Miridor

Cybera’s IDSaaS

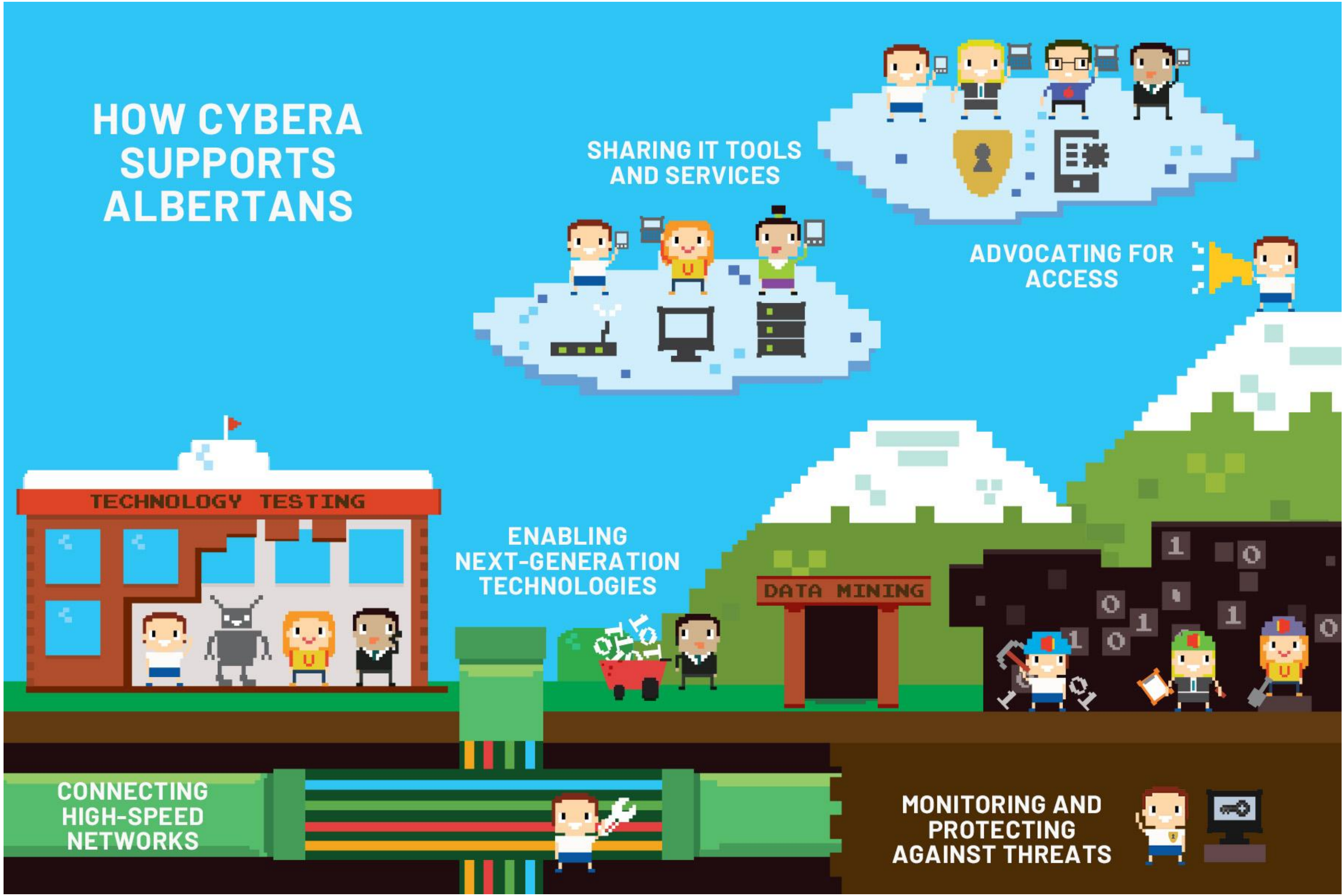
Joe Topjian | Director of Operations

cybera

