترل‌های قراردادی ضروری است. در این سرفصل مفهوم ریسک‌سنجی کمی بر اساس مدل‌های مالی مطرح می‌شود که CISO بتواند سناریوهای حمله را به خسارت مالی قابل‌فهم برای هیئت‌مدیره تبدیل کند. این فصل اهمیت تحلیل Residual Risk، مستندسازی تصمیمات و ایجاد مدل قابل‌دفاع (Defensible Model) تأکید دارد. با رویکرد MIT Managing Cyber Risk، فرآیند ATO معرفی می‌شود؛ یعنی هیچ سرویس یا پروژه‌ای بدون پذیرش رسمی ریسک وارد فاز عملیاتی نمی‌شود. این ترکیب، ستون اصلی حکمرانی ریسک در سازمان است.

سرفصل ۳: Maturity & Security Program, Architecture Strategy

Reference:

CISM Domain 3 – CCISO Domain 2 – ISSMP Domain 3 – MIT Professional Education "Cloud & Cybersecurity Strategy"

- طراحی ISMS در سطح مدیران ارشد
- معماری کلان امنیت (Zero Trust, Identity-First)
- مدل‌های بلوغ (NIST CSF, CMMI)
- سیستم اندازه‌گیری کارایی امنیت
- Talent Strategy و ساختار تیم امنیت

این فصل مسئولیت CISO را در ساخت و مدیریت برنامه امنیت تعریف می‌کند. در این سرفصل، موضوع طراحی ISMS در سطح اجرایی و نحوه ساخت Operating Model روشن می‌شود. مطابق ISSMP، CISO نقش «معمار کلان امنیت» را دارد: انتخاب استراتژی Zero Trust، تعریف اصول امنیت Cloud، تعیین مدل Identity-First و هماهنگ‌سازی این معماری‌ها با نیازهای عملیاتی سازمان. مدل‌های بلوغ مانند NIST CSF کمک می‌کنند امنیت از وضعیت فعلی به وضعیت هدف منتقل شود. همچنین، CCISO تأکید می‌کند CISO باید ساختار تیم امنیت، مدل مهارت‌ها، نقش MSSP و برنامه Talent Retention را طراحی کند. در این سرفصل به کمک رویکرد Cybersecurity Strategy & MIT Cloud، ارتباط بین معماری امنیت، تحول دیجیتال و KPIهای عملکرد نشان داده می‌شود تا امنیت یک برنامه قابل‌سنجش، قابل‌پایش و قابل‌دفاع باشد.

سرفصل ۴: Audit & Legal, Compliance, Data Governance

Reference:

CISM Domain 3 – CCISO Domain 4 – ISSMP Domain 1 – MIT “Cybersecurity & Privacy Law Essentials”

- مدیریت Data Governance و Data Privacy
- چارچوب‌های تطبیق: GDPR و ۲۷۰۰۱ و PCI
- کاهش مسئولیت حقوقی مدیران (Liability Reduction)
- مدیریت Audit و پاسخ به Findings
- الزامات حقوقی: SLA امنیتی، حق ممیزی، بیمه سایبری

این سرفصل با تأکید بر CCISO و MIT Privacy Law Essentials، نقش کلیدی CISO در کاهش مسئولیت حقوقی سازمان را توضیح می‌دهد. CISO باید بتواند Data Governance و اصول Privacy مانند Data Minimization، Data Residency و حفاظت از داده‌های حساس را پیاده‌سازی کند. مطابق ISSMP، الزامات قانونی بخشی از حاکمیت امنیت هستند و باید در قراردادها، SLA امنیتی، حق ممیزی، و الزامات بیمه سایبری گنجانده شوند. در بعد اجرایی، مدیریت Audit - شامل Internal Audit، External Audit و Certification Audit - اهمیت زیادی دارد و CISO باید بتواند Findings را تحلیل، اولویت‌بندی و رفع کند. همچنین CISMنشان می‌دهد که مدیریت تطبیق باید بخشی از برنامه امنیت باشد، نه یک فعالیت جداگانه. در مجموع، این سرفصل امنیت را به یک ساختار حقوقی‌ـــحاکمیتی تبدیل می‌کند که در برابر دعاوی یا جریمه‌ها دفاع‌پذیر باشد.

سرفصل ۵: Business Resilience & SOC Oversight, Incident Response

Reference:

CISM Domain 4 – CCISO Domain 5 – ISSMP Domain 5 – MIT “Cybersecurity Incident Response & Crisis Leadership”

- نظارت مدیریتی بر SOC و شاخص‌های عملکرد
- طراحیIncident Response Plan
- مدیریت بحران و رهبری War Room
- برنامه‌ریزی BCP/DR
- Threat Intelligence در سطح مدیریتی

این سرفصل مسئولیت CISO را در مدیریت بحران و نظارت بر عملیات امنیتی تشریح می‌کند. مطابق CISM ، CISOباید بتولند کارایی SOC مانند MTTD و MTTR را اندازه‌گیری و رویه‌های عملیاتی را تنظیم کند. CCISO بر نقش مدیر در طراحی IR Plan و هدایت عملیات پاسخ به حادثه تأکید دارد. ISSMPنشان می‌دهد که مدیریت بحران تنها فرآیند فنی نیست؛ بلکه هماهنگی واحدهای مختلف، مدیریت روابط عمومی، تصمیم‌گیری سریع و مستندسازی برای مسائل حقوقی آینده را نیز شامل می‌شود. با الهام از MIT Crisis Leadership، این سرفصل CISO را برای ساخت و مدیریت War Room آماده می‌کند. همچنین طراحی برنامه تداوم کسب‌وکار (BCP) و بازیابی (DR) تضمین می‌کند سازمان حتی در زمان حمله نیز به کار ادامه دهد. Threat Intelligence در این سرفصل نه به‌عنوان داده فنی، بلکه به‌عنوان ورودی تصمیم‌سازی برای مدیران بررسی می‌شود.

