CODEPATH.ORG

Capstone

Bryant Aguirre
Gulnaz Mukanbetova
Josh Philip
Rishi Nalam

CYB102 | Intermediate Cybersecurity

SSH Brute Force IP/User/Password

Attacks from the internet on an SSH server.

Data Card | Code (1) | Discussion (0) | Suggestions (0)

About Dataset

Context

I set up an SSH server, enabled password SSH authentication, and exposed port 22 to the internet. This data is from a little bit under a week of activity, updated versions will be posted in the future.

Content

1. Username the attacker used to try and authenticate, most went for root.
2. Foreign IP address that the attack came from.
3. Date of the attack.
4. Passwords used.

Inspiration

This was an excellent read, but I wanted some more up to date data:
http://people.scs.carleton.ca/~paulv/papers/passwords_full.pdf

brute_force_data.json (4.83 MB)

About this file

This is data related to the widespread brute force attempts from the internet. The username is the user account that the ssh attempt tried to use. Foreign IP is the IP address the attempt came from, and passwords is an array of the passwords that the attacker used. Password fields include Unicode.

There were other attempts not included here, which broadly fell into two categories: attempts with a key, and attempts that entered no username or password. This dataset only includes attempts using password authentication.

The data set we have chosen to analyze for The Data Dig is...

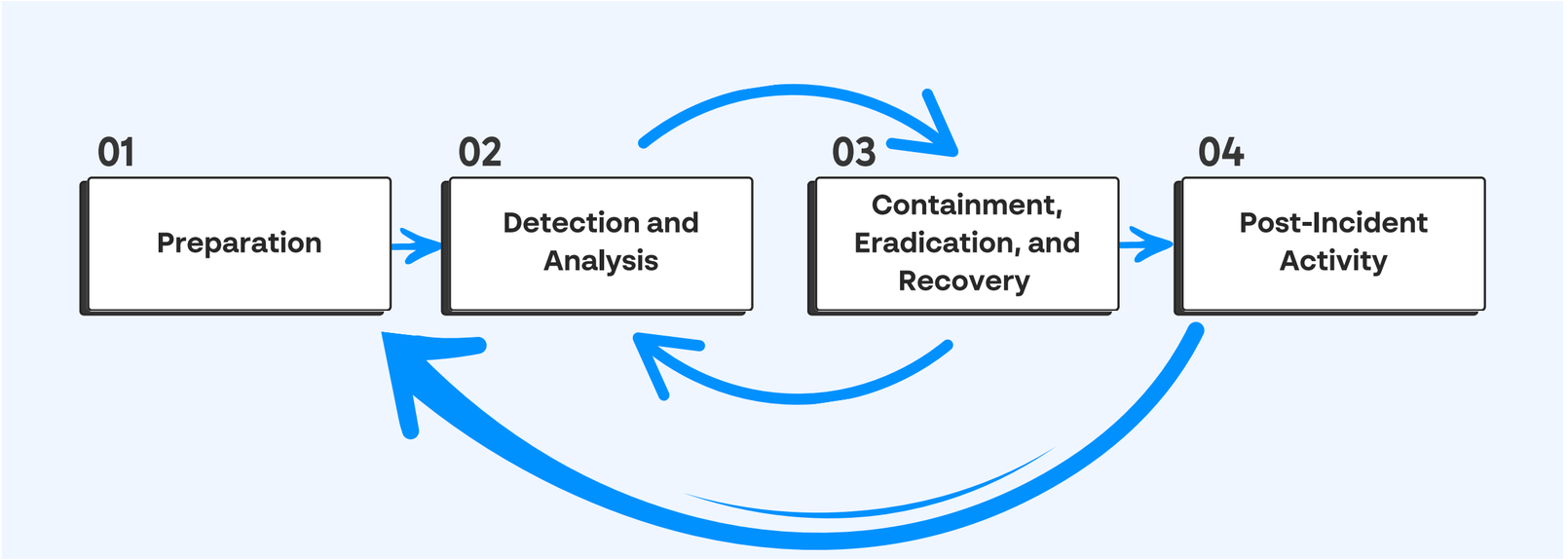
This dataset comes from a user who set up an SSH server specifically to collect login activity for research. The logs mainly capture network-based attacks, especially brute-force attempts where attackers try many username and password combinations to gain access. It was created to study how these attacks behave in real environments.

