FalconForce

FalconForce specialist trainings

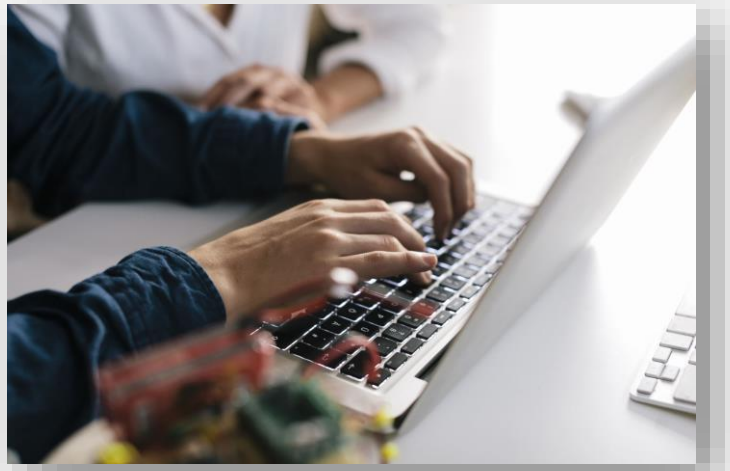
Detection engineering for Windows

BROCHURE

Specialist trainings: detecting engineering for Windows

FalconForce developed two specialist trainings for security professionals to help improving their detection capabilities.
One for maximum flexibility with your busy schedule and one advanced training to go all-in with additional lab and exercises.

Building good analytics and automated detection capabilities require a detailed understanding of attackers and their known or expected behavior. By understanding the different tools and techniques used by attackers and what indicators can be extracted, better detection capabilities can be developed.



This process is called Detection Engineering and it is a crucial aspect to be truly effective at discovering attackers in your network.

The instructor-led trainings focus on the entire detection engineering cycle. Guiding participants in defining a scope, researching the relevant (sub-)techniques, building the detection analytic, investigating which logs can be utilized, and validating the resilience of the analytic against evasion.

Student requirements

Students should be familiar with Windows and have basic PowerShell experience. Furthermore, at least some experience with Azure Sentinel and the Kusto query languages is required. To be able to connect to our lab environment, students should be able to use Microsoft RDP (Remote Desktop Protocol) via the Internet on port 3389 TCP.

Interactive training

The trainings are highly interactive and retain a good balance between theory and a lot of hands-on exercises for the students to get used to the detection engineering methodology and prepare them to start implementing this at their organizations. The student is free to decide whether to perform the hands-on exercises using Azure Sentinel and Defender. While hands-on exercises focus predominantly on the endpoint, the methodology can be applied to any part of an infrastructure.

Who should take the training

Aspiring detection engineers, SOC analysts, threat hunters, red teamers.

The methodology will enable anyone with a hands-on role in security to learn more to improve the security posture of a company.

The training contents in a nutshell

Maximum flexibility: Detection Engineering for Windows training

Besides an introduction into the field of threat hunting, the following topics are part of the training content:

- MITRE ATT&CK
- Detection engineering principles & theory
- Information resources and using threat information
- Understanding your data and developing hypothesis
- Researching technology and techniques
- Detection techniques & creating analytics for resilient detections
- (Open source) tooling
- Detection improvement and detection validation

In both trainings, the students will use tools like:

- Loads of Windows applications
- PowerShell
- IDA / Ghidra / Process Hacker / API Monitor / ETW
- Sysmon / Azure Sentinel / Defender for Endpoint
- Visual Studio 2019
- Windows virtualized network

Deep focus: Advanced Detection Engineering for Windows training

All content from the Detection Engineering for Windows training condensed and augmented with more challenging exercises.

Sentinel, Microsoft Defender for Endpoint and Sysmon will be utilized from day 2 onwards. Day 3 and 4 of the training are full days of purple detection engineering hands-on lab sessions, focusing on the following MITRE ATT&CK tactics:

- Initial Access.
- Privilege Escalation.
- Lateral Movement.
- Persistence.

For each tactic we will be analyzing tools, creating detections, modifying them for evasion, and building resilient detections. Every day has multiple exercises that guide you through the detection engineering methodology. This will enable you to immediately apply the gained skills within your organization.

Contact Us

+31 6 1034 4192

training@falconforce.nl

https://falconforce.nl

@falconforceteam

https://linkedin.com/company/falconforce