



Your Intelligence need
analysis




INTRODUCING
DG THREAT
INTELLIGENCE
& MANAGEMENT
TRAINING PROGRAM

Specialized program from beginning to advanced levels. Learn all the fundamental concepts with hands-on instructions that will let you combat the hackers.

A SEAT OF LEARNING THAT IS MORE THAN JUST A PLACE OF ACADEMIC VALUE

Knowledge and success come hand in hand. When people seek knowledge, they often aim to thrive and prosper, whatever their goals.

We deliver knowledge and technical know-how in a different way. Easy to follow, easy to understand and easy to put into practice. Attributes that make our students stand apart from others.

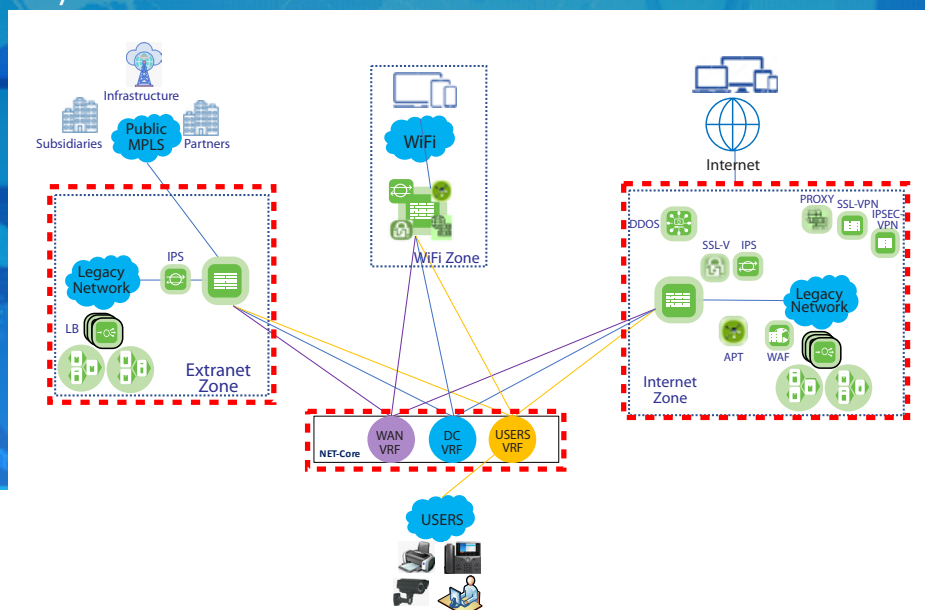


DG Academy is the place to realize such aspirations. Here, students and industry professionals can get first rate information and technological know-how focused on IT, telecom and cybersecurity.

LEARN, PRACTICE, REPEAT. ANYWHERE. AND ON ANY DEVICE.

DGACADEMY training material which includes lecture and 'Hands on Lab' (HOL) manuals are available online through secure LMS in electronic format. All enrolled students and industry professionals are entitled to have free access to these course materials for one year. All training contents are protected by copy rights and intellectual property rights.

DGACADEMY HOL is a state-of-the-art secure cloud hosted infrastructure where students and industry professionals practice course lab manuals, from anywhere, on any device and on any scheduled time frames.



‘INNOVATION’
 IS OUR DEFINING CHARACTERISTIC.
 AND IT MAKES ALL THE DIFFERENCE.