Tools Used

- Splunk
- Catalyst: to document all the findings with artefacts, so we can properly do step 4. Learn
- Virus Total

The playbook we have decided to follow for The Data Dig is...

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

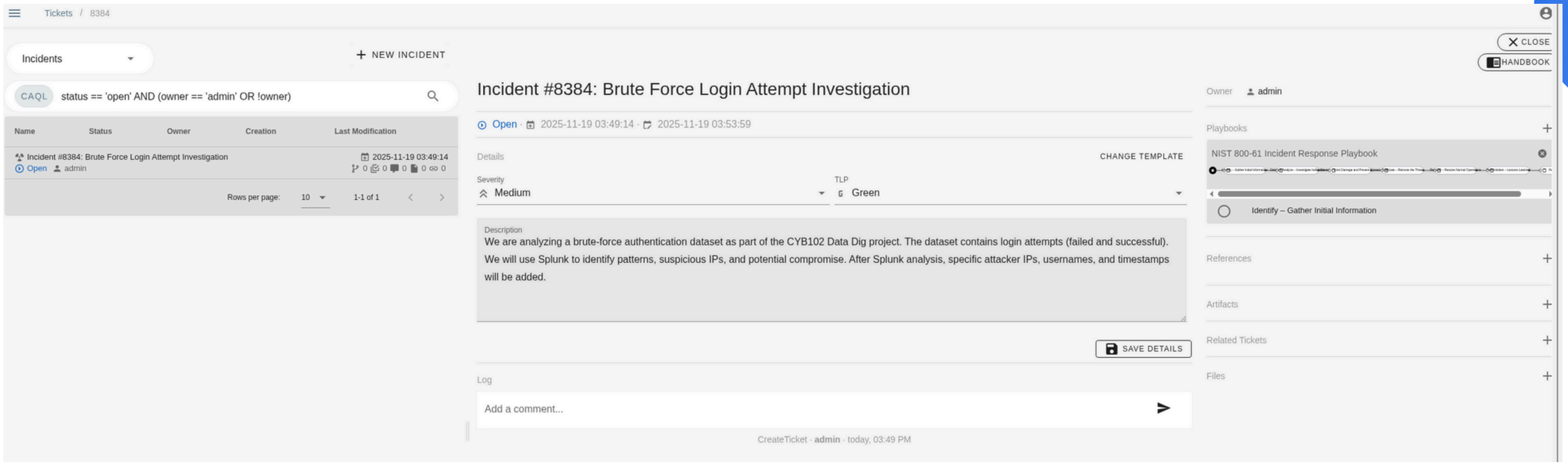


NIST Special Publication 800 NIST SP 800-61r3 Incident Response Recommendations and Considerations for Cybersecurity Risk Management A CSF 2.0 Community Profile

What happened?

