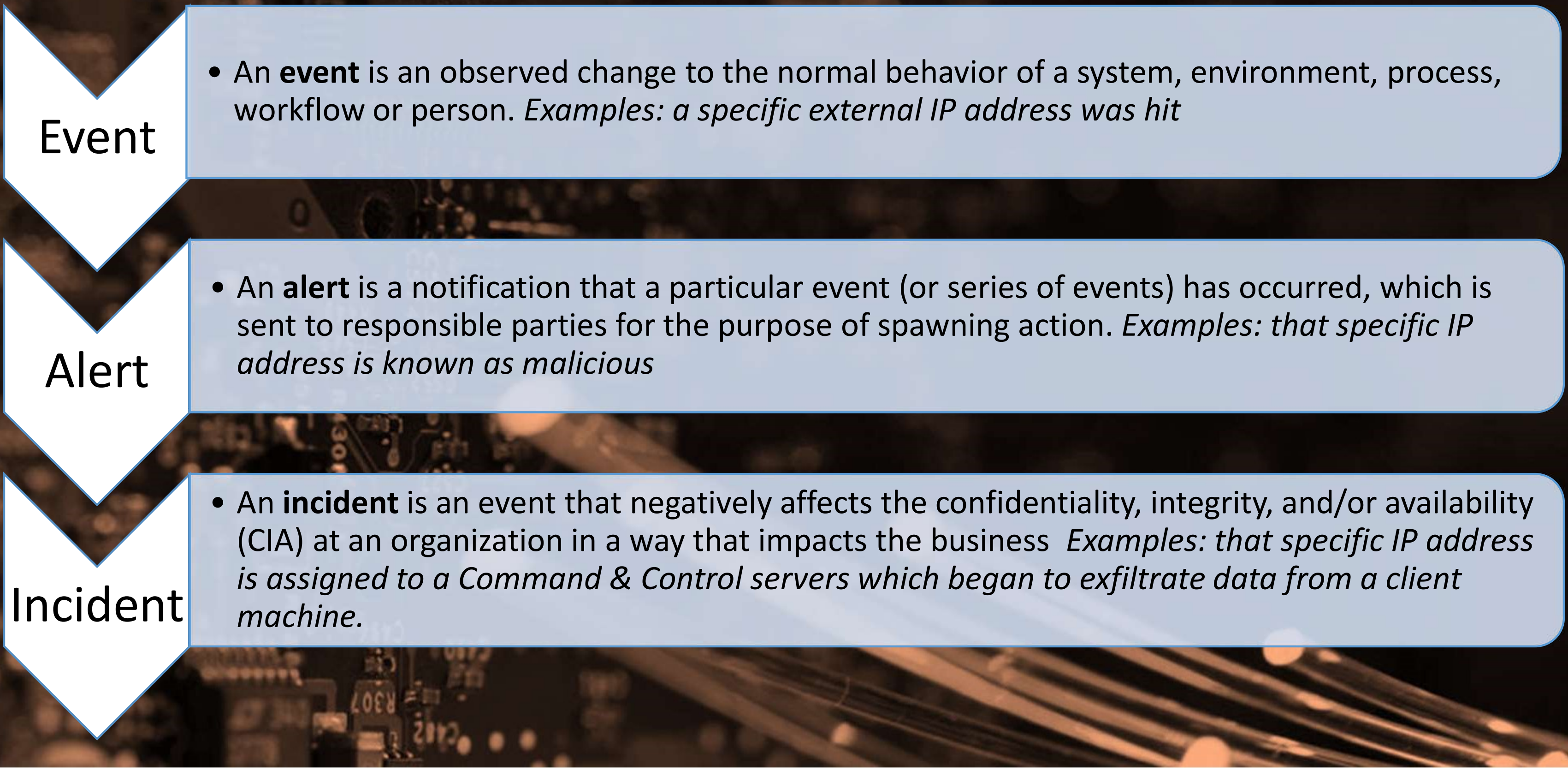
Course 4

- Alerts, events, incidents
- Incident management ticketing system
- Events Detection&prevention mechanisms: Yara Rules & Regex
- Usint Open-source Intelligence (OSINT)

Events, alerts, incidents



Event

- An **event** is an observed change to the normal behavior of a system, environment, process, workflow or person. *Examples: a specific external IP address was hit*

