Kaspersky Security Trainings

www.kaspersky.de
#truecybersecurity

Kaspersky Security Trainings

Sicherheitsschulungen sind angesichts der zunehmenden Bedrohungslage für Unternehmen unerlässlich. Sicherheitsmitarbeiter müssen in den erweiterten Sicherheitstechniken ausgebildet werden, die eine wichtige Komponente des effektiven Bedrohungsmanagements und der Strategien zur Risikominimierung im Unternehmen bilden.

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.

Servicevorteile

Digital Forensics und Advanced Digital Forensics

Vertieft das Fachwissen Ihres internen Teams für digitale Forensik und Vorfallsreaktion. Teilnehmer dieses Kurses können Erfahrungslücken schließen und ihre praktischen Fertigkeiten bei der Suche nach digitalen Spuren von Cyberkriminalität sowie bei der Analyse verschiedener Datentypen zur Ermittlung des zeitlichen Ablaufs und der Quellen des Angriffs entwickeln und verbessern. Nach Abschluss dieses Kurses können Teilnehmer Computervorfälle erfolgreich untersuchen und die Sicherheit des Unternehmens verbessern.

Malware Analysis and Reverse Engineering und Advanced Malware Analysis and Reverse Engineering

Die Reverse-Engineering-Schulung wurde entwickelt, um Vorfallsreaktionsteams bei der Untersuchung schädlicher Aktivitäten zu unterstützen. Dieser Kurs richtet sich an Mitarbeiter der IT-Abteilung und Systemadministratoren. Die Teilnehmer erfahren, wie sie Malware analysieren, IOCs erfassen, Signaturen zur Erkennung von Malware auf infizierten Geräten schreiben und infizierte/verschlüsselte Dateien und Dokumente wiederherstellen.

Incident Response

Der Kurs führt Ihr internes Team durch sämtliche Phasen der Vorfallsreaktion und stattet sie mit dem umfassenden Wissen aus, das für eine erfolgreiche Wiederherstellung nach Vorfällen erforderlich ist.

Yara

In diesem Kurs erfahren Sie, wie Sie effektive Yara-Regeln schreiben, testen und so verbessern können, dass sie Bedrohungen finden, die bisher unbekannt blieben.

KATA Administration

Die Schulung „KATA Administration" umfasst sämtliches Know-how zur Planung, Installation und Konfiguration der Lösung, mit dem Sie die Bedrohungserkennung optimieren können.

KATA Security Analyst

Der Schulungskurs beinhaltet eine Reihe praktischer Übungen, die auf tatsächlichen Bedrohungsszenarien basieren, und vermittelt das Wissen, das Sie für die Überwachung, Interpretation und Reaktion auf KATA-Warnungen benötigen.

Praktische Erfahrung

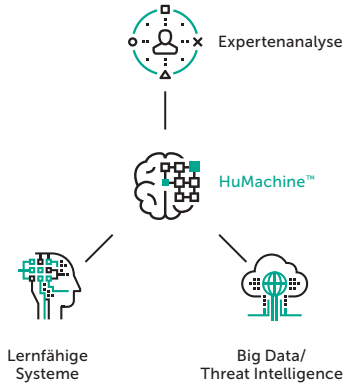
Von einem der führenden Sicherheitsanbieter, gemeinsames Arbeiten und Lernen zusammen mit unseren globalen Experten, die die Teilnehmer durch ihre eigene Erfahrung im alltäglichen Kampf gegen die Cyberkriminalität inspirieren.

