**Part 4 - Blocking Attacks**

**Objective**

We will configure a **Detection & Response (D&R) rule** to block **ransomware-like behavior**, specifically the **deletion of Volume Shadow Copies (VSS)**. Attackers delete VSS to prevent system recovery, making it a **high-confidence indicator of ransomware activity** with **low false positive risk**.

**Lab Steps**

**1. Simulating a Ransomware-Like Attack**

1. **Connect to the Sliver C2 session.**
2. **Open a system command shell:**

shell

* + When prompted with: *"This action is bad OPSEC, are you an adult?"*, type Y and press **Enter**.

1. **Attempt to delete Volume Shadow Copies:**

vssadmin delete shadows /all

* + Even if no shadow copies exist, running this command will generate the required telemetry.

1. **Verify the session is still active by running:**

whoami

**2. Detecting VSS Deletion in LimaCharlie**

1. **Navigate to LimaCharlie’s Detections tab.**
2. **Find the event generated by the vssadmin delete shadows /all command.**
3. **Examine the detection metadata** to understand why this event was flagged.

**3. Creating a Blocking Rule in LimaCharlie**

1. **View the raw event in the "Timeline" tab.**
2. **Craft a new Detection & Response (D&R) rule.**
   * The **first action (report)** logs the detection in **LimaCharlie’s Detections tab**.
   * The **second action (deny\_tree)** **terminates the parent process** responsible for running the VSS deletion command.
3. **Save the rule as vss\_deletion\_kill\_it and enable it.**

**Testing the Blocking Rule**

1. **Return to the Sliver C2 session and rerun:**

vssadmin delete shadows /all

1. **Check if the session was terminated** by running:

whoami

* + If the rule worked, the shell should **hang and fail to return output**, indicating the process was killed.

1. **Confirm the detection in LimaCharlie’s "Detections" tab.**

**Next Steps - Strengthening the Rule**

* **Test against a ransomware simulator** like Florian Roth’s ransomware simulator.
* **Expand the rule** to cover other VSS deletion methods, such as:
* **Fine-tune detection logic** to reduce false positives while ensuring maximum coverage.

**Conclusion**

This exercise demonstrates how to **proactively block attacks in real time**. By leveraging **LimaCharlie’s D&R engine**, we can **automate threat mitigation**, making the environment more resilient to ransomware and other adversarial activities.