ELYSIUM
ACADEMY

Milestone of Cognizance

Since 2007

VERSION 2.0

PROFESSIONAL

# COMPTIA-SECURITY+ (SY0-601)

ELYSIUM ACADEMY

COMPTIA-SECURITY+ (SY0-601)

**SR. CODE**

EAPL/PROF/PRTC20

**COURSE CODE**

EAPCS

**SUB CATEGORY**

CYBER SECURITY AND NETWORKING

| TOTAL DURATION | THEORY TAKEN | PRACTICAL TAKEN |
|---|---|---|
| 90 HOURS | 20 HOURS | 70 HOURS |

ELYSIUM ACADEMY COMPTIA-SECURITY+ (SY0-601)

ELYSIUM ACADEMY®
Milestone of Cognizance

Since 2007

## COURSE DESCRIPTION

The CompTIA Security+ (SY0-601) Course is a vendor-neutral course that validates the fundamental security concepts and skills required to perform core security functions and pursue an IT security career. It is designed for IT professionals who are new to security or who want to expand their knowledge and skills in this area.

## COURSE GOALS

- Understand the fundamentals of security concepts and technologies.
- Apply security best practices to protect systems and data
- Investigate and respond to security incidents
- Manage security risks

## FUTURE SCOPE

- You can become a Security Administrator/Engineer, Systems Administrator, DevOps / Software Developer, IT Auditors/IT Project Manager.
- Become an effective security technician in a business environment

ELYSIUM ACADEMY®
Milestone of Cognizance

Since 2007

01
CHAPTER

# 1. DIFFERENT TYPES OF SOCIAL ENGINEERING TECHNIQUES

30 MINS

01 HRS

01. Phishing
02. Smishing
03. Vishing
04. Spam
05. Spam over instant messaging (SPIM)
06. Spear phishing
07. Dumpster diving
08. Shoulder surfing
09. Pharming
10. Tailgating
11. Eliciting information
12. Whaling
13. Prepending
14. Identity fraud
15. Invoice scams
16. Credential harvesting
17. Reconnaissance
18. Hoax
19. Impersonation

20. Watering hole attack

21. Typosquatting

22. Pretexting

23. Influence campaigns

    a. Hybrid warfare

    b. Social media

24. Principles (reasons for effectiveness)

    a. Authority

    b. Intimidation

    c. Consensus

    d. Scarcity

    e. Familiarity

    f. Trust

    g. Urgency

02
CHAPTER

## 2. ANALYZE POTENTIAL INDICATORS TO DETERMINE THE TYPE OF ATTACK

30 MINS

2.5 HRS

1. Malware

    a. Ransomware

    b. Trojans

    c. Worms

    d. Potentially unwanted programs (PUPs)

    e. Fileless virus

f. Command and control
g. Bots
h. Cryptomalware
i. Logic bombs
j. Spyware
k. Keyloggers
l. Remote access Trojan (RAT)
m. Rootkit
n. Backdoor

## 2. Password attacks

a. Spraying
b. Dictionary
c. Brute force
d. Offline
e. Online
f. Rainbow table
g. Plaintext/unencrypted

## 3. Physical attacks

a. Malicious Universal
b. Serial Bus (USB) cable
c. Malicious flash drive
d. Card cloning
e. Skimming

## 4. Adversarial artificial intelligence (AI)

a. Tainted training data for machine learning (ML)
b. Security of machine learning algorithms

5. Supply-chain attacks
6. Cloud-based vs. on-premises attacks
7. Cryptographic attacks
   a. Birthday
   b. Collision
   c. Downgrade

03
CHAPTER

# ANALYZE POTENTIAL INDICATORS APPLICATION ATTACKS

30 MINS
2.5 HRS

01. Privilege escalation
02. Cross-site scripting
03. Injections
    a. Structured query language (SQL)
    b. Dynamic-link library (DLL)
    c. Lightweight Directory
    d. Access Protocol (LDAP)
    e. Extensible Markup Language (XML)
04. Pointer/object dereference
05. Directory traversal
06. Buffer overflows
07. Race conditions
    a. Time of check/time of use(XML)
08. Error handling
09. Improper input handling
10. Replay attack
    a. Session replays

11. Integer overflow
12. Request forgeries
    a. Server-side
    b. Cross-site
13. Application programming interface (API) attacks
14. Resource exhaustion
15. Memory leak
16. Secure Sockets Layer (SSL) stripping
17. Driver manipulation
    a. Shimming
    b. Refactoring
18. Pass the hash

04 CHAPTER

## ANALYZE POTENTIAL INDICATORS NETWORK ATTACKS

30 MINS

2.5 HRS

01. Wireless
    a. Evil twin
    b. Rogue access point
    c. Bluesnarfing
    d. Bluejacking
    e. Disassociation
    e. Jamming

g. Radio frequency identification (RFID)

h. Near-field communication (NFC)

i. Initialization vector (IV)