Programmbeschreibung

Themen	Dauer	Erlernte Fertigkeiten
Digital Forensics		
• 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
Malware-Analyse und Reverse Engineering		
• Ziele und Techniken für Malware-Analyse und Reverse Engineering • Windows-Interna, ausführbare Dateien, x86-Assembler • Grundlegende Analysetechniken (String-Extraktion, Import-Analyse,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
Advanced Digital Forensics		
• 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
Advanced Malware Analysis and Reverse Engineering		
• Ziele und Techniken für Malware-Analyse und Reverse Engineering • Erweiterte statische Analyseverfahren (statische Analyse von Shellcode, Analysieren von PE-Headern, TEB (Thread Environment Block, Datenstruktur in Windows NT), PEB (Process Environment Block, Datenstruktur in Windows NT), Ladefunktionen durch verschiedene Hash-Algorithmen) • Erweiterte dynamische Analysetechniken (PE-Struktur, manuelles und erweitertes Entpacken, Entpacken von schädlichen Packprogrammen, die die ausführbare Datei in verschlüsselter Form speichern) • APT Reverse Engineering (einschließlich APT-Angriffsszenario, angefangen bei Phishing-E-Mails bis hin zur möglichst tiefgreifenden Analyse) • Protokollanalyse (Analyse von verschlüsselten C2-Kommunikationsprotokollen, Entschlüsseln von Datenverkehr) • Analyse von Rootkits und Bootkits (Debuggen des Bootsektors mithilfe von Ida und VMWare, Kernel-Debugging mit zwei virtuellen Maschinen, Analyse von Rootkit-Proben)	5 Tage	• Befolgen von Best Practices im Bereich Reverse Engineering sowie Erkennung von Anti-Reverse-Engineering-Tricks (versteckte Bedrohungen, Anti-Debugging) • Anwendung erweiterter Malware-Analysen für die Zerlegung von Rootkits/ Bootkits • Analyse von in verschiedene Dateitypen eingebettetem Exploit-Shellcode und Nicht-Windows-Malware

Programmbeschreibung

Themen	Dauer	Erlernte Fertigkeiten
Incident Response		
• Einführung in die Vorfallsreaktion • Erkennung und primäre Analyse • Digitale Analyse • Erstellen von Erkennungsregeln (YARA, Snort, Bro)	5 Tage	• Abgrenzung von APTs von anderen Bedrohungen • Verstehen der verschiedenen Angreifertechniken und des Aufbaus gezielter Angriffe • Anwenden bestimmter Überwachungs- und Erkennungsmethoden • Einhaltung des Workflows für die Vorfallsreaktion • Rekonstruktion der Vorfallschronologie und -logik • Erstellen von Erkennungsregeln und Reporting
Yara		
• Kurze Einführung in die Yara-Syntax • Tipps und Tricks zur Erstellung schneller und effektiver Regeln • Yara-Generatoren • Testen von Yara-Regeln auf Fehlalarme (False-Positives) • Aufspüren neuer, unentdeckter Proben auf VT • Verwenden externer Module innerhalb von Yara zum effektiven Aufspüren von Bedrohungen • Suche nach Anomalien • Zahlreiche (!) Beispiele aus dem echten Leben • Übungen zur Vertiefung der Yara-Kenntnisse	2 Tage	• Erstellen effektiver Yara-Regeln • Testen von Yara-Regeln • Verbessern der Regeln, bis sie Bedrohungen finden, die sonst niemand findet
KATA Administration		
• Allgemeine Szenarien der Lösungsbereitstellung und Serverstandorte • Größenüberlegungen • Lizenzmodell • Sandbox-Server • Zentraler Node • Sensor • Integration in Infrastruktur • Installation von Endpoint-Sensor • Hinzufügung einer Lizenz und Aktualisierung der Datenbanken • Algorithmus für Lösungsbetrieb	1 Tag	• Entwurf des Implementierungsplans für die Kundenumgebung • Installation und Einrichtung aller KATA-Komponenten • Verwaltung und Überwachung der Lösung
KATA Security Analyst		
• Interpretation der KATA-Warnungen • Erklärung der Erkennungs- und Analysetechnologien • Erklärung der Bewertung und Risiko-Engines	1 Tag	• Verstehen der Bewertung und ihrer Verwendung durch Risiko-Engines • Überwachung, Interpretation und Reaktion auf KATA-Warnungen



Kaspersky Lab
Cybersicherheit für Unternehmen: **www.kaspersky.de/enterprise-security**
Neues über Cyberbedrohungen: **de.securelist.com**
IT-Sicherheitsnachrichten: **www.kaspersky.de/blog/b2b**

#truecybersecurity
#HuMachine

www.kaspersky.de

© 2017 Kaspersky Labs GmbH. Alle Rechte vorbehalten. Eingetragene Handelsmarken und Markenzeichen sind das Eigentum ihrer jeweiligen Rechtsinhaber.