

EXPECT THE
UNEXPECTED

ITWeb: Incident Response Bootcamp

Training Schedule

Powered By



Copyright

All information contained herein is copyrighted information that is proprietary, privileged, or confidential. It is intended only for the purpose specific, and directed to the recipients specifically identified by CyberGym Ltd. Any unauthorized review, disclosure, reproduction, distribution, copying of, or reliance upon this document, and any included exhibits is strictly prohibited. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, for purposes other than intended, without prior written permission of CyberGym.



Training Schedule

Day 1

Time	Session	Description
08:45 - 09:15	Training Kickoff	Training Kickoff
09:15 - 10:00	Hacker Point of View	Hacker profiles, attack vectors and APT stages from the offensive perspective
10:00 - 10:45	The First Responder	<ul style="list-style-type: none"> •Role and responsibilities •Methodology (Incident Handling)
10:45 - 11:00	Coffee break	Coffee break
11:00 - 11:30	Sysinternals Overview	<ul style="list-style-type: none"> •Process Explorer, TCP View, Process Monitor, Autoruns •Suspicious signs
11:30 - 12:30	Lockheed Martin	Lockheed Martin attack stages from offensive and defensive perspectives
12:30 - 13:15	Lunch	Lunch



13:15 - 14:30	Basic Forensics - Darkcomet	Trainees analyse an infected work station independently, evaluate the collected data and determine appropriate remediation actions
14:30 - 14:45	Coffee break	Coffee break
14:45 - 15:45	Basic Forensics - NJRAT	Trainees analyse an infected work station independently, evaluate the collected data and determine appropriate remediation actions
15:45 - 16:15	Training Summary	Debriefing and main learning points

Day 2

Time	Session	Description
09:00 - 09:15	Morning session	Daily schedule overview
09:15 - 10:15	Arena Introduction	Arena security systems and infrastructure
10:15 - 11:00	Shamoon Pt 1	Attackers are targeting the organisation's



		networks, trying to cause malicious damage. <i>Note: this scenario is modelled around the actual 2012 attack on Saudi Aramco.</i>
11:00 - 11:15	Coffee break	Coffee break
11:15 - 12:30	Shamoon Pt 2	APT continuation
12:30 - 13:15	Lunch	Lunch
13:15 - 14:30	Shamoon Pt 3	APT continuation
14:30 - 14:45	Coffee break	Coffee break
14:45 - 15:45	Shamoon Pt 4	APT conclusion
15:45 - 16:15	Workshop Summary Session	<ul style="list-style-type: none"> • Debriefing and main learning points • Completion of feedback questionnaires • Certificates of completion