Part 1: PowerShell Fundamentals

In this part, we are revisiting the PowerShell fundamentals necessary for getting started with PowerShell for cybersecurity. We will begin by reviewing the basics, including Object-Oriented Programming principles, the differences between Windows PowerShell and PowerShell Core, the fundamental concepts of PowerShell, as well as the security features introduced in each PowerShell version.

Next, we'll explore the essential foundations of PowerShell scripting. By the end of this part, you will have the skills to write PowerShell scripts utilizing various control structures, variables, and operators, enabling you to create reusable code efficiently.

You will also explore how to configure and utilize remote management technologies, with a special focus on PowerShell Remoting. You will gain insights into the security-specific facts and best practices regarding PowerShell Remoting and authentication.

Finally, we will look into PowerShell-related Event Logging: you will understand which Windows event logs and events are the most important ones when it comes to PowerShell cybersecurity. We'll examine how to configure Script Block Logging, Module Logging, and transcripts and how to analyze event logs most efficiently.

This part has the following chapters:

- ***Chapter 1***, *Getting Started with PowerShell*
- ***Chapter 2***, *PowerShell Scripting Fundamentals*

- ***Chapter 3***, *Exploring PowerShell Remote Management Technologies and PowerShell Remoting*
- ***Chapter 4***, *Detection – Auditing and Monitoring*