

What is the purpose of an incident responder

ChatGPT said:

The purpose of an **Incident Responder** is to **detect, investigate, and respond to cybersecurity incidents** to protect an organization's digital assets and reduce the impact of potential threats. Think of them as digital firefighters—jumping into action when there's suspicious activity or a confirmed breach.

Here's a breakdown of their main goals:

1. Detection

- Monitor networks, systems, and logs (often using SIEM tools like Splunk) to identify unusual or malicious activity.
- Analyze alerts from security tools (e.g., IDS/IPS, antivirus, EDR).

2. Investigation

- Determine the scope, nature, and impact of the incident.
- Use threat hunting, log analysis, and forensic tools to trace how the attack happened and what was affected.

3. Containment

- Stop the spread of the threat. This might mean isolating infected machines or disabling compromised accounts.

4. Eradication & Recovery

- Remove the threat from the environment.
- Restore affected systems, services, and data to normal operation.

5. Reporting & Documentation

- Create detailed incident reports for internal use, legal reasons, or compliance.
- Log lessons learned to improve future responses.

6. Prevention & Hardening

- Recommend security improvements based on findings (e.g., patching vulnerabilities, changing configurations).
- Help develop and test incident response plans and run simulations.

Would you like an example of a real-world incident response scenario?

40

You said:

yes give an example

ChatGPT said:

Cool! Here's a simplified real-world style **incident response scenario** to help you visualize the process:

Incident Scenario: Suspicious Login Behavior on a Company Server

Step 1: Detection

The SIEM tool (like Splunk) triggers an alert:

"Multiple failed login attempts followed by a successful login from a foreign IP address to a critical server."

An analyst sees that the login was successful from an IP in Russia, but the user is normally based in New York.

Step 2: Investigation

The Incident Responder starts digging:

- **Correlates logs:** Finds 50+ failed logins in 2 minutes before success.
- **Checks login time:** It happened at 3:12 AM local time—unusual for that user.
- **Pulls historical data:** This user has never logged in from that region or at that time before.
- **Inspects user activity:** After login, the attacker accessed sensitive HR files and tried to create a new user account.

Step 3: Containment

- Disable the compromised account immediately.
- Block the suspicious IP in the firewall.
- Isolate the affected server from the network for forensic analysis.

Step 4: Eradication & Recovery

- Remove any backdoors or rogue user accounts the attacker created.
- Re-image the compromised server to ensure it's clean.
- Reset passwords and force MFA for all critical accounts.

Step 5: Reporting

- Document the attack timeline, impact, actions taken, and lessons learned.
- Submit the report to leadership and, if necessary, legal/compliance teams.

Step 6: Lessons Learned

- Implement stricter geolocation-based login controls.
- Enforce MFA on all critical systems.
- Add anomaly detection for account behavior.

Let me know if you want to build a mini version of a scenario like this using Splunk logs—you could use it as part of your threat hunting project!

40

You said:

can you give me an image of how this project will look

ChatGPT said:

Image created

Search

Save As

Create Alert

Export



index=main "Failed password" OR "Accepted password" johndoe

Search

Show results 14,809 sec.

