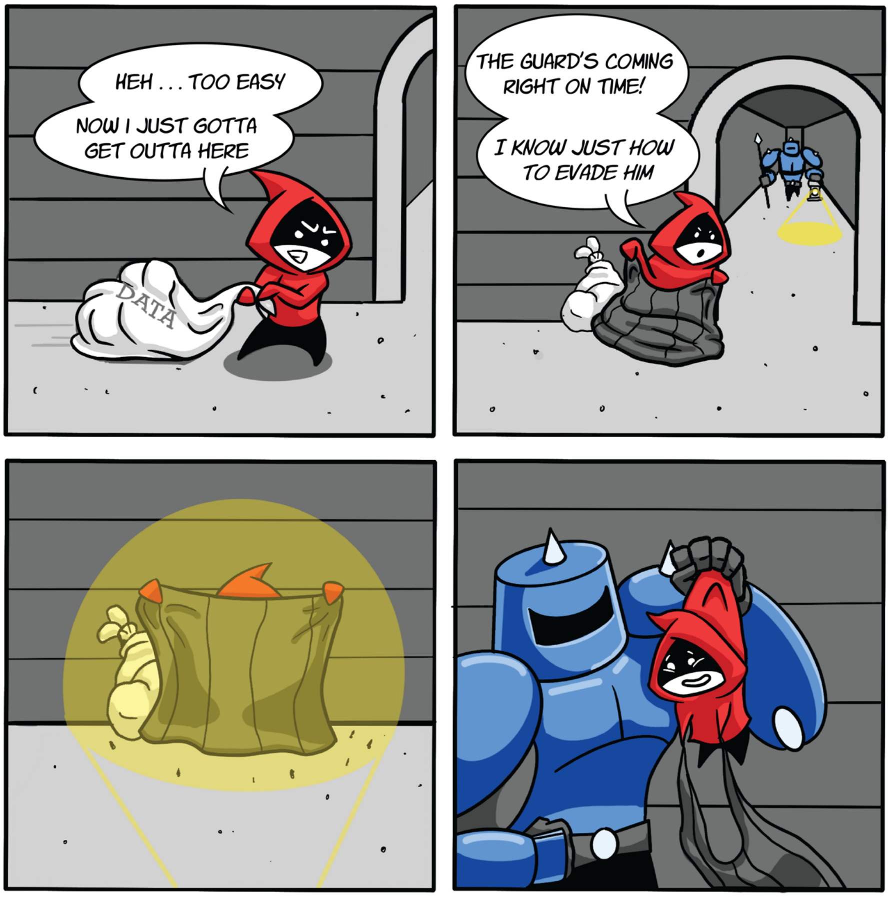
SUDO SCIENCE

AN UPTYCS COMYCS PROJECT


HEH . . . TOO EASY
NOW I JUST GOTTA GET OUTTA HERE
DATA
THE GUARD'S COMING RIGHT ON TIME!
I KNOW JUST HOW TO EVADE HIM

Scenario

This comic has Curly, our Red Team character, making it way farther down the ATT&CK Lifecycle than they ever have. Here they are actually just about to exfiltrate some data! It seems they have figured out Linus' patrol schedule and have prepared for it. Curly pulls out their handy dandy defense evasion cover and strikes a pose against the wall. The design on the cover seems to match the wall's stripes.

When Linus, our Blue Team Guard, shines a light onto the cover, they realize there is something wrong. Clearly, the stripes are in the wrong orientation. Also, Curly's hat is popping out of the top! Unfortunately for Curly, Linus has caught them again! Looks like defense evasion is harder than Curly thought.

Deep Dive

Defense evasion and persistence techniques can be quite the headache for Linux defenders, especially when they are using common Linux commands to do so. Adversaries are able to utilize commands like crontab to schedule commands to execute and specified intervals. They can use **`chattr`** and **`rm`** to alter attributes of a file or just remove it!

To start detecting persistence methods like scheduled program execution (T1053), we need to view the events in context and not isolation. We may see outlier processes that do not match up to historical data. We may even see commands that map to other MITRE ATT&CK techniques for discovery and lateral movement in the same chain of behaviors. We can also look for changes to the system that do not correlate with known patch cycles.