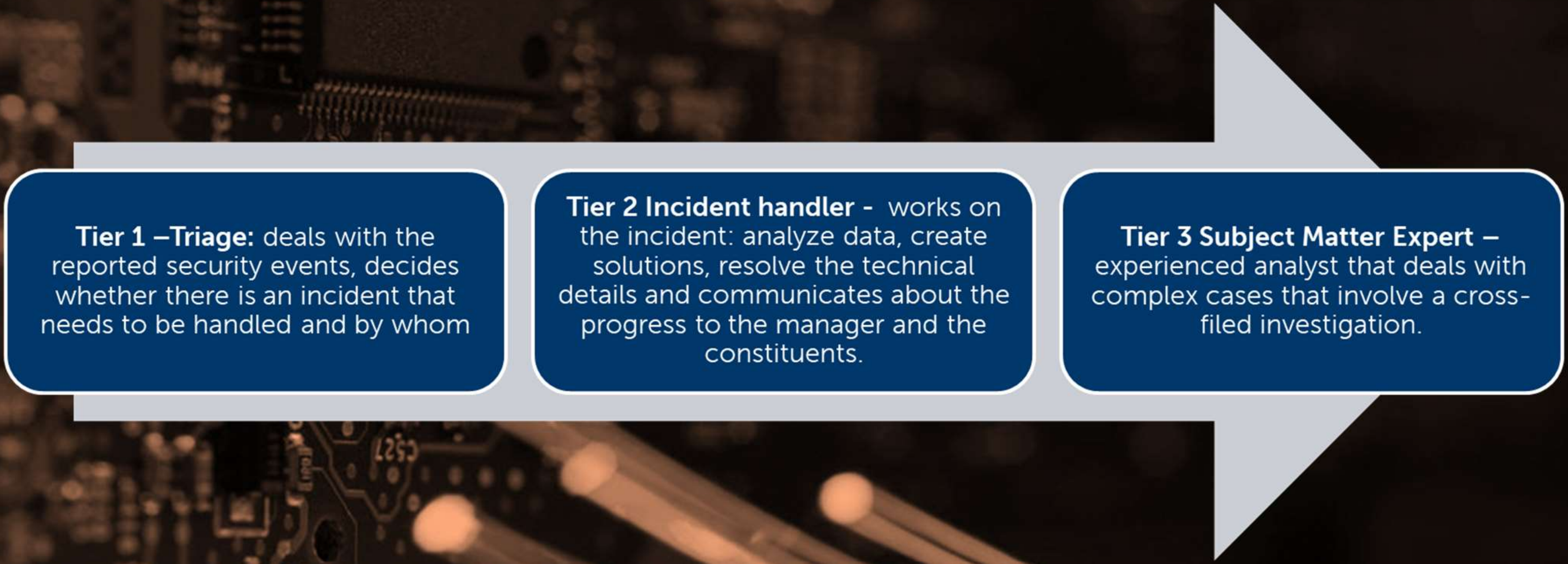
Alert

- An **alert** is a notification that a particular event (or series of events) has occurred, which is sent to responsible parties for the purpose of spawning action. *Examples: that specific IP address is known as malicious*

Incident

- An **incident** is an event that negatively affects the confidentiality, integrity, and/or availability (CIA) at an organization in a way that impacts the business *Examples: that specific IP address is assigned to a Command & Control servers which began to exfiltrate data from a client machine.*