Course Name	DG Cyber Threat Intelligence & Management
Course Code	DGSEC601
Outcome	Threat Intelligence, Vulnerability Assessment
Course Outline	<p>Module 1: Cyber Security Threat Management, Intelligence and hunting</p> <p>Module 2: Cyber Security Incident & Response Management</p> <p>Module 3: Cyber Security Vulnerability Management</p> <p>Module 4: Cyber War teams: Red, Blue and Green: Understanding, Roles and Responsibilities</p> <p>Module 5: Splunk Architecture</p> <p>Module 6: Design and Implement Splunk Enterprise Infrastructure</p> <p>Module 7: Install, Configure and Manage (ICM) Splunk Enterprise and Splunk Enterprise Security</p> <p>Module 8: Splunk Enterprise Security for Security Operation Center (SOC)</p> <p>Module 9: Splunk Security Orchestration, Automation and Response (SOAR)</p> <p>Module 10: Splunk Enterprise System Administration</p>
Practice Lab	Full access on DG-HOL Hand on Labs to practice all real-world scenarios taught by lectures
Length	60 hours
Days	4 Tracks – Full Day, Evening, Weekend, Customize
Price	3000 US\$ - Promotional and Group discount is available on request
Level	Beginners to Advance
Language	English, Arabic, Urdu, Hindi
Course Type	Instructor-led onsite and online, recorded, on-demand
Associated Certificate	DG Certified Cyber Threat Assurance Professional – DGCP-SEC601
Target Audience	<ul style="list-style-type: none"> • Information Security Analyst/Administrator. • Vulnerability Management Analyst/Engineer/Consultant. • Incident and Response Managers and Engineers. • Threat Intelligence and RISK Managers and Engineers. • Application Security Analyst. • SOC Engineer. • Splunk Administrator. • Splunk Architects. • Data Analysts. • Professionals who are looking to understand how to use Splunk and its concepts. • Professional looking to clear their relevant Splunk certification exams.



Welcome to DG ACADEMY «DG Cyber Threat Intelligence & Management Training Program: From Beginners to Advance».

The Cyber Security Threat Intelligence & Management Training Program will help you acquire the skills needed to find out who is behind an attack, what the specific threat group is, the nation from which the attack is being launched, as well as techniques being used to launch this attack.

You will know how to take a small piece of malware, find out who is responsible for launching it, the threat actor location and also how to take down that threat actor, with the support of your local law enforcement.

Gain in-depth knowledge of security threats, attacks, vulnerabilities, attacker's behaviors, cyber kill chain, SOC processes, procedures, technologies, and automation workflows and Able to identify attacker techniques, tactics, and procedures (TTP) to investigate on indicators of compromise to defend your organization from future attacks.

Gain knowledge of Incident Response Methodology, processes and in-depth knowledge on how to integrate Threat Intelligence processes with Incident Response processes using HIVE and learn how to automate them as a single workflow.

Next, you'll learn about the Splunk Threat Intelligence Framework and how to use it in order to enrich your data. Finally, you'll learn how to configure the threat intelligence sources and parse the data in order to get what you need for Splunk Enterprise Security.

As with all DG Training Program, lessons include practical exercises based on real cases handled by the DG TIM team. This approach was chosen to ensure that participants can immediately apply what they learn in their day-to-day activities.

Join Us! Get the opportunity to learn from this comprehensive course.

DG THREAT INTELLIGENCE & MANAGEMENT TRAINING PROGRAM

Cybersecurity Threat Management, Intelligence and hunting

- **Fundamentals of threat Management, Importance of threat intelligence in SIEM, and incident response.**
- **Cyber threat intelligence Strategic and operational Management.**
- **Threat intelligence data collection and acquisition.**
- **Intelligence applications and intrusion analysis, attribution, collecting and storing data sets.**
- **Creating effective threat intelligence reports.**

Threat intelligence enables us to make faster, more informed, data-backed security decisions and change their behavior from reactive to proactive in the fight against threat actors.

The main objective of Threat and Risk Assessment is to protect organizations against liabilities by identifying and understanding the various risks facing the client property and community.

This course is designed to teach students all required core understanding skills with hands-on labs practice to encounter these threats.

Module 1

Lab Scenarios

- No Hands-on Lab is associated.
- Real world case studies will be discussed.
- Student will be asked to demonstrate their understanding by writing artifacts and communication flow.

JOB ROLE

- VAPT Expert
- Application Security Analyst
- Information Security
- Risk/Vulnerability Analyst
- Blue Team Engineer\Expert

INDUSTRY ALIGNMENT



DG THREAT INTELLIGENCE & MANAGEMENT TRAINING PROGRAM

Cyber Security Incident & Response Management

- **Understanding of Security Incident & Response.**
- **Incident Response Policy, Plan, and Procedure Creation.**
- **Incident Response Team Structure.**
- **Handling an Incident.**

The main objective of Cyber Incident Response course will give students an understanding of how incidents are responded to at a high level, as well as allow them to build important technical skills through the hands-on labs and projects.

Module 2

Lab Scenarios

- Install Configure and Manage (ICM) Incident Response (IR)& (ICM) Vulnerability Management Software.
- Practice Labs to have full hands-on experience on how to install, configure and manage Incident Response (IR) Software.
- Demonstrating real-world scenarios.

