Cisco Inaugurates Cyber Range Lab in India

The Cyber Range Lab to simulate real-world cyber-attacks and incidents and cyber-defence tactics

Deepening its commitment to enhancing cybersecurity in India, Cisco India has inaugurated its Cyber Range Lab in Gurgaon, India. The Cisco® Cyber Range Lab aims to provide highly specialized technical training workshops to help security staff build the skills and experience necessary to combat new-age risks. Dr. Gulshan Rai, National Cyber Security Coordinator, Government of India, inaugurated the Cyber Range Lab in the presence of Dinesh Malkani, President, Cisco India and SAARC at the Cisco India Summit 2017.

The demand for cybersecurity experts has grown three times faster than any other IT job role, and training a cybersecurity workforce is a priority for many organizations. As per a Cisco report, there are more than 1 million unfulfilled security jobs worldwide currently, and the lack of skills and training hinders organizations from deploying advanced security. Thirty-one percent of organisations in India (24% globally) believe that a high requirement of various certifications is a barrier, and 29% of organisations in India consider their workload too heavy to take on new responsibilities on cyber security (23% globally), according to a Cisco study.

As cybersecurity threats have become more complex, targeted and persistent, modern cyber defences require proactive security operations run by highly trained staff with the experience and expertise to detect and disrupt sophisticated threats. Cisco® Cyber Range will immerse people in simulated real-world cyber attacks to train them on how to properly prepare for, respond to, and manage a broad variety of threats. This experience can be leveraged by companies, academicians, customers and government and their security teams.

Cisco Cyber Range Lab will use 200-500 different types of malware, ransomware and 100 attack cases to deliver realistic cyber-attack experiences. The facility can be accessed virtually from any part of the world and will be a living lab of technical knowledge for network security and how to mitigate cyber attacks.

As part of the Cyber Range experience, Cisco has designed real-world scenarios to help clients experience, defend against and shut down cyber attacks. The scenarios will also help train organizations with the necessary steps required to respond quickly in the wake of an incident, right from addressing a basic threat to a highly sophisticated one, monitoring and analysing malware infections and providing actionable information and intelligence to customers.

The Cisco Cyber Range Lab brings together Cisco security experts and its partners to offer a comprehensive integrated services portfolio, which includes:

- Cyber Range workshops of 3-5 days of intensive real-life experience reacting to and defending against rudimentary and complex cyber attacks at any location.
- Cyber Range subscriptions, which offer advance threat intelligence reports and help simulate customers' network environment in the lab to monitor for latest threats. As part of this lab, dedicated security experts will offer security consultancy services to customers.
- Assistance in re-creating similar cyber range labs at customers' premises and provide threat intelligence updates via subscription.
- The lab will also enable customers to tap into a pool of resources such as security specialists and test engineers at Cisco. Cisco security experts will work closely with organisations to understand their business goals, and security challenges and offer test runs on proposed cybersecurity solution/infrastructure.