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

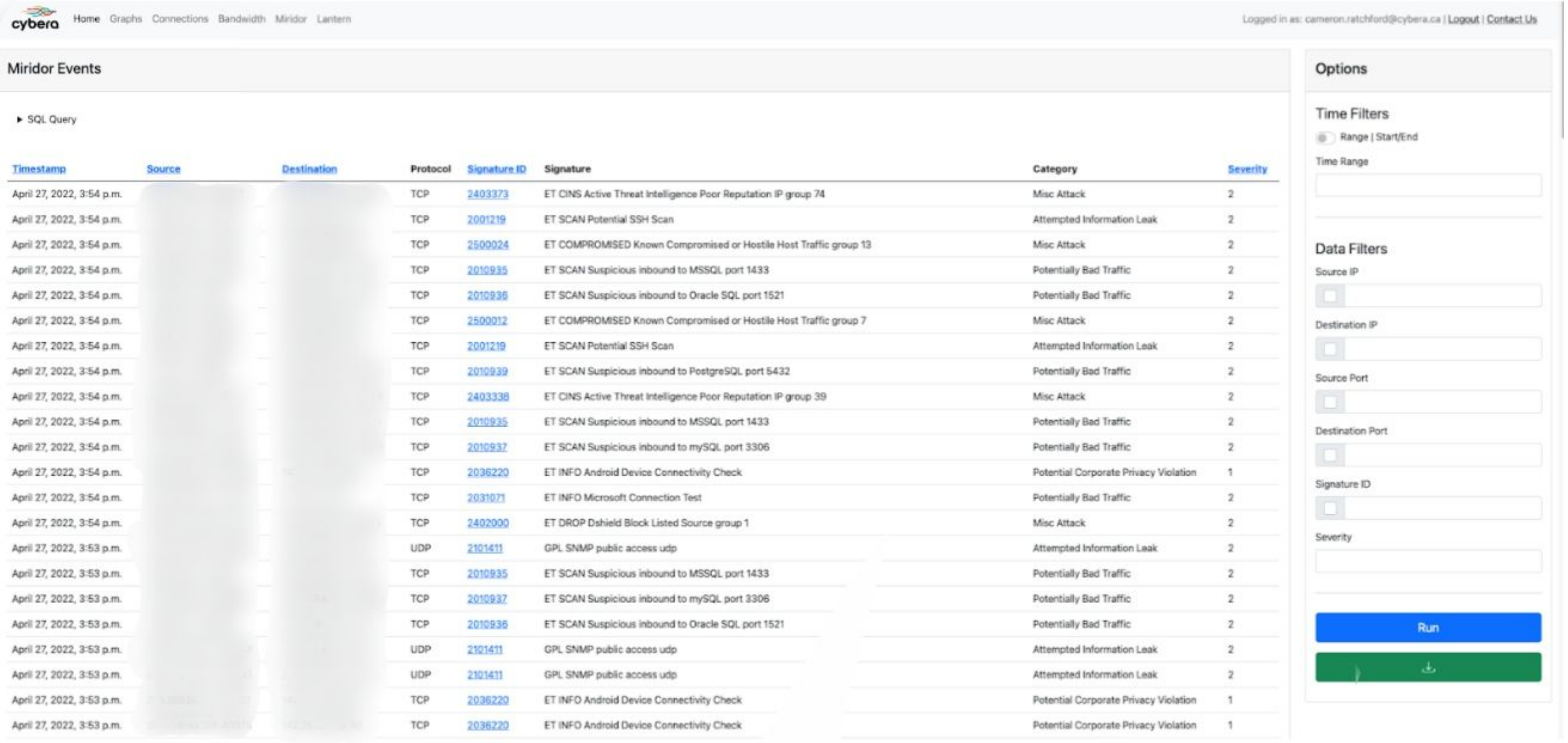
Miridor: What can it be used for?

