KASPERSKY lab

SICHERHEITS-AUSBILDUNG FÜR IT-MITARBEITER

www.kaspersky.de

SICHERHEITSAUSBILDUG FÜR IT-MITARBEITER

Diese Kurse umfassen eine breite Auswahl von Cybersicherheitsthemen und -techniken mit Assessments von der Einsteiger- bis zur Expertenebene. Alle Kurse werden am Kundenstandort oder ggf. in einer lokalen oder regionalen Niederlassung von Kaspersky Lab angeboten.

Die Kurse umfassen sowohl theoretische Lektionen als auch praktische Übungen. Nach Abschluss jedes Kurses können die Teilnehmer ihr Wissen in einem Test prüfen.

EINSTEIGER, FORTGESCHRITTENER ODER EXPERTE?

Das Programm deckt alles von den Sicherheitsgrundlagen bis zur erweiterten digitalen Forensik und Malware-Analyse ab. So helfen wir Unternehmen, ihr Wissen zu Cybersicherheit in drei Hauptbereichen zu erweitern:

- Grundwissen zum Thema
- Digitale Forensik und Vorfallsreaktion
- Malware-Analyse und Reverse Engineering

SERVICEVORTEILE

STUFE 1 – Grundlagen der Cybersicherheit
Vermittelt IT- und Sicherheitsadministratoren und Managern ein grundlegendes Verständnis aktueller Modelle der praktischen IT-Sicherheit.

STUFE 1 – Praktische Sicherheitsgrundlagen
Vermittelt anhand praktischer Übungen mit modernen Sicherheitstools ein detailliertes Verständnis für IT-Sicherheit.

STUFE 2-3 – Digitale Forensik
Verbessert das Fachwissen Ihres internen Teams für digitale Forensik und Vorfallsreaktion.

STUFE 2-3 – Malware-Analyse und Reverse Engineering
Verbessert die Expertise Ihres internen Teams für Malware-Analyse und Reverse Engineering.

PRAKTISCHE ERFAHRUNG

Von einem der führenden Sicherheitsanbieter, gemeinsames Arbeiten und Lernen zusammen mit unseren globalen Experten, die die Teilnehmer durch ihre eigene Erfahrung im alltäglichen Kampf gegen die Cyberkriminalität inspirieren.

PROGRAMMBESCHREIBUNG

THEMEN	Dauer	Erlernte Fertigkeiten
STUFE 1 – GRUNDLAGEN DER CYBERSICHERHEIT		
• Übersicht über Cyberbedrohungen und den Untergrundmarkt • Spam und Phishing, E-Mail-Sicherheit • Technologien zum Betrugsschutz • Exploits, mobile und hochentwickelte, hartnäckige Bedrohungen • Grundlagen der Untersuchung mit öffentlichen Webtools • Sicherung Ihres Arbeitsplatzes	2 Tage	• Erkennung und Behebung von Sicherheitsvorfällen • Reduzierung der Belastung für die Informationssicherheitsabteilungen • Erhöhung der Sicherheit für den Arbeitsplatz jedes einzelnen Mitarbeiters durch zusätzliche Tools • Ausführung von grundlegenden Untersuchungen • Analyse von Phishing-E-Mails • Erkennung von infizierten oder gefälschten Webseiten