## O2. On-path attack (previously known as man-in-the-middle attack/ man-in-the-browser attack)

## O3. Layer 2 attacks

a. Address Resolution

b. Protocol (ARP) poisoning

c. Media access control (MAC) flooding

d. MAC cloning

## O4. Domain name system (DNS)

a. Domain hijacking

b. DNS poisoning

c. Uniform Resource

d. Locator (URL) redirection

e. Domain reputation

## O5. Distributed denial-of-service (DDoS)

a. Network

b. Application

c. Operational technology (OT)

## O6. Malicious code or script execution

a. PowerShell

b. Python

c. Bash

d. Macros

e. Visual Basic for Applications (VBA)

ELYSIUM ACADEMY®
Milestone of Cognizance

Since 2007

05
CHAPTER

# DIFFERENT THREAT ACTORS, VECTORS, AND INTELLIGENCE SOURCES

30 MINS

2.5 HRS

## 01. Actors and threats

a. Advanced persistent threat (APT)

b. Insider threats

c. State actors

d. Hacktivists

e. Script kiddies

f. Criminal syndicates

g. Hackers

h. Authorized

i. Unauthorized

j. Semi-authorized

k. Shadow IT

l. Competitors

## 02. Attributes of actors

a. Internal/external

b. Level of sophistication/capability

c. Resources/funding

d. Intent/motivation

## O3. Vectors

a. Direct access
b. Wireless
c. Email
d. Supply chain
e. Social media
f. Removable media
g. Cloud

## O4. Threat intelligence sources

a. Open-source intelligence (OSINT)
b. Closed/proprietary
c. Vulnerability databases
d. Public/private information-
e. Sharing centers
f. Dark web
g. Indicators of compromise
h. Automated Indicator Sharing (AIS)
i. Structured Threat Information eXpression (STIX)/Trusted Automated eXchange of Intelligence Information (TAXII)
j. Predictive analysis
k. Threat maps
l. File/code repositories

## O5. Research sources

a. Vendor websites
b. Vulnerability feeds
c. Conferences
d. Academic journals
e. Request for comments (RFC)
f. Local industry groups
g. Social media
h. Threat feeds
i. Adversary tactics, techniques, and procedures (TTP)

06
CHAPTER

# VARIOUS TYPES OF VULNERABILITIES.

30 MINS
2.5 HRS

O1. Cloud-based vs. on-premises vulnerabilities
O2. Zero-day
O3. Weak configurations

a. Open permissions
b. Unsecure root accounts
c. Errors
d. Weak encryption
e. Unsecure protocols
f. Default settings
g. Open ports and services

## O4. Third-party risks

a. Vendor management

c. System integration

d. Lack of vendor support

e. Supply chain

f. Outsourced code development

g. Data storage

## O5. Improper or weak patch management

a. Firmware

b. Operating system (OS)

c. Applications

## O6. Legacy platforms

## O7. Impacts

a. Data loss

b. Data breaches

c. Data exfiltration

d. Identity theft

e. Financial

f. Reputation

g. Availability loss

ELYSIUM ACADEMY®
Milestone of Cognizance

Since 2007

07
CHAPTER

# SECURITY ASSESSMENTS

30 MINS

2.5 HRS

## 01. Threat hunting

a. Intelligence fusion

b. Threat feeds

c. Advisories and bulletins

d. Maneuver

## 02. Vulnerability scans

a. False positives

b. False negatives

c. Log reviews

d. Credentialed vs. non-credentialed

e. Intrusive vs. non-intrusive

f. Application

g. Web application

h. Network

i. Common Vulnerabilities and Exposures (CVE)/Common Vulnerability Scoring System (CVSS)

j. Configuration review

## 03. Syslog/Security information and event management (SIEM)

a. Review reports

b. Packet capture

c. Data inputs

d. User behavior analysis

e. Sentiment analysis

f. Security monitoring

g. Log aggregation

h. Log collectors

### 04. Security orchestration, automation, and response (SOAR)

08
CHAPTER

## PENETRATION TESTING

30 MINS

1.5 HRS

### 01. Penetration testing

a. Known environment

b. Unknown environment

c. Partially known environment

d. Rules of engagement

e. Lateral movement

f. Privilege escalation

g. Persistence

h. Cleanup

i. Bug bounty

j. Pivoting

### 02. Passive and active reconnaissance

a. Drones

b. War flying

c. War driving

d. Footprinting

e. OSINT

ELYSIUM ACADEMY®
Milestone of Cognizance

Since 2007

## O3. Exercise types

a. Red-team

b. Blue-team

c. White-team

d. Purple-team

09
CHAPTER

# IMPORTANCE OF SECURITY CONCEPTS

30 MINS

2.5 HRS

## O1. Configuration management

a. Diagrams

b. Baseline configuration

c. Standard naming conventions

d. Internet protocol (IP) schema

## O2. Data sovereignty

## O3. Data protection

a. Data loss prevention (DLP)

b. Masking

c. Encryption

d. At rest

e. In transit/motion

f. In processing

g. Tokenization

h. Rights management

O4. Geographical considerations
O5. Response and recovery controls
O6. Secure Sockets Layer (SSL)/ Transport Layer Security (TLS) inspection
O7. Hashing
O8. API considerations
O9. Site resiliency
   a. Hot site
   b. Cold site
   c. Warm site
10. Deception and disruption
   a. Honeypots
   b. Honeyfiles
   c. Honeynets
   d. Fake telemetry
   e. DNS sinkhole

