

# Incident Investigation with IBM Security QRadar

---

## The Incident Response Process



**Ricardo Reimao, OSCP, CISSP**  
Cybersecurity Consultant



# Investigating threats and responding to incidents



# QRadar Courses

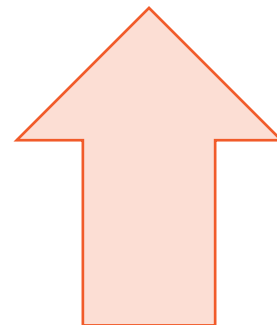
## IBM Security QRadar: Functions and Capabilities



**Monitor and Detect**  
(SOC Analyst)



**Incident Response**



**Admin and Engineer**



**Threat Hunting**



# Responsibilities of a Incident Response Specialist

**Review cases and  
declare incidents**

**Understand the  
scope and impact of  
an attack**

**Collect indicators of  
compromise  
(IoCs)**

**Determine  
impacted assets  
and impacted data**

**Eradicate and  
contain the threat**

**Help creating a  
recovery plan**



# QRadar and Incident Investigation



**QRadar centralizes security data in one place**

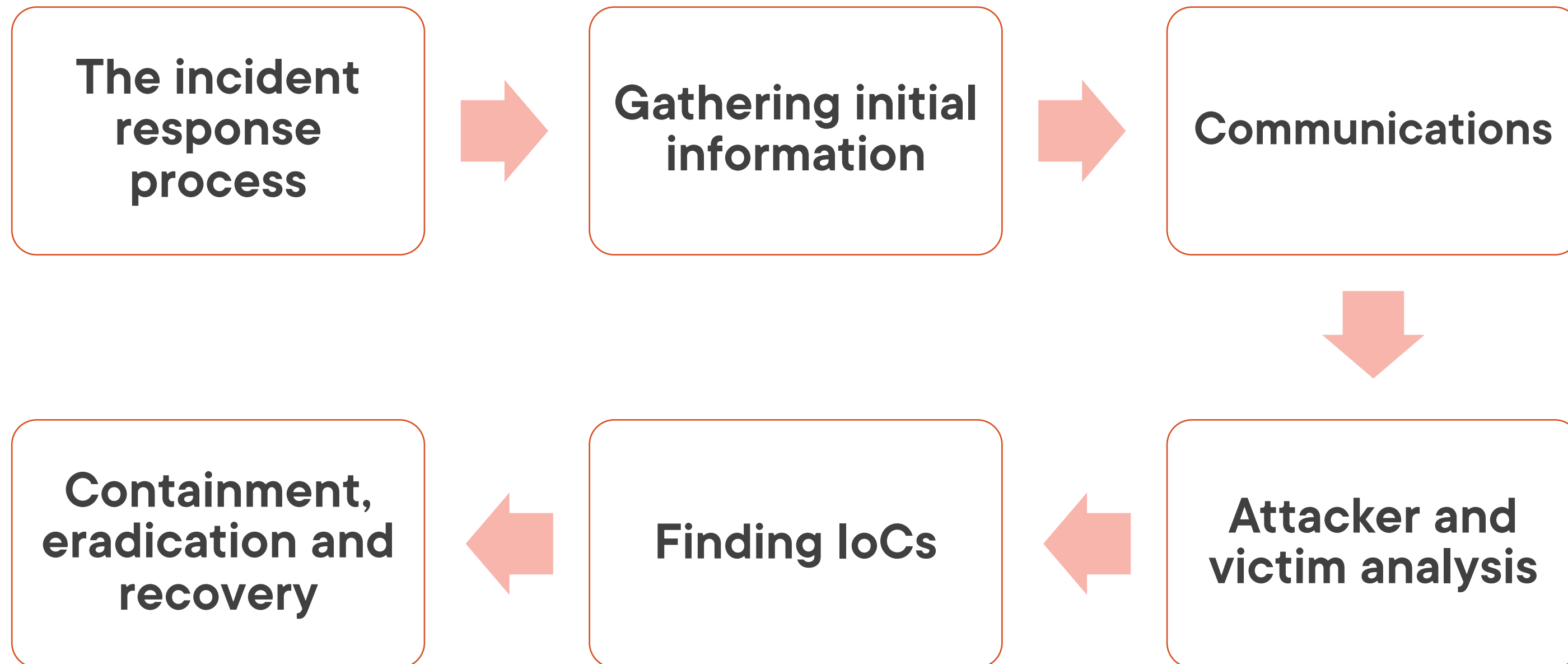
**Correlate data to identify threats**

- Logs, network traffic, vulnerabilities, etc.**

**Access historical data and previous cases**

**Setup detection rules**

# Course Overview



Two major incidents



# Scenario: The Globomantics QRadar



**You just got hired by Globomantics**

**You will work as an incident response (IR) specialist.**

**There are two major incidents to investigate**

**You are responsible for:**

- Investigating offenses raised by the SOC**
- Determining scope of the threats**
- Collecting indicators of compromise (IoCs)**
- Creating containment and eradication plans**