Last 7h. d.m.res.d.) ▾

1-5 ticks

Time line ▾

A-Z ▾

Sort ▾

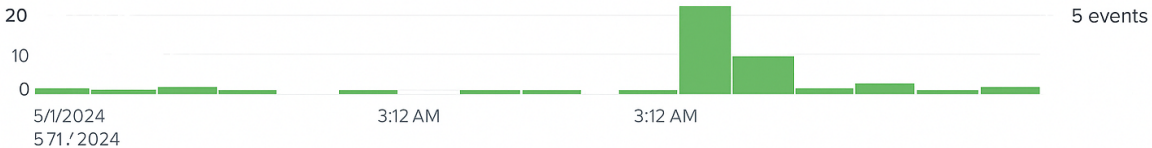
NoSalt ▾

Events

Patterns

Statistics

Visualization



Date ▾	Event	9 Times ▾	Selected Fields	
5/1/24 3:15:52.000	3:12:07.012.07 AM Accepted password for johndoe from 198.51.100.53 port 45672 ssh2		host	1
5/1/24 3:15:52.000	Failed password for johndoe from 192.168.1.50 port 54721 ssh2		192.0.2.1	
5/1/24 3:15:52.000	Failed password for johndoe from 192.168.1.60 port 54721 ssh2		source	3
5/1/24 3:15:52.000	Failed password for johndoe from 192.168.1.70 port 54711 ssh2		/var/log/secure	
5/1/24 3:15:52.000	Failed password for johndoe from 192.168.1.80 port 173.1.7.52		sourcetype	
5/1/24 3:15:52.000	Failed password for johndoe from 192.168.1.85 port 128.51.118		linux_secure	
			Interesting Fields	
			host	1

Search

Save As

Create Alert

Export



index=main "Failed password" OR "Accepted password" johndoe

Search

Show results 14,809 sec.

