Enhancing Network Security and Intelligent Agent Development in a Cyber Range

Guy Munn[1], Erik Feng[2], Vincent Huynh[3], Noah Spahn[2], Giovanni Vigna[2]

1. Norfolk State University, 2. UC Santa Barbara, 3. American River College

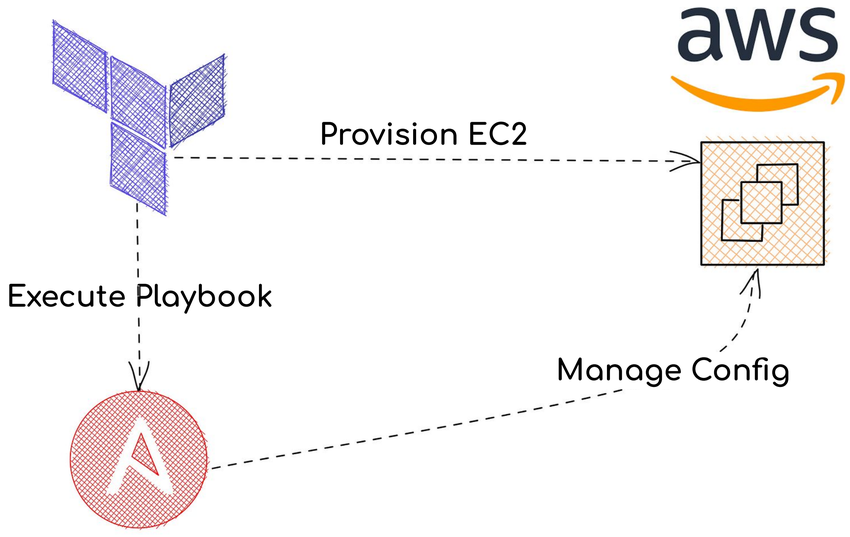
guy_munn | Erik Feng | thinh.vincent.huynh

TL;DR

1. Only first launched in early 2024, some aspects of our in-house cyber range (GATE) are still under development. We aim to test the cyber range and provide enhancements.
2. Our work utilizes network log data to improve GATE's network Intrusion Detection System (IDS) by adding a pipeline for deploying new rules.
3. We also implemented an algorithm to learn how to categorize events within the context of surrounding log entries.

Globally Accessible Testing Environment (GATE)

- Core security tasks that GATE will support:
  - Vulnerability analysis
  - Threat detection
  - Threat intel
  - Threat attribution
  - Response and recovery



Network Security

- Network security protects the network infrastructure from unauthorized access, misuse, or theft.
- The network in GATE is monitored using Suricata, an open-source detection engine that can act as a intrusion detection system (IDS) and intrusion prevention system (IPS).
- After a Suricata rule is detected and matched against a rule or set of rules, an alert is generated, and traffic is logged.
- To test the effectiveness of the rules, a script was made to trigger any denial of service (DoS) rules recently added to GATE.
- **Challenges faced:**
  - False positives
  - Alert fatigue
  - Complexity

Suricata DoS rules

```
alert udp any any -> any any (msg:"Possible UDP Flood DoS"; threshold: type both, track by_dst, count 200, seconds 1; classtype:attempted-dos; sid:1000055; rev:1;)
alert icmp any any -> any any (msg:"Possible ICMP Flood DoS"; itype:8; threshold: type both, track by_dst, count 200, seconds 1; classtype:attempted-dos; sid:1000054; rev:1;)
alert icmp any any -> $HOME_NET any (msg:"Ping of Death Attack"; itype:8; dsize:>1400; classtype:denial-of-service; sid:1000011; rev:1;)
```