JOB ROLE

- Security Cyber Incident Response Specialist
- Cyber Security Incident Response, Analyst
- Information Security Officer
- Security Incident Response Engineer

INDUSTRY ALIGNMENT



DG THREAT INTELLIGENCE & MANAGEMENT TRAINING PROGRAM

Cyber Security Vulnerability Management

- **Understanding of Vulnerability Management.**
- **Vulnerability Management Tool, Implementation and Integration.**
- **VAPT use cases with real world examples.**

The main objective of this course is to teach security vulnerability assessment fundamentals and in-depth coverage of the Vulnerability Assessment Framework, , VA tools by implement a transformational security vulnerability assessment program, Vulnerability, patch, and configuration management are the oldest security functions and student will be master in this domain.

Module 3

Lab Scenarios

- Install Configure and Manage (ICM) Vulnerability Management Software.
- Practice Labs to have full hands-on experience on how to install, configure and manage Vulnerability Management Software.
- Demonstrating real-world scenarios.

JOB ROLE

- VAPT Expert
- Application Security Analyst
- Information Security
- Risk/Vulnerability Analyst
- Blue Team Engineer\Expert

INDUSTRY ALIGNMENT



DG THREAT INTELLIGENCE & MANAGEMENT TRAINING PROGRAM

Cyber War teams: Red and Blue : Understanding, Roles and Responsibilities

- **Red Team with other Security Groups.**
- **Rules of Engagement.**
- **Blue Team in Defensive Security.**
- **Threat Intelligence and Responders.**

Both red teams and blue teams work toward improving an organization's security, but they do so differently. A red team plays the role of the attacker by trying to find vulnerabilities and break through cybersecurity defenses. A blue team defends against attacks and responds to incidents when they occur.

Student will be learning and practicing both side of the games.

Module 4

Lab Scenarios

- No Hands-on Lab is associated.
- Real world case studies will be discussed.
- Student will be asked to demonstrate their understanding by writing artifacts and communication flow.

JOB ROLE

- CISO/Manager Cyber Security
- IT Incident Responder

INDUSTRY ALIGNMENT



DG THREAT INTELLIGENCE & MANAGEMENT TRAINING PROGRAM

Splunk Architecture

- **Splunk Data Flow.**
- **Splunk Components.**
- **Splunk Topologies.**
- **Splunk Stages in the Data Pipeline.**

The main objective of this course is to teach Establish a thorough understanding of Splunk software and solution architecture, Deployment Methodology and best practices for planning, data collection and sizing a distributed deployment. Manage and troubleshoot standard deployments with indexer and search head clustering.

Module 5

Lab Scenarios

- No Hands-on Lab is associated.
- Real world case studies will be discussed.
- Student will be asked to demonstrate their understanding by writing artifacts and communication flow.

JOB ROLE

- Splunk architect
- Splunk Consultant

INDUSTRY ALIGNMENT



DG THREAT INTELLIGENCE & MANAGEMENT TRAINING PROGRAM

Design and Implement Splunk Enterprise Infrastructure

- **Understanding of Real world client requirement and design Splunk Deployment.**
- **Splunk Integration with other system and solution to provide end to end visibility and threat hunting.**
- **Splunk communication matrix.**
- **Component Placement use cases – WAN, Remote branches and DR Failover scenarios.**

The main objective of this course is to teach design principle of any enterprise Splunk project which includes HLD\LLD and Architecture design documents, communication matrix, Splunk deployment methodology and much more.

Module 6

Lab Scenarios

- No Hands-on Lab is associated.
- Real world case studies will be discussed.
- Student will be asked to demonstrate their understanding by writing artifacts and communication flow.

JOB ROLE

- Splunk Solution Architect
- Splunk Designer

INDUSTRY ALIGNMENT



DG THREAT INTELLIGENCE & MANAGEMENT TRAINING PROGRAM

Install, Configure and Manage (ICM) Splunk Enterprise and Splunk Enterprise Security

- **Splunk deployment, Splunk clusters and License management.**
- **Splunk apps and configuration files.**
- **Users, roles, and authentication.**
- **Distributed search.**
- **Deploy forwarders with Forwarder Management.**

The main objective of this course is to prepares architects and systems administrators to install and configure Splunk Enterprise Security (ES). It covers ES event processing and normalization, deployment requirements, technology add-ons, dashboard dependencies, data models, managing risk, and customizing threat intelligence.

