Ridgeback Network Defence

Reference Guide

Hyperscalers with Ridgeback Network Defence

Tuesday, 24 January 2023

1 CONTENTS

1 INTRODUCTION

Ridgeback is an active network threat detection, monitoring and response platform. Modern malware, ransomware, and spyware mostly spread through communication platforms like emails, where firewalls are not enough to safeguard your network. Traditional, signature-based end-point security solutions are unable to keep up with the daily emergence of more and more malware. Here is where Ridgeback defence comes into play: a unique, contemporary defence to identify and stop lateral attacks for your network. It is an effective real-time network defence system that runs at the core of your network and safeguards your data.

Ridgeback significantly raises the time and labour cost of attack to the attacker without requiring continual upgrades, giving the company back control.

Ridgeback is plug-and-play, doesn't require extensive configuration or infrastructure burden, starts working immediately after activation, needs little to no supervision, and won't interfere with or burden your live network.

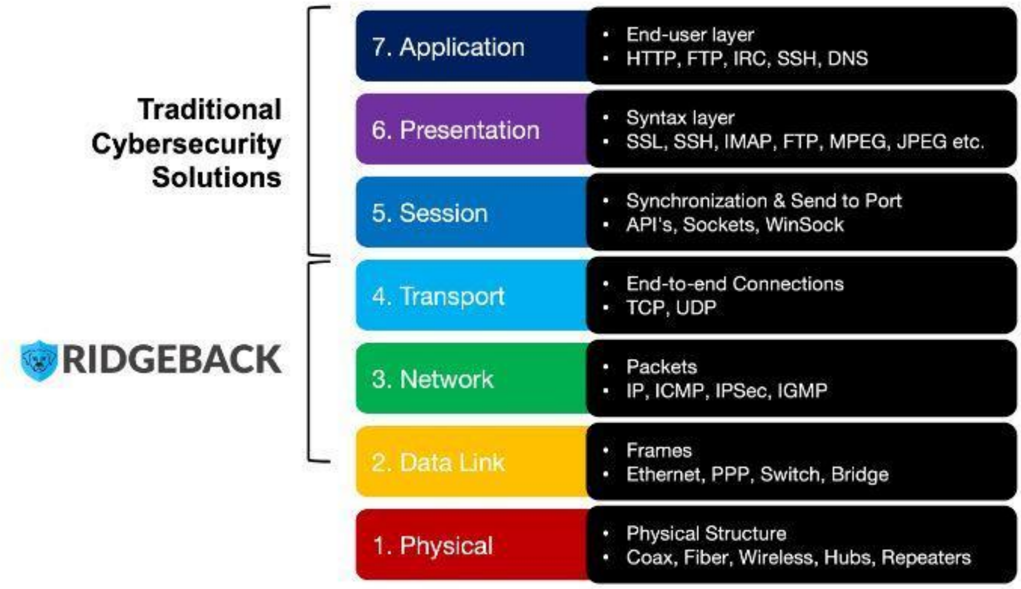

Traditional Cybersecurity Solutions
RIDGEBACK
7. Application
• End-user layer
• HTTP, FTP, IRC, SSH, DNS
6. Presentation
• Syntax layer
• SSL, SSH, IMAP, FTP, MPEG, JPEG etc.
5. Session
• Synchronization & Send to Port
• API's, Sockets, WinSock
4. Transport
• End-to-end Connections
• TCP, UDP
3. Network
• Packets
• IP, ICMP, IPSec, IGMP
2. Data Link
• Frames
• Ethernet, PPP, Switch, Bridge
1. Physical
• Physical Structure
• Coax, Fiber, Wireless, Hubs, Repeaters

Figure 1 Ridgeback location on network

While competing solutions function at higher levels requiring ubiquitous agents, using enormous amounts of resources, and producing many false positives, Ridgeback operates at OSI Layers 2, 3, and 4 and interrupts assaults in real-time by man-in-the-middle automation that engages, disables, and evicts attackers at the start of the attempted exploit.

Ridgeback Business use Cases:

Ridgeback can be used in any network, by all companies from small to major organizations, due to its strict network Defence features. Based on Ridgeback's design, any industry like insurance, education as well as government services can use this easy and cost-effective solution to safeguard your network from various threats.

Banking and financial services cybersecurity

Compliance with regulations necessitates complete, in-depth visibility into system operations. Ridgeback offers insights on weaknesses and productivity issues, particularly when branch office locations are involved across many network segments.

The Private Equity Life Cycle Management

Catastrophic cyber-attacks on a portfolio can now more than ever decimate a private equity owner's financial return. Ridgeback provides ownership life-cycle services, starting with pre-closing due diligence and ending with a smooth departure.

Managed Services and Managed Security Services security

Ridgeback satisfies situational awareness and security requirements across a wide and diverse client base for an IT services provider thanks to multi-tenancy and an architecture for deployment that is unmatched in its simplicity.

Cyber security for public utilities

As you may have seen in the news, foreign governments as well as ransomware-seeking criminals attack public utilities to interfere with the functioning of our nation. Ridgeback should be used to secure the networks of all public utilities since they are all too crucial.

Network Defence in the Manufacturing Sector

OT-heavy workplaces are managed by manufacturers. Ridgeback operates at layer 2, enclosing all networked endpoints within its security perimeter regardless of their hardware, operating systems, or status as managed or unmanaged devices.

Healthcare and cybersecurity

Healthcare and cybersecurity Ridgeback incorporates each networked endpoint, regardless of the kind, inside its security envelope, so you don't have to worry about patient information or the safety of lifesaving IoT healthcare equipment.

Why Hyperscalers

Hyperscalers [1] is the world's first open supply chain Original Equipment Manufacturer- OEM, solving Information Technology challenges through standardization of best practices and hyperscale inspired practices and efficiencies. Hyperscalers offers choice across two open hardware architectures:

- Hyperscale - high efficiency open compute equipment as used by macro service providers.
- Tier 1 Original – conventional equipment as per established Tier 1 OEM suppliers.

Each architecture is complete with network, compute, storage, and converged GP GPU infrastructure elements, and is open / free from vendor lock-in.

Hyperscalers' appliance solutions are packaged complete with hardware, software and pre-built (customisable) configurations. These were all pre-engineered using an in-house IP Appliance Design Process and validated in partnership with associated major software manufacturers. Many can be "test-driven" using Hyperscalers Lab as a Service (LaaS). Hyperscalers appliance solutions are ideally suited to IaaS PaaS and SaaS providers looking to implement their services from anywhere.