Last 7h. d.m.res.d.) ▾

1-5 ticks

Time line ▾

A-Z ▾

Sort ▾

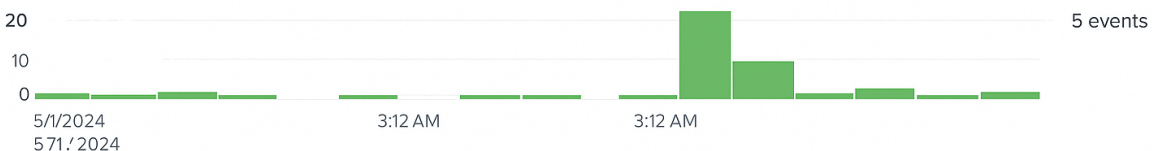
NoSalt ▾

Events

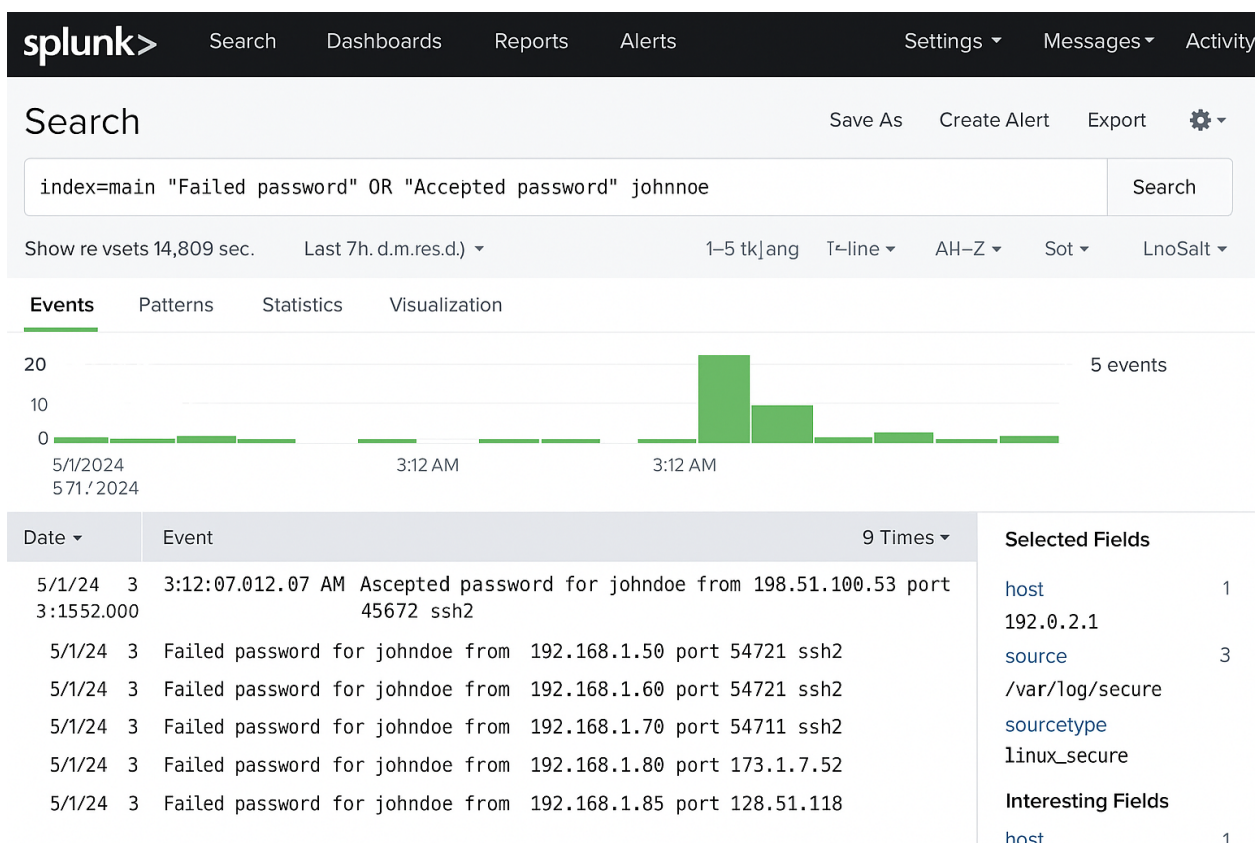
Patterns

Statistics

Visualization



Date ▾	Event	9 Times ▾	Selected Fields	
5/1/24 3:15:52.000	3:12:07.012.07 AM Accepted password for johndoe from 198.51.100.53 port 45672 ssh2		host	1
5/1/24 3:15:52.000	Failed password for johndoe from 192.168.1.50 port 54721 ssh2		192.0.2.1	
5/1/24 3:15:52.000	Failed password for johndoe from 192.168.1.60 port 54721 ssh2		source	3
5/1/24 3:15:52.000	Failed password for johndoe from 192.168.1.70 port 54711 ssh2		/var/log/secure	
5/1/24 3:15:52.000	Failed password for johndoe from 192.168.1.80 port 173.1.7.52		sourcetype	
5/1/24 3:15:52.000	Failed password for johndoe from 192.168.1.85 port 128.51.118		linux_secure	
			Interesting Fields	
			host	1



Rate this image

You said:

can you let me know how I will do this in 2 weeks timeline

ChatGPT said:

Absolutely! Here's a simple **2-week timeline** for your mini threat hunting project using Splunk. It's designed to keep things realistic and manageable while giving you time to explore, learn, and document.


🔥 Week 1 – Setup, Exploration & Hunting

✅ Day 1–2: Project Kickoff

- Define scope: What do you want to hunt? (e.g. failed logins, malware, lateral movement)
- Set goals: E.g., “Detect suspicious login patterns and write a report.”
- Get datasets: Use open Splunk datasets (e.g. Linux auth logs, Windows logs).
- Prepare your Splunk instance or lab environment.

✅ Day 3–4: Learn Splunk Search Basics

- Practice with `index=main` and basic `search`, `stats`, `timechart`, `eval`.

- Try:
`spl`


```
index=main sourcetype=linux_secure "Failed password"
```

-
- Watch out for trends in login failures or odd IPs.

✅ Day 5–7: Start Threat Hunting

- Create hunting hypotheses:
 - “If a user logs in after multiple failures from an unusual IP, it could be a brute-force.”
- Build Splunk queries to hunt:
 - Track failed logins, then successful logins from same IP.
 - Use fields like `user`, `src_ip`, `port`, `timestamp`.

Week 2 – Analysis, Reporting & Presentation

✅ Day 8–9: Deep Dive Investigation

- Isolate interesting events and build timelines.

- Link behaviors together: did the attacker try privilege escalation or data access?
- Optional: use diagrams or visuals.

Day 10–11: Documentation

- Write your report:
 - Summary of goals
 - Methodology (how you hunted)
 - Key findings
 - Recommendations
- Add screenshots (like the Splunk one we generated!).

Day 12–13: Final Review

- Review your queries and findings.
- Double-check for accuracy and clarity in your report.

Day 14: Wrap-Up & Share

- Present your findings to a mentor, class, or just for your portfolio.
- Reflect: What did you learn? What would you do differently?

Would you like a report template or a checklist to guide your documentation?