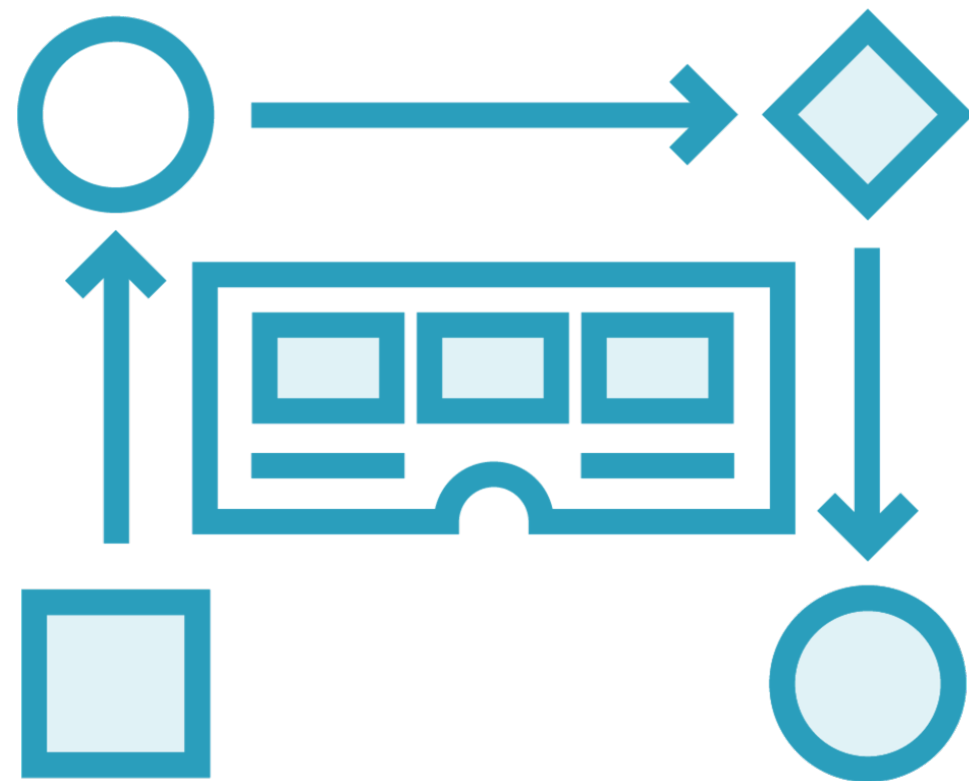


# The Incident Response Process

---



# The Importance of Following a Process



**During real incidents, the stress might lead to mistakes**

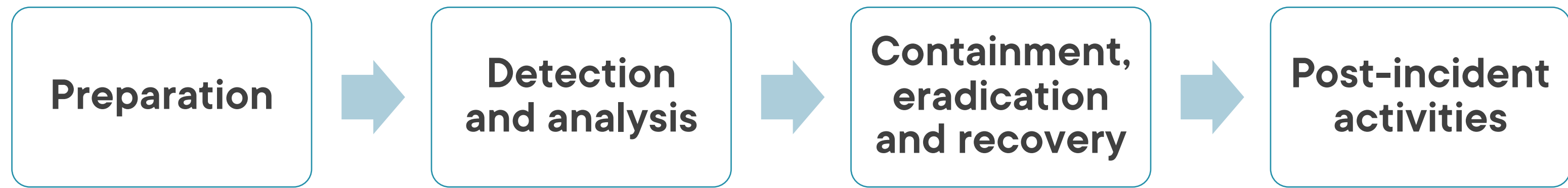
**The process ensures that best practices are followed**

