Incident Report 1 - With Excess Data

Incident 1: Insecure Data Transmission Over Unencrypted Protocols
Description: Transmission of sensitive data over HTTP instead of HTTPS leads to risks of data interception.
Possible Damage: Data leakage or tampering during transmission, which could lead to a breach of confidentiality.
Risk Priority: High
Status: In Progress
Mitigation: "{\"1\": \"Switch all sensitive traffic to HTTPS using strong ciphers.\"}"
Created At: 2025-10-05 10:00:00
Assigned Date: 2025-10-05 12:00:00
Mitigation Due Date: 2025-10-12 18:00:00
Extra Data: Unnecessary field 1 value
Extra Data: Unnecessary field 2 value
Extra Data: Unnecessary data for incident testing
— End of Incident —

Incident 2: Unpatched Vulnerability in Web Application
Description: A vulnerability in the login mechanism is identified that allows unauthorized access to user accounts.
Possible Damage: Compromise of user accounts and access to confidential information.
Risk Priority: Medium
Status: Assigned
Mitigation: "{\"1\": \"Patch the web application immediately and notify affected users.\"}"
Created At: 2025-10-06 13:00:00
Assigned Date: 2025-10-06 14:10:00
Mitigation Due Date: 2025-10-10 15:00:00
Extra Data: Unnecessary field 1 value
Extra Data: Unnecessary field 2 value
Extra Data: Unnecessary data for incident testing
— End of Incident —