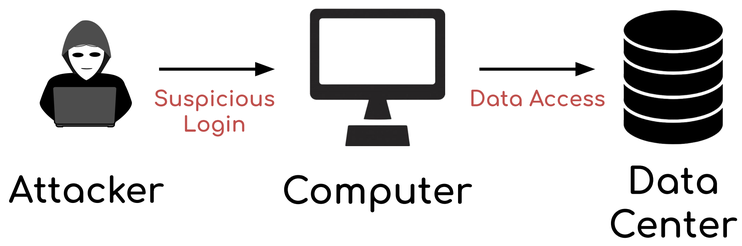
Alert output


```
{
  "timestamp": "2024-08-12T11:10:58.720351-0700",
  "flow_id": 1957032578424668,
  "in_iface": "ens5",
  "event_type": "alert",
  "src_ip": "10.0.1.10",
  "src_port": 0,
  "dest_ip": "10.0.0.10",
  "dest_port": 0,
  "proto": "ICMP",
  "icmp_type": 8,
  "icmp_code": 0,
  "pkt_src": "wire/pcap",
  "alert": {
    "action": "allowed",
    "gid": 1,
    "signature_id": 1000011,
    "rev": 1,
    "signature": "Ping of Death Attack",
    "category": "Detection of a Denial of Service Attack",
    "severity": 2
  },
  "direction": "to_server",
  "flow": {
    "pkts_toserver": 21,
    "pkts_toclient": 20,
    "bytes_toserver": 32382,
    "bytes_toclient": 30840,
    "start": "2024-08-12T11:10:38.717801-0700",
    "src_ip": "10.0.1.10",
    "dest_ip": "10.0.0.10"
  }
}
{
```


Intelligent Agent

Cyber attack: Any malicious activity against a computer system, such as attempting to steal passwords from a data center.

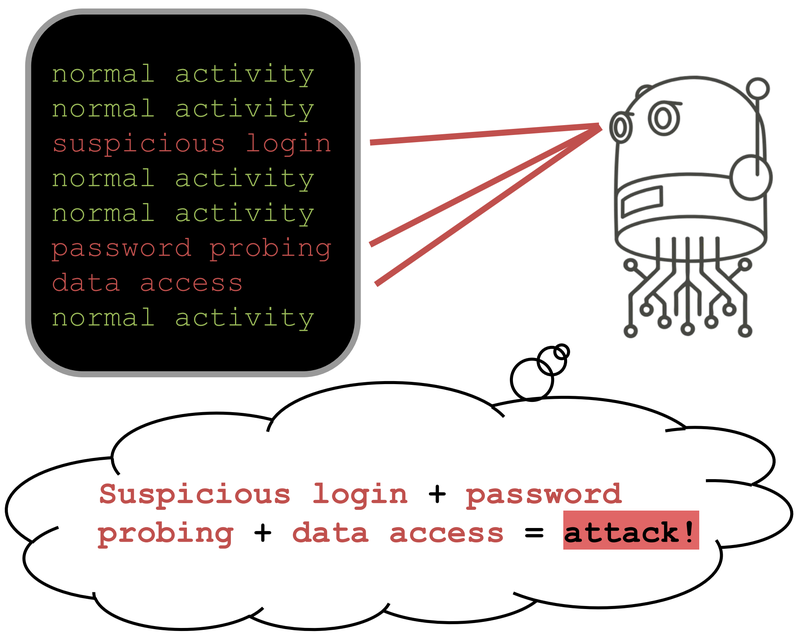
Insight: Whenever attackers access a system, their actions are saved to log files

