Cyber Threat Detection and Incident Response Training

Data Sheet: Symantec Education Services

Overview of threat landscape

The threat landscape continues to evolve; cybercrime remains rampant. Technologies that promise greater productivity and convenience, such as mobile devices, file-sharing applications and cloud-based services, are under attack. Last year, a 93 percent increase in mobile vulnerabilities accompanied the increased use of mobile devices; and both mobile use and mobile vulnerabilities are expected to rise. In addition, employee mistakes and negligence continue to be a significant cause of data breach incidents, while criminal attacks are the second top cause of the data breaches, and growing increasingly stealthy and more sophisticated.

Symantec blocked over 5.5 billion malware attacks in 2011, an 81 percent increase over 2010.

Here is a snapshot of the 2011 threat landscape:

• Web based attacks increased by 36 percent with over 4,500 new attacks each day.

• 403 million new variants of malware were created in 2011, a 41 percent increase over 2010.

• 39 percent of malware attacks via email used a link to a web page.

• The number of targeted attacks increased from 77 per day in 2010 to 82 per day in 2011.

Targeted threats are not limited to the Enterprise. 50 percent of attacks focused on companies with fewer than 2500 employees and 18 percent on organizations with less than 250. No one is immune. Targeted attacks are a risk for businesses of all sizes.

Attackers’ motivations and backgrounds vary widely. Criminals might attack companies for financial gain, stealing valuable customer or employee data. Unscrupulous competitors might use targeted attacks as part of a longer-term campaign of espionage, typically targeting high value intellectual property or other industry and government secrets.

Regardless of motivation, the costs are high. The cost includes not just the fines and penalties but also the impact to brand and reputation, loss of customer goodwill, revenue, time and productivity. Based on the Ponemon Institute’s Annual Study on Cost of a Data Breach, the average company cost per breach in 2011 was $5.5M, and the cost per record was $194.

Considering the prevalence of attacks and the cost of a data breach, organizations of every size and type need to be prepared for the next cyber-attack.

Course Overview

Symantec’s Cyber Threat Detection and Incident Response Training provides the IT professional with cyber-defense theory, tools and response. The course covers how to think about and analyze network security, methods for detecting intrusion/malware, as well as incident response and event handling activities. This is an instructor-led course with practical hands-on exercises that enable you to test your new skill sets and use them in a working environment. You will learn:

• to identify common web threats and how to defend against them;

• the incident management phases and how to handle incident response and recovery;

• to understand incident and forensic readiness, including event handling and forensic analysis.

The training can also be tailored to meet your specific needs.

1 Symantec Internet Security Threat Report, vol. 17
Why Symantec?
Symantec, the world leader in security and data loss prevention, maintains some of the most comprehensive sources of Internet threat data in the world.
Spam, phishing and malware data is captured through a system of more than 5 million decoy accounts. With Response Centers located throughout the world, the Symantec Security Technology and Response (STAR) organization monitors malicious code reports from more than 130 million systems across the Internet, and receives data from 240,000 network sensors in more than 200 countries.
Trusted by over 25 percent of the Fortune 100, the Symantec team uses this vast intelligence to develop and deliver the world’s most comprehensive security protection.
As a recognized global leader in security intelligence and security training, Symantec helps organizations understand the threat landscape, detect malware and intrusion, and learn to effectively respond to such incidents. This course was developed by professionals with backgrounds in instructional design and security best practices, and leverages Symantec’s vast security database and expertise to give you the essentials necessary to minimize the cyber-security risk to your business.

More Information
Visit our website
www.symantec.com/training

To speak with a Product Specialist in the U.S.
Call toll-free 1 (800) 327-2232 (option 4) or in Canada at (416) 774-0045, or Email:
americas_education@symantec.com

To speak with a Product Specialist outside the U.S.
For specific country offices and contact numbers, please visit our website. Email: Europe, Middle East & Africa - edu_sales_emea@symantec.com. Asia, Pacific, Japan - apj_education@symantec.com

About Symantec
Symantec protects the world’s information, and is a global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device, to the enterprise data center, to cloud-based systems. Our world-renowned expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.

Symantec World Headquarters
350 Ellis St. | Mountain View, CA 94043 USA
+1 (650) 527 8000 | 1 (800) 721 3934
www.symantec.com