BlueCat Security and Advanced Configuration Instructor-led Training

BlueCat Training Services empower your staff with hands-on training that keeps pace with the design and deployment of your BlueCat solution. BlueCat experts design distinct learning paths to address the comprehensive needs of your IT organization. Our training offerings equip your staff with the skills needed to optimize your BlueCat solution and realize its full potential.

BlueCat Security and Advanced Configuration is an 8-hour course designed to teach topics related to DNS security and advanced IPAM concepts to administrators. This course assumes that attendees have a general understanding of networking concepts and TCP/IP protocols, as well as a strong grasp of DNS, DHCP and IPv4 addressing. Students should also have completed the BlueCat Integrity Fundamentals course prior to taking this course.

COURSE VENUES

Your staff can attend **BlueCat Security and Advanced Configuration** at your facilities or join one of our BlueCat-hosted on-site instructor-led classes. You can also take our virtual instructor-led course. Successful completion of this course includes access to the BlueCat Advanced Certified Professional exam.

COURSE OBJECTIVES

Upon successful completion of the **BlueCat Security and Advanced Configuration** course, attendees are able to:

- Understand Ways in which BlueCat Secures DNS Components
- Use IPv4 Modeling Tools to Manipulate the IPv4 Address Space
- Use Best Practices to Further Secure Your BlueCat Systems
- Understand DNS Architectures
- Configure DNS Query Logging and DNS Logging Channels

- Enhance TSIG Security for Zone Transfers
- Configure DNSSEC Signed Zones and Validating Resolvers
- Configure Response Rate Limiting to Mitigate Denial of Service Attacks
- Configure DNS Threat Protection to Help Prevent DNS Redirection to Malicious Sites

MODULE 1: SECURING ADDRESS MANAGER

- User Account Security
- Configure HTTPS Support

MODULE 2: IPV4 MODELING TOOLS

- Working with Various IPv4 Modeling Tools

MODULE 3: SECURING DNS

- Goals of DNS Security
- Secure the Host Platform
- Secure the DNS Software

MODULE 4: DNS SECURE ARCHITECTURES

- DNS Roles and Responsibilities
- Understand the DNS Four Quadrant Architecture

MODULE 5: DNS ZONE TRANSFERS

- Securing Zone Transfers
- Using Transaction Signature Keys (TSIG)

MODULE 6: DNS LOGGING

- Configure Query Logging
- Configure Logging Channels

MODULE 7: UNDERSTANDING CACHE POISONING

- Securing Zone Transfers
- Using Transaction Signature Keys (TSIG)

MODULE 8: DNSSEC

- What Does DNSSEC Do For You?
- Understand DNSSEC Components
- Configure DNSSEC Policies
- Sign Forward and Reverse DNS Zones
- Understand Key Management including Emergency Key Rollovers
- Configure a Validating Server

MODULE 9: DNS DDOS ATTACKS

- Understand and Mitigate DNS DDoS Attacks
- Understand Response Rate Limiting

MODULE 10: DNSSEC

- What is DNS Threat Protection?
- Configure DNS Threat Protection and Response Policy (RPZ) zones

Get Started Today

To inquire about our course schedules and to obtain more information about our training courses.

Email learn@bluecatnetworks.com or
Visit https://www.bluecatnetworks.com/training/