



Securing Critical Information Infrastructures

## Training Course – Addressing Zero-Day Attacks with Netflow and CS-MARS

Length – 4 Hours

---

### Course Description

This course will train the students to use Netflow with the CS-MARS to create baselines of network traffic. This can be used to detect attacks using anomaly detection, or unexpected changes in the network. Students will also learn how to deploy BGP based routing to divert suspect traffic to honeypots within the network. The goal of this class is enable the students to be able to use CS-MARS to deal with Zero-Day attacks.

---

### Course Outline

- Detailed description of netflow?
  - Zero-Day attacks versus normal vulnerabilities
  - How to use anomaly detection using CS-MARS
  - Configuring netflow devices and setting up Netflow based event rules
  - Creating honeypots using BGP routing
  - Dealing with internal bot-nets and infected users
  - Deploying honeypots within the network
- 

For more information on this or any other Lofty Perch training, contact us at [training@loftyperch.com](mailto:training@loftyperch.com)