Blue Team: Summary of Operations

Table of Contents

- Network Topology

- Description of Targets

- Monitoring the Targets

Network Topology

The following machines were identified on the network:

192.168.1.1 – Windows 10 Pro – Hyper-V Host Machine (ML-RefVm-684427)

192.168.1.100 – Ubuntu/Linux – Kibana SIEM Machine

192.168.1.105 – Ubuntu/Linux – Capstone Machine

192.168.1.110 – Debian/Linux – Target 1 Machine (Exploited)

192.168.1.115 – Debian/Linux – Target 2 Machine

192.168.1.90 – Kali/Linux - Attacker Machine

Description of Targets

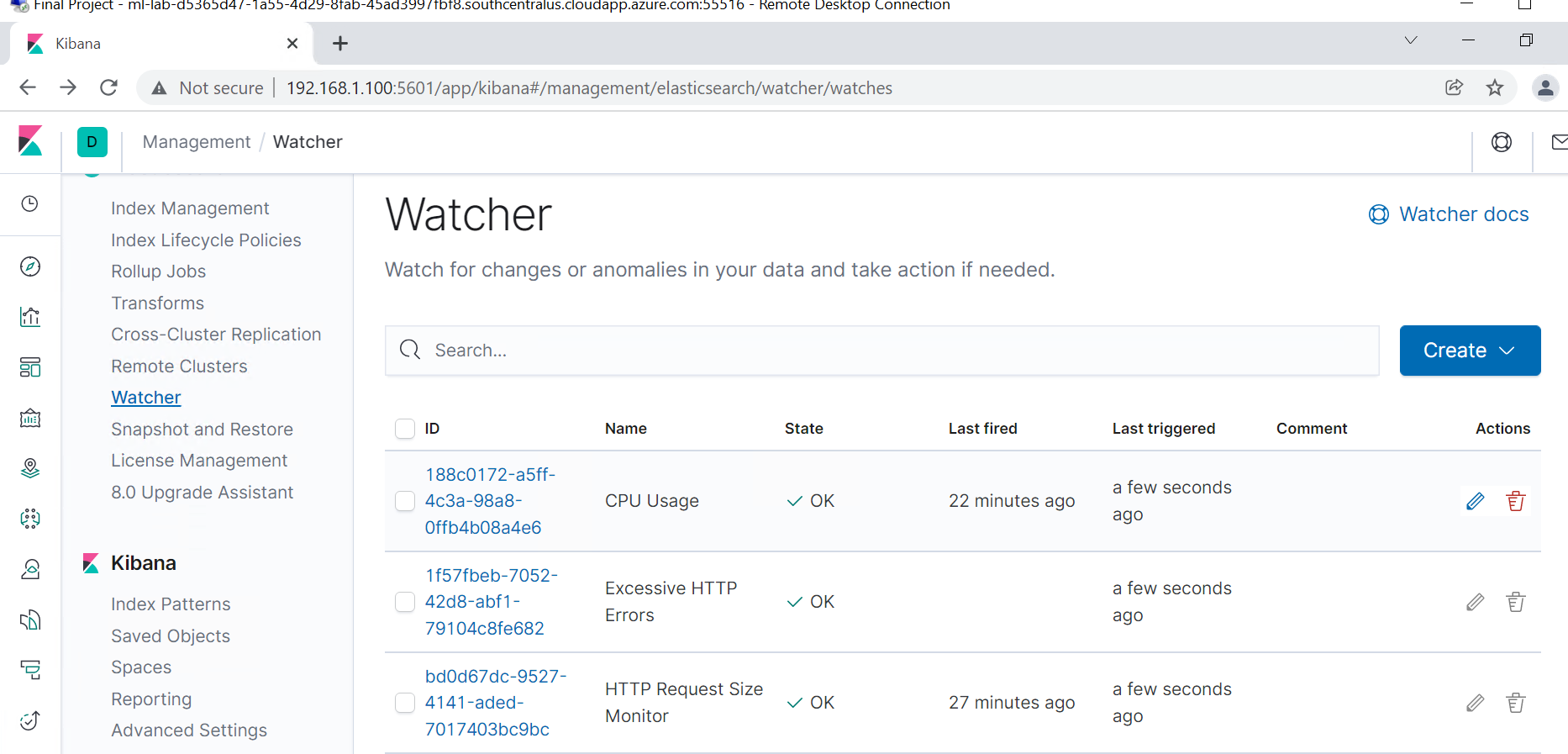
The target of this attack was: `Target 1` - 192.168.1.110

Target 1 is an Apache web server and has SSH enabled, so ports 80 and 22 are possible ports of entry for attackers. As such, the following alerts have been implemented:

1. Excessive HTTP Errors - HTTP Error codes in the 400 status range. This is usually for Unauthorized/Forbidden access. Massive amounts might indicate someone is trying to Brute Force the system.

