Use case name	**Investigate & Block Suspicious Activity**
Participating actors	**Actor:** Security Analyst **System Components:** MIRS Dashboard (UI), Incident Controller, Log Repo & SIEM **External Systems:** Threat Intel Feed, Firewall API
Flow of events	1. The **Log Repo & SIEM** processes incoming NetFlow/Syslogs from the **Firewall**, detects a signature match, and triggers a "High Severity" alert (ID: #9921). 2. The **Security Analyst** clicks "View Details," and the **Incident Controller** retrieves L3/L4 headers and payload snippets from the database. 3. The **Security Analyst** requests a "Deep Dive"; the system executes parallel tasks to retrieve **PCAP files** from the Repo and query the **Threat Intel Feed** (Result: Malicious 98/100). 4. The **Security Analyst** selects "Block Source IP"; the **Incident Controller** maps the action to a **MITRE ID** and logs the decision logic. 5. The **Incident Controller** sends a synchronous POST /acl/rules request (Action=Deny) to the **Firewall API**. 6. Upon receiving a "200 OK" confirmation from the Firewall, the **Incident Controller** updates the status to "Resolved" and notifies the **Security Analyst**.
Entry condition	The **Security Analyst** is logged into the **MIRS Dashboard**, and the **Firewall** is actively sending logs to the SIEM.
Exit condition	A "Deny" rule is enforced on the **Firewall**, and the incident is closed with a "Resolved" status in the **Log Repo**.
Quality requirements	The parallel execution of PCAP retrieval and Threat Intel lookup must minimize wait time. The **Firewall API** integration must support real-time rule propagation.