- 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


cybera
Home
Graphs
Connections
Bandwidth
Miridor
Lantern
Logged in as: cameron.ratchford@cybera.ca | Logout | Contact Us

Miridor Events

▸ SQL Query

Timestamp	Source	Destination	Protocol	Signature ID	Signature	Category	Severity
April 27, 2022, 3:54 p.m.	[redacted]	[redacted]	TCP	2403373	ET CINS Active Threat Intelligence Poor Reputation IP group 74	Misc Attack	2
April 27, 2022, 3:54 p.m.	[redacted]	[redacted]	TCP	2001219	ET SCAN Potential SSH Scan	Attempted Information Leak	2
April 27, 2022, 3:54 p.m.	[redacted]	[redacted]	TCP	2500024	ET COMPROMISED Known Compromised or Hostile Host Traffic group 13	Misc Attack	2
April 27, 2022, 3:54 p.m.	[redacted]	[redacted]	TCP	2010935	ET SCAN Suspicious inbound to MSSQL port 1433	Potentially Bad Traffic	2
April 27, 2022, 3:54 p.m.	[redacted]	[redacted]	TCP	2010936	ET SCAN Suspicious inbound to Oracle SQL port 1521	Potentially Bad Traffic	2
April 27, 2022, 3:54 p.m.	[redacted]	[redacted]	TCP	2500012	ET COMPROMISED Known Compromised or Hostile Host Traffic group 7	Misc Attack	2
April 27, 2022, 3:54 p.m.	[redacted]	[redacted]	TCP	2001219	ET SCAN Potential SSH Scan	Attempted Information Leak	2
April 27, 2022, 3:54 p.m.	[redacted]	[redacted]	TCP	2010939	ET SCAN Suspicious inbound to PostgreSQL port 5432	Potentially Bad Traffic	2
April 27, 2022, 3:54 p.m.	[redacted]	[redacted]	TCP	2403338	ET CINS Active Threat Intelligence Poor Reputation IP group 39	Misc Attack	2
April 27, 2022, 3:54 p.m.	[redacted]	[redacted]	TCP	2010935	ET SCAN Suspicious inbound to MSSQL port 1433	Potentially Bad Traffic	2
April 27, 2022, 3:54 p.m.	[redacted]	[redacted]	TCP	2010937	ET SCAN Suspicious inbound to mySQL port 3306	Potentially Bad Traffic	2
April 27, 2022, 3:54 p.m.	[redacted]	[redacted]	TCP	2036220	ET INFO Android Device Connectivity Check	Potential Corporate Privacy Violation	1
April 27, 2022, 3:54 p.m.	[redacted]	[redacted]	TCP	2031071	ET INFO Microsoft Connection Test	Potentially Bad Traffic	2
April 27, 2022, 3:54 p.m.	[redacted]	[redacted]	TCP	2402000	ET DROP Dshield Block Listed Source group 1	Misc Attack	2
April 27, 2022, 3:53 p.m.	[redacted]	[redacted]	UDP	2101411	GPL SNMP public access udp	Attempted Information Leak	2
April 27, 2022, 3:53 p.m.	[redacted]	[redacted]	TCP	2010935	ET SCAN Suspicious inbound to MSSQL port 1433	Potentially Bad Traffic	2
April 27, 2022, 3:53 p.m.	[redacted]	[redacted]	TCP	2010937	ET SCAN Suspicious inbound to mySQL port 3306	Potentially Bad Traffic	2
April 27, 2022, 3:53 p.m.	[redacted]	[redacted]	TCP	2010936	ET SCAN Suspicious inbound to Oracle SQL port 1521	Potentially Bad Traffic	2
April 27, 2022, 3:53 p.m.	[redacted]	[redacted]	UDP	2101411	GPL SNMP public access udp	Attempted Information Leak	2
April 27, 2022, 3:53 p.m.	[redacted]	[redacted]	UDP	2101411	GPL SNMP public access udp	Attempted Information Leak	2
April 27, 2022, 3:53 p.m.	[redacted]	[redacted]	TCP	2036220	ET INFO Android Device Connectivity Check	Potential Corporate Privacy Violation	1
April 27, 2022, 3:53 p.m.	[redacted]	[redacted]	TCP	2036220	ET INFO Android Device Connectivity Check	Potential Corporate Privacy Violation	1

