CySA+

Cybersecurity Analyst

CCI
Post Office Box 9627
Mississippi State, MS 39762

CySA+

Part 4
Security Architectures

Putting in Compensating Controls

Chapter 13

Outline

- Security Data Analytics
- Manual Review
- Defense in Depth
- Quiz

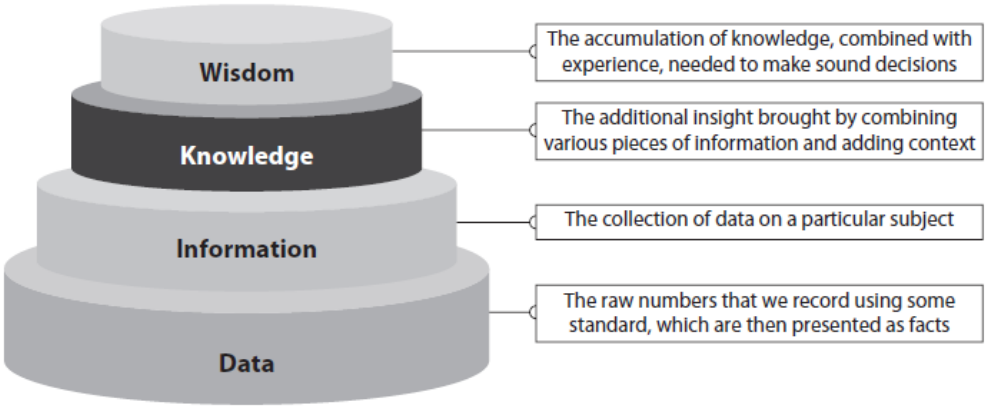
Security Data Analytics

- **Security Data Analytics**
  - **Managing network environment data requires clear strategy and tactical tools**
  - **Objectives**
    - **Given all the network data, create a clear picture of the network activity**
    - **With the clear picture determine the best actions to take for the organization**

[1]

Security Data Analytics

- The figure to the right shows
  - The relationship between data collected at the technical level and the goal of actionable intelligence
- Relationship among various levels of data
  - Data
    - Collecting data
  - Information
    - Refining data into useful information
  - Knowledge
    - Adding context to information
  - Wisdom
    - Knowledge developed over time



[1]

Security Data Analytics

- **Data Aggregation and Correlation**
  - **Data Aggregation**
    - The process of collecting, labeling, and organizing data in such a way that it is useful for analysis
  - **Log Manager**
    - Collects and normalizes data from different network sources
    - The normalized collected data is then displayed on a timeline for easy search
  - **Correlation**
    - The process of forming a connection between two or more sources of data
    - Several SIEM applications offer the ability to create correlation rules to derive more meaningful information

[1]

Security Data Analytics

- **Trend Analysis**
  - **Used to help predict future events and tends to be a forward-looking analysis**
  - **In security data analytics this helps to determine the right controls to use within an environment to mitigate threats**
- **Historical Analysis**
  - **Used to compare new observations to past ones and tends to focus on the past**
  - **This is the practice of observing network behavior over a given period and used to**
    - **Develop defensive plans**
    - **Improve network efficiency**
    - **Prevent attacks**

[1]

Interactive Exercise: 1

What are the objectives of security data analytics?	
What happens in the process of data aggregation?	
How is trend analysis used?	

Interactive Exercise Answer: 1

What are the objectives of security data analytics?	- Given all the network data, create a clear picture of the network activity - With the clear picture determine the best actions to take for the organization
What happens in the process of data aggregation?	It is the process of collecting, labeling, and organizing data in such a way that it is useful for analysis
How is trend analysis used?	- Used to help predict future events and tends to be a forward-looking analysis - In security data analytics this helps to determine the right controls to use within an environment to mitigate threats

