Activity logs of an Intrusion Defense System for Intelligent Family Network

Field list in the dataset:

1. device\_dev\_name
2. device\_family\_name
3. device\_hashed\_mac
4. device\_os\_name
5. device\_type\_name
6. device\_vendor\_name
7. event\_protocol\_id: PROTOCOL number (1:ICMP, 6:TCP, 17:UDP,...)
8. event\_flow\_outbound\_or\_inbound : When an event was triggered, is it outbound or inbound? (It is used to judge whether it attacked or was attacked)
9. event\_role\_device\_or\_router: Is the device where the event was triggered just a device or router?
10. event\_role\_server\_or\_client: Is the device where the event was triggered a server or client?
11. event\_rule\_id
12. event\_rule\_name
13. event\_rule\_reference
14. event\_rule\_severity: severity scale ranges from 1 to 5.
15. event\_self\_ipv4: Device IP address where the event was triggered. Mostly, it would be a private IP; however, if it is a public IP, it has been obfuscated to avoid possible connections to any real-world IPs and misunderstanding.
16. event\_time
17. router\_ip: It is also obfuscated and is only used for indicating same router sources.

-----

‧train\_DefenseSystem.csv: a training dataset that contains 5,000 data samples.

‧Target Prediction Field：**event\_rule\_category** with only two classes: “Access Control” and “Web Attack.”

‧test\_DefenseSystem.csv: a test dataset that contains 1,020 data samples.