Key Findings

Description of the incident

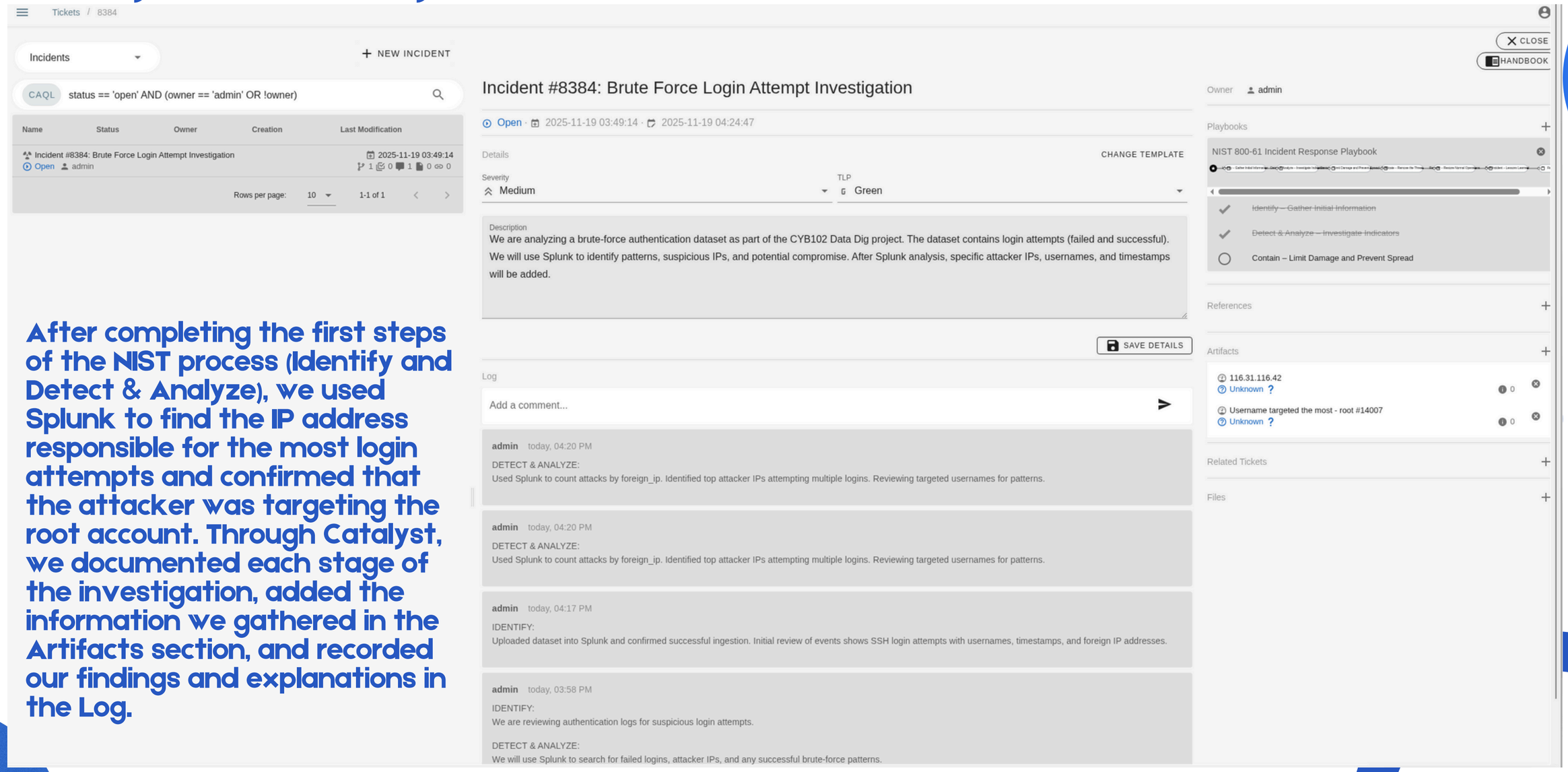


We are analyzing a dataset that captures brute-force authentication activity against an SSH server. The data includes both failed and successful login attempts, allowing us to observe attacker behavior and login patterns. Splunk will be used to investigate the logs, identify suspicious IP addresses, detect targeted usernames, and determine whether any compromises occurred. Once the analysis is complete, we will add the specific attacker IPs, targeted accounts, and timestamps to this incident for full documentation.