10 CHAPTER

## CLOUD COMPUTING CONCEPTS

30 MINS
1.5 HRS

O1. Cloud models
   a. Infrastructure as a service (IaaS)
   b. Platform as a service (PaaS)
   c. Software as a service (SaaS)
   d. Anything as a service (XaaS)
   e. Public
   f. Community

- g. Private
- h. Hybrid

O2. Cloud service providers
O3. Managed service provider (MSP)/ managed security service provider (MSSP)
O4. On-premises vs. off-premises
O5. Fog computing
O6. Edge computing
O7. Thin client
O8. Containers
O9. Microservices/AP
10. Infrastructure as code

- a. Software-defined networking (SDN)
- b. Software-defined visibility (SDV)

11 . Serverless architecture
12.Services integration
13. Transit gateway
14. Virtualization

- a. Virtual machine (VM) sprawl avoidance
- b. VM escape protection

ELYSIUM ACADEMY®
Milestone of Cognizance

Since 2007

11

CHAPTER

# AUTOMATION CONCEPTS

30 MINS

1.5 HRS

## 01. Environment

a. Development

b. Test

c. Staging

d. Production

e. Quality assurance (QA)

## 02. Provisioning and deprovisioning

## 03. Integrity measurement

## 04. Secure coding techniques

a. Normalization

b. Stored procedures

c. Obfuscation/camouflage

d. Code reuse/dead code

e. Server-side vs. client-side execution and validation

f. Memory management

g. Use of third-party libraries and software development kits (SDKs)

h. Data exposure

## 05. Open Web Application Security Project (OWASP)

## 06. Software diversity

a. Compiler

b. Binary

ELYSIUM ACADEMY
Milestone of Cognizance

Since 2007

## O7. Automation/scripting

a. Automated courses of action

b. Continuous monitoring

c. Continuous validation

d. Continuous integration

e. Continuous delivery

f. Continuous deployment

## O8. Elasticity
## O9. Scalability
## 10. Version control

12 CHAPTER

# IAM CONCEPTS

30 MINS

2.5 HRS

## O1. Authentication methods

a. Directory services

b. Federation

c. Attestation

d. Technologies

e. Time-based one-time password (TOTP)

f. HMAC-based one-time password (HOTP)

g. Short message service (SMS)

h. Token key

- g. Private
- h. Hybrid

O2. Cloud service providers
O3. Managed service provider (MSP)/ managed security service provider (MSSP)
O4. On-premises vs. off-premises
O5. Fog computing
O6. Edge computing
O7. Thin client
O8. Containers
O9. Microservices/AP
10. Infrastructure as code

- a. Software-defined networking (SDN)
- b. Software-defined visibility (SDV)

11 . Serverless architecture
12.Services integration
13. Transit gateway
14. Virtualization

- a. Virtual machine (VM) sprawl avoidance
- b. VM escape protection

h. Something you exhibit

i. Someone you know

O4 · Authentication, authorization, and accounting (AAA)

O5. Cloud vs. on-premises requirements

13 CHAPTER

# IMPLEMENT CYBERSECURITY RESILIENCE

30 MINS

2.5 HRS

## O1. Redundancy

a. Geographic dispersal

b. Disk

c. Redundant array of inexpensive disks (RAID) levels

d. Multipath

e. Network

f. Load balancers

g. Network interface card (NIC) teaming

h. Power

i. Uninterruptible power supply (UPS)

j. Generator

k. Dual supply

l. Managed power distribution units (PDUs)

## O2 · Replication

- a. Storage area network
- b. VM

## O3 · On-premises vs. cloud

## O4 · Backup types

- a. Full
- b. Incremental
- c. Snapshot
- d. Differential
- e. Tape
- f. Disk
- g. Copy
- h. Network-attached storage (NAS)
- i. Storage area network
- j. Cloud
- k. Image
- l. Online vs. offline
- m. Offsite storage
- n. Distance considerations

## O5 · Non-persistence

- a. Revert to known state
- b. Last known-good configuration
- c. Live boot media

