Miridor

Cybera’s IDSaaS

Joe Topjian | Director of Operations
About Cybera

Cybera is Alberta’s research and education network facilitator, responsible for driving connections, collaborations and skills growth through the use of digital technology.

Our mission is to connect Alberta to the world, enabling and advocating for better services, collaborations and skills growth through the use of digital technology.
HOW CYBERA SUPPORTS ALBERTANS

SHARING IT TOOLS AND SERVICES

ADVOCATING FOR ACCESS

TECHNOLOGY TESTING

ENABLING NEXT-GENERATION TECHNOLOGIES

DATA MINING

CONNECTING HIGH-SPEED NETWORKS

MONITORING AND PROTECTING AGAINST THREATS
Part 1: The Service
Miridor

From Spanish: mir·a·dor

/ˈmirədôr/
noun
1. a turret or tower attached to a building and providing an extensive view.
Miridor: What is it?

- A multi-tenant Intrusion Detection System
- Based on Suricata
- Available to our members
- Requiring no software, agents, or hardware
Miridor: Why did we make it?

- For our members
- Little budget and resources required for members to run this on their own
- Low barrier to entry
- Novel combination of Systems, Network, and Systems Operations
Miridor: What does it do?

- Captures / analyses member traffic
- Stores and displays alerts
  - Abnormal activity
  - Active attacks
  - Insecure applications
  - Flag dangerous domains and IP addresses
- Filters and exports results for further analysis
Miridor: What can it be used for?

- Identifying potential vulnerabilities
- Provide an external point of view
- Enhancing firewall rules
- Root cause analysis
Miridor: What doesn’t it do?

- Capture internal network traffic
- Deep packet inspection
- Malware analysis
- Function as a SIEM replacement
Miridor Portal: Authentication

Select an authentication source

The selected authentication source will be used to authenticate you and to create a valid session.

- Microsoft Accounts (OAuth2)
- Google Accounts (OAuth2)
- Canadian Federated Access (SAML)
## Miridor Portal: Table View

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Signature ID</th>
<th>Signature</th>
<th>Category</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 29, 2022, 11:10 a.m.</td>
<td></td>
<td></td>
<td>TCP</td>
<td>2001219</td>
<td>ET SCAN Potential SSH Scan</td>
<td>Attempted Information Leak</td>
<td>2</td>
</tr>
<tr>
<td>April 29, 2022, 11:10 a.m.</td>
<td></td>
<td></td>
<td>TCP</td>
<td>2500024</td>
<td>ET COMPROMISED Known Compromised or Hostile Host Traffic group 13</td>
<td>Misc Attack</td>
<td>2</td>
</tr>
<tr>
<td>April 29, 2022, 11:10 a.m.</td>
<td></td>
<td></td>
<td>TCP</td>
<td>2010935</td>
<td>ET SCAN Suspicious inbound to MSSQL port 1433</td>
<td>Potentially Bad Traffic</td>
<td>2</td>
</tr>
</tbody>
</table>
Part 2: How it Works
Suricata: What is it?

- High performance Intrusion Detection System
- Signature-based
- Open source
Suricata: Why did we choose it?

- Choice between Zeek and Suricata
- How useful is it to us now?
- How much work is required to make it useful?
Miridor: Data Flow

Member Traffic

Router
Miridor: Data Flow

Member Traffic → Router → Mirror

Original Destination
Miridor: Data Flow

Member Traffic

Router

Original Destination

Mirror

LXD
Miridor: Data Flow

Member Traffic

Router

Mirror

LXD

Suricata

Fluentd

PostgreSQL

Original Destination
Miridor: Data Flow

Member Traffic

Router

Mirror

Suricata

Fluentd

PostgreSQL

User Portal

Original Destination
Thank you!

Questions? Contact security@cybera.ca