Incident Management 101 BY P3NGU1N

Basic Definitions About Incident Management

> 🎯 A web attack alert has occurred because I have logged into the following URL address. Is this alert a false positive or a true positive?
>
> https://www.w3schools.com/sql/trysql.asp?filename=trysql_select_union3
>
> ANSWER: false positive

Incident Management Systems (IMS)

> 🎯 Which button in the “Investigation Channel” should we click to open a record on “Case Management” on the LetsDefend platform?
>
> ANSWER: create case

> 🎯 Which is not a feature of the Incident Management System
>
> - Workflow
> - Automation / API access
> - Close, open, edit action
> - Prevention
>
> ANSWER: prevention

Case/Alert Naming

🎯 The case/ticket format in LetsDefend is as follows:

EventID: {Alert ID Number} - [{Alert Name}]

According to this information, how can the ticket be created for the alert with ID number 25 and rule name "SOC15 - Malware Detected" be named?

ANSWER: eventid: 25 - [soc15 - malware detected]

QUIZ:

🎯 **What is IMS?**

ANSWER: **Incident Management System**

🎯 **What is the main reason to use a standard naming convention in Ticket/Alert names?**

ANSWER: **In order to have an idea when looking at the Ticket/Alert names**

🎯 **Which of the following may be a ticket name for an IMS using a naming convention like EventID: {Alert ID Number} - [{Alert Name}]**

ANSWER: **EventID: 15 - [Log4j Detected]**

🎯 **Why are Playbooks in SOAR and IMS important?**

ANSWER: **For providing the establishment of an analysis standard**

🎯 **What should the SOC analyst do for analysis after an alert in SIEM?**

ANSWER: **Create a ticket in IMS/SOAR and follow the playbook**