دوره جامع تخصصی شکار تهدیدات سایبری

مرکز آموزش‌های تخصصی و مهارت‌افزایی دانشگاه خاتم
آکادمی راوین و اسپارا برگزار می‌کنند.

۱۲۵ ساعت آموزش تخصصی شکار تهدیدات سایبری – مجازی و حضوری

درس پیشرفته‌ی سامانه‌های SIEM و Splunk

درس شکار تهدیدات سایبری با Sysmon

درس شکار تهدیدات سایبری پیشرفته

درس تحلیل بدافزار

اسپارا

آکادمی راوین

www.khatam.ac.ir | www.spara.ir | www.ravinacademy.com

شیوه‌ی برگزاری و تدریس دوره

این دوره به صورت آنلاین و حضوری و بر روی سامانه‌ی LMS دانشگاه خاتم (Adobe Connect) برگزار می‌شود. لازم به ذکر است تمام موضوعات به همراه مثال‌های کاربردی و عملی تدریس می‌شود. همچنین با توجه به موضوع در حال تدریس، دانشجویان با سامانه‌های آزمایشگاهی به منظور انجام تکالیف یا تمرین عملی آموخته‌های خود، دسترسی خواهند داشت.

تجهیزات مورد نیاز برای حضور در دوره

برای حضور در این دوره تنها به یک دستگاه رایانه (لپ‌تاپ یا PC) و میکروفون نیاز است. همچنین مخاطبین بر روی رایانه‌های خود باید حداقل یک سیستم‌عامل ویندوز و یک سیستم‌عامل لینوکس (ترجیحا Ubuntu) داشته باشند.

آزمون و ارزش‌یابی دوره

دانشجویان پس از گذراندن کامل دوره، برای دریافت گواهی‌نامه‌های خود باید به صورت حضوری در دو آزمون نظری و عملی (دفاع در محیط آزمایشگاهی) شرکت کنند. در صورت دریافت نمره‌ی قبولی (۷۰ از ۱۰۰) در هریک از دو زمینه‌ی ذکر شده، گواهی‌نامه‌ی مربوط به آن را دریافت خواهند کرد.

مزایای این دوره

- بهره‌گیری از مجموعه‌ای از اساتید به‌نام و مجرب
- تدریس کاربردی در محیط آزمایشگاهی
- تدریس مباحث امنیتی بر اساس بررسی سناریوهای متعدد حملات سایبری دفاع و حمله در طول دوره
- اعطای دو گواهی معتبر (در صورت قبولی در آزمون)
- نشست برگزیدگان دوره با مدیران ارشد امنیت سایبری کشور
- دسترسی دانشجویان به محیط آزمایشگاهی

مخاطبان دوره

- مدیران و مشاوران امنیت سایبری
- کارشناسان شکار تهدیدات سایبری
- کارشناسان امنیت سایبری شامل تیم آبی، تیم‌های SOC و غیره
- سازمان‌هایی که قصد تشکیل یا ارتقای تیم آبی را دارند
- دانشجویان و فارغ‌التحصیلان رشته‌ی کارشناسی ارشد گرایش امنیت سایبری

پیش‌نیاز دوره

- آشنایی با مفاهیم و تعاریف امنیت سایبری
- آشنایی با مفاهیم حملات و تهدیدات سایبری
- آشنایی با سیستم‌عامل‌های مبتنی بر لینوکس و ویندوز
- آشنایی با مفاهیم شبکه‌های کامپیوتری
- آشنایی با پروتکل‌های پرکاربرد TCP/IP
- حداقل دو سال تجربه‌ی فعالیت در زمینه‌ی امنیت سایبری
- آشنایی با حداقل یکی از زبان‌های برنامه‌نویسی توصیه می‌شود

یکم آذر ماه ۱۴۰۰
دوشنبه‌ها و پنج‌شنبه‌ها

۰۲۱-۸۹۱۷۴۰۶۹

training@khatam.ac.ir

برای ثبت‌نام به سایت دانشگاه خاتم، قسمت مرکز آموزش‌های تخصصی مراجعه کنید.
khatam.ac.ir

درس پیشرفته‌ی سامانه‌های SIEM و Splunk پیشرفته

مدت آموزش: ۳۳ ساعت

مدرس: دکتر سید هادی موسوی

در این درس می‌توان به بررسی ساختار استاندارد یک SIEM، معرفی Splunk به همراه آموزش معماری و ویژگی‌های آن و در نهایت جمع‌آوری وقایع و شکار تهدیدات سایبری با استفاده از Splunk، اشاره کرد. لازم به ذکر است در روز پایانی، سناریوهای مختلف شناسایی تهدیدات سایبری، بر اساس سناریوهای تهدیدات پرکاربرد در دنیای واقعی به صورت عملی و با همراهی مخاطبان درس اجرا و تحلیل می‌شود.