Options

Time Filters

○ Range | Start/End

Time Range

Data Filters

Source IP

□

Destination IP

□

Source Port

□

Destination Port

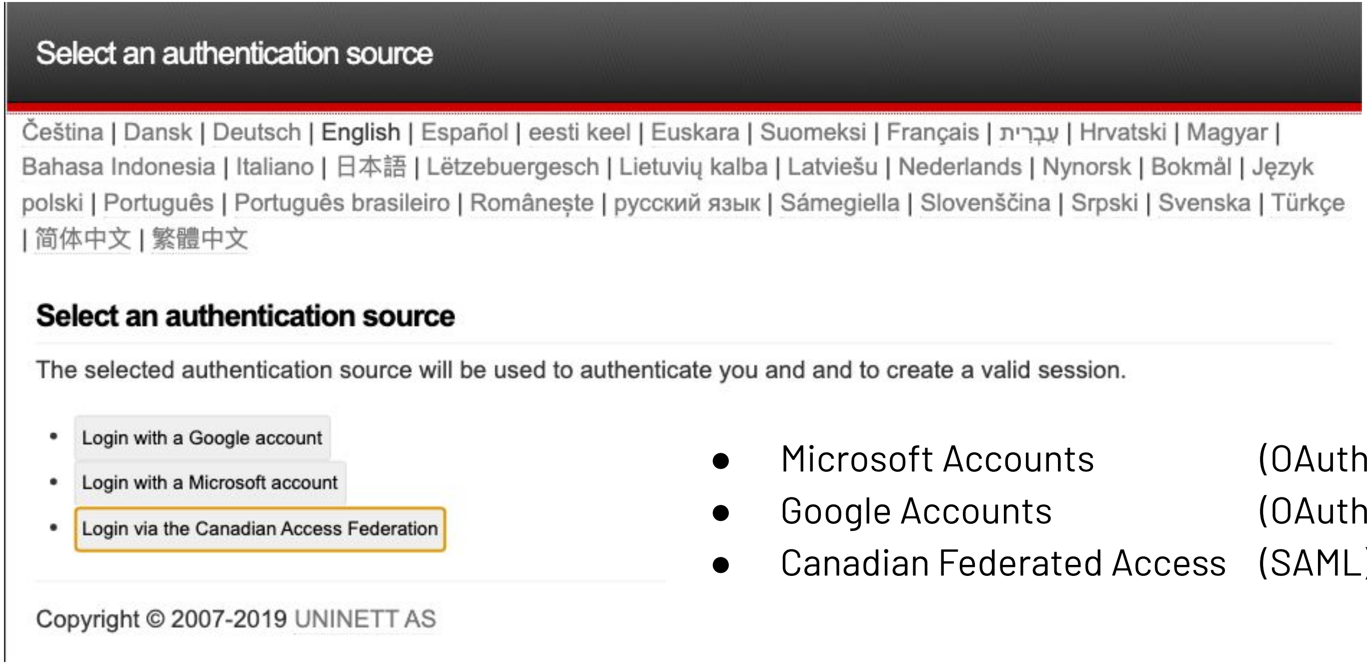
□

Signature ID

□

Severity

Miridor Portal: Authentication



Select an authentication source
Čeština | Dansk | Deutsch | English | Español | eesti keel | Euskara | Suomeksi | Français | עִבְרִית | Hrvatski | Magyar | Bahasa Indonesia | Italiano | 日本語 | Lëtzebuergesch | Lietuvių kalba | Latviešu | Nederlands | Nynorsk | Bokmål | Język polski | Português | Português brasileiro | Românește | русский язык | Sámegiella | Slovenščina | Srpski | Svenska | Türkçe | 简体中文 | 繁體中文

Select an authentication source

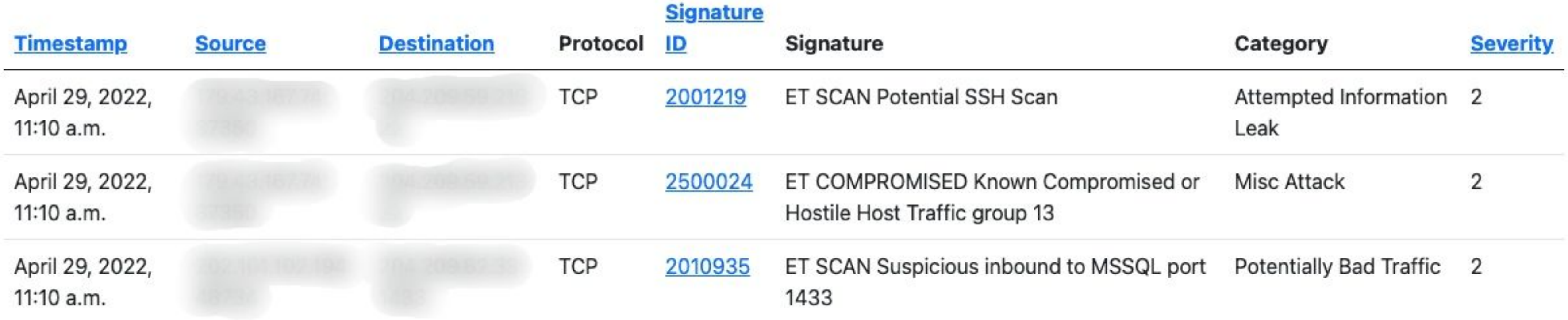
The selected authentication source will be used to authenticate you and and to create a valid session.