Incident Handling – Roles

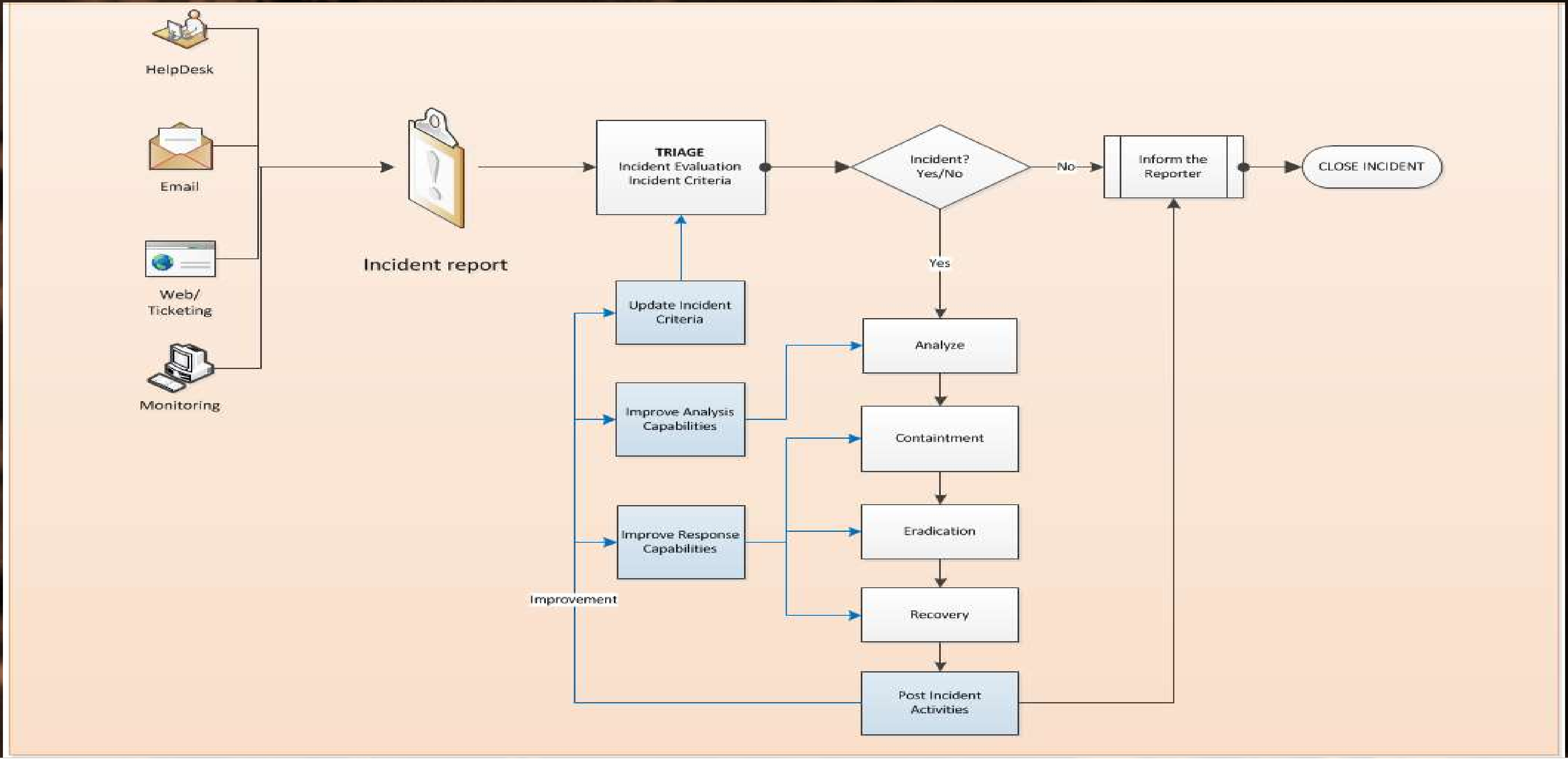


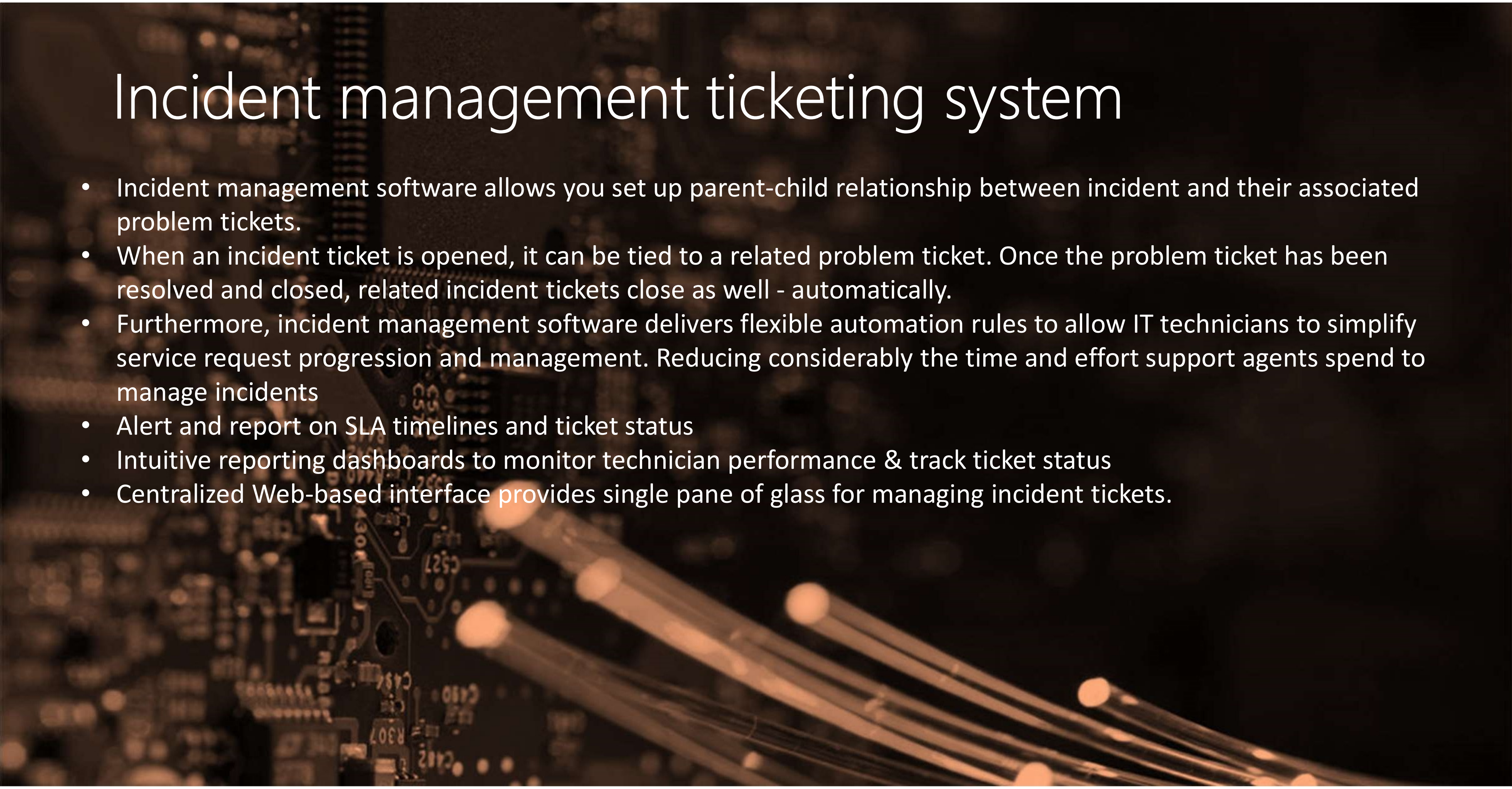
Tier 1 –Triage: deals with the reported security events, decides whether there is an incident that needs to be handled and by whom