2. HTTP Request Size Monitor - Indicates data being parsed in a recent timeframe. Excessive amounts could indicate a scan in progress.

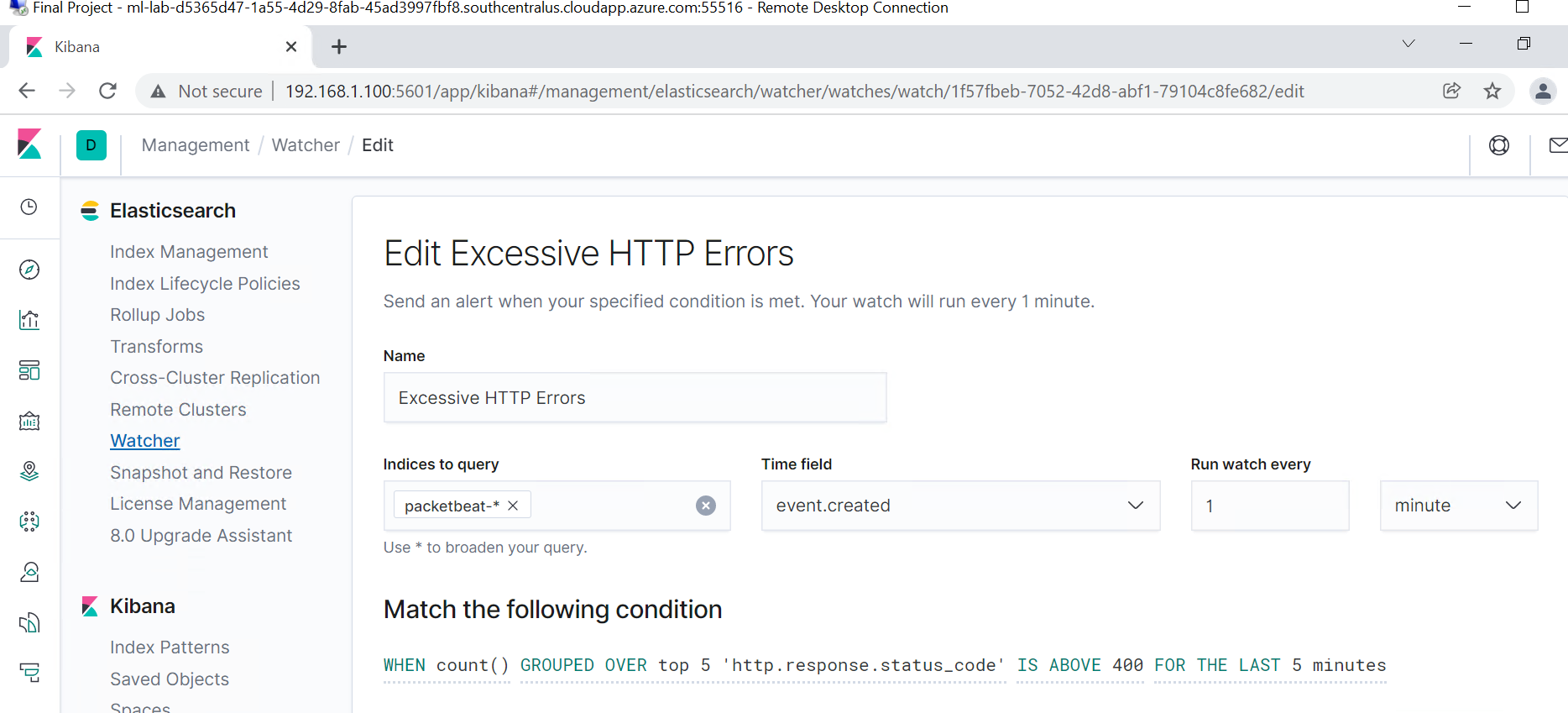
3. CPU Usage Monitor - Indicates when an abnormal load is being placed on the system. Ex., an app is being accessed that consumes resources or a flood of requests are coming into the processor.