Login with a Google account
Login with a Microsoft account
Login via the Canadian Access Federation

Copyright © 2007-2019 UNINETT AS

- Microsoft Accounts (OAuth2)
- Google Accounts (OAuth2)
- Canadian Federated Access (SAML)

Miridor Portal: Table View



Timestamp	Source	Destination	Protocol	Signature ID	Signature	Category	Severity
April 29, 2022, 11:10 a.m.	[redacted]	[redacted]	TCP	2001219	ET SCAN Potential SSH Scan	Attempted Information Leak	2
April 29, 2022, 11:10 a.m.	[redacted]	[redacted]	TCP	2500024	ET COMPROMISED Known Compromised or Hostile Host Traffic group 13	Misc Attack	2
April 29, 2022, 11:10 a.m.	[redacted]	[redacted]	TCP	2010935	ET SCAN Suspicious inbound to MSSQL port 1433	Potentially Bad Traffic	2

Part 2: How it Works

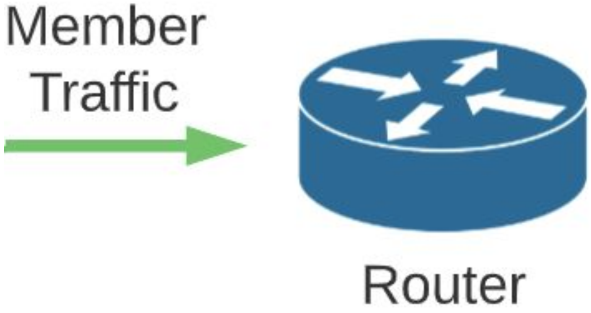
Suricata: What is it?

- High performance Intrusion Detection System
- Signature-based
- Open source

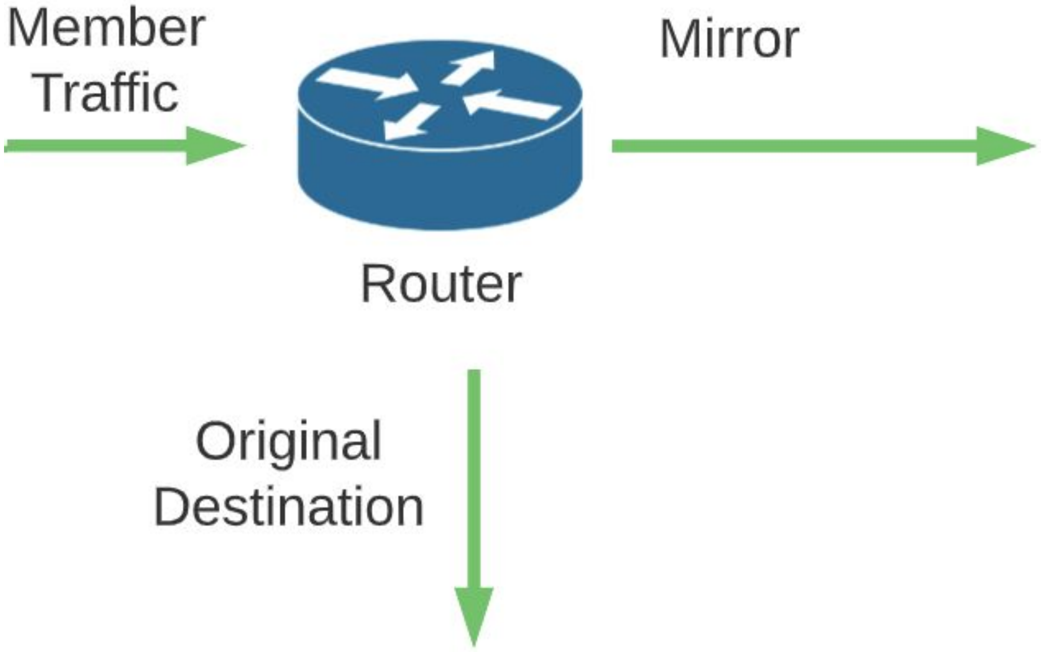
Suricata: Why did we choose it?