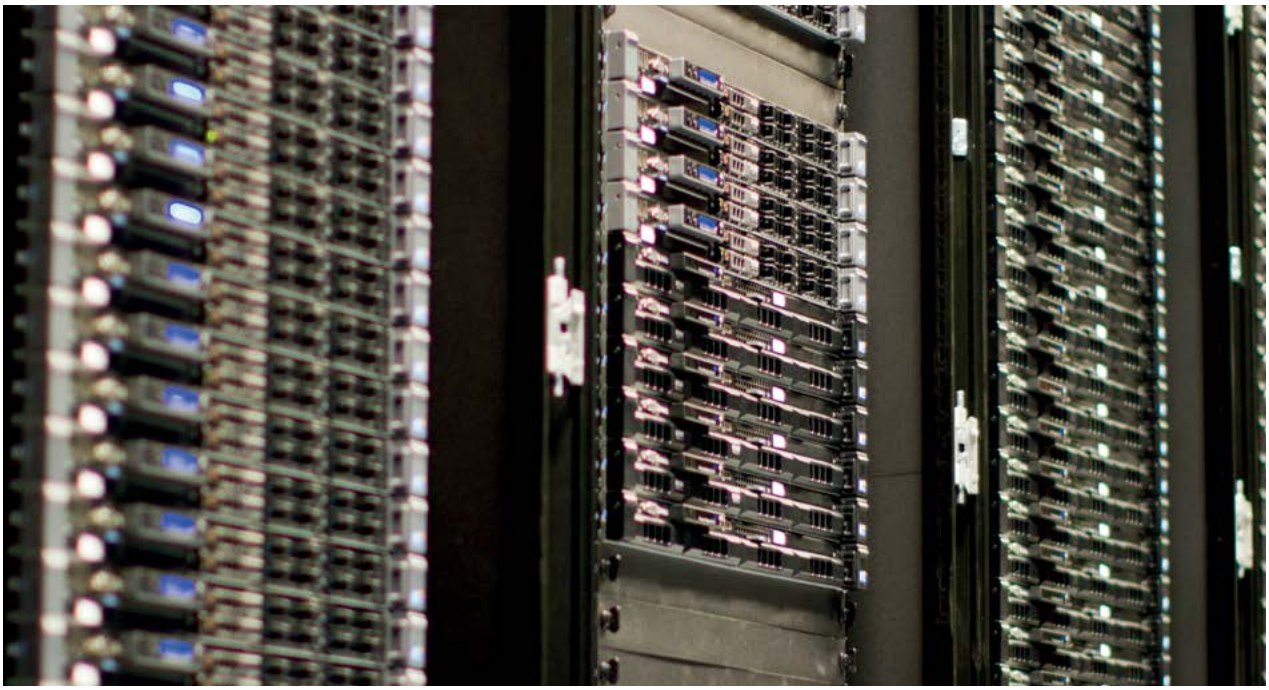

Photo: © Victorgrigas

The launch of the Cyber Range Lab is part of cybersecurity initiatives announced by Cisco India during December 2016. In addition to the Cyber Range Lab, Cisco had launched a Security Operations Center (SOC) in Pune to provide a broad range of services, from monitoring and management to comprehensive threat solutions and hosted security that can be customized to meet customer/partner needs. With India as the fourth location in addition to Poland, the U.S. and Japan, this structure allows Cisco to provide a 24-hour service for customers and partners regardless of time zone, using a "follow the sun" model. Also launched in December 2016, the Cisco India Security & Trust Organization (STO) - India works with public and private sector customers to help analyze their infrastructure, understand cyber risks, identify and mitigate vulnerabilities, and assist in building networks on a foundation of highly secure, resilient, and trustworthy products.

Dynamic changes in the technology landscape, led by digitization, are creating opportunities for cyber criminals. Advance threat intelligence and faster time to detection is critical to constrain attackers' operational space and minimize damage from intrusions. As per the Cisco Cybersecurity Report 2017 Cisco has reduced "Time to Detection" to six hours. The report also states that over one-third of organizations that experienced a breach in 2016 reported substantial customer, opportunity and revenue losses of more than 20 percent.

To help increase the pool of talent with critical cybersecurity proficiency, Cisco announced a $10 million Cybersecurity Scholarship globally in June 2016. The Cisco Networking Academy® program has enhanced its security portfolio with a new Cybersecurity Essentials course. In India, the Cisco Networking Academy program has trained 122,000 students and is committed to training an additional 250,000 students by 2020.

For more information: https://newsroom.cisco.com

Cisco (NASDAQ: CSCO) is the worldwide technology leader that has been making the Internet work since 1984. Our people, products, and partners help society securely connect and seize tomorrow's digital opportunity today. Discover more at newsroom.cisco.com and follow us on Twitter at @Cisco.

Used with the permission of http://thenetwork.cisco.com/.