First NIST Steps + Tools Used During Investigation

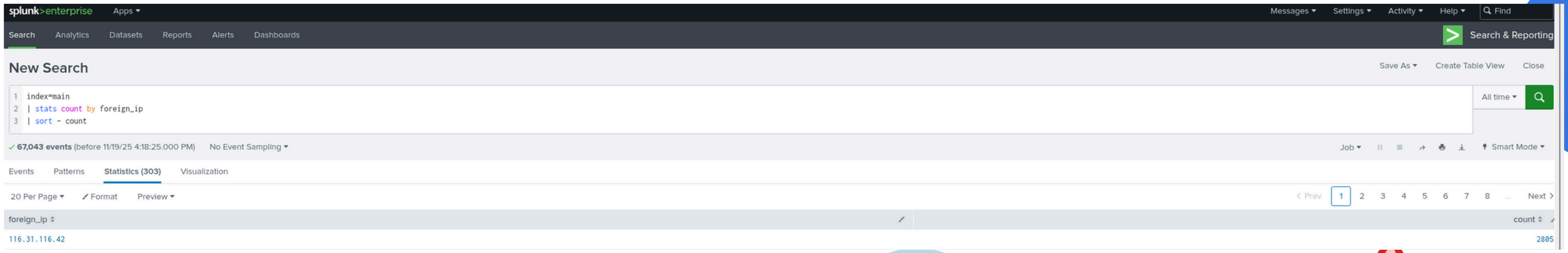
Identify → Detect → Analyze steps

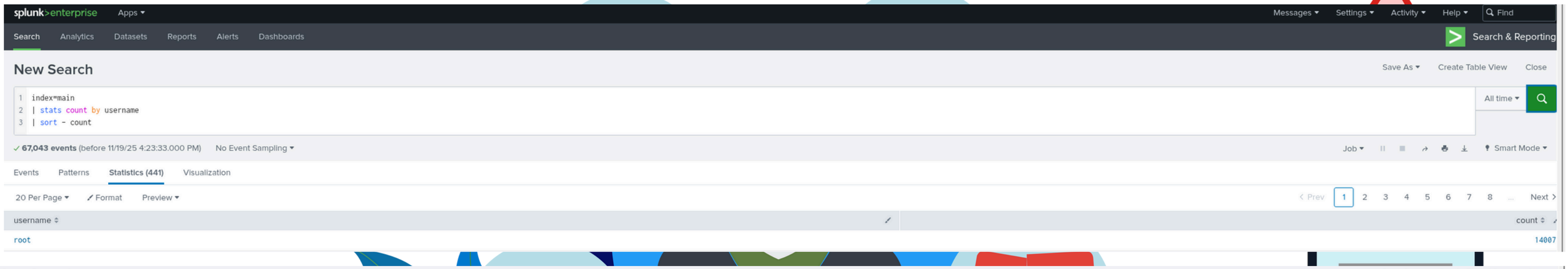
Early Incident Analysis Results

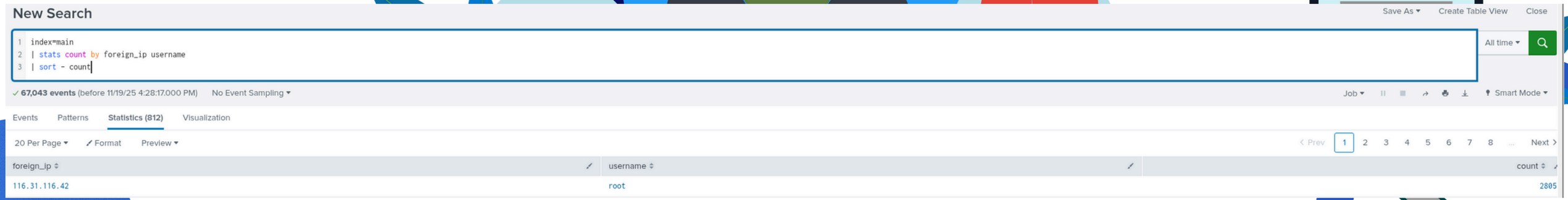


After completing the first steps of the NIST process (Identify and Detect & Analyze), we used Splunk to find the IP address responsible for the most login attempts and confirmed that the attacker was targeting the root account. Through Catalyst, we documented each stage of the investigation, added the information we gathered in the Artifacts section, and recorded our findings and explanations in the Log.