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

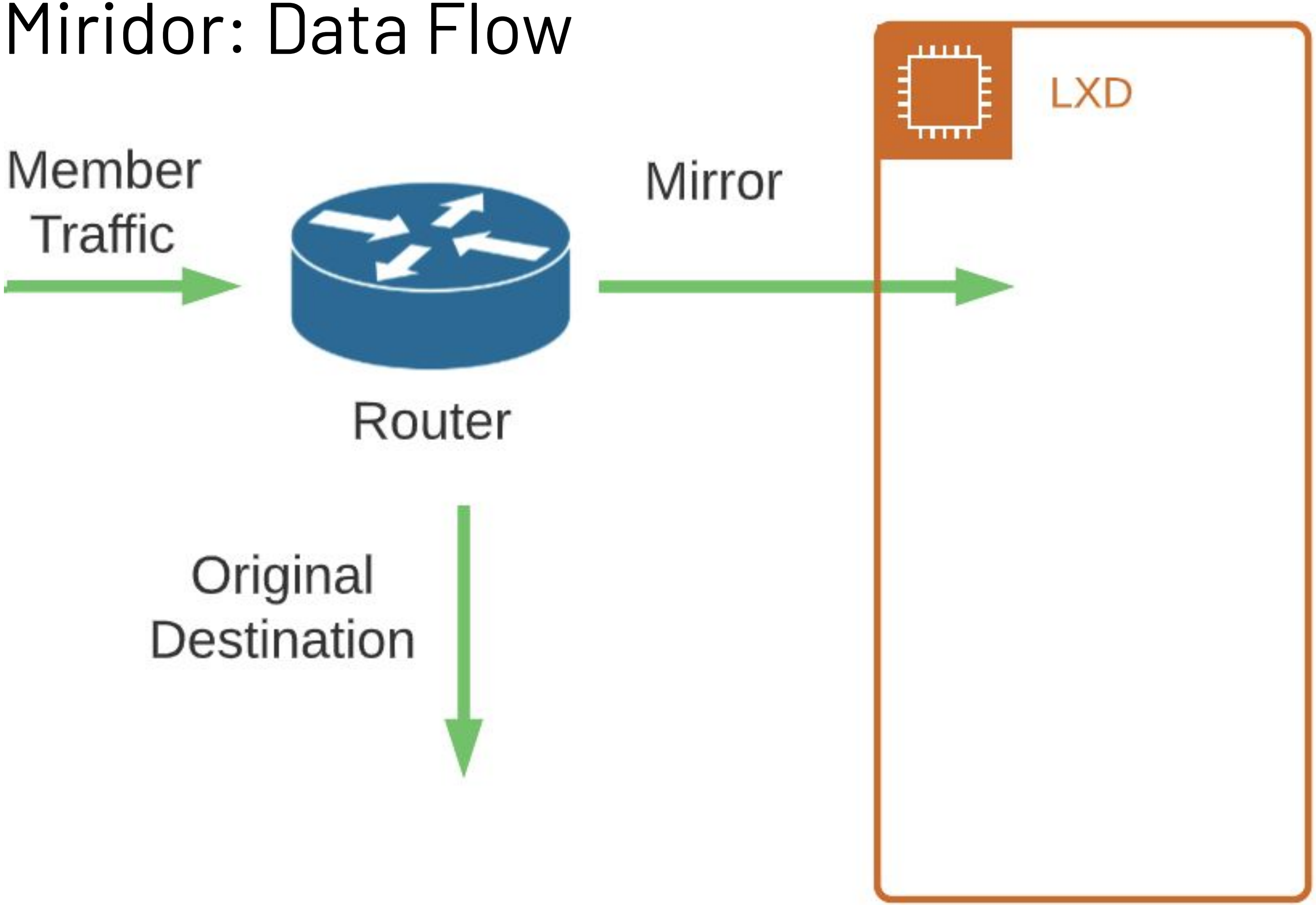
Miridor: Data Flow