سرفصل‌های آموزشی

- SIEM Fundamentals
- Introducing Splunk
- Creating and Using Lookups
- Searching
- Using Fields in Searching
- Creating Reports and Dashboards
- Splunk's Search Language Fundamentals
- Using Transforming Commands for isualizations
- Using basic Transforming Commands
- Creating Alerts and Scheduled Reports
- Using Mapping and Single Value Commands
- Creating and Using Macros
- Beyond Search Fundamentals
- Introduction to Knowledge Objects
- Splunk Enterprise Security
- Using the Common Information Model (CIM) Add-On
- Creating and Managing Fields
- Creating Field Aliases and Calculated Fields
- Creating Tags and Event Types
- Correlating Events
- Filtering and Formatting Results
- Creating and Using Workflow Actions
- Creating Data Models
- Creating Data Models
- Creating and Using Macros
- Splunk Stream App
- Administer Splunk

درس شکار تهدیدات سایبری با Sysmon

مدت آموزش: ۹ ساعت

مدرس: مهندس مهدی حاتمی

در این درس با Sysmon، پیکربندی آن آشنا خواهید شد، تعدادی رول‌های شکار تهدیدات سایبری و بسیاری از موارد دیگر را به صورت عملی خواهید آموخت. همچنین چندین سناریوی حملات سایبری در دنیای واقعی و شیوه‌ی شکار آن‌ها را در کنار هم تحلیل خواهیم کرد.

سرفصل‌های آموزشی

- How Attackers Bypass Sysmon
- Develop Hunting Rules
- Sysmon Configuration
- Sysmon Integration with SIEM
- How to Hunt Real World APT Techniques with Sysmon
- Sysmon Event IDs

درس شکار تهدیدات سایبری

مدت آموزش: ۵۰ ساعت

مدرس: مهندس مهدی حاتمی و مهندس طاها توکلی

انواع تکنیک‌ها، ابزارهای مورد نیاز، فرآیندها و سایر روش‌های مورد نیاز برای شناسایی و شکار تهدیدات سایبری در سه دسته‌ی شکار با استفاده از تحلیل وقایع، تحلیل ترافیک و تحلیل باینری‌های مشکوک را خواهید آموخت. همچنین به شکل عملی می‌آموزید که چگونه فعالیت‌های مهاجمان سایبری و گروه‌های APT را با روش‌های مختلف در سطح شبکه، سرورها و سیستم کاربران شکار کنید.

سرفصل‌های آموزشی

- Introduction to Hunting
- Threat Hunting Methodology
- Endpoint Hunting
- Malware Analysis Techniques
- Network Hunting
- Malware Hunting
- Hunting Web Shells

درس تحلیل بدافزار

مدت آموزش: ۳۳ ساعت

مدرس: مهندس طاها توکلی

این درس با هدف آموزش دانش، تکنیک‌ها و ابزارهای مورد نیاز برای تحلیل انواع بدافزار به منظور مقابله و شناسایی آن‌ها ارایه شده است. شما با گذراندن این درس، انواع تکنیک‌های تحلیل داینامیک و استاتیک، Sandboxing، Deobfucation، استخراج مشخصه‌های بدافزار، نگاشت کردن آن‌ها با فریم‌ورک MITRE ATT&CK، بهره‌برداری از یافته‌ها در راستای مقابله با بدافزارها و بسیاری موارد دیگر را به صورت عملی خواهید آموخت. این درس به صورت سناریو محور بوده و در طی آن سناریوهای بدافزارهای مختلف را مشاهده و تجربه خواهید کرد.

سرفصل‌های آموزشی

- Challenge Solutions
- Debugging and Anti-Analysis Going Deep
- Reporting and Weaponizing Your Findings
- Basic Techniques