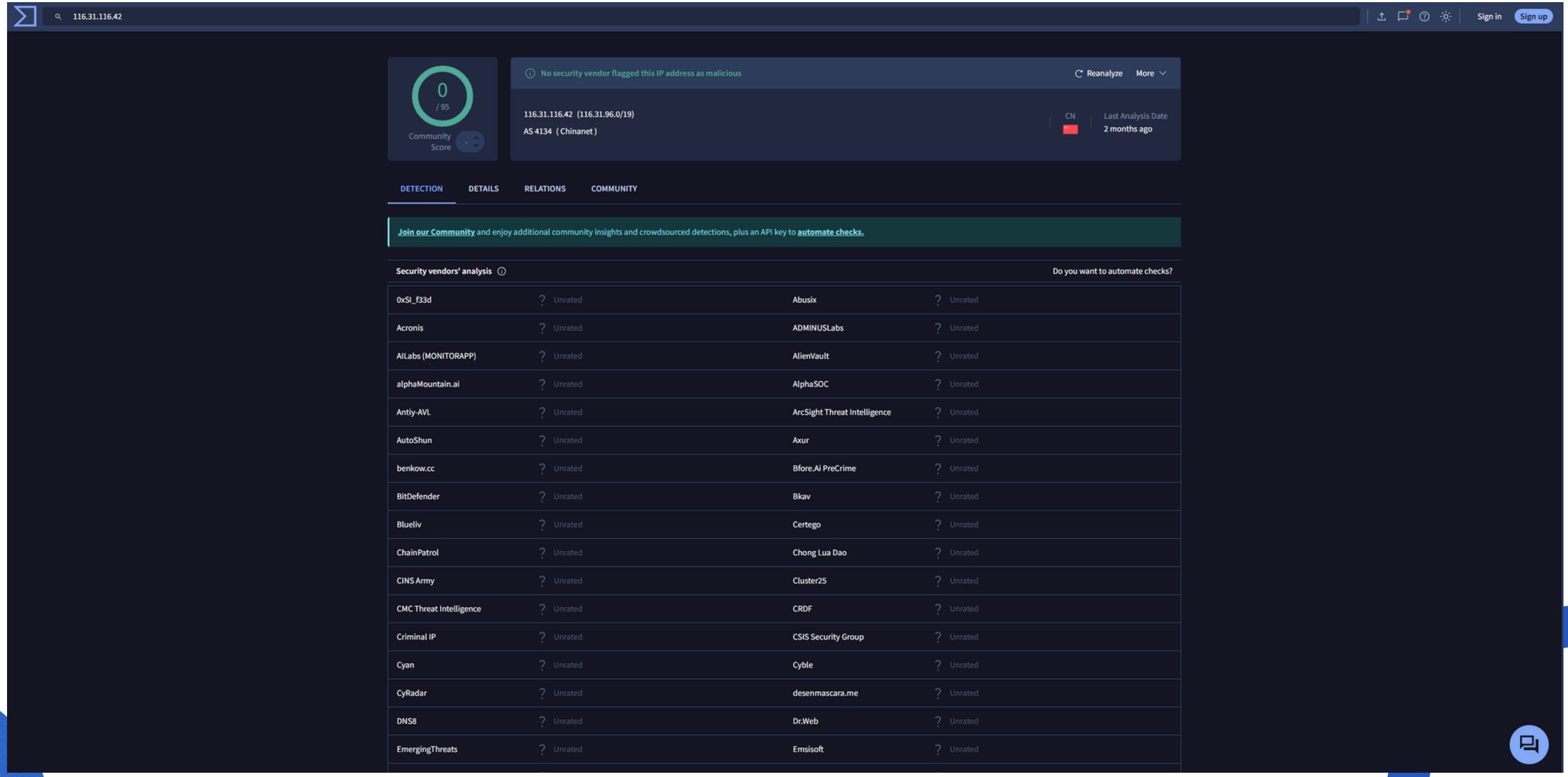
Using Splunk, we were able to identify the attacker's IP address, the targeted username, and confirm that this specific IP was repeatedly attempting to log in to that user account.







VirusTotal Screenshot of the Attacker IP



Containment, eradication and recovery

CONTAINMENT:

We blocked the attacker IPs to stop more login attempts. We also locked the user accounts that were being targeted and added limits on how many login attempts can happen in a short time. These actions helped stop the brute-force attack and prevented any further damage.

ERADICATION:

We would reset passwords and change our password policies to make them stronger. We would turn on MFA (Multifactor Authentication to make logins more secure. We would also nullify any unauthorized sessions accessed by the attacker.

To enhance network security, we would update firewall rules to block any malicious IP address ranges and make sure no suspicious SSH keys, accounts, or settings were left behind. This ensures the attacker is fully removed from the system.