THEMEN	Dauer	Erlernte Fertigkeiten
STUFE 1 – PRAKTISCHE SICHERHEITSGRUNDLAGEN		
• Sicherheitsgrundlagen • Informationen aus frei verfügbaren Quellen • Netzwerksicherheit in Unternehmen • Programmsicherheit & Exploit-Schutz • DDoS-Angriffe & Banking-Attacken • WLAN-Sicherheit & globales mobiles Netzwerk • Banking & mobile Bedrohungen • Reaktion bei Sicherheitsvorfällen in Cloud- und virtuellen Umgebungen	5 Tage	• Grundlegende Untersuchungsmethoden mithilfe von öffentlichen Ressourcen, speziellen Suchmaschinen und Sozialen Netzwerken • Erstellen eines abgesicherten Netzwerkperimeters • Grundlagen von Penetrationstests • Analyse des Datenverkehrs auf unterschiedliche Angriffstypen • Entwicklung sicherer Software • Identifizierung von Schadcode-Injektion • Grundlagen der Malware-Analyse und der digitalen Forensik
STUFE 2 – ALLGEMEINE DIGITALE FORENSIK		
• Einführung in die digitale Forensik • Live-Reaktion und Erfassung von Beweisen • Details der Windows-Registrierung • Windows-Artefaktanalyse • Browser-Forensik • E-Mail-Analyse	5 Tage	• Aufbau eines digitalen Forensiklabors • Sammeln von digitalen Beweisen und entsprechende Nutzung • Rekonstruieren eines Vorfalls und Verwenden von Zeitstempeln • Analyse von Eindringspuren anhand von Windows-Artefakten • Finden und Analysieren von Browser- und E-Mail-Verlauf • Anwenden der Tools und Instrumente der digitalen Forensik
STUFE 2 – ALLGEMEINE MALWARE-ANALYSE UND REVERSE ENGINEERING		
• Ziele und Techniken für Malware-Analyse und Reverse Engineering • Windows-Interna, ausführbare Dateien, x86-Assembler • Grundlegende statische Analysetechniken (Extrahierung von Zeichenfolgen, Importanalyse, PE-Zugangspunkte auf einen Blick, automatisches Entpacken usw.) • Grundlegende dynamische Analysetechniken (Debugging, Überwachungstools, Abfangen von Datenverkehr usw.) • .NET, Visual Basic, Win64-Dateianalyse • Skript- und Nicht-PE-Analysetechniken (Batch-Dateien, Autoit, Python, Jscript, JavaScript, VBS)	5 Tage	• Aufbau einer sicheren Umgebung für Malware-Analyse: Bereitstellung der Sandbox und aller benötigten Tools • Verstehen der Prinzipien der Windows-Programmausführung • Entpacken, Debugging und Analyse von schädlichen Objekten und Identifizierung ihrer Funktionen • Erkennen von schädlichen Webseiten über die skriptbasierte Malware-Analyse • Durchführung von Malware-Expressanalysen
STUFE 3 – ERWEITERTE DIGITALE FORENSIK		
• Umfassende Windows-Forensik • Datenwiederherstellung • Netzwerk- und Cloud-Forensik • Speicherforensik • Timeline-Analyse • Forensikübung eines realen gezielten Angriffs	5 Tage	• Durchführen einer umfassenden Dateisystemanalyse • Wiederherstellung gelöschter Dateien • Analyse des Netzwerkdatenverkehrs • Erkennung von schädlichen Aktivitäten in Speicherauszügen • Rekonstruieren des Vorfallablaufs
STUFE 3 – ERWEITERTE MALWARE-ANALYSE UND REVERSE ENGINEERING		
• Ziele und Techniken für Malware-Analyse und Reverse Engineering • Techniken der fortgeschrittenen statischen & dynamischen Analyse • (manuelles Entpacken) • Aufdeckungstechniken • Rootkit- und Bootkit-Analyse • Exploit-Analyse (.pdf, .doc, .swf usw.) • Analyse von Nicht-Windows-Malware (Android, Linux, Mac OS)	5 Tage	• Verwenden von Best Practices für Reverse Engineering aus der ganzen Welt • Erkennung von Techniken gegen Reverse Engineering (Verschleierung, Anti-Debugging) • Anwenden von erweiterten Malware-Analysen für Rootkits/Bootkits • Analysieren von in unterschiedlichen Dateitypen integriertem Exploit-Shellcode • Analyse von Nicht-Windows-Malware

KASPERSKY lab

KASPERSKY lab