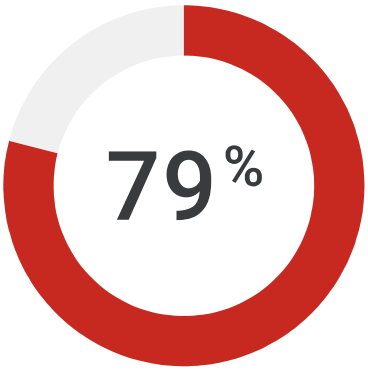
Completed: Jun 29 - 8:14 AM
Venkata Sai tharun Gontla



Assessment Failed

Thank you for completing the assessment. Unfortunately, you did not answer enough questions correctly to receive a passing grade.

Total Points: 59/75 **Correct Answers:** 59/75

View Response Details

Close

Response Details

Print

Section Results

Section 1 Points: 59/75

Your Responses

Question 1 of 75 +1

When is it impossible to secure SaaS data? 14068168

- [x] when a user uses an unmanaged device to access an unsanctioned SaaS instance
- [ ] when a user uses a managed device to access an unsanctioned SaaS instance
- [ ] when a user uses an unmanaged device to access a sanctioned SaaS instance
- [ ] when a user uses a managed device to access a sanctioned SaaS instance

Question 2 of 75 +1

Which option is an example of a static routing protocol?

14068168

- [ ] Open Shortest Path First (OSPF)
- [x] Border Gateway Protocol (BGP)
- [ ] Routing Information Protocol (RIP)
- [ ] Split horizon

Question 3 of 75 +0 / 1

Which two malware types are self-replicating? (Choose two.) 14068168

- [ ] logic bomb
- [ ] back door
- [x] virus
- [x] trojan horse
- [x] worm

The correct answer was "virus, worm".

Question 4 of 75 +1

Which type of attack includes an email advertisement for a dry cleaning service? 14068168

- [x] spamming
- [ ] phishing
- [ ] spear phishing
- [ ] whaling

Question 5 of 75 +1

Who is the most likely target of social engineering? 14068168

- [ ] executive management, because it has the most permissions
- [ ] senior IT engineers, because the attacker hopes to get them to disable the security infrastructure

- [x] junior people, because they are easier to stress and probably not as well trained
- [ ] the accounting department, because it can wire money directly to the attacker's account

---

Question 6 of 75 +1

Which two attacks typically use a botnet? (Choose two.) 14068168

- [ ] social engineering
- [ ] DoS
- [x] DDoS
- [x] sending spam to a lengthy mailing list
- [ ] spear phishing

Question 7 of 75 +0 / 1

An analysis tool raised an alert, but the security analyst who researched it discovered it wasn't a problem. Which type of finding is this? 14068168

- [x] False positive
- [x] True positive
- [ ] False negative
- [ ] True negative

The correct answer was "False positive".

Question 8 of 75

Which Palo Alto Networks product suite is used to manage alerts, obtain additional information, and orchestrate responses?

- Strata
- Prisma
- Cortex
- WildFire

Question 9 of 75 +0 / 1

Which stage of the cyber attack lifecycle makes it important to provide ongoing education to users on spear phishing links, unknown emails, and risky websites?

- Delivery
- Exploitation
- Installation
- Reconnaissance

The correct answer was "Delivery".

Question 10 of 75 +1

Which DNS record type do you use to find the IPv4 address of a host?

- A
- AAAA
- PTR

MX

Question 11 of 75 +1

Which device is M2M (machine to machine)? 14068168

- Internet-connected TV
- home alarm that dials the police for response
- car GPS
- ✓ temperature sensor connected to a fire suppression system

Question 12 of 75 +1

How many bytes are in an IPv6 address? 14068168

- 4
- 8
- ✓ 16
- 32

Question 13 of 75 +1

Which three security functions are integrated with a UTM device? (Choose three.) 14068168

- cloud access security broker (CASB)
- Remote Browser Isolation (RBI)
- DevOps automation
- ✓ firewall

- [x] Intrusion Detection System (IDS)
- [x] anti-spam

Question 14 of 75 +1

Which type of malware protection requires in-depth knowledge of applications and how they communicate? 14068168

- [ ] signature-based
- [x] container-based
- [ ] application allow lists
- [ ] anomaly detection

Question 15 of 75 +1

Which item accurately describes a security weakness that is caused by implementing a “ports first” data security solution in a traditional data center? 14068168

- [x] You may have to open up multiple ports and these ports could also be used to gain unauthorized entry into your datacenter.
- [ ] You may not be able to assign the correct port to your business-critical applications.
- [ ] You may have to use port numbers greater than 1024 for your business-critical applications.
- [ ] You may not be able to open up enough ports for your business-critical applications which will increase the attack surface area.

Question 16 of 75 +1

Which feature of the NGFW can distinguish between reading Facebook and commenting? 14068168

- [x] App-ID
- [ ] Content-ID
- [ ] User-ID
- [ ] Global Protect

Question 17 of 75 +1

What is the collective term for software versions, OS settings, and configuration file settings? 14068168

- [x] configuration items
- [ ] configurable values
- [ ] computer settings
- [ ] the configuration

Question 18 of 75 +1

A provider's applications run on a cloud infrastructure. The consumer does not manage or control the underlying infrastructure. Which cloud computing service model is this? 14068168

- [x] platform as a service (PaaS)
- [ ] infrastructure as a service (IaaS)
- [ ] software as a service (SaaS)

public cloud

Question 19 of 75 +1

Which NIST cloud deployment model would you recommend for a startup that does not have much money to pay for hosting or a data center and needs a 24x7 server? 14068168

- [x] public
- [ ] private
- [ ] community
- [ ] hybrid

Question 20 of 75 +1

Which component may be shared with other cloud tenants even when using IaaS? 14068168

- [ ] application
- [ ] runtime
- [ ] virtual machine (guest)
- [x] physical machine (host)

Question 21 of 75 +1

Which of the following security issues can cause a long patched vulnerability to resurface? 14068168

- [ ] VM sprawl

- intra-vm communications
- hypervisor vulnerabilities
- ✓ dormant virtual machines

Question 22 of 75 +1 ✓

What are the two meanings of the CI/CD pipeline? (Choose two.) 14068168

- ✓ ☑ continuous integration/continuous delivery
- ☐ continuous implementation/continuous delivery
- ✓ ☑ continuous integration/continuous deployment
- ☐ continuous implementation/continuous deployment

Question 23 of 75 +0 / 1 ✗

Which systems must you secure to ensure compliance with security standards? 14068168

- the servers in the data center
- ✗ the devices owned by the enterprise, whether they are servers in the data center, cloud vms you manage, or user endpoint devices
- ✓ any system where the data for which you are responsible goes
- every device that is either owned by the enterprise, or used by enterprise employees

The correct answer was "any system where the data for which you are responsible goes".

Question 24 of 75 +1

Which action is part of the compute security pillar? 14068168

- user and entity behavior analytics (UEBA)
- Microservice-aware micro-segmentation
- ✓ integration with the CI/CD workflow
- automated asset inventory

Question 25 of 75 +1

Which action is part of the identity security pillar? 14068168

- ✓ user and entity behavior analytics (UEBA)
- Microservice-aware micro-segmentation
- integration with the CI/CD workflow
- automated asset inventory

Question 26 of 75 +1

Which type of traffic can stay contained in a single physical server? 14068168

- North-south
- ✓ East-west
- unknown

trusted

Question 27 of 75 +1

Why is it important to protect East-West traffic within a private cloud?

14068168

- East-West traffic contains more threats than other traffic
- East-West traffic uses IPV6 which is less secure than IPV4
- ✓ All traffic contains threats, so enterprises must protect against threats across the entire network
- East-West traffic contains more session-oriented traffic than other traffic

---

Question 28 of 75 +0 / 1

Which option is a Prisma Access security service?

14068168

- Virtual Private Networks (VPNs)
- Software-defined wide-area networks (SD-WANs)
- ✓ Firewall as a Service (FWaaS)
- ✗ Compute Security

The correct answer was "Firewall as a Service (FWaaS) ".

Question 29 of 75 +1

Which SecOp function is proactive? 14068168

- Identify
- Investigate
- Mitigate
- ✓ Improve

Question 30 of 75 +1 ✓

Which environment allows you to install an appliance that sees all traffic? 14068168

- LAN when people work from home
- ✓ Non-virtualized data center
- virtualized data center
- VPC network

Question 31 of 75 +1 ✓

What does SIEM stand for? 14068168

- Security Infosec and Event Management
- Secure Infrastructure and Event Monitoring
- Standard Installation and Event Media
- ✓ Security Information and Event Management

Question 32 of 75

What does Cortex XSOAR use to automate security processes? 14068168

- bash scripts
- Windows PowerShell
- ✓ playbooks
- Python scripts

Question 33 of 75 +0 / 1 ✗

Which three options partially comprise the six elements of SecOps? (Choose three.) 14068168

- ✓ ☑ People
- ✗ ☑ Networking
- ☐ Data storage
- ✓ ☐ Technology
- ✓ ☑ Processes

The correct answer was "People, Technology, Processes".

Question 34 of 75 +1 ✓

What is the relationship between SIEM and SOAR? 14068168

- SIEM products implement the SOAR business process.
- SIEM and SOAR are different names for the same product category.
- ✓ SIEM systems collect information to identify issues that SOAR products help mitigate.

SOAR systems collect information to identify issues that SIEM products help mitigate.

Question 35 of 75 +1

Which three operating systems are supported by Cortex XDR? (Choose three.) 14068168

- [ ] z/OS
- [x] Linux
- [x] macOS
- [ ] Minix
- [x] Android

Question 36 of 75 +1

Of the endpoint checks, what is bypassed for known programs? 14068168

- [ ] WildFire query
- [ ] behavioral threat protection
- [x] local analysis
- [ ] Firewall analysis

Question 37 of 75 +1

Which three options partially comprise the six elements of SecOps? (Choose three.) 14068168

- [x] Visibility

- [ ] Disaster recovery
- [x] Business
- [x] Interfaces
- [ ] Regular audits

Question 38 of 75 +1

Which Palo Alto Networks NGFW subscription service enables you to identify and control access to websites that host malware and phishing pages? 14068168

- [ ] Threat Prevention
- [x] URL Filtering
- [ ] DNS Security
- [ ] WildFire

Question 39 of 75 +1

Which technique changes protocols at random during a session? 14068168

- [x] port hopping
- [ ] use of non-standard ports
- [ ] tunneling within commonly used services
- [ ] hiding within SSL encryption

Question 40 of 75

The customer is responsible only for which type of security when using a SaaS application? 14068168

- [x] data
- [ ] platform
- [ ] physical
- [ ] infrastructure

Question 41 of 75 +1

Anthem server breaches disclosed Personally Identifiable Information (PII) from a number of its servers. The infiltration by hackers was attributed to which type of vulnerability? 14068168

- [ ] exploitation of an unpatched security vulnerability
- [x] a phishing scheme that captured a database administrator's password
- [ ] an intranet-accessed contractor's system that was compromised
- [ ] access by using a third-party vendor's password

Question 42 of 75 +1

Which defensive tool is installed on endpoints to mitigate malware attacks? 14068168

- [x] antivirus software
- [ ] germ scans
- [ ] DNS client

DHCP client

Question 43 of 75 +1

Which attacker profile uses the internet to recruit members to an ideology, to train them, and to spread fear and induce panic?

- cybercriminals
- state-affiliated groups
- hacktivists
- ✓ cyberterrorists

Question 44 of 75 +0 / 1

In which step of the cyber-attack lifecycle do hackers embed intruder code within seemingly innocuous files?

- delivery
- ✓ weaponization
- ✗ reconnaissance
- exploitation

The correct answer was "weaponization".

Question 45 of 75 +1

What is the key to “taking down” a botnet?

- install openvas software on endpoints
- use LDAP as a directory service
- ✓ prevent bots from communicating with the C2
- block Docker engine software on endpoints

Question 46 of 75 +1 ✓

Which type of Wi-Fi attack depends on the victim initiating the connection?

- Jasager
- Mirai
- ✓ Evil twin
- Parager

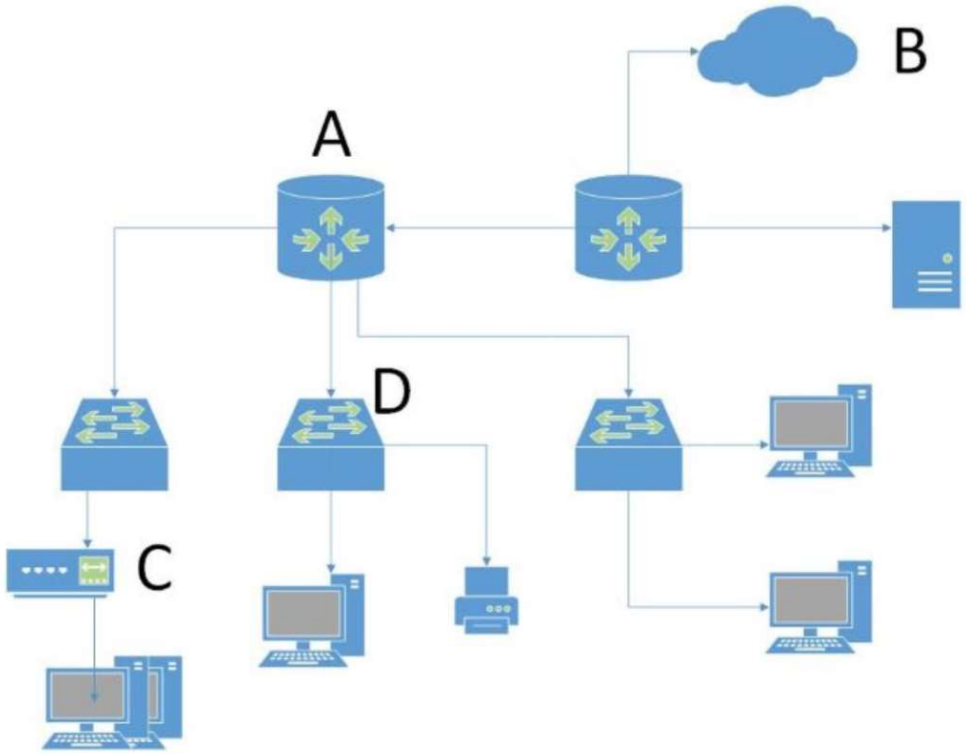
Question 47 of 75 +1 ✓

Which option is an example of a North-South traffic flow?

- Traffic between an internal server and internal user
- ✓ Client-server interactions that cross the edge perimeter
- An internal three-tier application
- Lateral movement within a cloud or data center

Question 48 of 75

In the attached network diagram, which device is the switch?



- A
- B
- C
- ✓ D

Question 49 of 75 +0 / 1 ✗

Which key component is used to configure a static route?

- routing protocol
- ✓ next hop IP address
- enable setting
- ✗ router ID

The correct answer was "next hop IP address ".

Question 50 of 75 +1

Routing Information Protocol (RIP), uses what metric to determine how network traffic should flow? 14068168

- Shortest Path
- Split Horizon
- Path Vector
- ✓ Hop Count

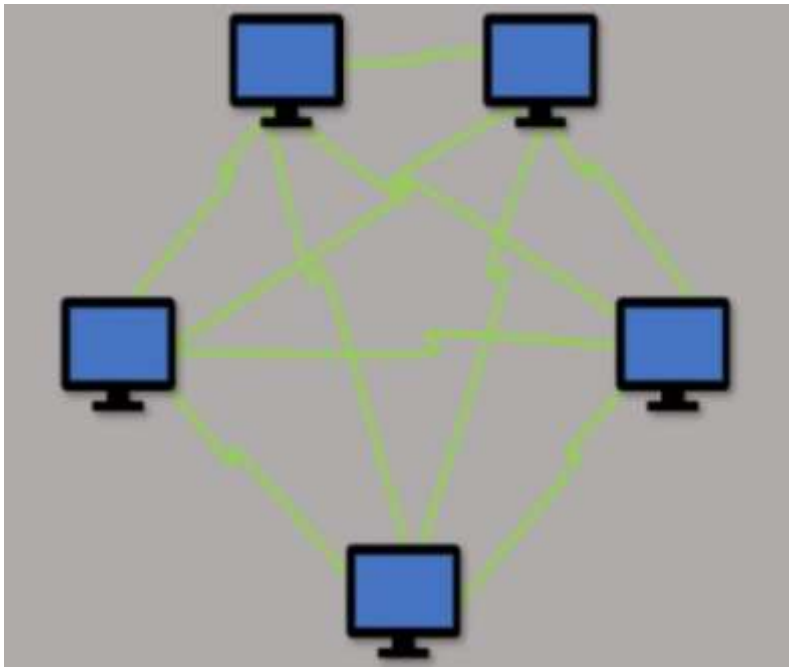
Question 51 of 75 +1

Which networking device increases the number of collision domains? 14068168

- Router
- ✓ Switch
- Hub
- Wireless repeater

Question 52 of 75

Which type of LAN technology is being displayed in the diagram? 14068168



- Star Topology
- Bus Topology
- Spine Leaf Topology
- ✓ Mesh Topology

Question 53 of 75 +1 ✓

Which TCP/IP sub-protocol operates at Layer4 of the OSI model? 14068168

- ✓ UDP
- SSH
- FTP
- HTTPS

Question 54 of 75

Which TCP/IP sub-protocol operates at the Layer7 of the OSI model?

- ✗ UDP
- MAC
- NFS
- ✓ SNMP

The correct answer was "SNMP".

Question 55 of 75 +1 ✓

During the OSI layer 3 step of the encapsulation process, what is the Protocol Data Unit (PDU) called when the IP stack adds source (sender) and destination (receiver) IP addresses?

- Data
- Segment
- ✓ Packet
- Frame

Question 56 of 75 +1 ✓

Which IPsec feature allows device traffic to go directly to the Internet?

- IKE Security Association
- ✓ Split tunneling
- Diffie-Hellman groups

Authentication Header (AH)

Question 57 of 75 +1

Which option would be an example of PII that you need to prevent from leaving your enterprise network? 14068168

- [x] Credit card number
- [ ] Trade secret
- [ ] National security information
- [ ] A symmetric encryption key

Question 58 of 75 +1

When signature-based antivirus software detects malware, what three things does it do to provide protection? (Choose three.) 14068168

- [x] quarantine the infected file
- [x] delete the infected file
- [ ] remove the infected file's extension
- [x] alert system administrators
- [ ] decrypt the infected file using base64

Question 59 of 75 +0 / 1

In an IDS/IPS, which type of alarm occurs when legitimate traffic is improperly identified as malicious traffic? 14068168

- ✗ ● False-negative
- ○ True-negative
- ✓ ○ False-positive
- ○ True-positive

The correct answer was "False-positive ".

Question 60 of 75 +1 ✓

Which two network resources does a directory service database contain? (Choose two.)

14068168

- ✓ ☑ Users
- ☐ Terminal shell types on endpoints
- ☐ /etc/shadow files
- ✓ ☑ Services

Question 61 of 75 +1 ✓

Which Palo Alto Networks subscription service complements App-ID by enabling you to configure the next-generation firewall to identify and control access to websites and to protect your organization from websites hosting malware and phishing pages?

14068168

- ○ DNS Security
- ○ WildFire
- ✓ ● URL Filtering

Threat Prevention

Question 62 of 75 +1

What does a directory service associate with users in order to control access to resources?

14068168

- position descriptions
- ✓ permissions
- supervisor status
- tenure within an organization

Question 63 of 75 +1

What User identification for network and services access is implemented by applying policies? 14068168

- Key Security Management
- Identity Tag Management
- Network Management Protocols
- ✓ Identity and Access Management

Question 64 of 75 +1

A native hypervisor runs: 14068168

- within an operating system's environment
- ✓ directly on the host computer's hardware

- only on certain platforms
- with extreme demands on network throughput

Question 65 of 75 +0 / 1

What are two key characteristics of a Type 2 hypervisor? (Choose two.)

14068168

- runs without any vulnerability issues
- [x] runs within an operating system
- [x] is hardened against cyber attacks
- allows multiple, virtual (or guest) operating systems to run concurrently on a single physical host computer

The correct answer was "runs within an operating system, allows multiple, virtual (or guest) operating systems to run concurrently on a single physical host computer".

Question 66 of 75 +1

Why have software developers widely embraced the use of containers?

14068168

- Containers require separate development and production environments to promote authentic code.
- Containers simplify the building and deploying of cloud native applications.
- Containers share application dependencies with other containers and with their host computer.

Containers are host specific and are not portable across different virtual machine hosts.

Question 67 of 75 +0 / 1

How does adopting a serverless model impact application development? 14068168

- prevents developers from focusing on just the application code because you need to provision the underlying infrastructure to run the code
- slows down the deployment of application code, but it improves the quality of code development
- ✓ reduces the operational overhead necessary to deploy application code
- ✗ costs more to develop application code because it uses more compute resources

The correct answer was "reduces the operational overhead necessary to deploy application code ".

Question 68 of 75 +0 / 1

Which characteristic of serverless computing enables developers to quickly deploy application code? 14068168

- ✗ Using Container as a Service (CaaS) to deploy application containers to run their code.
- Uploading cloud service autoscaling services to deploy more virtual machines to run their application code based on user demand
- Using cloud service spot pricing to reduce the cost of using virtual machines to run their application code
- ✓ Uploading the application code itself, without having to provision a full container image or any OS virtual machine components

The correct answer was "Uploading the application code itself, without having to provision a full container image or any OS virtual machine components ".

Question 69 of 75 +1

How does DevSecOps improve the Continuous Integration/Continuous Deployment (CI/CD) pipeline? 14068168

- DevSecOps ensures the pipeline has horizontal intersections for application code deployment
- DevSecOps does security checking after the application code has been processed through the CI/CD pipeline
- ✓ DevSecOps unites the Security team with the Development and Operations teams to integrate security into the CI/CD pipeline
- DevSecOps improves pipeline security by assigning the security team as the lead team for continuous deployment

---

Question 70 of 75 +1

Which model would a customer choose if they want full control over the operating system(s) running on their cloud computing platform?

14068168

- PaaS
- SaaS
- DaaS
- ✓ IaaS

Question 71 of 75 +1

On an endpoint, which method is used to protect proprietary data stored on a laptop that has been stolen?

- Operating system patches
- Endpoint-based firewall
- Periodic data backups
- ✓ Full-disk encryption

Question 72 of 75 +0 / 1

Which Palo Alto Networks tool enables a proactive, prevention-based approach to network automation that accelerates security analysis?

- WildFire
- ✗ Cortex XDR
- ✓ AutoFocus
- MineMeld

The correct answer was "AutoFocus".

Question 73 of 75 +1

Which act establishes national standards to protect individuals' medical information?

- ✓ HIPAA
- FISMA

CISA

SOX

Question 74 of 75 +0 / 1

What is a weakness of a perimeter-based network security strategy to protect an organization's endpoint systems?

14068168

- It assumes that every internal endpoint can be trusted.
- It cannot monitor all potential network ports.
- It cannot identify command-and-control traffic.
- It assumes that all internal devices are untrusted.

The correct answer was "It assumes that every internal endpoint can be trusted.".

Question 75 of 75 +0 / 1

What do you need to create in order to implement DLP? 14068168

- A data identification search function to list all sensitive data
- A data pattern to identify sensitive data
- A data identification encryption program to encrypt all sensitive data
- A data hash nosql database containing all the sensitive data

The correct answer was "A data pattern to identify sensitive data".