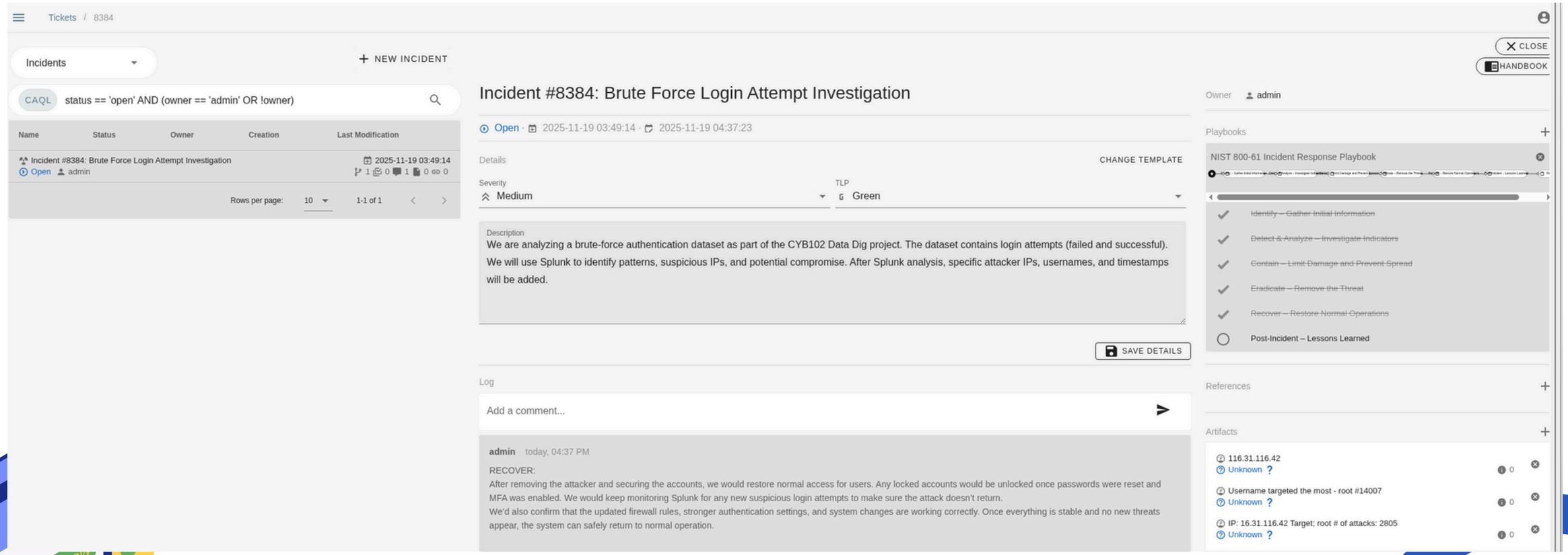
RECOVERY:

After removing the attacker and securing the accounts, we would restore normal access for users. Any locked accounts would be unlocked once passwords were reset and MFA was enabled. We would keep monitoring Splunk for any new suspicious login attempts to make sure the attack doesn't return.

We'd also confirm that the updated firewall rules, stronger authentication settings, and system changes are working correctly. Once everything is stable and no new threats appear, the system can safely return to normal operation.

We would also begin a series of mandatory seminars to educate employees on proper security hygiene and identifying suspicious behavior effective immediately. Afterall, security is maximized when technology, process and PEOPLE are all functioning cohesively.