**Ensures consistency on investigations**

**Ensures that the case can be investigated by multiple specialists**



# Process Overview



**Based on National Institute of Standards and Technology (NIST) process:**

**Computer Incident Handling Guide (NIST 800-61)**

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>



# Preparation



**Define an incident response plan**

**Define roles and responsibilities**

**Creating support documentation**

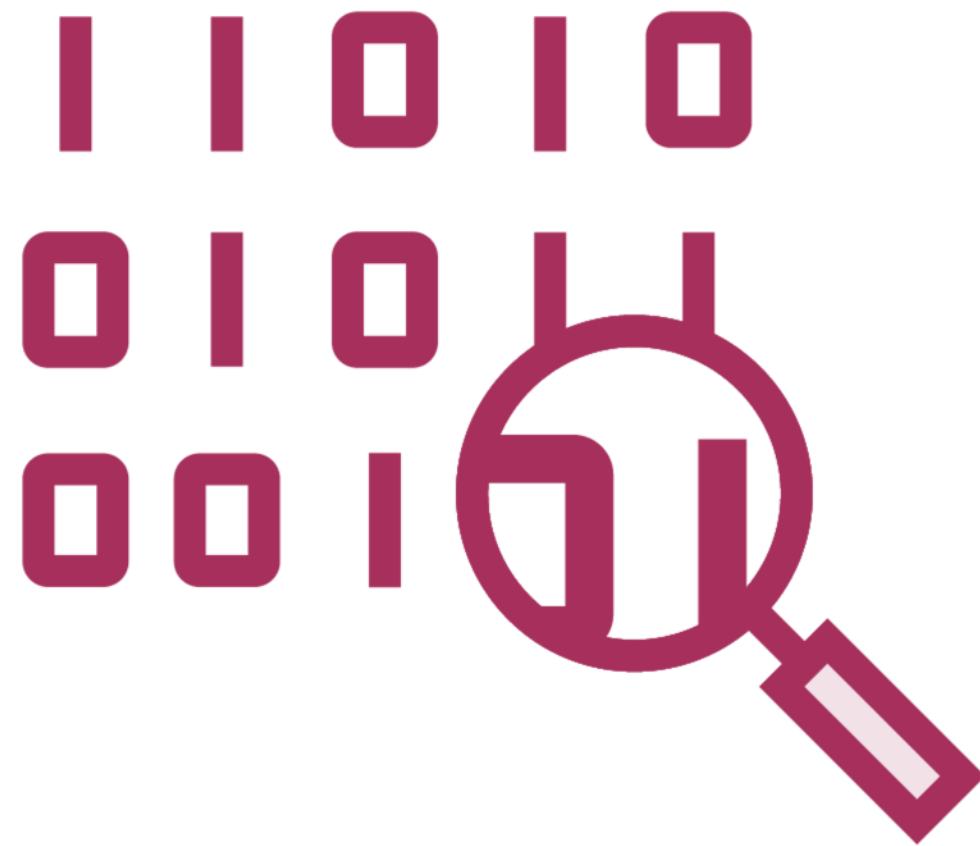
**– Templates, procedures, etc.**

**Rehearsing processes and simulating incidents**

**Courses focused on preparation**



# Detection and Analysis



**Main topic of this course**

**Confirm the incident**

**Understand the impact and scope**

**Analyze the targets and attackers**

**Collect indicators of compromise (IoCs)**

**Create an incident timeline**

**Communicate stakeholders**



# Containment, Eradication and Recovery



## Decide on the containment goals

- Restore business
- Preserve evidences
- etc.

## Contain the threat

- Isolate machines, block traffic, etc.

## Eradicate the threat

- Remove malware, remove backdoors, delete accounts, fix vulnerabilities, etc.

## Recover from the incident

- Restore from backups, re-image devices, system hardening, etc.