Module 7

Lab Scenarios

- Practice Labs to have full hands-on experience on how to install, configure and manage Splunk Enterprise and Splunk Enterprise Security.
- Demonstrating real-world scenarios.

JOB ROLE

- Splunk Operations Engineer
- Splunk SIEM Engineer

INDUSTRY ALIGNMENT



DG THREAT INTELLIGENCE & MANAGEMENT TRAINING PROGRAM

Splunk Enterprise Security for Security Operation Center (SOC)

Module 8

Lab Scenarios

- Practice Labs to have full hands-on experience on SOC use cases with real-world complex scenarios.

JOB ROLE

- Splunk Operations Engineer
- Splunk Operations Engineer
- Info Security Analyst-Splunk
- Splunk SIEM Engineer

INDUSTRY ALIGNMENT



- **Creating an incident workflow in Splunk Enterprise Security.**
- **Onboarding data to Splunk Enterprise Security.**
- **Sending Splunk Observability events as Alert Actions from Splunk Enterprise Security.**
- **Using threat intelligence in Splunk Enterprise Security.**
- **Implementing risk-based alerting.**
- **Splunk Enterprise Security with Intelligence Management.**
- **Using the Splunk Enterprise Security assets and identities framework.**

This course will build student technical competence such as network topologies, identify threats, possible breaches & collect audit logs for security and compliance. what a security operations center is?, formulate various mitigation strategies, phishing & firewalls, intrusion detection and prevention systems. capability in information security attack vectors, phishing techniques, You will be able to conduct investigations and provide evidence.

DG THREAT INTELLIGENCE & MANAGEMENT TRAINING PROGRAM

Splunk Security Orchestration, Automation and Response (SOAR)

- **Install, Configure and Manage (ICM) Splunk SOAR.**
- **Managing cases in SOAR.**
- **SOAR Indicator Enrichment Playbook and Intelligence Management.**
- **Responding to security incidents using SOAR.**

This course Security orchestration, automation, and response (SOAR) primarily focuses on threat management, security operations automation, and security incident responses. SOAR platforms can instantly assess, detect, intervene, or search through incidents and processes without the consistent need for human interaction.

Module 9

Lab Scenarios

- Practice Labs to have full hands-on experience on how to install, configure and manage Splunk Security Orchestration, Automation and Response (SOAR).
- Demonstrating real-world complex scenarios.

JOB ROLE

- Cyber Security Automation Phantom/Splunk SOAR Engineer
- Security Orchestration, Automation, and Response (SOAR) Splunk Engineer Level II
- Splunk Cybersecurity SOAR, Senior

INDUSTRY ALIGNMENT



DG THREAT INTELLIGENCE & MANAGEMENT TRAINING PROGRAM

Splunk Enterprise System Administration

Module 10

- **Introduction to Data Administration.**
- **Working with Time.**
- **Statistical Processing.**
- **Comparing Values.**
- **Result Modification.**
- **Correlation Analysis.**
- **Creating Knowledge Objects.**
- **Creating Field Extractions.**
- **Data Models.**
- **Introduction to Dashboards.**
- **Dynamic Dashboards.**

This course is designed to teach fundamental skills of Splunk Deployment, Splunk Apps, system administration on Enterprise environment, knowledge of Splunk license manager, indexers and search heads. It covers configuration, management, and monitoring core Splunk Enterprise components.

Lab Scenarios

- Practice Labs to have full hands-on experience on Splunk Enterprise System Administration use cases with real-world complex scenarios.

JOB ROLE

- Splunk Administrator
- Splunk Admin Engineer

INDUSTRY ALIGNMENT





Join our DG THREAT Intelligence & MANAGEMENT TRAINING PROGRAM

dgacademy.diginfo.net

A product of DIGINFO



Amber Estate, Main Shahrah-e-Faisal, Near Bloch Colony Flyover, Karachi 75350, Sindh, Pakistan. Tel : +92 21 34325505

Email : info@diginfo.net | www.diginfo.net | dgacademy.diginfo.net