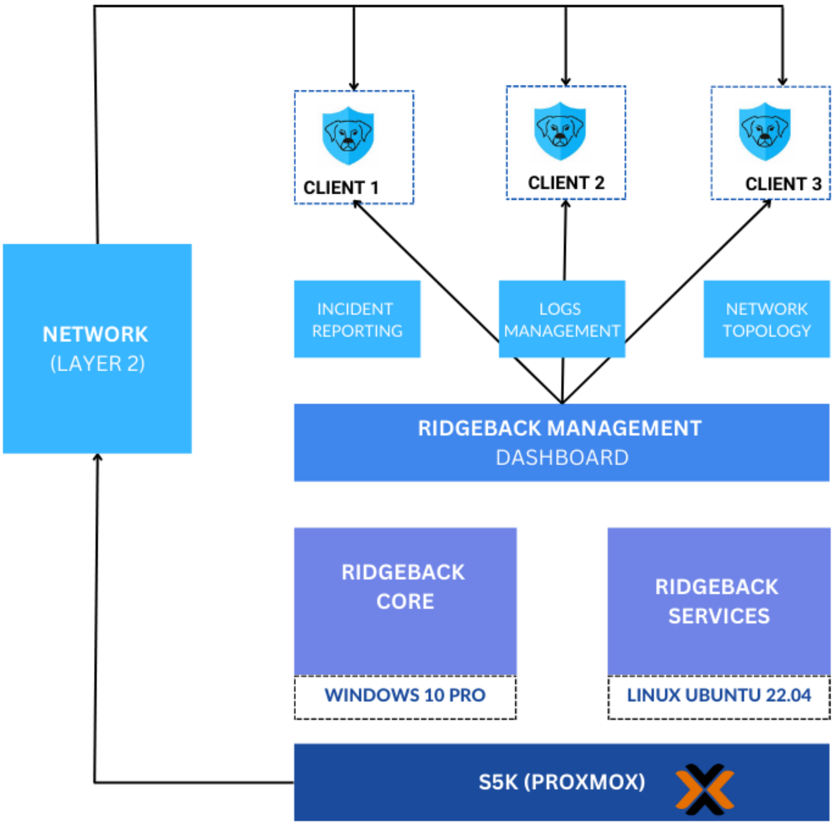


Figure 2 Ridgeback Network Defence Architecture Design

In this reference guide, we will discuss on the deployment steps and features of Ridgeback network Defence for a cyber threat protection and monitoring.

Audience and Purpose

Engineers, Enthusiasts, Executives, and IT professionals with background in Computer Science/ Electronics/ Information Technology with understanding in Linux commands and network layers.

The purpose of this documentation is to provide in depth knowledge about the basic overview, appliance requirements and steps to deploy into your network.

Documents, Knowledge Base, and Technical Support

Hyperscalers reference architectures and appliance / solutions demonstrations are available at: https://www.hyperscalers.com/OCP-hyperscale-rack-solutions

For technical queries regarding this document and for managing virtualized, mobile, and cloud technologies, you can contact Hyperscalers technical support at support@hyperscalers.com

Additional reference to the Ridgeback Defence on open rack platforms (OCP) can be found in Hyperscalers whitepapers and reference architecture section link - https://www.hyperscalers.com/red-hat-ceph-openstack-13-world-record-saas-paas-openshift-paas-appliance-open-compute-ocp-hyperscale-how-to-build-cloud-world-record

Readers are recommended to have a prior knowledge and expertise with container, network layer and Linux programming to better understand the following documentation.

Contact info@hyperscalers.com for more information.

Features and benefits of Ridgeback:

Network Protection:

When a hacker tries to get into our systems, Ridgeback defends them with security measures that turns the tables on any intruder. By deploying automated layers of protection to access any network assets, when an intruder tries to discover or access any asset in the dark space - where there are none - Ridgeback automatically steps in to notify you while simultaneously denying the attacker any access to the system.

Lateral movement Prevention:

Ridgeback enhances security by providing helpful remediation tools that stop security risks' damaging lateral movement. When an attacker gains access to your system, they seek to further enter your network to expand their control of your environment and do more damage. This is known as lateral movement. By limiting the harm done by intruders, the programme rapidly neutralises these security concerns, ensuring the safety and security of your network.

Continuous visibility:

The solution offers total visibility by constantly keeping an eye on your whole network and all the communication data/information it contains. Your network-connected laptops, mobile devices, and tablets - even operating technology in a hospital or in the manufacturing process - are all regularly scanned for and evaluated for security vulnerabilities by Ridgeback. It makes sure that only people with permission may access your information.

Policy Enforcement:

Ridgeback makes sure that your security policy is strictly followed. Every asset on your network has its permissions constantly checked by the system, which ensures that all your policies are carefully followed.

Integration:

The programme has useful integrations, such as support for SIEM (security information and event management), so it may be easily integrated into your current security framework.

User friendly:

Ridgeback's cloud-hosted design allows quick and easy setup. Once it is operating, the system is basically autonomous and doesn't need much supervision.

Important Considerations:

The following documentation gives a detailed step-by-step deployment guide of Ridgeback network Defence along with all the requirements to setup. The architecture is specific and tailored for enabling enterprises to provision a platform for their service delivery within or outside the organisation. Hyperscalers recommends the below important considerations before proceeding to the deployment phase.

The Ridgeback requires minimum of 2 or more cores intel processor with 2 GB memory, 20 GB Hard Drive space minimum. These can be VMs or standard Linux Box. It supports Ubuntu 16 or higher Ubuntu or Debian version 8 or higher.

Digital IP Appliance Design Process

Hyperscalers has developed a Digital- IP-Appliance Design Process and associated Appliance Optimizer Utility which can enable the productization of IT-appliances for Digital-IP owners needing to hyperscale their services very quickly, reliably and at a fraction of traditional costs.

Appliance Optimizer Utility AOU

The Appliance Optimizer Utility (AOU) automates the discovery of appliance bottlenecks by pinging all layers in the proposed solution stack. A live dashboard unifies all key performance characteristics to provide a head-to-head performance assessment between all data-path layers in the appliance, as well as a comparison between holistic appliances.