Monitoring the Targets

Traffic to these services should be carefully monitored. To this end, we have implemented the alerts below:

1. Excessive HTTP Errors



Alert 1 is implemented as follows:

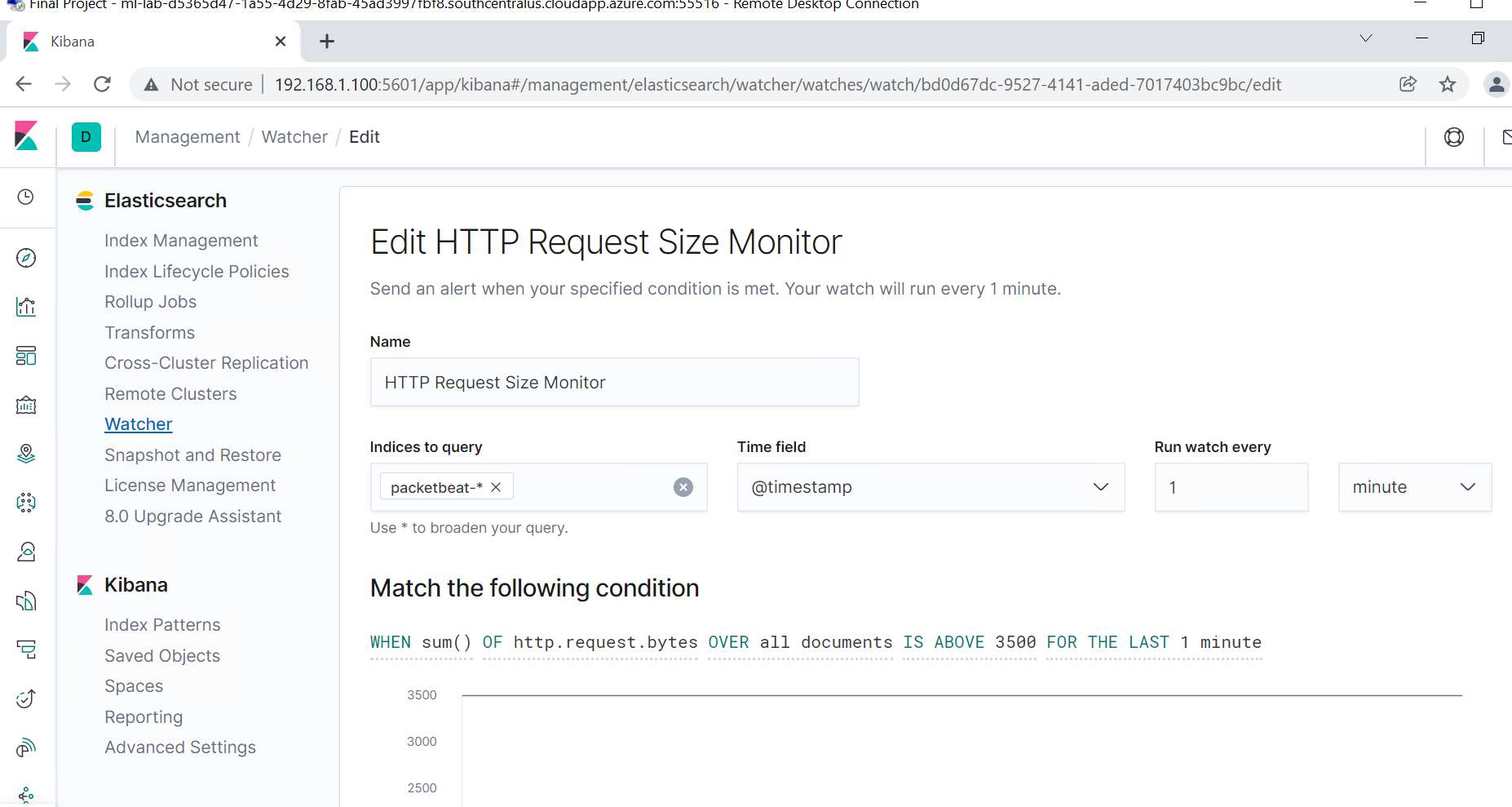
- \*\*Metric\*\*: Top 5 ‘http.response.status\_code’

- \*\*Threshold\*\*: > 400 for last 5 min.

- \*\*Vulnerability Mitigated\*\*: Alert about Unauthorized codes during potential Brute Force attempts.