Manual Review

- **Manual Review**
  - **Is the story of the incident developed by the analyst using the collected data**
- **Software-Defined Networking (SDN)**
  - **To optimize the performance, the network is centrally controlled**
  - **Perfect for data collection tasks given it can be performed across the network**
  - **Reduces the need to perform collecting, formatting, and normalizing tasks for each device**
- **Firewall Logs**
  - **Can be used on their own to detect problems on the network**
  - **SIEM systems display the information in a more user-friendly way**

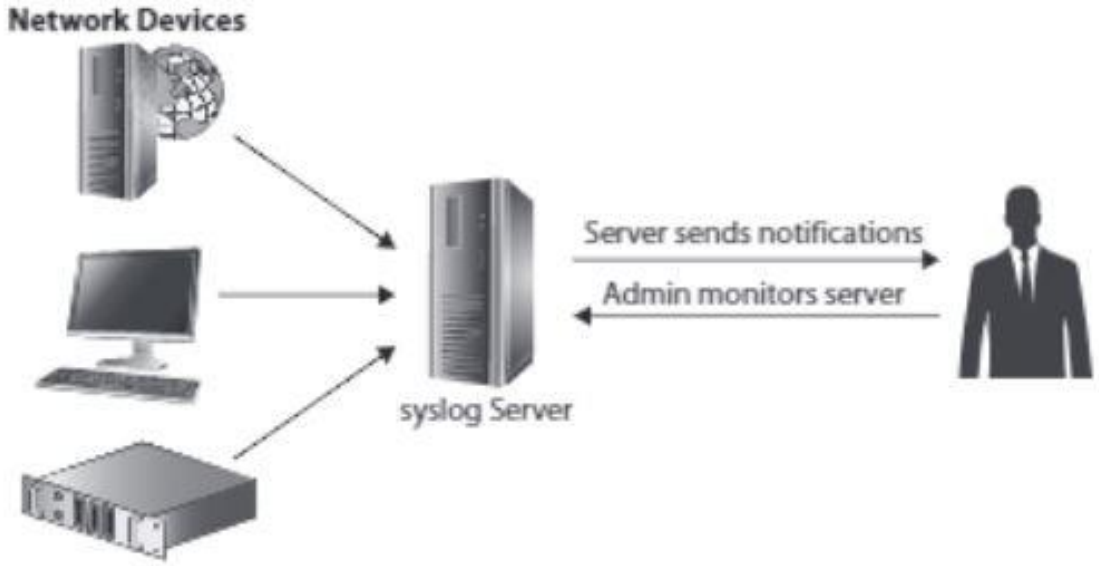
[1]

Manual Review

- **Syslog**
  - **Developed by the University of California, Berkeley**
  - **It is a messaging protocol used to standardize system event reporting**
    - **The protocol provides a standardized way to get the messages from the client to the server**
    - **Great way to consolidate logging information on a single machine**
    - **The log files can be sent to a central server for analysis**
  - **Linux and Unix environments**
    - **The syslog process in these environments is called syslogd**
    - **This includes embedded systems found in routers, switches, and firewalls**
  - **Windows Environment**
    - **Does not have a preinstalled syslog agent**
  - **Side Note**
    - **Does not specify how messages should be formatted**

[1]

Manual Review



Manual Review

- **Syslog**
  - **The figure is a list of syslog severity codes, keywords and descriptions**

Value	Severity	Keyword	Description
0	Emergency	emerg	System is unusable.
1	Alert	alert	Action must be taken immediately.
2	Critical	crit	Critical conditions.
3	Error	err	Error conditions.
4	Warning	warning	Warning conditions.
5	Notice	notice	Normal but significant conditions.
6	Informational	info	Informational messages.
7	Debug	debug	Debug-level messages.

[1]

Manual Review

- **Authentication Logs**
  - **Logs successful and unsuccessful login attempts**
    - **Login events are critical for auditing and analysis**
  - **Pay attention to the successful login attempts**
    - **Consider time zones for each device**
- **Event Logs**
  - **Event Viewer**
    - **Used in Windows systems to allow users to view event logs**
  - **/var/log Directory**
    - **Default location for the Linux operating system and application logs**

[1]

Interactive Exercise: 2

Why is manual review important?	
What is the syslog process in Linux and Unix called?	
What do authentication logs record?	

Interactive Exercise Answer: 2

Why is manual review important?	Although it's tempting to believe that machines can do it all, at the end of the day a security team's success will be defined by how well its human analysts can piece together the story of an incident.
What is the syslog process in Linux and Unix called?	The syslog process in these environments is called syslogd
What do authentication logs record?	They record information about successful and unsuccessful login attempts

Defense in Depth

- **Defense in Depth**
  - **Military concept that is used to force enemies to expand resources in preparing for and conducting attacks**
  - **Implementing defense in depth by**
    - **Using several different types of defense systems**
    - **Periodically changing how the defense systems are implemented**
    - **Spreading resources across locations**
  - **It is a non-static, multifaceted approach for physical and network defense**
    - **An organization should not suffer from one significant flaw**
    - **The defense plan must be reevaluated and updated regularly**
  - **Counterattack**
    - **Secondary defense to combat an adversary**
    - **Not best practice since there are possible legal repercussions**

[1]

Defense in Depth

- **Personnel**
  - **Human capital is an organization's most important asset**
  - **Challenges**
    - **Humans make errors, learn differently, and have different motivations**
- **Training**
  - **General Security Awareness Training**
    - **The focus is the typical employee with an average technical level**
    - **These users' understanding of security awareness is a large part of the networks defense plan**
  - **Security Staff Training**
    - **This train should cover the latest types of malware**
    - **Organization should provide in-house or external training** [1]

Defense in Depth

- **Dual Control**
  - **A practice that requires the two or more groups to complete a task**
    - **For Example, the missile launch process for some ships requires two senior military officers, with special keys, inserted at physically separate locations to launch the missile**
    - **The goal is to not give any one person all the power**
  - **Implementation of this principle in Cybersecurity**
    - **Two-factor authentication**
      - **The user must use a password and a hardware token**
      - **To login**
        - » **Each user has their own unique password and is required to call operations center for the code on the hardware token**

[1]

Defense in Depth

- **Separation of Duties**
  - **Is used to prevent one individual from being able to adversely affect sensitive processes**
  - **For example**
    - **Usually an organization will break down the requirements to delete sensitive data into different tasks such as verify, execute, and approve**
    - **This ensures no one person can perform the deletion task alone**
- **Third Parties and Consultants**
  - **Are usually called in to assist in a special area of knowledge**
  - **Nondisclosed agreement (NDA)**
    - **Ensure consultants sign an NDA since they are typically exposed to the organization's confidential or proprietary**
    - **Should clearly define policies for the use of outside deceives on the company's network and the contractor's expectations**

[1]

Defense in Depth

- **Cross-Training**
  - Exposes employees to other jobs outside their own and gives them additional context for the role they play in the organization
  - Benefits
    - It is cost-effective way to provide additional training
    - Is a great way to ensure there is backup if primary staff is unavailable
    - It encourages team development
- **Rotation of Duties**
  - Used to minimize dishonesty and forces the organization to focus on the role rather than the individual
- **Mandatory Vacation**
  - Can expose possible problems that were hidden by the individual
  - Prevents employees from getting burned-out or complacent

[1]

Defense in Depth

- **Succession Planning**
  - **Is planning for the enviable departure of any employee to ensure their role in the company can be continued by another employee**
  - **Ensure that all tasks of the employee's role is documented**
    - **A succession plan can be tested during a job rotation**
- **Processes**
  - **Is the part between the organization's employees and technology tools**
  - **Should be reviewed yearly to ensure the organization mirrors current trends in technology**
  - **Should be flexible enough to address evolving threats**

[1]

Defense in Depth

- **Continual Improvement**
  - **Reason for continual improvement**
    - Personal and technology are continuously changing
  - **Continuously changing environment**
    - Requires processes to be continuously changed
    - Changing processes is a good time to find ways to improve those processes
    - Changes must be implemented carefully using a change control process
- **Change control process**
  - **This process should be documented in a change control policy**
  - **Example steps that should be in any change control policy**
    1. Request for change to take place
    2. Approval of the change
    3. Documentation of the change
    4. Testing and certification
    5. Implementation
    6. Reporting the finalized change to management

[1]

Defense in Depth

- **Scheduled Reviews**
  - **Should plan recurring reviews of its security plan**
    - **This review will validate the existing security policies usefulness**
  - **In a regulatory environment these reviews are required to stay in compliance**
  - **Is essential to prevent the decline of the organization's security posture**
- **Retirement of Processes**
  - **Natural part of improvement is retiring unneeded processes**
  - **The steps of this process are similar to the change control process**
    - **Review the process with relevant personnel**
    - **Make adjustments to the process**
    - **Clearly communicate the replacement police to the organization**

[1]

Defense in Depth

- **Technology**
  - **Use technology in place of humans when the tasks are repetitive such as**
    - **Enforcing policies, monitoring traffic, preventing data from leaving the network**
- **Automated Reporting**
  - **Is in most security applications and security suits**
  - **Alert Fatigue**
    - **Can be caused if there are constant pings from your security device**
    - **It is important to spend some time determining exactly what should be reported**

[1]

Defense in Depth

- **Security Appliances**
  - Many security appliances can act as a firewall, content filters, IDSs/IPSs, and load balancer
  - Many also have seamless integration between functions with a central management console
  - They provide an overview of the organization's traffic, anomalies, usage, and additional information on client and application behavior
- **Security Suites**
  - Provides multiple security and management related functions
  - Most security suits include
    - Endpoint scanning and protection, mobile device management MDM, and phishing detection
  - Multilayered Security
    - Many security suits will rely on threat databases to have the most up-to-date detection and protection against network threats

[1]

Defense in Depth

- **Outsourcing**
  - Can be risky entrusting the security of your network to outside parties
  - Here are several steps that can be taken to protect your organization's network
    - Access control
      - Access via an interface should be inspected thoroughly
    - Contractor vetting
      - Background checks should be conducted and verified
      - Ensure that the outsourced organization's processes are aligned to your own
    - Incident handling and reporting
      - There should be an agreement made on the nest procedures for incident handling
      - Ensure the outsourced company is aware if your organization operates in a regulatory environment

[1]

Defense in Depth

- **Security as a Service (SECaaS)**
  - **Subscription model where a security company acts as a services provider for all security-related services**
  - **Companies can have the latest protection and be protected by security specialists**
  - **Companies can also invest less in expensive onsite security infrastructure**
- **Cryptography**
  - **It is highly encouraged for companies to utilize encryption to**
    - **Protect the integrity and the confidentially of their data**

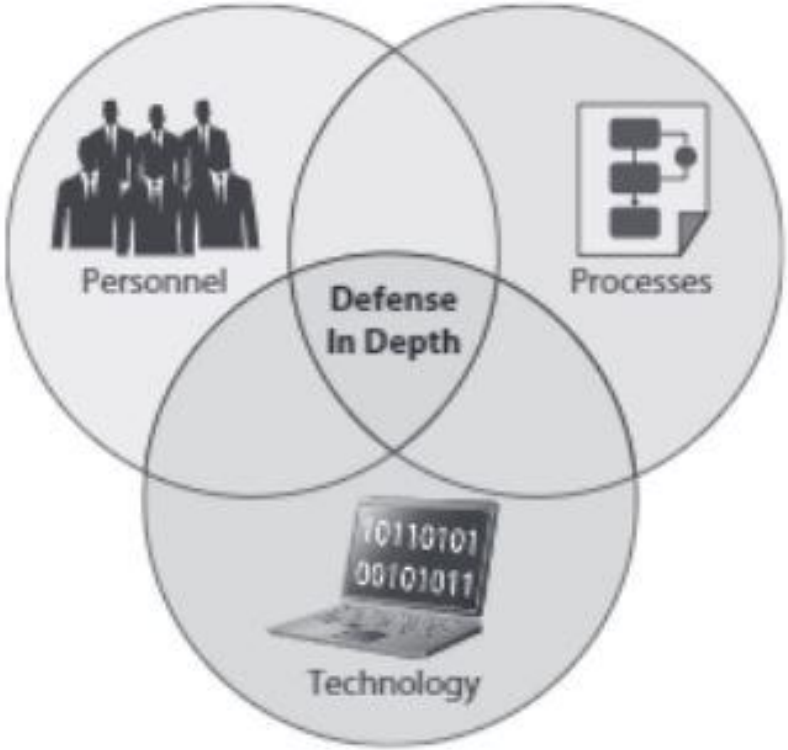
[1]

Defense in Depth

- **Other Security Concepts**
  - **Security Policies**
    - **Need to be both strong enough to address known threats and agile enough to adjust to new threats**
  - **Network defense plan**
    - **Will significantly improve your organization security posture**
- **Network Design**
  - **The use of Cloud services, IaaS, SECaaS, and BYOD means**
    - **Your organization's perimeter is no longer the primary defense**
    - **The people and processes of the network security is critically more important to maintaining your company's data**
- **Network Segmentation**
  - **Improves security by creating separation between usage and access**
  - **Allows companies to remain compliant with regulation regarding sensitive data**

[1]

Defense in Depth



Interactive Exercise: 3

How is dual control implemented in cybersecurity?	
What are the benefits of cross-training?	
What are the 6 steps in the change control process?	
How does alert fatigue happen and how can it be avoided?	

Interactive Exercise Answer: 3

How is dual control implemented in cybersecurity?	It is implemented through two-factor authentication. For example each user has their own unique password and is required to call operations center for the code on a hardware token
What are the benefits of cross-training?	- It is cost-effective way to provide additional training - Is a great way to ensure there is backup if primary staff is unavailable - It encourages team development
What are the 6 steps in the change control process?	1.Request for change to take place 2.Approval of the change 3.Documentation of the change 4.Testing and certification 5.Implementation 6.Reporting the finalized change to management
How does alert fatigue happen and how can it be avoided?	- It can be caused if there are constant pings from your security device - A way is to spend some time determining exactly what should be reported

Quiz

Chapter 13

Scenario Questions 1 – 3

You notice a very high volume of traffic from a host in your network to an external one. You don't notice any related malware alerts, and the remote host does not show up on your threat intelligence reports as having a suspected malicious IP address. The source host is a Windows workstation belonging to an employee who was involved in an altercation with a manager last week.

[1]

Question #1

- **You are not sure if this is suspicious or not. How can you best determine whether this behavior is normal?**
  - **A. Manual review of syslog files**
  - **B. Historical analysis**
  - **C. Packet analysis**
  - **D. Heuristic analysis**

[1]

Answer #1

- **B**
  - **Historical analysis allows you to compare a new data point to previously captured ones.**
  - **Syslog files and captured packets would be unlikely to tell whether the behavior is normal unless they contained evidence of compromise.**
  - **Heuristic analysis could potentially be useful but is not as good of an answer as historical analysis.**

[1]

Question #2

- **You decide to do a manual review of log files. Which of the following data sources is least likely to be useful?**
  - **A. Firewall logs**
  - **B. Security event logs**
  - **C. Application event logs**
  - **D. Syslog logs**

[1]

Answer #2

- **D**
  - **Windows systems are not normally configured to use syslog.**
  - **All other log files would likely be present and might provide useful information.**

[1]

Question #3

- **Which of the following personnel security practices might be helpful in determining whether the employee is an insider threat?**
  - **A. Security awareness training**
  - **B. Separation vacation**
  - **C. Mandatory vacation**
  - **D. Succession Planning**

[1]

Answer #3

- **C**
  - **If the employee is required to go on vacation and the unusual activity ceases, then it is likely due to employee activity.**
  - **Because the replacement individual would have the exact same duties, the absence of such activity by the substitute might indicate malicious or at least suspicious behavior.**

[1]

Question #4

- **Your organization requires that new user accounts be initiated by human resources staff and activated by IT operations staff. Neither group can perform the other's role. No employee belongs to both groups, so nobody can create an account by themselves. Of which personnel security principle is this an example?**
  - **A. Dual control**
  - **B. Separation of duties**
  - **C. Succession**
  - **D. Cross-training**

[1]

Answer #4

- **B**
  - **Separation of duties is characterized by having multiple individuals perform different but complementary subtasks that, together, accomplish a sensitive tasks.**

[1]

Question #5

- **Your organization stores digital evidence under a two-lock rule in which anyone holding a key to the evidence room cannot also hold a to an evidence locker. Each lead investigator is issued a locker with key, but they can only enter the room if the evidence custodian unlocks the door to the evidence room. Of which personnel security principle is this an example?**
  - **A. Dual control**
  - **B. Separation of duties**
  - **C. Succession**
  - **D. Cross-training**

[1]

Answer #5

- **A**
  - **Dual control is characterized by requiring two people to perform similar tasks in order to gain access to a controlled asset.**

[1]

Question #6

- **Your organization has a process for regularly examining assets, threats, and controls and making changes to your staffing, processes, and/or technologies in order to optimize your security posture. What kind of process is this?**
  - **A. Succession planning**
  - **B. Trend analysis**
  - **C. Security as a service**
  - **D. Continual improvement**

[1]

Answer #6

- **D**
  - **Continual improvement is aimed at optimizing the organization in the face of ever-changing conditions.**
  - **Trend analysis could be a source of data for this effort, but this would be an incomplete answer at best.**

[1]

Scenario Question 7 – 9

You notice an unusual amount of traffic to a backup DNS server in your DMZ. You examine the log files and see the results illustrated here. All your internal addresses are in the 10.0.0.0/8 network, while your DMZ addresses are in the 172.16.0.0/12 network. The time is now 3:20 pm (local) on April 6th.

```
Apr 6 15:17:02 mercury sshd[2092]: Failed password for invalid user root from
192.168.192.6 port 34443 ssh2
Apr 6 15:17:02 mercury sshd[2092]: Failed password for invalid user root from
192.168.192.6 port 34443 ssh2
Apr 6 15:17:02 mercury sshd[2092]: Failed password for invalid user root from
192.168.192.6 port 34443 ssh2
Apr 6 15:17:03 mercury sshd[2097]: Failed none for invalid user root from
192.168.192.6 port 34444 ssh2
Apr 6 15:17:05 mercury sshd[2097]: Failed password for invalid user root from
192.168.192.6 port 34444 ssh2
Apr 6 15:17:07 mercury sshd[2097]: Failed password for invalid user root from
192.168.192.6 port 34444 ssh2
Apr 6 15:17:07 mercury sshd[2097]: Failed password for invalid user root from
192.168.192.6 port 34444 ssh2
Apr 6 15:17:08 mercury sshd[2099]: Failed none for invalid user root from
192.168.192.6 port 34445 ssh2
Apr 6 15:17:12 mercury sshd[2099]: Failed password for invalid user root from
192.168.192.6 port 34445 ssh2
Apr 6 15:17:12 mercury sshd[2099]: Failed password for invalid user root from
192.168.192.6 port 34445 ssh2
Apr 6 15:17:12 mercury sshd[2099]: Failed password for invalid user root from
192.168.192.6 port 34445 ssh2
Apr 6 15:19:25 mercury sshd[2153]: Failed none for invalid user root from
192.168.192.6 port 34475 ssh2
Apr 6 15:19:29 mercury sshd[2153]: Failed password for invalid user root from
192.168.192.6 port 34475 ssh2
Apr 6 15:19:34 mercury sshd[2153]: Failed password for invalid user root from
192.168.192.6 port 34475 ssh2
Apr 6 15:19:35 mercury sshd[2153]: Session opened for user root from
192.168.192.6 port 34475 ssh2
```

[1]

Question #7

- **What does the log file indicate?**
  - **A. Use of a brute-force password cracker against an SSH service.**
  - **B. Need for additional user training on remembering passwords.**
  - **C. Manual password-guessing attack against an SSH service**
  - **D. Pivoting from an internal host to the SSH service**

[1]

Answer #7

- **A**
  - **The speed at which successive attempts were made make it unlikely that this incident was the result of a manual attack or a forgetful user.**
  - **There is no evidence to indicate that pivoting, which is lateral movement inside a target network once an initial breach is made, has taken place yet, given that the connection was established less than a minute ago.**

[1]

Question #8

- **What would be your best immediate respond to this incident?**
  - **A. Implement an ACL to block incoming traffic from 192.168.192.6.**
  - **B. Drop the connection at the perimeter router and begin forensic analysis of the server to determine the extent of the compromise.**
  - **C. Start full packet captures of all traffic between 192.168.192.6 and the server.**
  - **D. Drop the connection at the perimeter router and put the server in an isolation VLAN**

[1]

Answer #8

- **D**
  - **The immediate goal of the response should be to isolate the host suspected of being compromised.**
  - **Blocking future attempts and learning what the attacker is up to are both prudent steps but should be done only after the server is isolated.**

[1]

Question #9

- **How could you improve your security processes to prevent this attack from working in the future?**
  - **A. Block traffic from 192.168.192.6.**
  - **B. Improve end-user password security training.**
  - **C. Implement automated log Aggregation and reporting.**
  - **D. Disallow external connections to SSH service.**

[1]

Answer #9

- **D**
  - **The only given choice that would stop this attack in the future is to prevent external connections to SSH.**
  - **Remote users who need such access should be required to connect over a VPN first, which would give them an internal IP address.**

[1]

Scenario for Questions 10 – 11

You were hired as a security consultant for a mid-sized business struggling under the increasing costs of cyber attacks. The number of security incidents resulting from phishing attacks is trending upward, which is putting an increased load on the business's understaffed security operations team. That team is no longer able to keep up with both incident responses and an abundance of processes, most of which are not being followed anyway. Personnel turnover in the security shop is becoming a real problem. The CEO wants to stop or reverse the infection trend and get security costs under control.

[1]

Question #10

- **What approach would you recommend to quickly reduce the rate of compromises?**
  - **A. Trend analysis**
  - **B. Automated reporting**
  - **C. Security as a Service**
  - **D. Security awareness training**

[1]

Answer #10

- **D**
  - **The issues to be that users are more often falling for phishing attacks, which points to a need form improved personnel training more so than any other approach.**

[1]

Question #11

- **How would you address the challenge of an overworked security team?(Choose two.)**
  - **A. Cross-training the security staff**
  - **B. Outsourcing security functions**
  - **C. Retirement of processes**
  - **D. Mandatory vacations**
  - **E. Increasing salaries and/or bonuses**

[1]

Answer #11

- **B, C**
  - **Outsourcing some of the security operations can strike a balance between the need to keep some functions in-house while freeing up time for the security team.**
  - **Additionally, the organization appears to have excessive processes that are not being followed, so retiring some of those would likely lead free up some more time.**
  - **Cross-training might be helpful if the workload was uneven compared to the skillsets, but there is no mention of that being the case in this scenario.**

[1]

References

1. Maymí Fernando, and Brent Chapman. CompTIA CSA+ Cybersecurity Analyst Certification All-in-One Exam Guide (Exam CS0-001). McGraw-Hill Education, 2018.