# Post-incident Activities



**In-depth review of the incident**

**Understand the point of entry and hardening the environment**

**Implementing detection mechanisms**

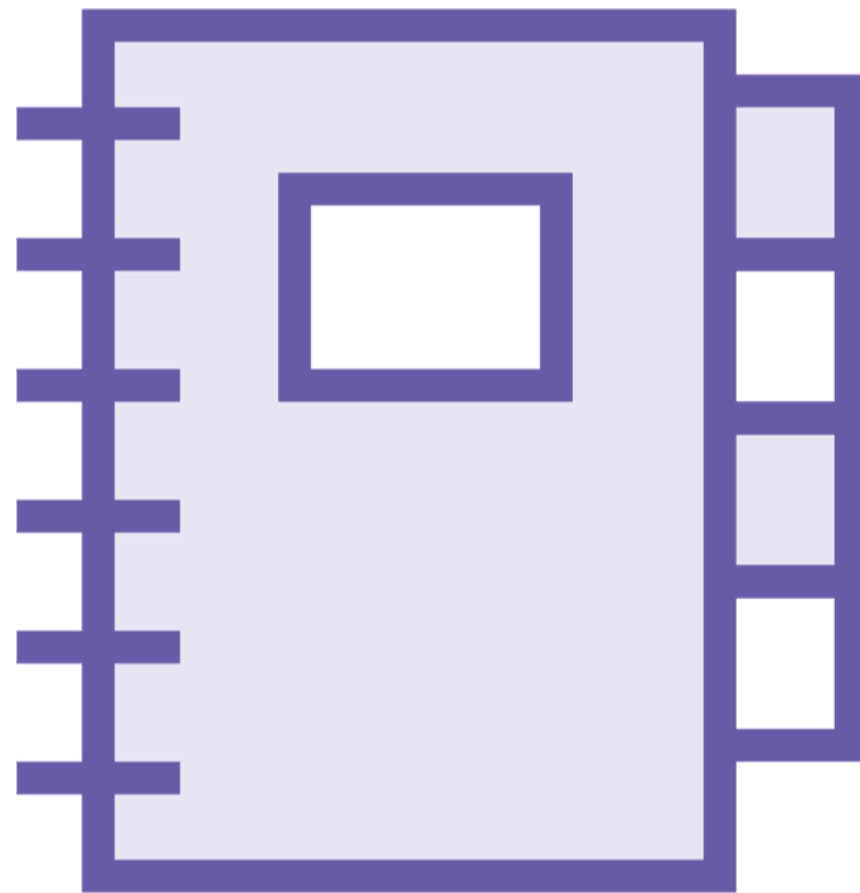
**Performing lessons-learned analysis**

# Incident Notes and Timeline

---



# The Importance of Notes and Documentation



**Large amounts of data during an incident**

**Stress factor during real incidents**

**Take notes right away**

**Document everything you find and every step of your investigation**

**Reporting the case to stakeholders or even law enforcement**



# Main Information to Note

**Impacted  
servers**

**Attacker  
information**

**Indicators of  
Compromise  
(IoCs)**

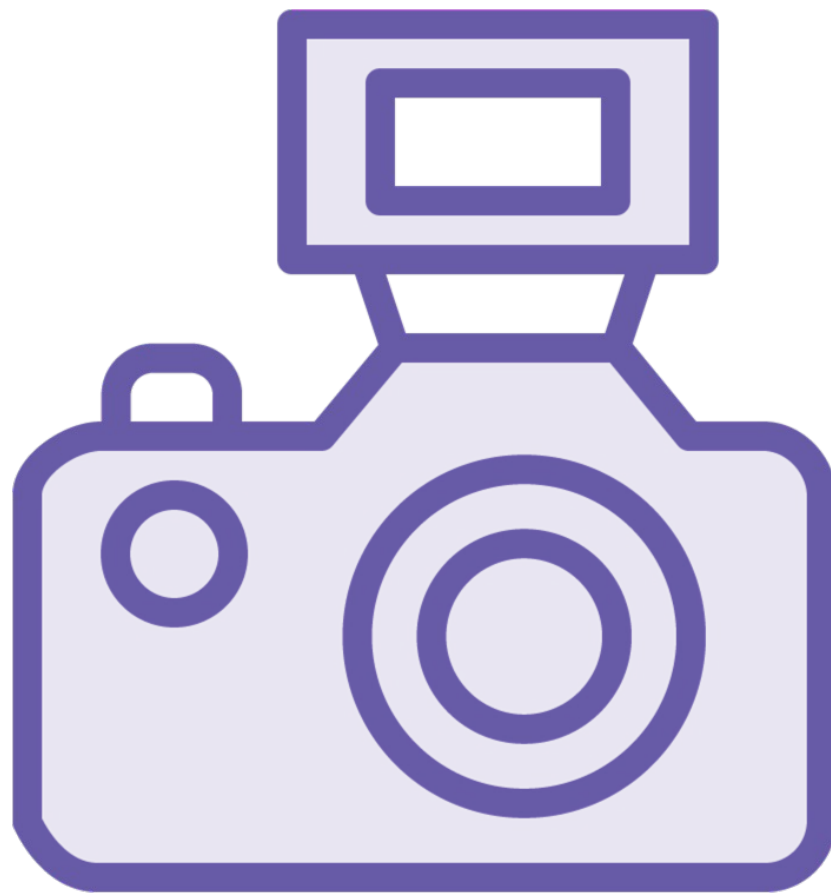
**Investigation  
steps**

**To-do tasks**

**...any other  
information**



# Collecting Evidences



**In case you need to report the incident**

- **Specially for law enforcement**

**Ensure you are not tampering the evidence**

**Most common evidences:**

- **Logs, network traffic, malicious software, compromised accounts, etc.**

# Incident Timeline

Timestamp	Action
2023-06-30 @ 09:50	User (robertf) received an email containing malware
2023-06-30 @ 12:18	Ransomware start to run and files start to be encrypted
2023-06-30 @ 14:23	User (robertf) called IT support regarding ransomware on his laptop
2023-06-30 @ 14:56	Incident escalated to the IR team (Lead: Ricardo)