سرفصل ۶: Executive Communication & Security Culture, Human Risk

Reference:

CISM Domain 1 – ISSMP Domain 2 – MIT Sloan "Organizational Behavior & Influence Without Authority"

- مدیریت ریسک انسانی
- طراحی و اجرای برنامه فرهنگ امنیت
- ارتباطات مدیریتی و Storytelling
- جلب همکاری مدیران واحدهای مختلف
- مدل‌سازی رفتار کارکنان بر اساس روانشناسی سازمانی

CISO موفق کسی است که بتواند امنیت را از سطح کنترل‌های فنی به سطح رفتار سازمانی منتقل کند. مطابق ISSMP، تغییر فرهنگ سازمانی و مدیریت ریسک انسانی بخشی حیاتی از وظایف CISO است. در این سرفصل مفاهیم رفتارشناسی، انگیزه‌های کارمندان، مقاومت نسبت به تغییر و روش‌های اعمال نفوذ بدون قدرت رسمی مورد بررسی قرار می‌گیرند. MIT Sloan در کورس Organizational Behavior نشان می‌دهد که موفقیت امنیتی بیشتر از آنکه حاصل ابزار باشد، حاصل مدیریت رفتار انسان است. CISM نیز بیان می‌کند که ایجاد فرهنگ امنیتی یکی از عناصر سیستم حکمرانی امنیت است. در این سرفصل، روش‌های ساخت روایت‌های مدیریتی (Storytelling)، نحوه ارتباط با C-Levelها، طراحی برنامه آموزش امنیتی متناسب با نقش‌ها و مدیریت مقاومت کارمندان آموزش داده می‌شود. هدف اصلی ایجاد فرهنگی است که در آن امنیت یک مسئولیت مشترک باشد.

سرفصل ۷: Cloud/Container Governance & Data Security, Identity Security

Reference:

CCISO Domain 2 – ISSMP Domain 3 – MIT “Cloud Security & Zero Trust Architecture Program”

- Data Classification و Data Protection Lifecycle
- Identity Security: IAM و PAM
- Shared Responsibility و Cloud Governance
- Container Security Governance
- API Security و Secrets Management

در این بخش، نقش CISO در طراحی و نظارت بر امنیت داده‌ها، هویت‌ها و محیط‌های Cloud/Container بررسی می‌شود. مطابق ISSMP، معماری امنیت باید از داده و هویت شروع شود. CCISO نیز بر مسئولیت CISO در مدیریت امنیت Cloud، طراحی کنترل‌ها، تعریف Shared Responsibility و نظارت بر امنیت سرویس‌های SaaS/IaaS تأکید دارد. در این سرفصل Data Protection Lifecycle از طبقه‌بندی داده تا حذف امن بررسی می‌شود. همچنین در راستای رویکرد MIT Zero Trust Architecture، امنیت هویت‌ها به‌عنوان ستون اصلی امنیت معرفی می‌شود و اصول Least Privilege، MFA و مدیریت دسترسی مبتنی بر نقش‌های پویا بررسی می‌گردد. موضوع Container Governance شامل کنترل Image Trust، Drift، و مدیریت Secrets است. در نهایت API Security نیز به‌عنوان برداری کلیدی مطرح می‌شود. این سرفصل ستون فنی-معماری برنامه امنیت است.

سرفصل ۸: Strategic Innovation & Emerging Technologies, AI Security

Reference:

CCISO Domain 5 – ISSMP Domain 3 – MIT “Responsible AI & AI Governance”

- حاکمیت هوش مصنوعی و ریسک LLM
- امنیت سیستم‌های خودکار (Autonomous Systems)
- ریسک‌های فناوری‌های نوظهور
- Ethical AI و تنظیم‌گری
- Security by Design در محصولات آینده

فناوری‌های نوظهور دائماً مرزهای امنیت را تغییر می‌دهند. CCISO نقش CISO را در تحول دیجیتال و مدیریت نوآوری بررسی می‌کند. ISSMP نیز معماری امنیت برای فناوری‌های آینده را پوشش می‌دهد. در این سرفصل، مفهوم AI Governance و نقش CISO در طراحی کنترل‌های هوش مصنوعی مطرح می‌شود. MIT Responsible AI تمرکز دارد بر مسئولیت‌پذیری، شفافیت، Bias، و مدیریت ریسک مدل‌ها. CISO باید بتواند LLM Risk، Prompt Injection، Data Leakage و Model Poisoning را ارزیابی و کنترل کند. همچنین فناوری‌هایی مانند سیستم‌های خودکار، OT هوشمند، کوانتوم و پلتفرم‌های Edge ریسک‌های جدیدی ایجاد می‌کنند که نیازمند تحلیل دقیق و سند استراتژی می‌باشند. این سرفصل به CISO کمک می‌کند یک نقشه راه امنیتی برای ۵ سال آینده تدوین کند و امنیت را در مراحل طراحی محصول (Security by Design) وارد کند.