- \*\*Reliability\*\*: LOW – alert never fired during any phase of the Kali attack.

1. HTTP Request Size Monitor



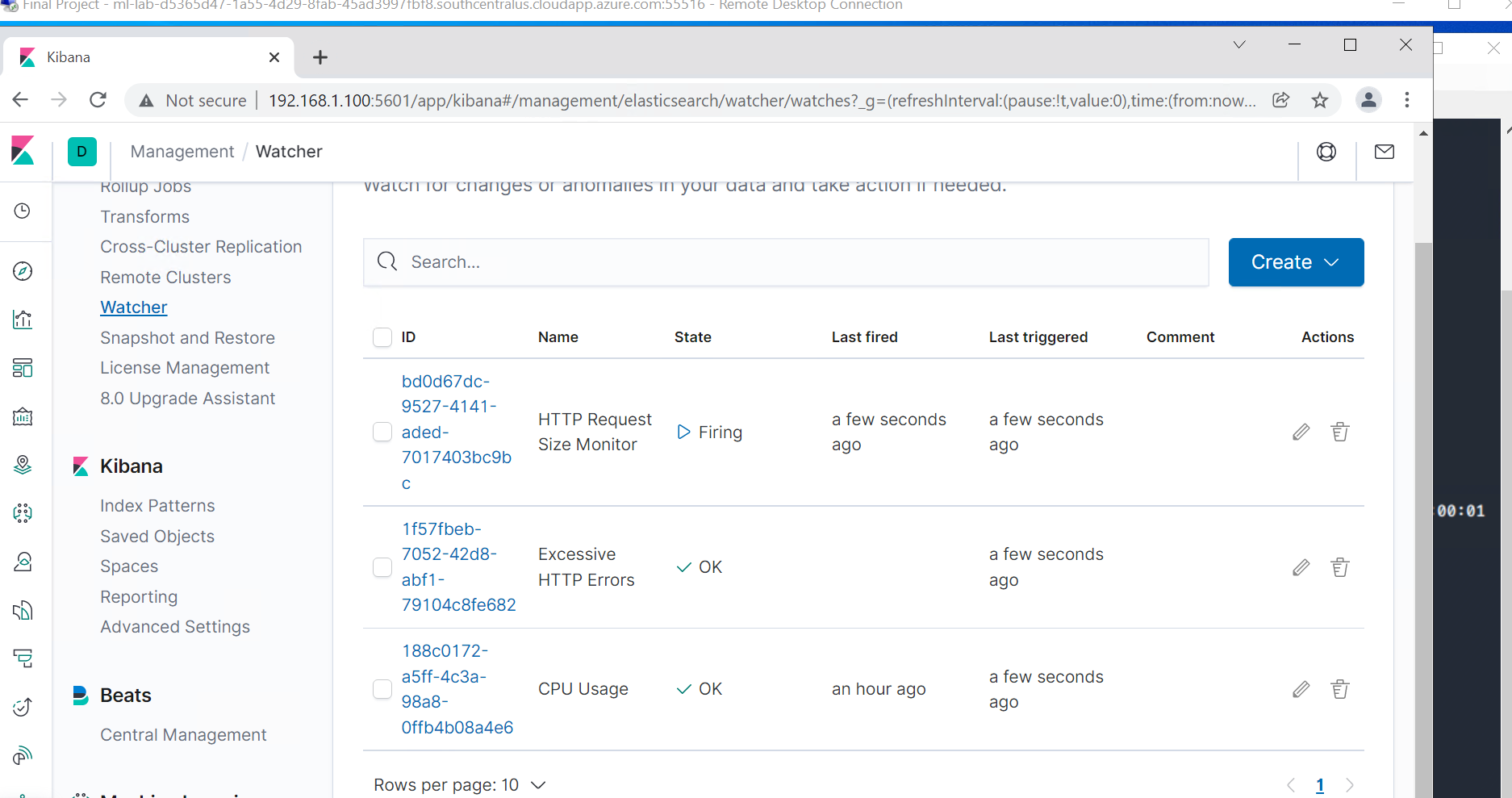
Alert 2 is implemented as follows:

- \*\*Metric\*\*: Sum of http.request.bytes over all documents

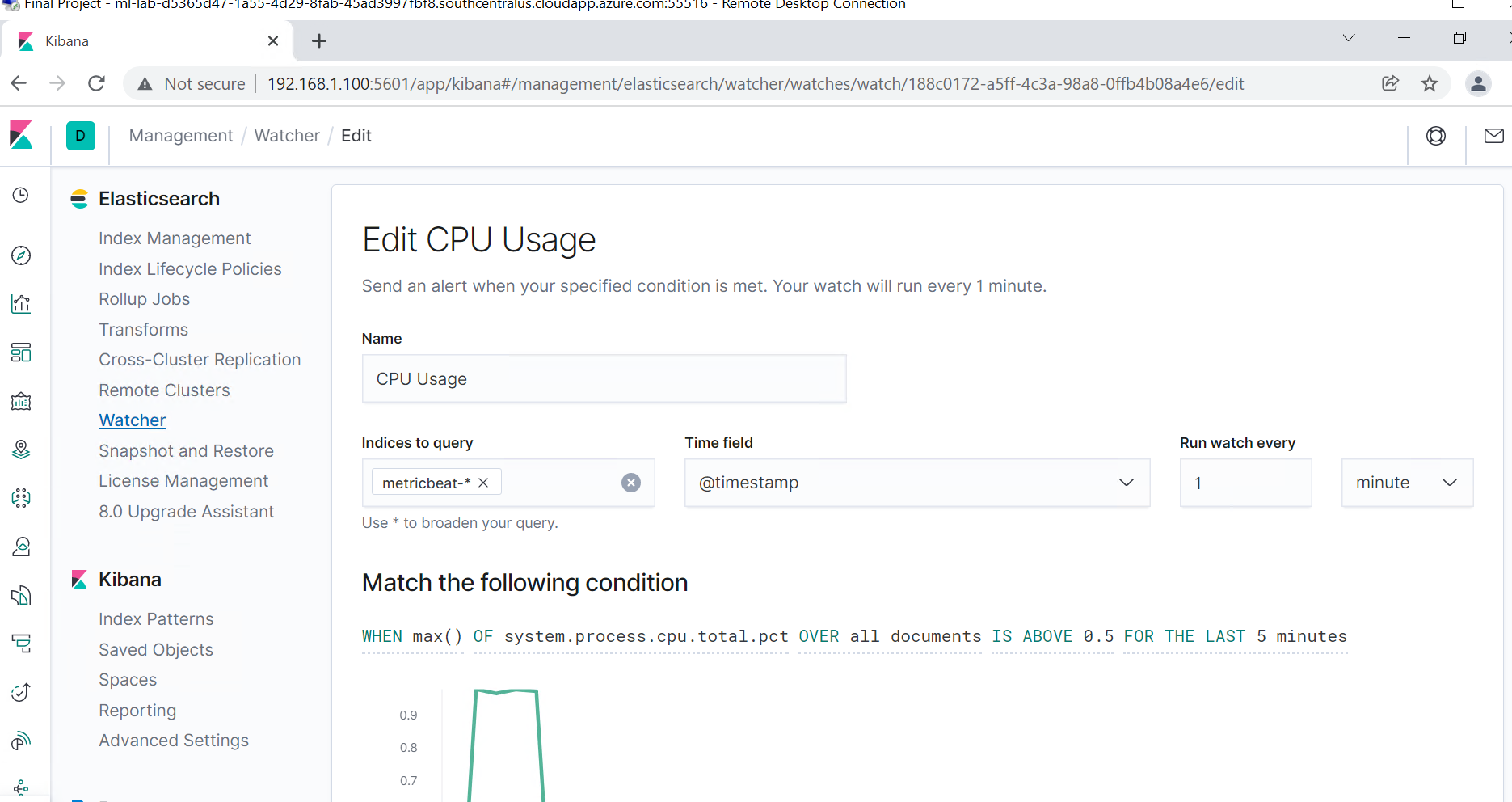
- \*\*Threshold\*\*: >3500 for last 1 min.

- \*\*Vulnerability Mitigated\*\*: Alert about attempts to Exfiltrate Data.

- \*\*Reliability\*\*: HIGH – alert triggered below as a Kali WordPress Scan was in progress.



1. CPU Usage Monitor



Alert 3 is implemented as follows:

- \*\*Metric\*\*: Max of system.process.cpu.total.pct over all documents

- \*\*Threshold\*\*: >0.5 for last 5 min.

- \*\*Vulnerability Mitigated\*\*: Show system expenditures during periods of heavy processing, indicating possible attack in progress.

- \*\*Reliability\*\*: MEDIUM – alert fires at other times, but not specifically during the attack.