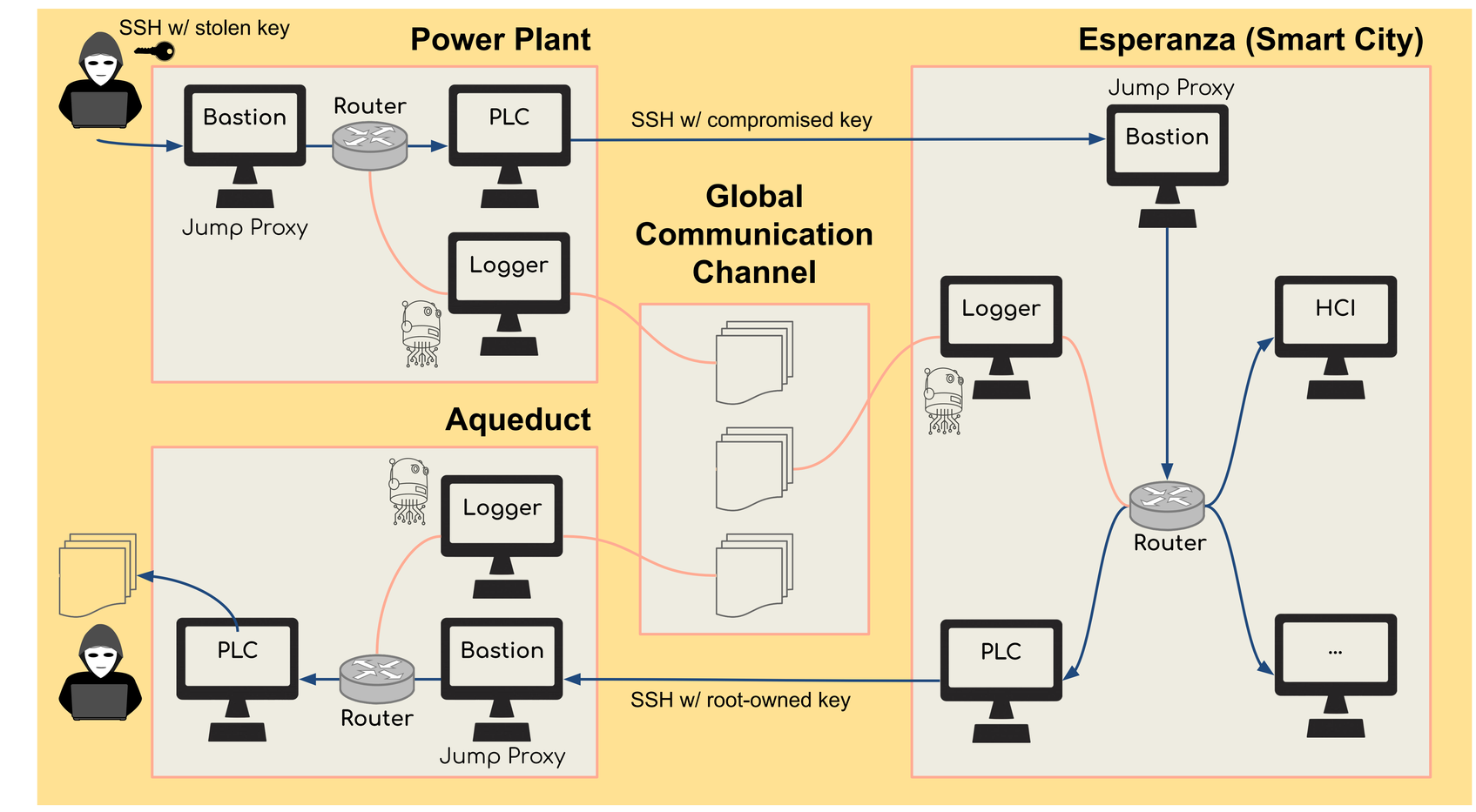


Solution: Analyze logs with an intelligent agent!

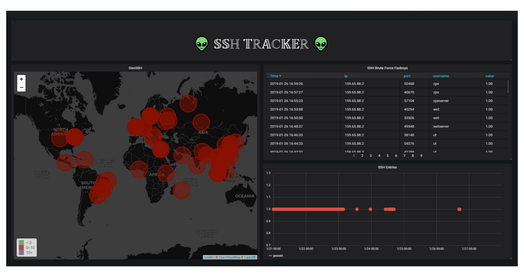
What is an intelligent agent?
An agent is any piece of software (code) that can detect and act based on their observations.

Log File



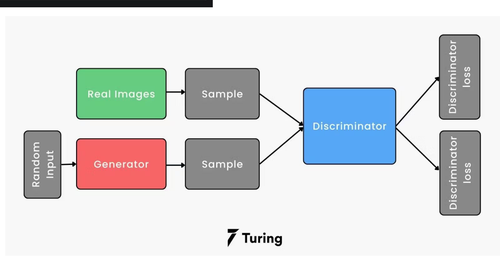


Future Research



Visualizing Data

Synthesizing Data



Reference

[1] T. v. Ede et al., "DEEPCASE: Semi-Supervised Contextual Analysis of Security Events," 2022 IEEE Symposium on Security and Privacy (SP), doi: 10.1109/SP46214.2022.9833671.

AI Institute for Agent-based Cyber Threat Intelligence and Operation (ACTION)

Supported by the National Science Foundation under grant no. IIS-2229876 and is supported in part by funds provided by the NSF, by the Department of Homeland Security, and by IBM.

https://action.ucsb.edu