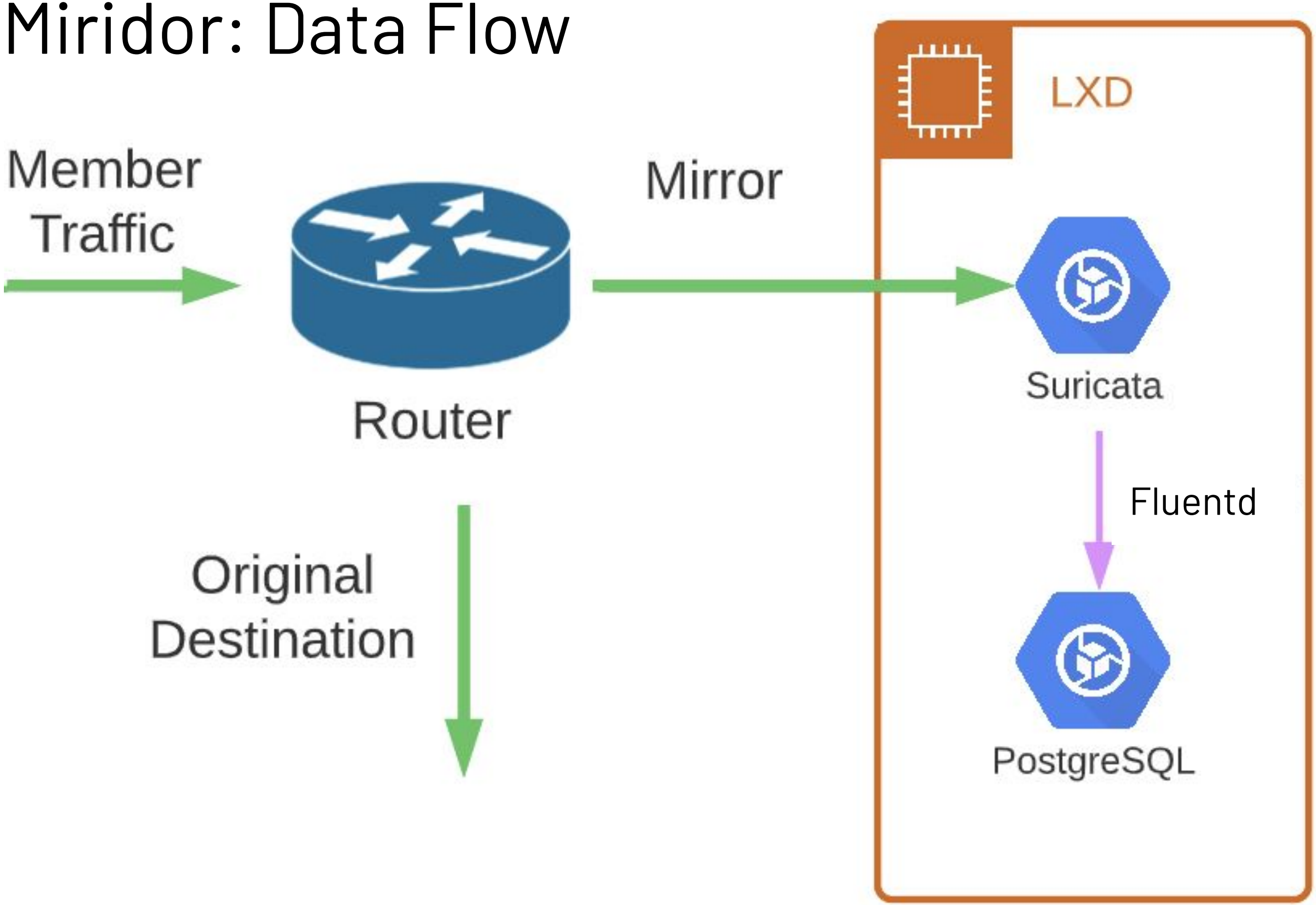
Miridor: Data Flow



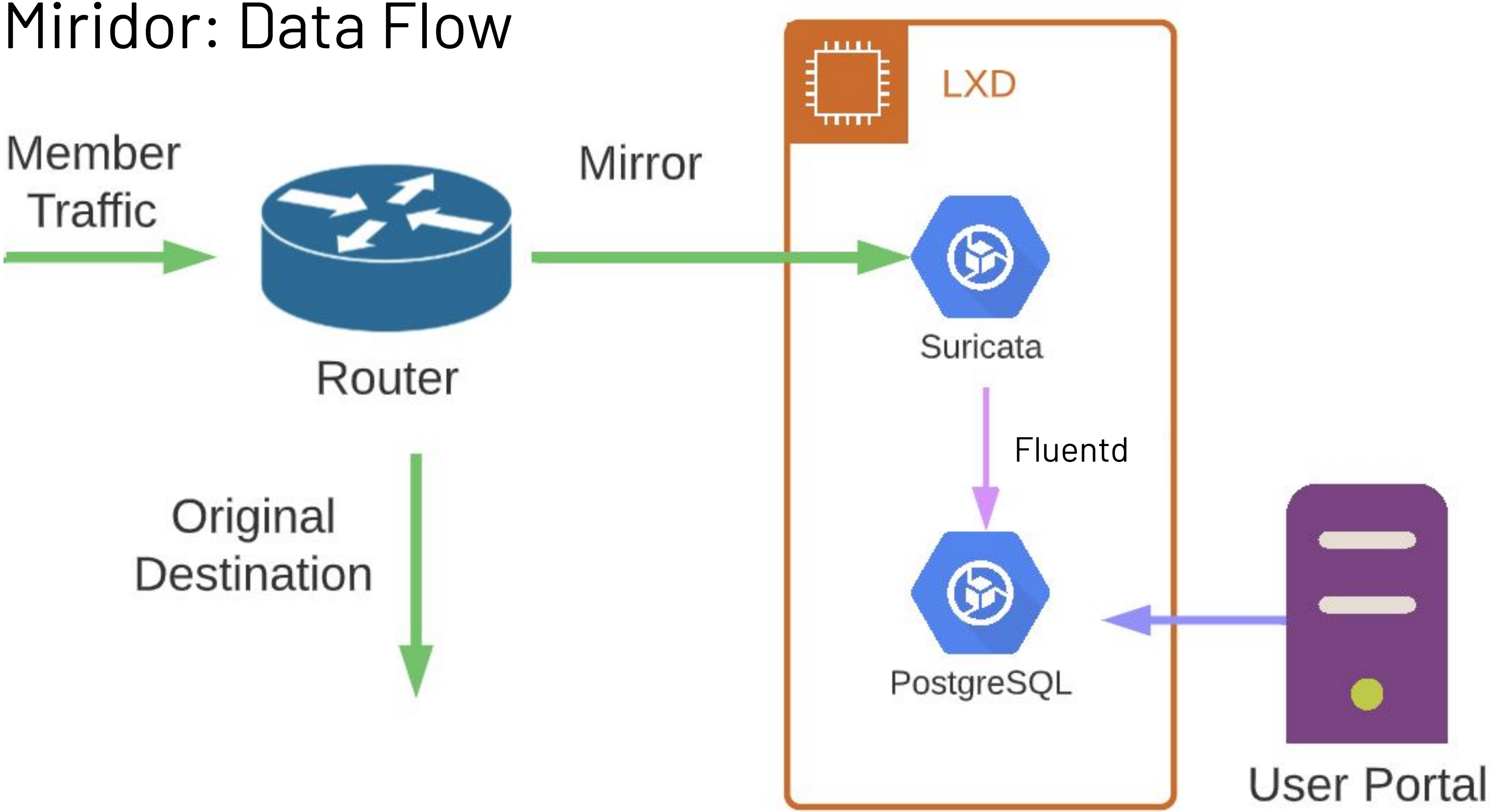
Miridor: Data Flow



Miridor: Data Flow



Miridor: Data Flow



Thank you!

Questions? Contact security@cybera.ca

cybera