O6 · High availability

a. Scalability

O7 · Restoration order

O8. Diversity

a. Technologies

b. Vendors

c. Crypto

d. Controls

14 CHAPTER

# EMBEDDED AND SPECIALIZED SYSTEMS

30 MINS

2.5 HRS

O1. Embedded systems

a. Raspberry Pi

b. Field-programmable gate array (FPGA)

c. Arduino

O2. Supervisory control and data acquisition (SCADA)/industrial control system (ICS)

a. Facilities

b. Industrial

c. Manufacturing

d. Energy

e. Logistics

ELYSIUM ACADEMY®
Milestone of Cognizance

Since 2007

## O3 · Internet of Things (IoT)

a. Sensors

b. Smart devices

c. Wearables

d. Facility automation

e. Weak defaults

## O4 · Specialized

a. Medical systems

b. Vehicles

c. Aircraft

d. Smart meters

O5 · Voice over IP (VoIP)

O6. Heating, ventilation, air conditioning (HVAC)

O7. Drones

O8. Multifunction printer (MFP)

O9. Real-time operating system (RTOS)

10. Surveillance systems

11. System on chip (SoC)

12. Communication considerations

a. 5G

b. Narrow-band

c. Baseband radio

d. Subscriber identity module (SIM) cards

e. Zigbee

## 13 · Constraints

a. Power

b. Compute

c. Network

d. Crypto

e. Inability to patch

f. Authentication

g. Range

h. Cost

i. Implied trust

15 CHAPTER

# PHYSICAL SECURITY CONTROLS

30 MINS

2.5 HRS

O1. Bollards/barricades
O2. Access control vestibules
O3. Badges
O4. Alarms
O5. Signage
O6. Cameras

a. Motion recognition

b. Object detection

O7. Closed-circuit television (CCTV)
O8. Industrial camouflage
O9. Personnel

a.Guards

b. Robot sentries

c. Reception

d. Two-person integrity/control

10 · Locks

a. Biometrics

b. Electronic

c. Physical

d. Cable locks

11 · USB data blocker

12. Lighting

13. Fencing

14. Fire suppression

15. Sensors

a. Motion detection

b. Noise detection

c. Proximity reader

d. Moisture detection

e. Cards

f. Temperature

16 · Drones

17. Visitor logs

18. Faraday cages

19. Air gap

20. Screened subnet (previously known as demilitarized zone)

21. Protected cable distribution

22. Secure areas

a. Air gap
b. Vault
c. Safe
d. Hot aisle
e. Cold aisle

### 23 · Secure data destruction

a. Burning
b. Shredding
c. Pulping
d. Pulverizing
e. Degaussing
f. Third-party solutions

16 CHAPTER

## CRYPTOGRAPHIC CONCEPTS

30 MINS
2.5 HRS

01. Digital signatures
02. Key length
03. Key stretching
04. Salting
05. Hashing
06. Key exchange
07. Elliptic-curve cryptography
08. Perfect forward secrecy
09. Quantum

a. Communications
b. Computing

10. Post-quantum
11. Ephemeral
12. Modes of operation
    a. Authenticated
    b. Unauthenticated
    c. Counter
13. Blockchain
    a. Public ledgers
14. Cipher suites
    a. Stream
    b. Block
15. Symmetric vs. asymmetric
16. Lightweight cryptography
17. Steganography
    a. Audio
    b. Video
    c. Image
18. Homomorphic encryption
19. Common use cases
    a. Low power devices
    b. Low latency
    c. High resiliency
    d. Supporting confidentiality
    e. Supporting integrity
    f. Supporting obfuscation
    g. Supporting authentication
    h. Supporting non-repudiation

## 20 · Limitations

a. Speed

b. Size

c. Weak keys

d. Time

e. Longevity

f. Predictability

g. Reuse

h. Entropy

i. Computational overheads

j. Resource vs. security constraints

17 CHAPTER

# IMPLEMENT SECURE PROTOCOLS

30 MINS

2.5 HRS

## 01. Protocols

a. Domain Name System Security Extensions (DNSSEC)

b. SSH

c. Secure/Multipurpose Internet Mail Extensions (S/MIME)

d. Secure Real-time Transport Protocol (SRTP)

e. Lightweight Directory Access Protocol Over SSL (LDAPS)

f. File Transfer Protocol, Secure (FTPS)

g. SSH File Transfer Protocol (SFTP)

h. Simple Network Management Protocol, version 3 (SNMPv3)

i. Hypertext transfer protocol over SSL/TLS (HTTPS)

j. IPSec

k. Authentication header (AH)/ Encapsulating Security Payloads (ESP)

l. Tunnel/transport

m. Post Office Protocol (POP)/ Internet Message Access Protocol (IMAP)

## O2 · Use cases

a. Voice and video

b. Time synchronization

c. Email and web

d. File transfer

e. Directory services

f. Remote access

g. Domain name resolution

h. Routing and switching

i. Network address allocation

j. Subscription services

ELYSIUM ACADEMY®
Milestone of Cognizance

Since 2007

CHAPTER 18

# HOST OR APPLICATION SECURITY SOLUTIONS

30 MINS

2.5 HRS

## O1. Endpoint protection

a. Antivirus
b. Anti-malware
c. Endpoint detection and response (EDR)
d. DLP
e. Next-generation firewall (NGFW)
f. Host-based intrusion prevention system (HIPS)
g. Host-based intrusion detection system (HIDS)
h. Host-based firewall

