IOprotect Schulung

Incident Live Response Basic

Datum:
April 2018

IOprotect GmbH
Dürstelenstrasse 136
8335 Hittnau
+41 (0)44 533 00 05
info@ioprotect.ch
www.ioprotect.ch

Incident Live Response Basic

Ziel / Beschreibung	Heutzutage kommen nicht nur Security-Experten oder Incident Handler in Kontakt mit potentiell bösartigen Dateien oder kompromittierten Systemen. Die Frage, wie damit umgegangen werden soll, stellt sich beispielsweise auch für Helpdesk-Mitarbeiter oder Systemadministratoren. In dieser eintägigen Einführung wird das Vorgehen bei Malware-Verdachtsfällen in Form von Flussdiagrammen erarbeitet. Die Teilnehmer lernen frei verfügbare Hilfsmittel kennen und können die Resultate interpretieren. Ausserdem werden Do's & Don't beim Incident Live Response aufgezeigt. Dieser Einführungskurs richtet sich an Mitarbeitende, welche wenig oder gar keine Erfahrung im Bereich Malware-Analyse / Incident Response haben.

Inhalte	• Übersicht IR-Prozess
	• Unterscheidung zweier Fälle
	• Erarbeitung des Vorgehens in Form von Flussdiagrammen
	• Bearbeitung Fall 1
	  ▪ Stolpersteine
	  ▪ Vorstellung der Tools
	  ▪ Interpretation der Resultate
	  ▪ Lessons Learned
	• Bearbeitung Fall 2
	  ▪ Stolpersteine
	  ▪ Vorstellung der Tools
	  ▪ Interpretation der Resultate
	  ▪ Lessons Learned
	• Ausblick auf weiterführende Themen
	  ▪ Memory Forensics
	  ▪ Internetsimulation
	  ▪ OSINT

Zielpublikum	Mitarbeitende, welche mit potentiell bösartigen Dateien, Schadcode oder kompromittierten Systemen in Berührung kommen, jedoch wenig oder gar keine Erfahrung im Bereich Malware-Analyse / Incident Response haben.

Schlüsselwörter	Windows Bordmittel, Sysinternals Suite, VirusTotal, dynamische Analysen mittels Sandboxen, persistente und volatile Daten.
Anmerkungen	Während der Schulung werden keine Windows-Systeme von uns zur Verfügung gestellt. Wir zeigen die Tools via Beamer auf unseren Systemen. Selbstverständlich steht es jedem Teilnehmer frei, sein eigenes Windows-System mitzubringen und die Tests so nachzubilden.
Dauer	1 Tag
Zeit	09:00 - 16:00
Verpflegung	Mittagessen zu Lasten Teilnehmer
Kosten	• SCS-Mitglieder: 2 Personen kostenlos, jede weitere Person CHF 50.- • Bestehende IOprotect Kunden: CHF 100.- pro Person • Weitere Interessenten: CHF 250.-