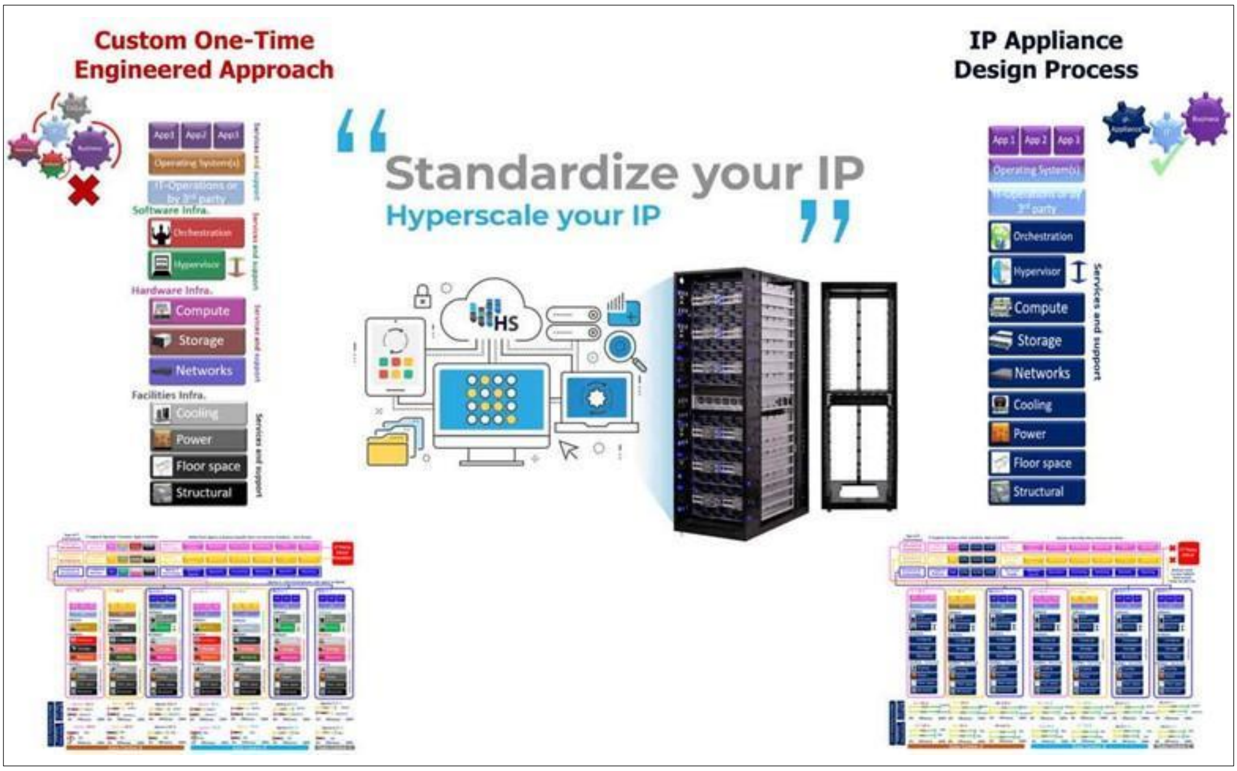


Figure 3 Digital IP-Appliance Design Process

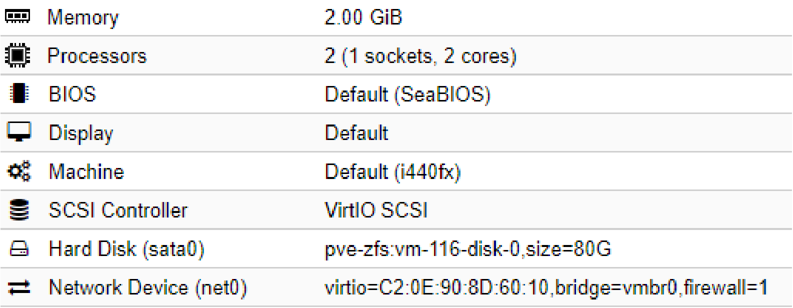
Infrastructure Setup:

To demonstrate a scalable and resilient Ridgeback network Defence, we have used the below configuration:

D43K-1U (S5K) – 1U as a Highly Available two node Proxmox 7.2-11 cluster:

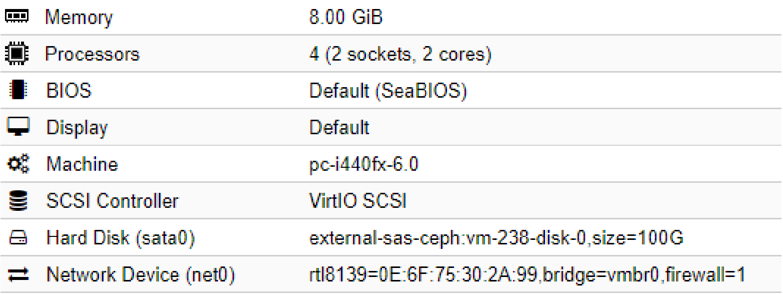
- 2x AMD EPYC 7313 16-Core Processor
- 16x DDR4 3200Mhz 32GB Register Samsung M393A4K40DB3-CWE
- 1x Dual port 10GbE Mellanox Technologies MT27800 Family [ConnectX-5]
- 2x OS SSD WD_Green_M.2_2280 240GB
- 1x Data SSD 2.5" U.2 NVMe SSD Samsung PM9A3 3.84TB NVMe PCIe MZQL23T8HCLS-00A07

Ridgeback Container VM:



Memory	2.00 GiB
Processors	2 (1 sockets, 2 cores)
BIOS	Default (SeaBIOS)
Display	Default
Machine	Default (i440fx)
SCSI Controller	VirtIO SCSI
Hard Disk (sata0)	pve-zfs:vm-116-disk-0,size=80G
Network Device (net0)	virtio=C2:0E:90:8D:60:10,bridge=vmbr0,firewall=1

Ridgeback Core VM:



Memory	8.00 GiB
Processors	4 (2 sockets, 2 cores)
BIOS	Default (SeaBIOS)
Display	Default
Machine	pc-i440fx-6.0
SCSI Controller	VirtIO SCSI
Hard Disk (sata0)	external-sas-ceph:vm-238-disk-0,size=100G
Network Device (net0)	rtl8139=0E:6F:75:30:2A:99,bridge=vmbr0,firewall=1

Building Blocks:

S5K | D43K-1U Ultimate 1U Server for AMD EPYC Milan 3rd Gen Processors

Native design for AMD EPYC™ 7003 Processors, ready for PCIe 4.0 eco-system deployment. Up to 128-core within 1U form factor, optimized for HPC workloads. With 4 AMD xGMI-2 between dual EPYC™ processors up to 16GT/sec of CPU interconnect speed. Up to 5 PCIe expansion slots in a 1U chassis. Flexible I/O options with a variety of SAS mezzanine and OCP mezzanine option for diverse configurations. Flexible storage configurations, tailored for diversified software defined workloads. NUMA balanced PCIe topology for NVMe drives.

S5X 2.5" | D53X-1U Ultimate 1U Server for Intel Xeon 3rd Gen Processors

The S5X 2.5" (D53X-1U) based on PCIe Gen 4.0 and Intel's 3rd Generation Processor Family (Ice-lake) offers: Two (2) CPU Sockets for up to 80 cores using Intel® Xeon® Platinum 8380 Processor 40cores each. 32 Memory slots for up to 8TB DIMM or Up to 12TB DIMM+DCPM (PMEM 200 series). 12 Front Storage drive bays 2.5" hot-plug U.2 NVMe or SATA/SAS. Five (5) x PCIe 4.0 expansions slots for Network Interface Cards NIC. Two (2) M.2 onboard storage. Three (3) accelerators like NVIDIA T4 GPU.

S5Z | T43Z-2U The Power of Hyper Convergence

The S5Z | T43Z-2U based on PCIe Gen 4.0 and Intel's 3rd Generation Processor Family (Ice-lake) is a high performance, multi node server offering eight (8) CPU in 2RU as part of four (4) independent nodes. Each node offers two (2) CPU Sockets for up to 80 cores using Intel® Xeon® Platinum 8380 Processor 40cores each, 16 Memory slots for up to 4TB DIMM or up to 6TB DIMM+DCPM (PMEM 200 series), four (4) 2.5" U.2 NVMe front storage drive bays with two (2) M.2 NVMe for OS or caching, and three (3) x PCIe 4.0 expansions slots for Network Interface Cards NIC or accelerators like GPU.

Access and Default Credentials

To access the Hyperscalers Lab as a Service (LaaS) portal, navigate to https://www.hyperscale2.com which is a repository of enterprise appliances that can be used to test drive the use cases before deploying on a mass scale.

Ridgeback cyber Defence can be accessed from https://ridgeback.hyperscale2.com/ (Please request for the credentials to info@hyperscalers.com and we can assist you.)

Terminologies:

Network layer:

In the context of computer networking, the network layer is a layer in the OSI (Open Systems Interconnection) model that is responsible for providing logical addressing and routing services. The network layer is responsible for routing data packets between devices on a network. It does this by assigning a unique address to each device on the network, and then using this address to determine the best path for the data to take from its source to its destination.

Containers:

A container is a lightweight, standalone, and executable package that includes everything an application needs to run, including the application code, system tools, libraries, and runtime. Containers are often used in conjunction with container orchestration tools, which are used to manage and deploy large numbers of containers across a network. Container orchestration tools allow users to define and automate the deployment, scaling, and management of containerized applications, making it easier to manage complex distributed applications.

Lateral Movement:

Lateral movement refers to the process an intruder uses to expand their control from of moving from one network resource to many another within an organization's network. It is often used by attackers to gain access to additional systems and data once they have compromised a single device or system. Lateral movement is a common technique used by attackers to gain a foothold in an organization's network and to escalate their privileges. It is often used in conjunction with other tactics, such as phishing attacks or malware, to gain initial access to a network, and then to move laterally within the network to gain access to sensitive data or systems or disrupt operations where they are most critical.

2 BASE PRODUCT DEPLOYMENT

The Ridgeback network Defence appliance is installed using the docker platform in a Linux or Windows platform. Following steps are followed to deploy the Ridgeback appliance in a datacentre network.

Preinstallation Requirements:

The Ridgeback requires minimum of 2 or more cores intel processor with 2 GB memory, 20 GB Hard Drive space minimum. It supports Ubuntu 16 or higher and windows 10 or 11.

Installation Components

The Ridgeback network Defence installation components can be divided into three parts.

Database: A MySQL-compatible database is the initial component of deployment. If long-term data preservation is not necessary, the database can be operated in a container or as a standalone installation.

Containers: A group of containers makes up the second phase of deployment. Different Ridgeback services are run by the containers.

Core: One Core must be deployed for each network segment that you want to use Ridgeback to defend. A network segment may be read from and written to using a tiny programme called a Core.

Deployment:

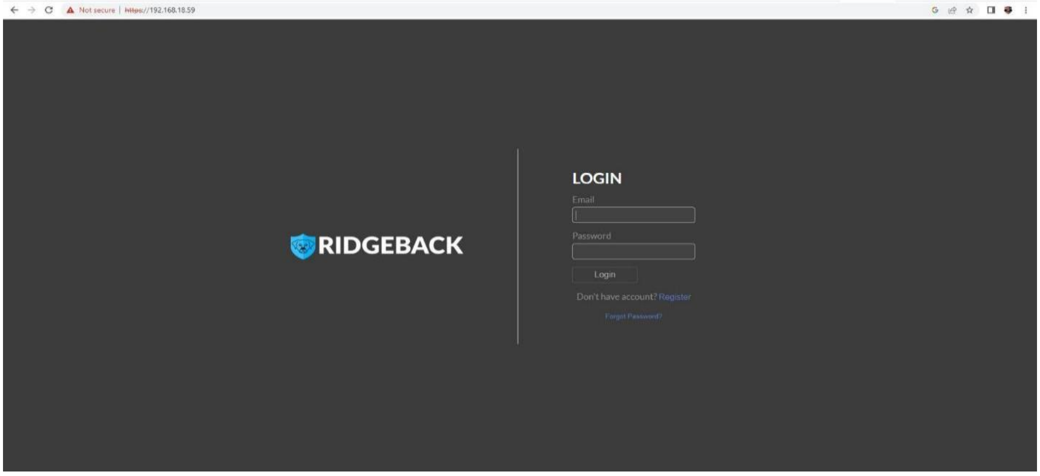
Part 1: setting up and containers.

- Acquire a computer with an Intel CPU, at least 2 cores, 8GB of RAM, and Windows 10 or 11.
- Install a container system such as Docker for Desktop.
- Use docker login to access the Ridgeback container repository at ridgebacknet.azurecr.io.
- Get the Npcap driver and instal it by visiting https://npcap.com/#download.
- Setup the container system's project directory ($PROJECT).
- Copy the file docker-compose.yml to the $PROJECT directory.
- Transfer sample-env to $PROJECT.env
- Log in to the Ridgeback container image repository from the $PROJECT directory.
- Set the LicenseName entry in the $PROJECT.env file.
- The LicenseKey entry in the $PROJECT.env file should be set.
- Add your email address in the SuperAdmin box of the $PROJECT.env file.
- 12.Set the ManagerIpAddress field to 127.0.0.1 in the $PROJECT.env file.
- 13.Set the ServerIpAddress column to 127.0.0.1 in the $PROJECT.env file.
- 14. Change the DatabasePassword entry in the $PROJECT.env file to an alternative password.15.
- Docker compose up —no-start in the $PROJECT.env file
- 16. Docker compose start database is entered in the $PROJECT.env file.
- 17. Docker compose execute db-init in the $PROJECT.env environment variable
- 18. Start the server manager enrichment with docker compose in the $PROJECT.env file.
- 19. Enter the following command in the $PROJECT.env file: docker compose start surface policy # optional services.
- 20.Connect to https://localhost with a web browser at number.

Part 2: Core

Install/Manage a Core (using an administrator PowerShell)

```
New-Item "C:\opt\ridgeback\bin" -Type Directory
New-Item "C:\opt\ridgeback\conf" -Type Directory
Copy ridgeback-core.exe to C:\opt\ridgeback\bin
Use rloader to create ridgeback.conf
Copy ridgeback.conf to C:\opt\ridgeback\conf
New-Service -Name "RidgebackCoreNet" -BinaryPathName
"C:\opt\ridgeback\bin\ridgeback-core.exe" -DisplayName "Ridgeback
Core Net" -StartupType "Automatic" -Description "RidgebackCoreNet provides network
security."

# To start the rcore service:
Start-Service -Name "RidgebackCoreNet"

# To stop the rcore service:
taskkill /IM ridgeback-core.exe /F

# To delete the rcore service in PowerShell <= 5.1
(Get-WmiObject -Class Win32_Service -Filter
"Name='RidgebackCoreNet'").delete()
```



Not secure | https://192.168.18.59

RIDGEBACK

LOGIN

Email

Password

Login

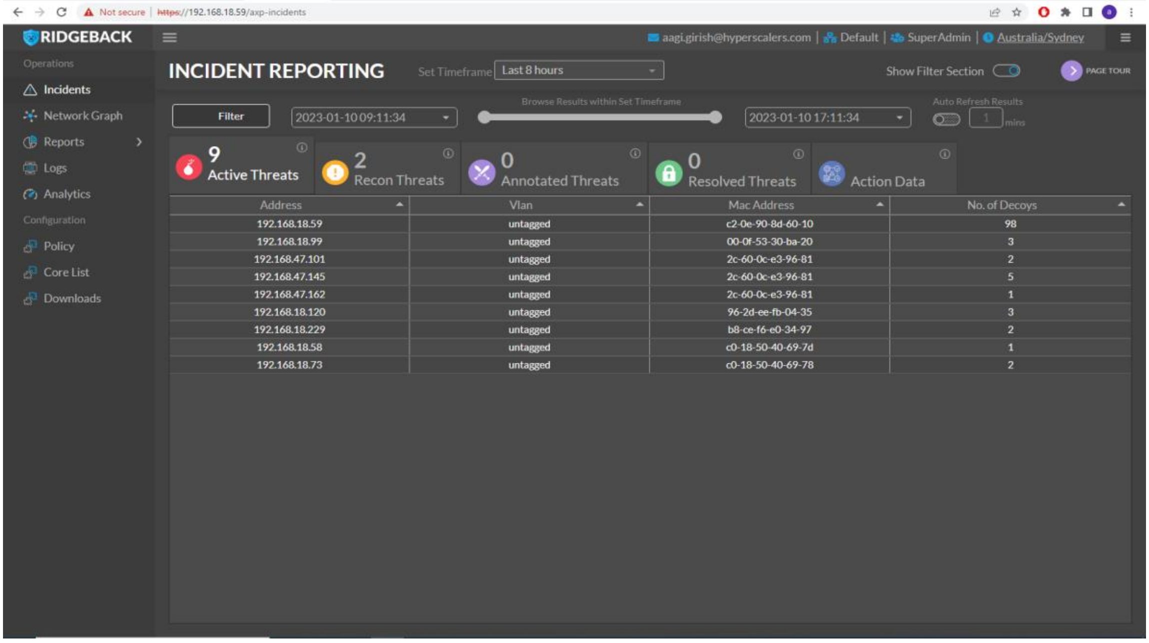
Don't have account? Register

Forgot Password?

Figure 4 Ridgeback Dashboard

3 Configure the Appliance

After deploying the ridgeback software, the dashboard can be accessed to configure and customise the appliance. Below screen shows the incident reporting section that shows the active and recommended threats that can be resolved or actioned by the administrator. Filtering the required subnets and IP addresses can help to isolate and investigate a specific incident.



Not secure | https://192.168.18.59/axp-incidents

RIDGEBACK

aagi.girish@hyperscalers.com | Default | SuperAdmin | Australia/Sydney

Operations

- Incidents
- Network Graph
- Reports
- Logs
- Analytics

Configuration

- Policy
- Core List
- Downloads

INCIDENT REPORTING

Set Timeframe: Last 8 hours

Show Filter Section

PAGE TOUR

Filter

2023-01-10 09:11:34

Browse Results within Set Timeframe

2023-01-10 17:11:34

Auto Refresh Results: 1 mins

9 Active Threats

2 Recon Threats

0 Annotated Threats

0 Resolved Threats

Action Data

Address	Vlan	Mac Address	No. of Decoys
192.168.18.59	untagged	c2-0e-90-8d-60-10	98
192.168.18.99	untagged	00-0f-53-30-ba-20	3
192.168.47.101	untagged	2c-60-0c-e3-96-81	2
192.168.47.145	untagged	2c-60-0c-e3-96-81	5
192.168.47.162	untagged	2c-60-0c-e3-96-81	1
192.168.18.120	untagged	96-2d-ee-fb-04-35	3
192.168.18.229	untagged	b8-ce-f6-e0-34-97	2
192.168.18.58	untagged	c0-18-50-40-69-7d	1
192.168.18.73	untagged	c0-18-50-40-69-78	2

Figure 5 Ridgeback incident reporting

More intuitive information can be see in a graph structure by navigating to the network graph section. It shows the arp, tcp and llmnr queries in the network layer 2. Any unavailable IP address in the network is morphed as a live machine by ridgeback to identify any lateral movement of hackers and unauthorised users in the network. These activities are monitored from the network graph with the below icons:

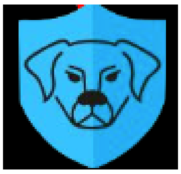


Figure 3 Phantom - Mock IP

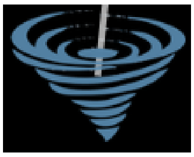


Figure 2 Whirlpool - Unrecognised access

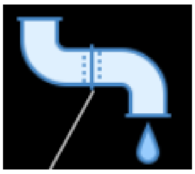
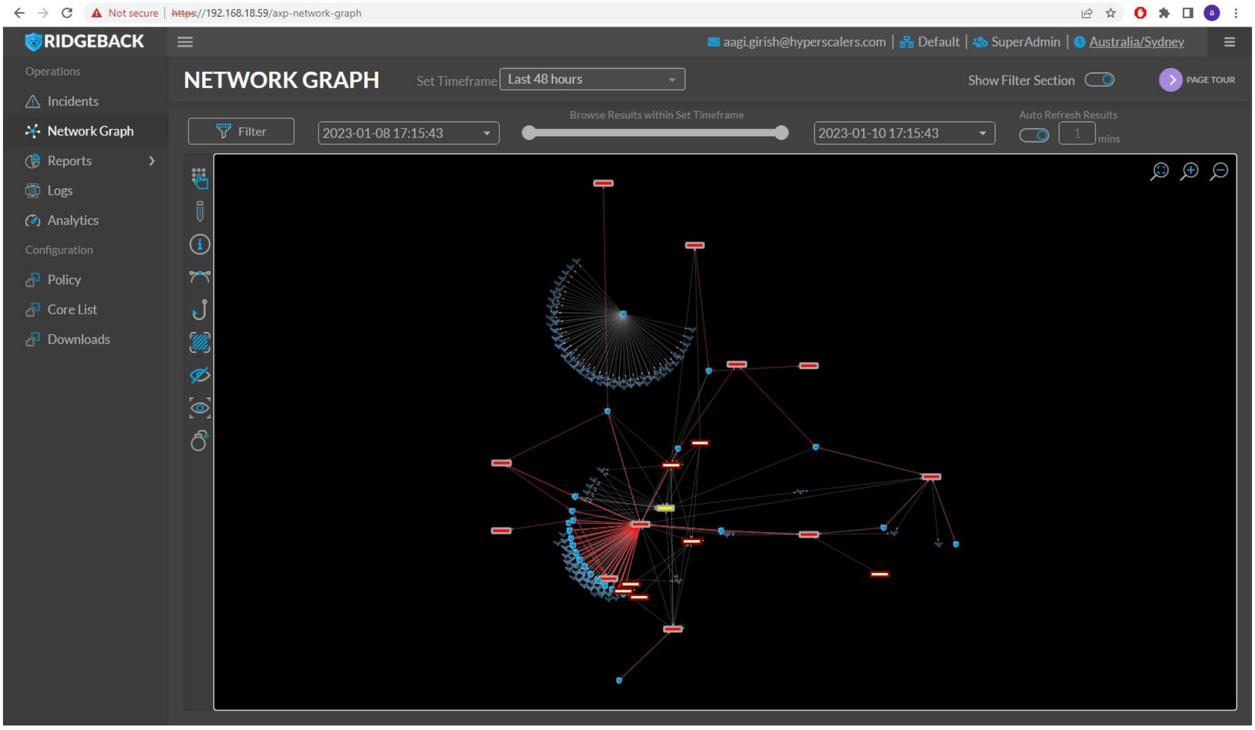


Figure 1 LLMNR hostname requests



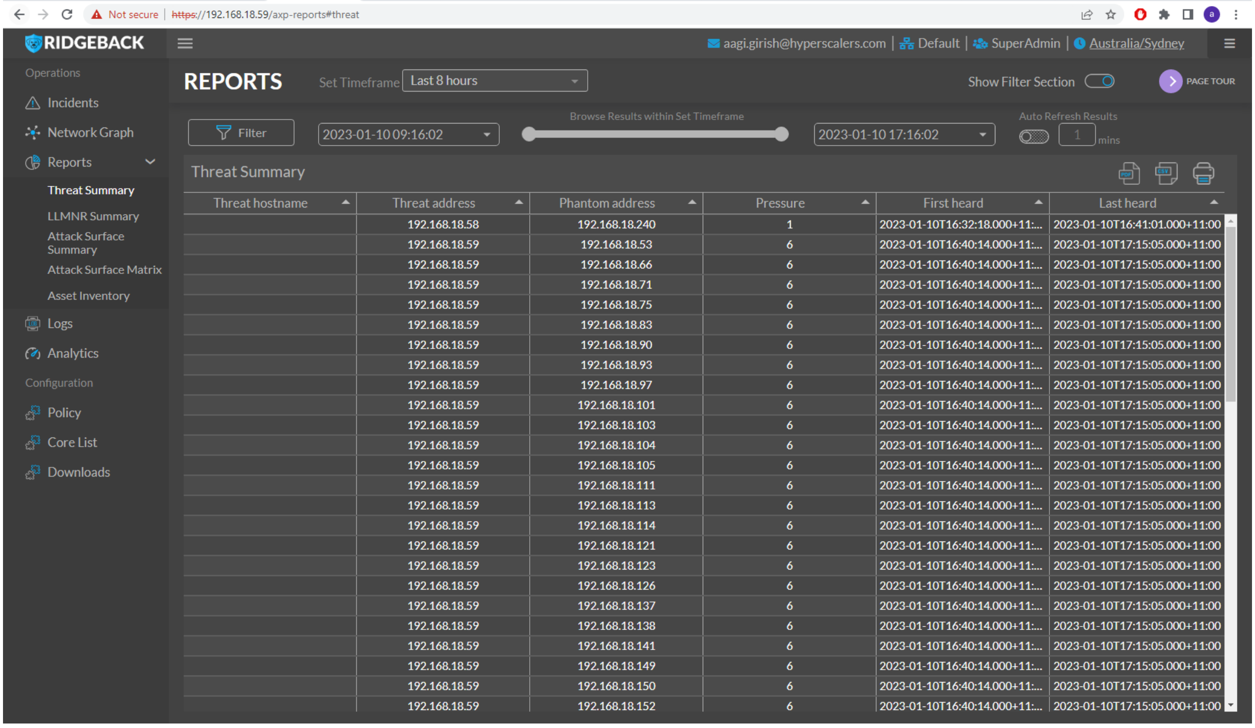
Set Timeframe: Last 48 hours

2023-01-08 17:15:43 – 2023-01-10 17:15:43

Auto Refresh Results: 1 mins

Figure 9 Ridgeback Network Graph

To audit the threat incidents, reports section in the ridgeback dashboard is helpful and intuitive as shown in the screenshot below.



Set Timeframe: Last 8 hours

2023-01-10 09:16:02 – 2023-01-10 17:16:02

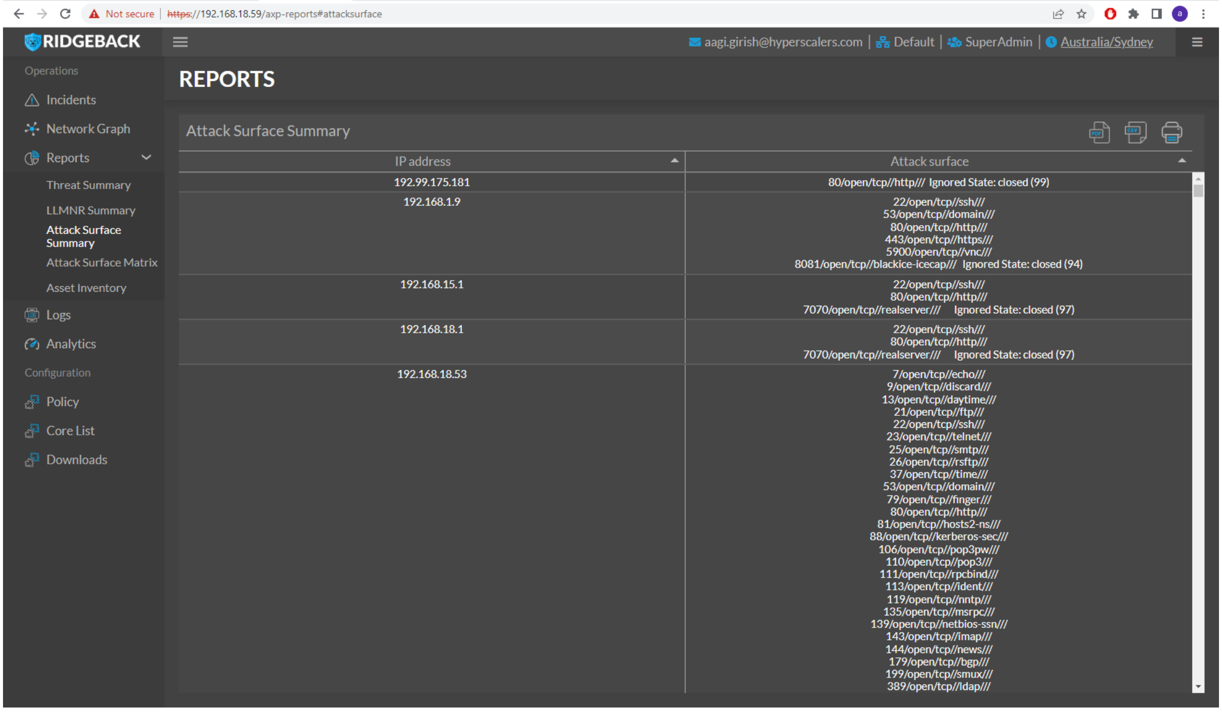
Auto Refresh Results: 1 mins

Threat Summary

Threat hostname	Threat address	Phantom address	Pressure	First heard	Last heard
	192.168.18.58	192.168.18.240	1	2023-01-10T16:32:18.000+11:...	2023-01-10T16:41:01.000+11:00
	192.168.18.59	192.168.18.53	6	2023-01-10T16:40:14.000+11:...	2023-01-10T17:15:05.000+11:00
	192.168.18.59	192.168.18.66	6	2023-01-10T16:40:14.000+11:...	2023-01-10T17:15:05.000+11:00
	192.168.18.59	192.168.18.71	6	2023-01-10T16:40:14.000+11:...	2023-01-10T17:15:05.000+11:00
	192.168.18.59	192.168.18.75	6	2023-01-10T16:40:14.000+11:...	2023-01-10T17:15:05.000+11:00
	192.168.18.59	192.168.18.83	6	2023-01-10T16:40:14.000+11:...	2023-01-10T17:15:05.000+11:00
	192.168.18.59	192.168.18.90	6	2023-01-10T16:40:14.000+11:...	2023-01-10T17:15:05.000+11:00
	192.168.18.59	192.168.18.93	6	2023-01-10T16:40:14.000+11:...	2023-01-10T17:15:05.000+11:00
	192.168.18.59	192.168.18.97	6	2023-01-10T16:40:14.000+11:...	2023-01-10T17:15:05.000+11:00
	192.168.18.59	192.168.18.101	6	2023-01-10T16:40:14.000+11:...	2023-01-10T17:15:05.000+11:00
	192.168.18.59	192.168.18.103	6	2023-01-10T16:40:14.000+11:...	2023-01-10T17:15:05.000+11:00
	192.168.18.59	192.168.18.104	6	2023-01-10T16:40:14.000+11:...	2023-01-10T17:15:05.000+11:00
	192.168.18.59	192.168.18.105	6	2023-01-10T16:40:14.000+11:...	2023-01-10T17:15:05.000+11:00
	192.168.18.59	192.168.18.111	6	2023-01-10T16:40:14.000+11:...	2023-01-10T17:15:05.000+11:00
	192.168.18.59	192.168.18.113	6	2023-01-10T16:40:14.000+11:...	2023-01-10T17:15:05.000+11:00
	192.168.18.59	192.168.18.114	6	2023-01-10T16:40:14.000+11:...	2023-01-10T17:15:05.000+11:00
	192.168.18.59	192.168.18.121	6	2023-01-10T16:40:14.000+11:...	2023-01-10T17:15:05.000+11:00
	192.168.18.59	192.168.18.123	6	2023-01-10T16:40:14.000+11:...	2023-01-10T17:15:05.000+11:00
	192.168.18.59	192.168.18.126	6	2023-01-10T16:40:14.000+11:...	2023-01-10T17:15:05.000+11:00
	192.168.18.59	192.168.18.137	6	2023-01-10T16:40:14.000+11:...	2023-01-10T17:15:05.000+11:00
	192.168.18.59	192.168.18.138	6	2023-01-10T16:40:14.000+11:...	2023-01-10T17:15:05.000+11:00
	192.168.18.59	192.168.18.141	6	2023-01-10T16:40:14.000+11:...	2023-01-10T17:15:05.000+11:00
	192.168.18.59	192.168.18.149	6	2023-01-10T16:40:14.000+11:...	2023-01-10T17:15:05.000+11:00
	192.168.18.59	192.168.18.150	6	2023-01-10T16:40:14.000+11:...	2023-01-10T17:15:05.000+11:00
	192.168.18.59	192.168.18.152	6	2023-01-10T16:40:14.000+11:...	2023-01-10T17:15:05.000+11:00

Figure 10 Deep dive into threat summary

Ridgeback attack surface summary monitors the port numbers accessed by the IPs identified as threat