Tier 2 Incident handler - works on the incident: analyze data, create solutions, resolve the technical details and communicates about the progress to the manager and the constituents.

Tier 3 Subject Matter Expert – experienced analyst that deals with complex cases that involve a cross-filed investigation.

Incident Handling - Workflows

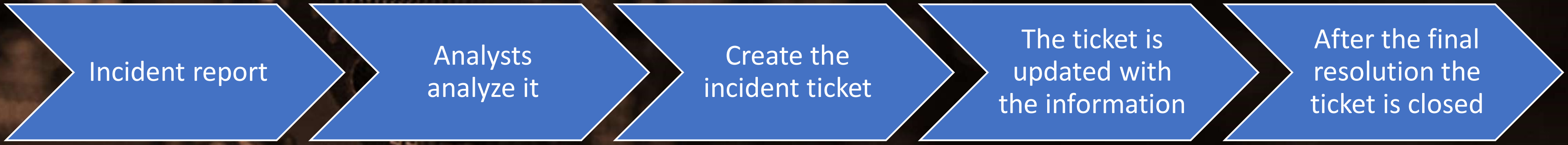




Incident management ticketing system

- Incident management software allows you set up parent-child relationship between incident and their associated problem tickets.
- When an incident ticket is opened, it can be tied to a related problem ticket. Once the problem ticket has been resolved and closed, related incident tickets close as well - automatically.
- Furthermore, incident management software delivers flexible automation rules to allow IT technicians to simplify service request progression and management. Reducing considerably the time and effort support agents spend to manage incidents
- Alert and report on SLA timelines and ticket status
- Intuitive reporting dashboards to monitor technician performance & track ticket status
- Centralized Web-based interface provides single pane of glass for managing incident tickets.

Incident management ticketing system - workflow



Incident report

Analysts analyze it

Create the incident ticket

The ticket is updated with the information

After the final resolution the ticket is closed

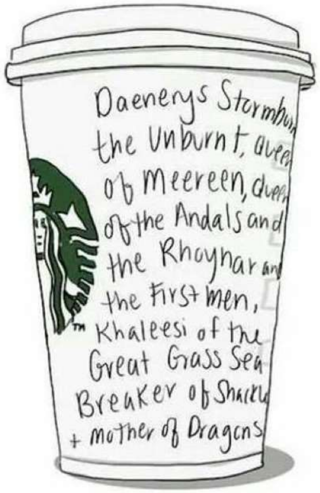
servicenow

solarwinds

salesforce

If the problem is not fully resolved, the ticket will be reopened once the technician receives new information from the customer

Questions?



NOW let's drink some coffee!

THANK YOU