LevelBlue

Endpoint Security with SentinelOne® – Syllabus

© 2024 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners.

Contents

Course Overview 3
Module 1: Introduction 3
Module 2: Technology Overview 3
Module 3: SentinelOne Agent 4
Module 4: Threat Detection 4
Module 5: Tuning and Automatic Protection 5
Module 6: Advanced BlueApp for SentinelOne 5

© 2024 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners.

Course Overview

The *Endpoint Security with SentinelOne®* course teaches students how to install, configure, and use SentinelOne to protect their endpoints. Students will also learn how SentinelOne interacts with USM Anywhere™ to augment existing USM Anywhere capabilities.

The course is practical with approximately

- 25% slides
- 35% demonstrations
- 40% labs exercises.

Module 1: Introduction

Description

This module introduces students to the technologies used in the lab environment, including the HTML5 interface, SentinelOne Management Console, and USM Anywhere.

Topics

- Course Outline
- Connect to the HTML5 interface
- Connect to the SentinelOne Management Console
- Connect to USM Anywhere

Module 2: Technology Overview

Description

This module teaches students about the capabilities of USM Anywhere and SentinelOne. Students will learn how these technologies may complement each other.

Topics

- What Is USM Anywhere?
- What Is SentinelOne?
- Site Details
- Filtering Endpoints

© 2024 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners.

- Creating Static and Dynamic Groups
- User Scope

Module 3: SentinelOne Agent

Description

This module teaches students how to install and troubleshoot the SentinelOne® Agent.

Topics

- Agent Deployment to Microsoft Windows and Linux
- Advanced Installation Options
- What Are Rogues?
- Endpoint Control with the sentinelctl CLI Tool
- Installation Troubleshooting with the sentinelctl CLI Tool
- Connectivity Troubleshooting

Module 4: Threat Detection

Description

This module teaches students how SentinelOne uses the Static and Dynamic AI engines to detect suspicious and malicious activity. They will learn how to use Threat Views and Deep Visibility for threat hunting. Finally, they will remediate threats on Windows.

Topics

- Static Detection Engine
- Dynamic Detection Engine
- The difference between Suspicious and Malicious Activity
- Using Threat Views to Track an Incident
- Using Deep Visibility Queries for Threat Hunting
- Remediating Windows Ransomware

© 2024 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners.

Module 5: Tuning and Automatic Protection

Description

This module teaches students how to use policies to control how SentinelOne reacts to suspicious and malicious activity. They will learn how to modify what is detected as benign, suspicious, and malicious. They will learn how to control devices and firewalls on endpoints. Finally, students will learn how to prevent threats from occurring.

Topics

- Policy and Configuration
- Blocklists and Exclusions
- Device Control
- Network Control
- Enabling Automatic Protection Using Policies
- Automatic Remediation of a Malicious Threat on Windows
- Respond to a Network Attack Against Windows

Module 6: Advanced BlueApp for SentinelOne

Description

This module teaches students how USM Anywhere uses an Advanced BlueApp with which to interact and control SentinelOne. They will learn how to use the built-in capabilities of USM Anywhere, augmented with SentinelOne, to protect their environment.

Topics

- Connect the Advanced BlueApp
- Retrieve SentinelOne Information
- Merge SentinelOne Data with USM Anywhere Data
- Use Investigations to Track Threats
- Mitigating Threats
- Detecting and Remediating a Ransomware Attack
- Reports

© 2024 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners.