12.2.4 Isolate and Containment Facts

This lesson covers the following topics:

- Isolation, containment, and segmentation
- Security orchestration, automation and response (SOAR)
- Incident plans

Isolation, Containment, and Segmentation

Data, whether good or malicious, must be handled correctly. You can use isolation and containment for malicious or suspect data. You can use segmentation as a strategic network architecture tool to prevent outside data from accessing internal network appliances.

Strategy	Description
Isolation	Isolation limits the ability of a compromised process or application from doing more harm to the network or its assets. One way to protect the network is process isolation. This ensures that if a process is compromised, only the resources that are used by that process are at risk.
Containment	Containment is the first step after an event has been detected and identified. This action can take a few forms. You can disconnect a machine from the network by unplugging the Ethernet cable or disabling the NIC. If a network is connected to other networks, you can terminate those connections.
Segmentation	Segmentation is a strategic network design. The concept is simple; keep the sections of a network separated so that malicious actors cannot pivot within a network. You can segment using VLANs, software defined networks, switches, subnetting, or even physical segmentation. Being on a different subnet is not enough. You must implement rules to control the kind of communications that occur between assets on the network. You can also create a demilitarized zone (DMZ). It is a virtual area where you separate assets from internal network assets. A network with a DMZ may have a single firewall or two firewalls depending on how secure the segment needs to be. No matter the topography, access between the DMZ and the internal network is access controlled.

Security Orchestration, Automation and Response (SOAR)

SOAR is a platform to compile security data generated by different security endpoints. This compiled information is then sent to a security analyst for further action. SOAR frees an analyst from constantly receiving security alerts as they are generated. Analysts can use parameters to automate solutions for security incidents that meet certain criteria. SOAR:

- Gathers alert data and places it in specified location.
- Facilitates application data integration.
- Facilitates focused analysis.
- Creates a single security case.
- Allows for multiple playbooks and playbook step automation.

Incident Plans

As part of the incident response process, you can use playbooks and runbooks together to achieve a more effective response that can be automated and include tasks that are automatically assigned to analysts to complete. These two plans can also help to meet and comply with regulatory frameworks like GDPR or NIST if necessary.

Plan Type	Description
Runbooks	Runbooks are a condition-based series of protocols you can use to establish automated processes for security incident response. Assessment, investigation, and mitigation are accelerated with the use of a runbook. Even though processes are automated, human analysis is still used in some cases.
Playbooks	A playbook is a checklist style document that specifies the steps to be taken in response to a threat or incident. The steps are listed in the order to be performed. A playbook ensures a consistent approach to security issues.