CYBER SECURITY DIFENCE

PRESENTED BY SRIMATHI.R

THE KAVERY ENGINEERING COLLEGE

CYBER SECURITY DEFENCE

OUTLINE

1. Security operations
2. Security operations diagram
3. Security Information event management
4. Incident response team
5. Containment
6. Conclusion

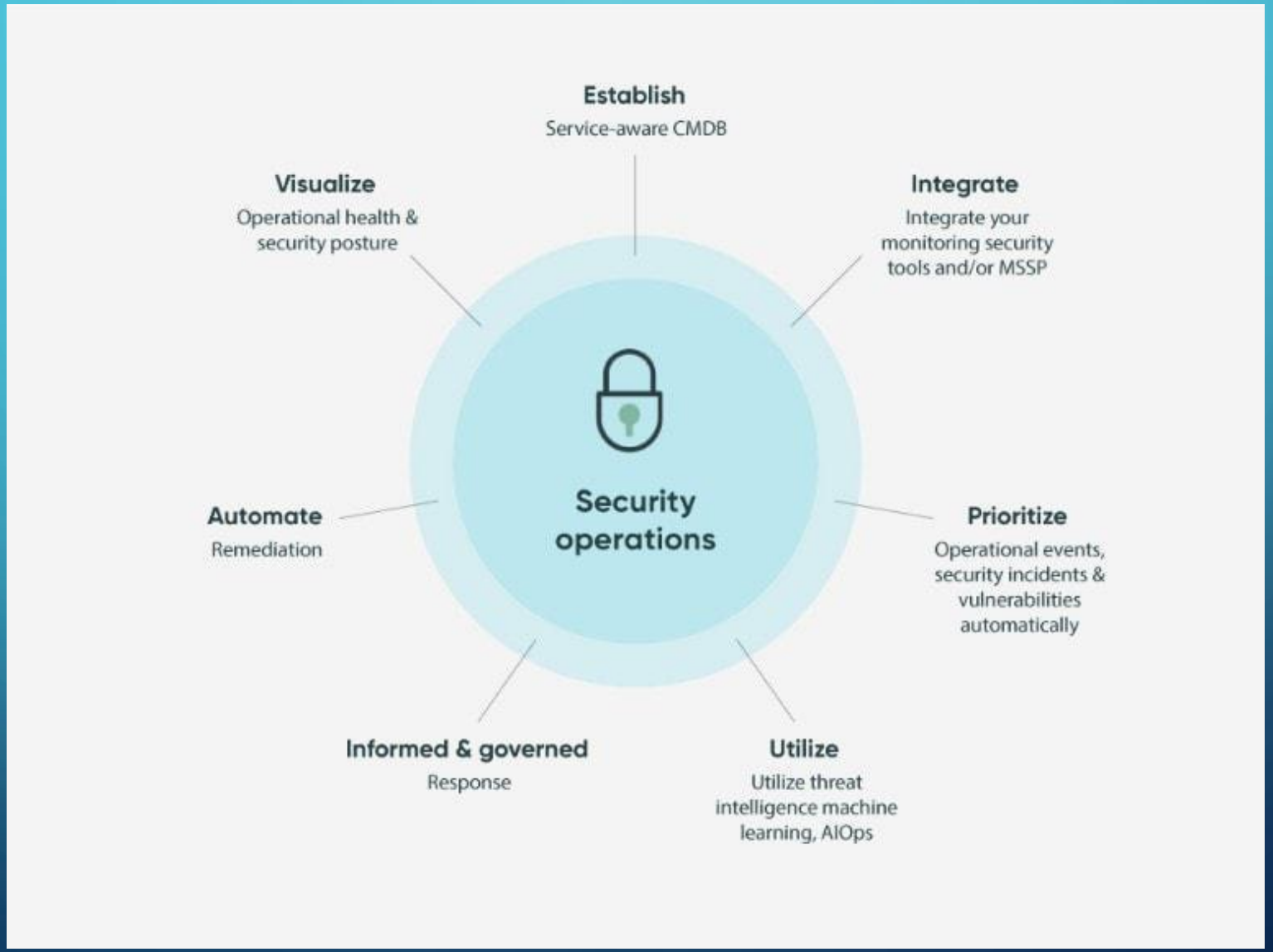
SECURITY OPERATIONS

Security Operations is often contained within a SOC ("Security Operations Center").

Terms are used interchangeably.

Typically the SOC's responsibility is to detect threats in the environment and stop them from developing into expensive problems.

SECURITY OPERATIONS DIAGRAM



SECURITY INFORMATION EVENT MANAGEMENT

Most systems produces logs often containing important security information.

An event is simply observations we can determine from logs and information from the network, for example:

- Users logging in
- Attacks observed in the network
- Transactions within applications

An incident is something negative we believe will impact our organization. It might be a definitive threat or the potential of such a threat happening. The SOC should do their best to determine which events can be concluded to actual incidents, which should be responded to.

INCIDENT RESPONSE TEAM

An IRT is a dedicated team to tackle Cyber Security Incidents. The team may consist of Cyber Security specialists only, but may synergize greatly if resources from other grouping are also included. Consider how having the following units can greatly impact how your team can perform in certain situations:

- Cyber Security Specialist - We all know these belong on the team.
- Security Operations - They might have insights into developing matters and can support with a birds eye view of the situation.
- IT-Operations
- Network Operations
- Development
- Legal
- HR

CONTAINMENT

Containment should try stop the attackers in their tracks and prevent further damages. This step should ensure the organization does not incur any more damages and ensure the attackers can not reach their objectives.

The IRT should as soon as possible consider if a backup and imaging should be done. Backup and imaging is useful to preserve evidence for later. This process should try to secure.

•A copy of the hard-drives involved for file forensics
•A copy of the memory of the involved systems for memory forensics

There are many actions the IRT can do to stop the attackers, which very much depends on the incident in question:

CONCLUSION

Tools and documentation should be up to date and safe communication channels already negotiated. The team should ensure the necessary business units and managers can receive continuous updates on the development of incidents which impact them.