## O2. Boot integrity

a. Boot security/Unified Extensible Firmware Interface (UEFI)
b. Measured boot
c. Boot attestation

## O3. Database

a. Tokenization
b. Salting
c. Hashing

## O4. Application security

a. Input validations
b. Secure cookies
c. Hypertext Transfer Protocol (HTTP) headers

d. Code signing
e. Allow list
f. Block list/deny list
g. Secure coding practices
h. Static code analysis
i. Manual code review
j. Dynamic code analysis
k. Fuzzing

## O5 · Hardening

a. Open ports and services
b. Registry
c. Disk encryption
d. OS
e. Patch management
f. Third-party updates
g. Auto-update

## O6 · Self-encrypting drive (SED)/ full-disk encryption (FDE)

a. Opal

## O7· Hardware root of trust
## O8. Trusted Platform Module (TPM)
## O9. Sandboxing

ELYSIUM ACADEMY®
Milestone of Cognizance

Since 2007

CHAPTER 19

# SECURE NETWORK DESIGNS

30 MINS

2.5 HRS

## O1. Load balancing

a. Active/active
b. Active/passive
c. Scheduling
d. Virtual IP
e. Persistence

## O2. Network segmentation

a. Virtual local area network (VLAN)
b. Screened subnet (previously known as demilitarized zone)
c. East-west traffic
d. Extranet
e. Intranet
f. Zero Trust

## O3. Virtual private network (VPN)

a. Always-on
B. Split tunnel vs. full tunnel
C. Remote access vs. site-to-site
D. IPSec
E. SSL/TLS
F. HTML5
G. Layer 2 tunneling protocol (L2TP)

ELYSIUM ACADEMY®
Milestone of Cognizance

Since 2007

O4 · DNS

O5. Network access control (NAC)

a. Agent and agentless

O6 · Out-of-band management

O7. Port security

a. Broadcast storm prevention

B. Bridge Protocol Data Unit (BPDU) guard

C. Loop prevention

D. Dynamic Host Configuration Protocol (DHCP) snooping

E. Media access control (MAC) filtering

O8 · Network appliances

a. Jump servers

B. Proxy servers

C. Forward

D. Reverse

E. Network-based intrusion detection system (NIDS) /network-based intrusion prevention system (NIPS)

F. Signature-based

G. Heuristic/behavior

H. Anomaly

I. Inline vs. passive

J. HSM

K. Sensors

L. Collectors

M. Aggregators

N. Firewalls

O. Web application firewall (WAF)

P. NGFW

Q. Stateful

R. Stateless

S. Unified threat management (UTM)

T. Network address translation (NAT) gateway

U. Content/URL filter

V. Open-source vs. proprietary

W. Hardware vs. software

X. Appliance vs. host-based vs. virtua

O9 ·Access control list (ACL)

10. Route security

11. Quality of service (QoS)

12. Implications of IPv6

13. Port spanning/port mirroring

A. CPort taps

14 · Monitoring services

15. File integrity monitors

ELYSIUM GROUPS
NEXT GENERATION THOUGHTS

ELYSIUM ACADEMY®
Milestone of Cognizance

Since 2007

CHAPTER 20

# INSTALL AND CONFIGURE WIRELESS SECURITY SETTINGS

30 MINS

01 HRS

## 01. Cryptographic protocols

a. WiFi Protected Access 2 (WPA2)

B. WiFi Protected Access 3 (WPA3)

C. Counter-mode/CBC-MAC Protocol (CCMP)

D. Simultaneous Authentication of Equals (SAE)

## 02. Authentication protocols

a. Extensible Authentication Protocol (EAP)

B. Protected Extensible Authentication Protocol (PEAP)

C. EAP-FAST

D. EAP-TLS

E. EAP-TTLS

F. IEEE 802.1X

G. Remote Authentication Dial-in User Service (RADIUS) Federation

## 03. Methods

a. Pre-shared key (PSK) vs Enterprise vs. Open

B. WiFi Protected Setup (WPS)

C. Captive portals

ELYSIUM ACADEMY®
Milestone of Cognizance

Since 2007

## O4 · Installation considerations

a. Site surveys

b. Heat maps

c. WiFi analyzers

d. Channel overlaps

e. Wireless access point (WAP) placement

f. Controller and access point security

21 CHAPTER

## IMPLEMENT SECURE MOBILE SOLUTIONS

30 MINS

2.5 HRS

O1. Connection methods and receivers

a. Cellular

b. WiFi

c. Bluetooth

d. NFC

e. Infrared

f. USB

g. Point-to-point

h. Point-to-multipoint

i. Global Positioning System (GPS)

j. RFID

## O2· Mobile device management (MDM)

a. Application management

b. Content management

c. Remote wipe

d. Geofencing

e. Geolocation

f. Screen locks

g. Push notifications

h. Passwords and PINs

i. Biometrics

j. Context-aware authentication

k. Containerization

l. Storage segmentation

m. Full device encryption

## O3· Mobile devices

a. MicroSD hardware security module (HSM)

b. MDM/Unified Endpoint Management (UEM)

c. Mobile application management (MAM)

d. SEAndroid

## O4· Enforcement and monitoring of:

a. Third-party application stores

b. Rooting/jailbreaking

c. Sideloading

d. Custom firmware

e. Carrier unlocking

ELYSIUM ACADEMY®
Milestone of Cognizance

Since 2007

a. Firmware over-the-air (OTA) updates
b. Camera use
c. SMS/Multimedia Messaging Service (MMS)/Rich Communication Services (RCS)
d. External media
e. USB On-The-Go (USB OTG)
f. Recording microphone
g. GPS tagging
h. WiFi direct/ad hoc
i. Tethering
j. Hotspot
k. Payment methods

## O5· Deployment models

a. Bring your own device (BYOD)
b. Corporate-owned personally enabled (COPE)
c. Choose your own device (CYOD)
d. Corporate-owned
e. Virtual desktop infrastructure (VDI)

22
CHAPTER

# CYBERSECURITY SOLUTIONS TO THE CLOUD

30 MINS
1.5 HRS

## O1.Cloud security controls

a. High availability across zones
b. Resource policies
c. Secrets management
d. Integration and auditing
e. Storage

f. Permissions

g. Encryption

h. Replication

i. High availability

j. Network

k.Virtual networks

l. Public and private subnets

m. Segmentation

n. API inspection and integration

o. Compute

p. Security groups

q. Dynamic resource allocation

r. Instance awareness

s. Virtual private cloud (VPC) endpoint

t. Container security

## O2.Solutions

a. CASB

b. Application security

c. Next-generation secure web gateway (SWG)

d. Firewall considerations in a cloud environment

e. Cost

f. Need for segmentation

g. Open Systems Interconnection (OSI) layers

## O3. Cloud native controls vs. third-party solutions

ELYSIUM ACADEMY®
Milestone of Cognizance

Since 2007

23
CHAPTER

# IDENTITY AND ACCOUNT MANAGEMENT CONTROLS

30 MINS

2.5 HRS

## O1. Identity

a. Identity provider (IdP)

b. Attributes

c. Certificates

d. Tokens

e. SSH keys

f. Smart cards

## O2. Account types

a. User account

b. Shared and generic accounts/credentials

c. Guest accounts

d. Service accounts

## O3. Account policies

a. Password complexity

b. Password history

c. Password reuse

d. Network location

e. Geofencing

f. Geotagging

g. Geolocation

h. Time-based logins

i. Access policies

j. Account permissions

k. Account audits

l. Impossible travel time/risky login

m. Lockout

n. Disablement

ELYSIUM ACADEMY®
Milestone of Cognizance

Since 2007

CHAPTER 24

# AUTHENTICATION AND AUTHORIZATION SOLUTIONS

30 MINS

1.5 HRS

## 01. Authentication management

a. Password keys
b. Password vaults
c. TPM
d. HSM
e. Knowledge-based authentication

## 02. Authentication/authorization

a. EAP
b. Challenge-Handshake Authentication Protocol (CHAP)
c. Password Authentication Protocol (PAP)
d. 802.1X
e. RADIUS
f. Single sign-on (SSO)
g. Security Assertion Markup Language (SAML)
h. Terminal Access Controller Access Control System Plus (TACACS+)
i. OAuth
j. OpenID
k. Kerberos

## 03. Access control schemes

a. Attribute-based access control (ABAC)
b. Role-based access control
c. Rule-based access control

d. MAC
e. Discretionary access control (DAC)
f. Conditional access
g. Privileged access management
h. Filesystem permissions

25 CHAPTER

# PUBLIC KEY INFRASTRUCTURE

30 MINS
2.5 HRS

## O1. Public key infrastructure (PKI)

a. Key management
b. Certificate authority (CA)
c. Intermediate CA
d. Registration authority (RA)
e. Certificate revocation list (CRL)
f. Certificate attributes
g. Online Certificate Status Protocol (OCSP)
h. Certificate signing request (CSR)
i. CN
j. Subject alternative name
k. Expiration

## O2. Types of certificates

a. Wildcard
b. Subject alternative name
c. Code signing
d. Self-signed

e. Machine/computer

f. Email

g. User

h. Root

i. Domain validation

j. Extended validation

## 03. Certificate formats

a. Distinguished encoding rules (DER)

b. Privacy enhanced mail (PEM)

c. Personal information exchange (PFX)

d. cer

e. P12

f. P7B

## 04. Concepts

a. Online vs. offline CA

b. Stapling

c. Pinning

d. Trust model

e. Key escrow

f. Certificate chaining

ELYSIUM ACADEMY®
Milestone of Cognizance

Since 2007

CHAPTER 26

# ASSESS ORGANIZATIONAL SECURITY

30 MINS

2.5 HRS

## O1. Network reconnaissance and discovery

a. tracert/traceroute
b. nslookup/dig
c. ipconfig/ifconfig
d. nmap
e. ping/pathping
f. hping
g. netstat
h. netcat
i. IP scanners
j. arp
k. route
l. curl
m. theHarvester
m. sn1per
n. scanless
o. dnsenum
p. Nessus
q. Cuckoo

## O2. File manipulation

a. head
b. tail
c. cat

d. grep
e. chmod
f. logger

## O3. Shell and script environments

a. SSH
b. PowerShell
c. Python
d. OpenSSL

## O4. Packet capture and replay

a. Tcpreplay
b. Tcpdump
c. Wireshark

## O5. Forensics

a. dd
b. Memdump
c. WinHex
d. FTK imager
e. Autopsy

## O6. Exploitation frameworks
## O7. Password crackers
## O8. Data sanitization

ELYSIUM ACADEMY®
Milestone of Cognizance

Since 2007

27
CHAPTER

# POLICIES, PROCESSES, AND PROCEDURES FOR INCIDENT RESPONSE

30 MINS

1.5 HRS

O1. Incident response plans
O2. Incident response process
- a. Preparation
- b. Identification
- c. Containment
- d. Eradication
- e. Recovery
- f. Lessons learned

O3. Exercises
- a. Tabletop
- b. Walkthroughs
- c. Simulations

O4. Attack frameworks
- a. MITRE ATT&CK
- b. The Diamond Model of Intrusion Analysis
- c. Cyber Kill Chain

O5. Stakeholder management
O6. Communication plan
O7. Disaster recovery plan
O8. Business continuity plan
O9. Continuity of operations planning (COOP)
10. Incident response team
11. Retention policies

ELYSIUM ACADEMY®
Milestone of Cognizance

Since 2007

CHAPTER 28

# DATA SOURCES TO SUPPORT AN INVESTIGATION

30 MINS

2.5 HRS

O1. Vulnerability scan output
O2. SIEM dashboards

a. Sensor
b. Sensitivity
c. Trends
d. Alerts
e. Correlation

O3. Log files

a. Network
b. System
c. Application
d. Security
e. Web
f. DNS
g. Authentication
h. Dump files
i. VoIP and call managers
j. Session Initiation Protocol (SIP) traffic

O4. syslog/rsyslog/syslog-ng
O5. journalctl
O6. NXLog
O7. Bandwidth monitors
O8. Metadata

a. Email
b. Mobile
c. Web
d. File

09. Netflow/sFlow
a. Netflow
b. sFlow
c. IPFIX

10. Protocol analyzer output

29 CHAPTER

# MITIGATION TECHNIQUES

30 MINS
1.5 HRS

01. Reconfigure endpoint security solutions
a. Application approved list
b. Application blocklist/deny list
c. Quarantine

02. Configuration changes
a. Firewall rules
b. MDM
c. DLP
d. Content filter/URL filter
e. Update or revoke certificates

03. Isolation
04. Containment
05. Segmentation

ELYSIUM ACADEMY®
Milestone of Cognizance

Since 2007

## 06. SOAR

a. Runbooks

b. Playbooks

30 CHAPTER

# KEY ASPECTS OF DIGITAL FORENSICS

30 MINS

02 HRS

## 01. Documentation/evidence

a. Legal hold

b. Video

c. Admissibility

d. Chain of custody

e. Timelines of sequence of events

f. Time stamps

g. Time offset

h. Tags

i. Reports

j. Event logs

k. Interviews

## 02. Acquisition

a. Order of volatility

b. Disk

c. Random-access memory (RAM)

d. Swap/pagefile

e. OS

f. Device

g. Firmware
h. Snapshot
i. Cache
j. Network
k. Artifacts

## O3. On-premises vs. cloud

a. Right-to-audit clauses
b. Regulatory/jurisdiction
c. Data breach notification laws

## O4. Integrity

a. Hashing
b. Checksums
c. Provenance

## O5. Preservation
## O6. E-discovery
## O7. Data recovery
## O8. Non-repudiation
## O9. Strategic intelligence/ counterintelligence

ELYSIUM ACADEMY®
Milestone of Cognizance

Since 2007

31 CHAPTER

# VARIOUS TYPES OF CONTROLS

30 MINS

1.5 HRS

## O1. Category

a. Managerial

b. Operational

c. Technical

## O2. · Control type

a. Preventive

b. Detective

c. Corrective

d. Deterrent

e. Compensating

f. Physical

32 CHAPTER

# APPLICABLE REGULATIONS, STANDARDS, OR FRAMEWORKS

30 MINS

1.5 HRS

## O1. Regulations, standards, and legislation

a. General Data Protection Regulation (GDPR)

b. National, territory, or state laws

c. Payment Card Industry Data Security Standard (PCI DSS)