2023-06-30 @ 16:15	The machine was isolated and re-imaged. Investigating the scope
2023-06-30 @ 17:10	Few other users received same email, but none of them opened. Created email filtering rule and new detection rules.

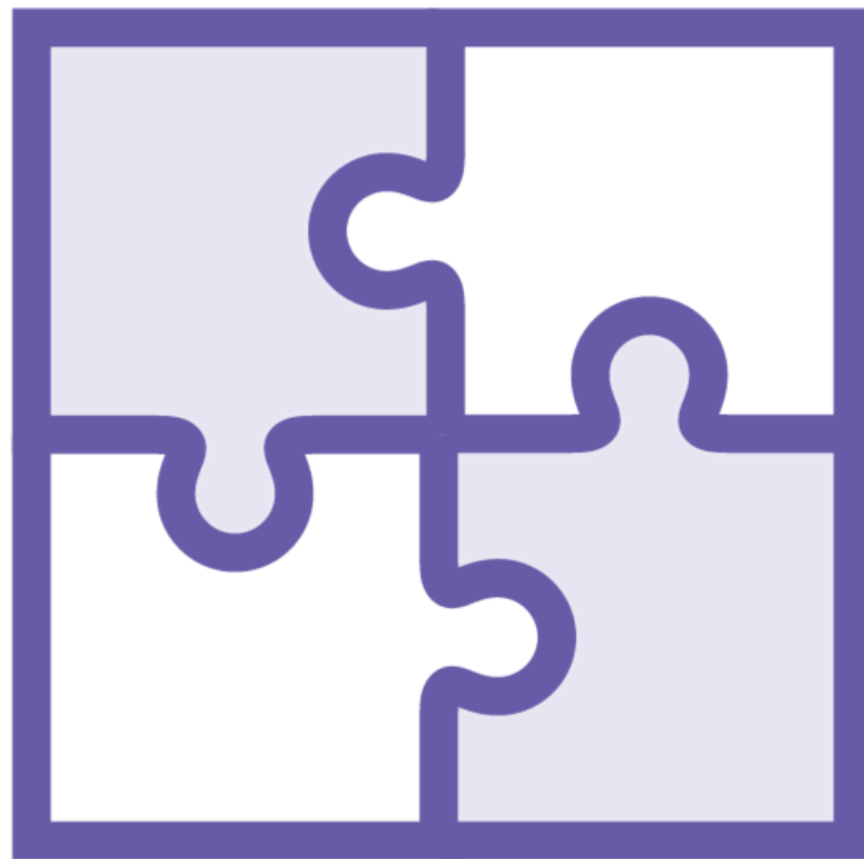


# Working with SOAR Platforms

---



# What Are SOAR Platforms?



## **Security Orchestration Automation and Response (SOAR)**

**A platform that collects data from QRadar (and other tools) so you can automate some responses**

**Allows you to review data and automate tasks across multiple security platforms**

- SIEM, IPS, DLP, firewall, vulnerability scanner, etc.**

**Common in large companies with several security tools**



# Main SOAR Platforms

**IBM Security  
SOAR**

**Splunk SOAR**

**Swimlane**

**Siemplify**

**FortiSOAR**

**20+ other vendors**



# Investigating Incidents Using SOAR



**All data is in one place**

**Some of the remediation actions might already be automated**

- Example: Blocking IPs on the firewall**

**Investigating the case and reviewing remediation actions**

# Summary



**The role of an IR specialist**

**The IR processes phases**

- **Preparation**
- **Detection and analysis**
- **Eradication, containment and recovery**
- **Post-incident activities**

**The importance of notes and timelines**

**How to work with SOAR platforms**



**Next up:**  
Incident Investigations