STEPS DONE IN CATALYST

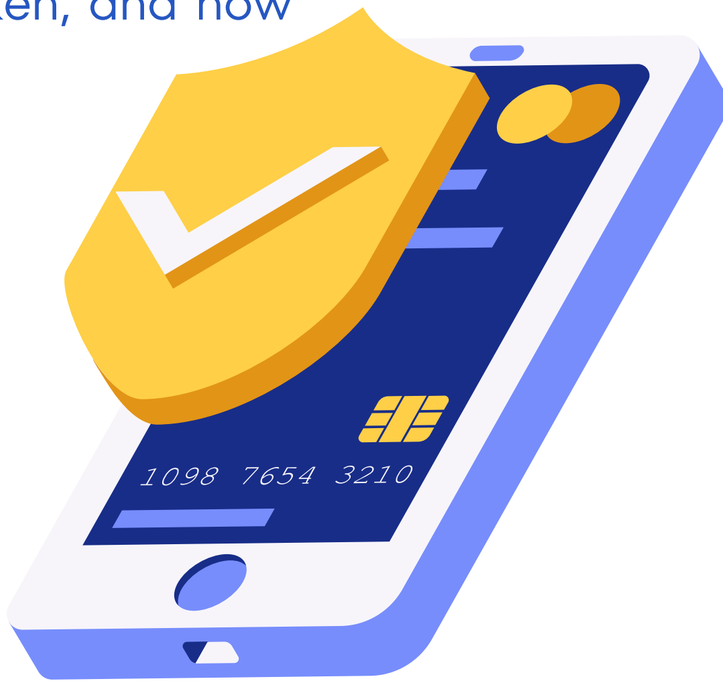


Post-Incident Documentation & Remediation

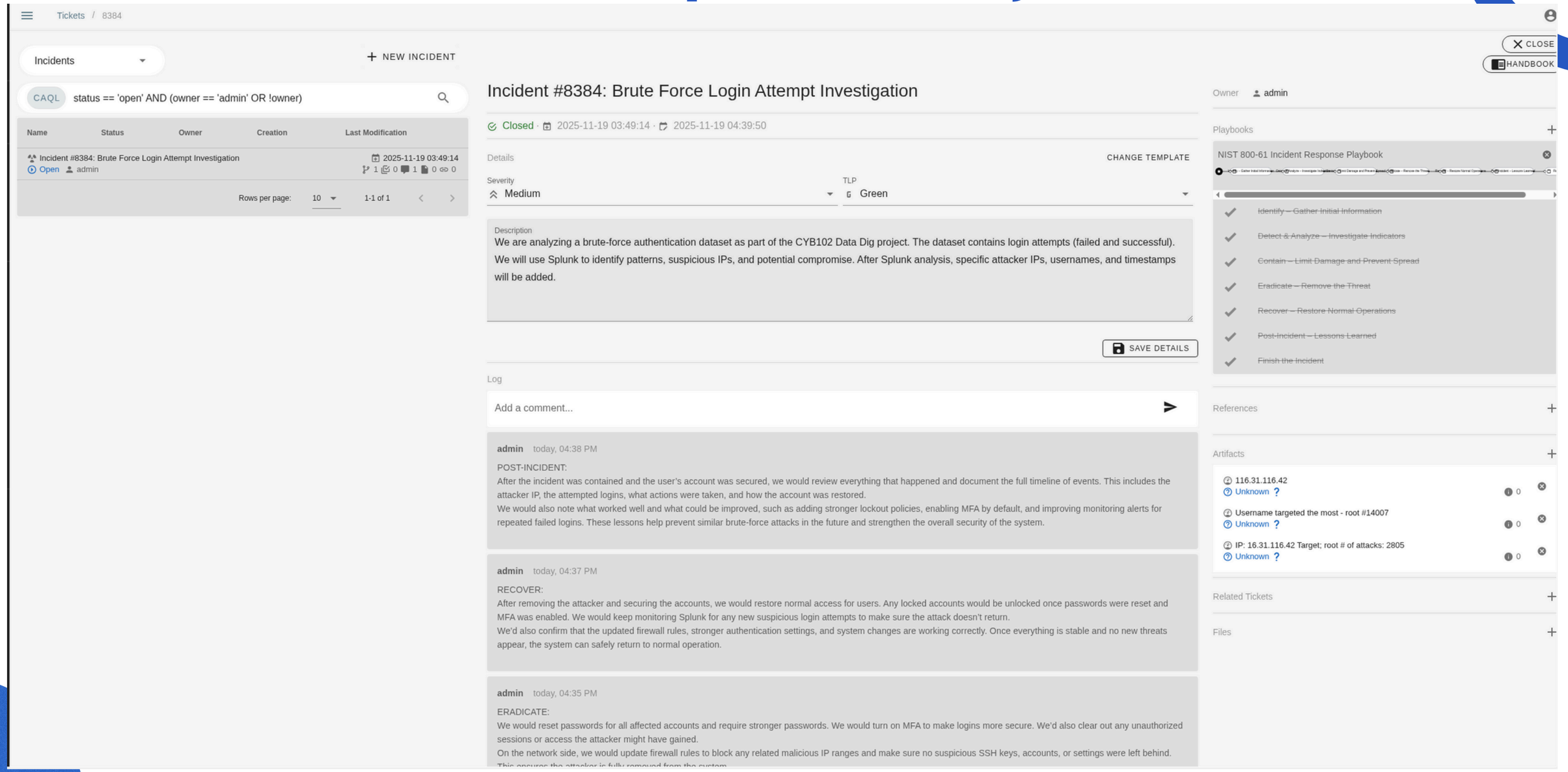
After the incident was contained and the user's account was secured,
we would review everything that happened and document the full timeline of events.
This includes the attacker IP, the attempted logins, what actions were taken, and how the account was restored.

What could be improved:

- adding stronger lockout policies,
- enabling MFA by default,
- improving monitoring alerts for repeated failed logins.



Final Steps in Catalyst



Thank You!

Pod 79