## O2. Key frameworks

a. Center for Internet Security (CIS)
b. National Institute of Standards and Technology (NIST) Risk Management Framework (RMF)/ Cybersecurity Framework(CSF)
c. International Organization for Standardization (ISO) 27001/27002/27701/31000
d. SSAE SOC 2 Type I/II
e. Cloud security alliance
f. Cloud control matrix
g. Reference architecture

## O3. Benchmarks /secure configuration guides

a. Platform/vendor-specific guides
b. Web server
c. OS
d. Application server
e. Network infrastructure devices

ELYSIUM ACADEMY®
Milestone of Cognizance

Since 2007

33 CHAPTER

# IMPORTANCE OF POLICIES TO ORGANIZATIONAL SECURITY

30 MINS

02 HRS

## O1. Personnel

a. Acceptable use policy
b. Job rotation
c. Mandatory vacation
d. Separation of duties
e. Least privilege
f. Clean desk space
g. Background checks
h. Non-disclosure agreement (NDA)
i. Social media analysis
j. Onboarding
k. Offboarding
l. User training
m. Gamification
n. Capture the flag
o. Phishing campaigns
p. Phishing simulations
q. Computer-based training (CBT)
r. Role-based training

## O2. Diversity of training techniques

## O3. Third-party risk management

a. Vendors
b. Supply chain
c. Business partners

d. Service level agreement (SLA)
e. Memorandum of understanding (MOU)
f. Measurement systems analysis (MSA)
g. Business partnership agreement (BPA)
h. End of life (EOL)
i. End of service life (EOSL)
j. NDA

## 04. Data

a. Classification
b. Governance
c. Retention

## 05. Credential policies

a. Personnel
b. Third-party
c. Devices
d. Service accounts
e. Administrator/root accounts

## 06. Organizational policies

a. Change management
b. Change control
c. Asset management

ELYSIUM ACADEMY®
Milestone of Cognizance

Since 2007

34
CHAPTER

# RISK MANAGEMENT PROCESSES AND CONCEPTS

30 MINS

02 HRS

## O1. Risk types

a. External
b. Internal
c. Legacy systems
d. Multiparty
e. IP theft
f. Software compliance/licensing

## O2. Risk management strategies

a. Acceptance
b. Avoidance
c. Transference
d. Cybersecurity insurance
e. Mitigation

## O3. Risk analysis

a. Risk register
b. Risk matrix/heat map
c. Risk control assessment
d. Risk control self-assessment
e. Risk awareness
f. Inherent risk
g. Residual risk
h. Control risk
i. Risk appetite
j. Regulations that affect risk posture

k. Risk assessment types
l. Qualitative
m. Quantitative
n. Likelihood of occurrence
o. Impact
p. Asset value
q. Single-loss expectancy (SLE)
r. Annualized loss expectancy (ALE)
s. Annualized rate of occurrence (ARO)

## 04. Disasters

a. Environmental
b. Person-made
c. Internal vs. external

## 05. Business impact analysis

a. Recovery time objective (RTO)
b. Recovery point objective (RPO)
c. Mean time to repair (MTTR)
d. Mean time between failures (MTBF)
e. Functional recovery plans
f. Single point of failure
g. Disaster recovery plan (DRP)
h. Mission essential functions
i. Identification of critical systems
j. Site risk assessment

ELYSIUM ACADEMY®
Milestone of Cognizance

Since 2007

35 CHAPTER

# PRIVACY AND SENSITIVE DATA CONCEPTS

30 MINS

2.5 HRS

## O1. Organizational consequences of privacy and data breaches

a. Reputation damage
b. Identity theft
c. Fines
d. IP theft

## O2. Notifications of breaches

a. Escalation
b. Public notifications and disclosures

## O3. Data types

a. Classifications
b. Public
c. Private
d. Sensitive
e. Confidential
f. Critical
g. Proprietary
h. Personally identifiable information (PII)
i. Health information
j. Financial information
k. Government data
l. Customer data

## O4. Privacy enhancing technologies

a. Data minimization
b. Data masking
c. Tokenization
d. Anonymization
e. Pseudo-anonymization

## O5. Roles and responsibilities

a. Data owners
b. Data controller
c. Data processor
d. Data custodian/steward
e. Data protection officer (DPO)

## O6. Information life cycle
## O7. Impact assessment
## O8. Terms of agreement
## O9. Privacy notice

ELYSIUM ACADEMY®
Milestone of Cognizance

Since 2007

Placement Assistance 100%

135+ Professional Courses

Practical Sessions 90%

67+ Global Pacts

Corporate Placements 65%

170+ IT Companies Tie-Up

# ELYSIUM GROUP OF COMPANIES

# ELYSIUM ACADEMY PRIVATE LIMITED

## Authorized International Partners

Microsoft · CompTIA · Cisco · aws · Google · SUSE · Rocheston · C++