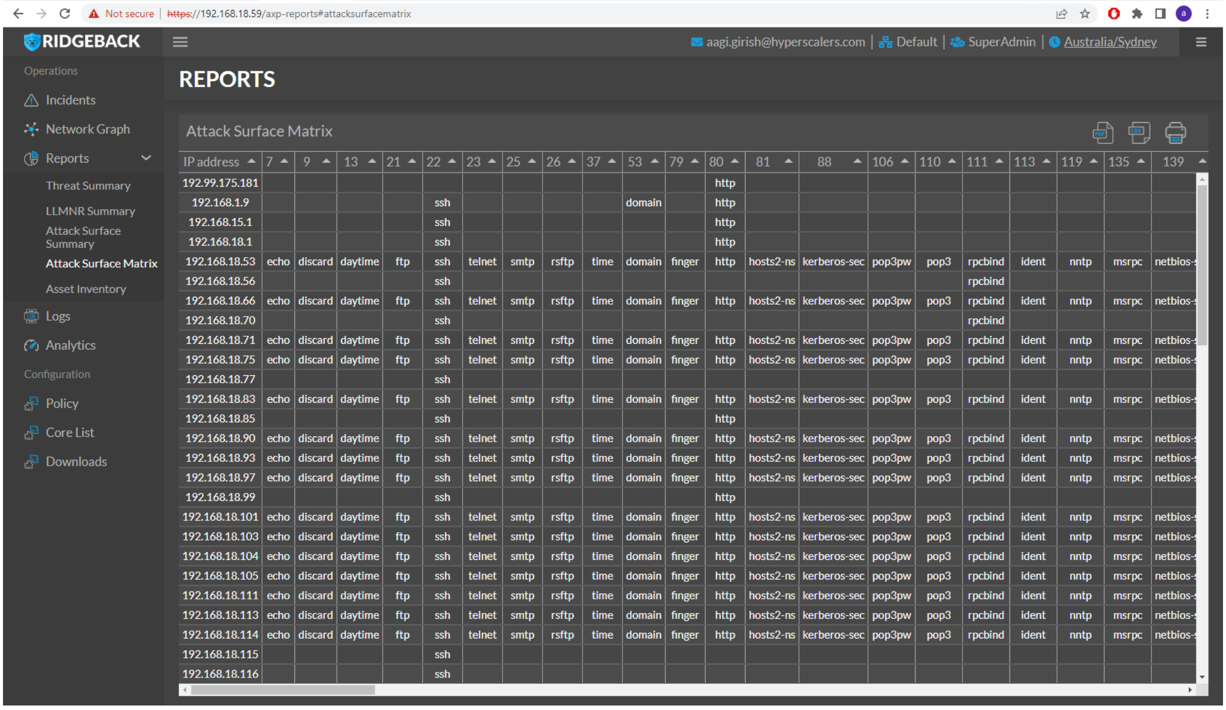
REPORTS

Attack Surface Summary

IP address	Attack surface
192.99.175.181	80/open/tcp//http/// Ignored State: closed (99)
192.168.1.9	22/open/tcp//ssh/// 53/open/tcp//domain/// 80/open/tcp//http/// 443/open/tcp//https/// 5900/open/tcp//vnc/// 8081/open/tcp//blackice-icecap/// Ignored State: closed (94)
192.168.15.1	22/open/tcp//ssh/// 80/open/tcp//http/// 7070/open/tcp//realserver/// Ignored State: closed (97)
192.168.18.1	22/open/tcp//ssh/// 80/open/tcp//http/// 7070/open/tcp//realserver/// Ignored State: closed (97)
192.168.18.53	7/open/tcp//echo/// 9/open/tcp//discard/// 13/open/tcp//daytime/// 21/open/tcp//ftp/// 22/open/tcp//ssh/// 23/open/tcp//telnet/// 25/open/tcp//smtp/// 26/open/tcp//rsftp/// 37/open/tcp//time/// 53/open/tcp//domain/// 79/open/tcp//finger/// 80/open/tcp//http/// 81/open/tcp//hosts2-ns/// 88/open/tcp//kerberos-sec/// 106/open/tcp//pop3pw/// 110/open/tcp//pop3/// 111/open/tcp//rpcbind/// 113/open/tcp//ident/// 119/open/tcp//nntp/// 135/open/tcp//msrpc/// 139/open/tcp//netbios-ssn/// 143/open/tcp//imap/// 144/open/tcp//news/// 179/open/tcp//bgp/// 199/open/tcp//smux/// 389/open/tcp//ldap///

Figure 11 Attack surface summary

The ridgeback attack surface matrix provides the protocol and application level details regarding the suspicious IP address.



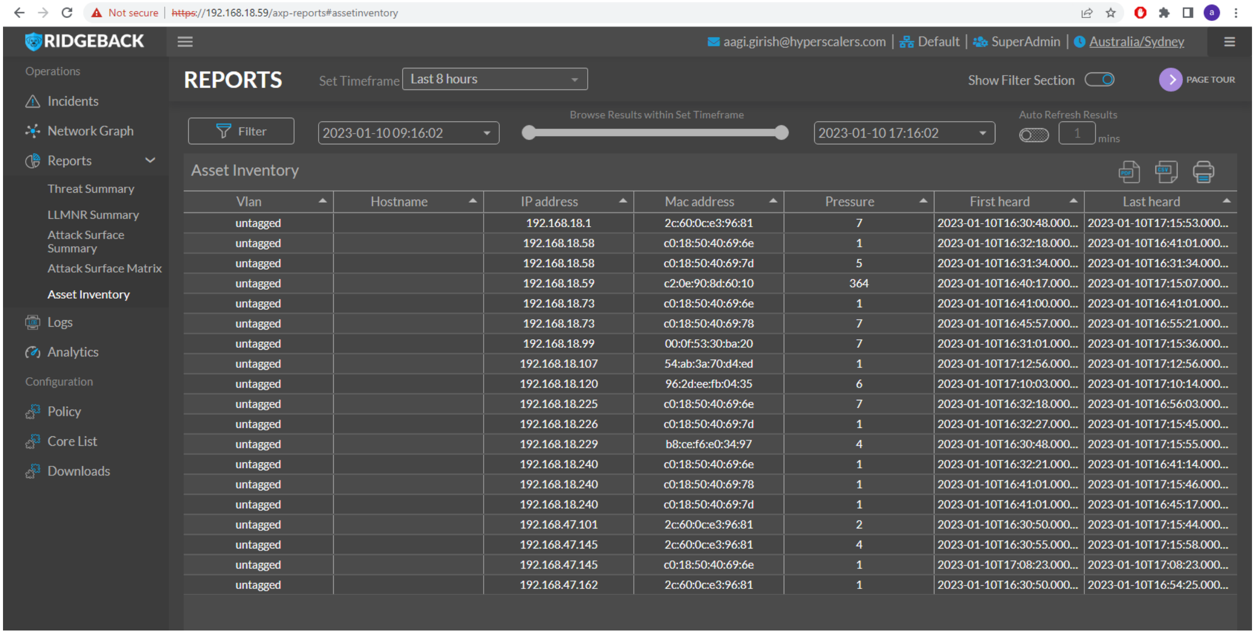
REPORTS

Attack Surface Matrix

IP address	7	9	13	21	22	23	25	26	37	53	79	80	81	88	106	110	111	113	119	135	139
192.99.175.181												http									
192.168.1.9					ssh					domain		http									
192.168.15.1					ssh							http									
192.168.18.1					ssh							http									
192.168.18.53	echo	discard	daytime	ftp	ssh	telnet	smtp	rsftp	time	domain	finger	http	hosts2-ns	kerberos-sec	pop3pw	pop3	rpcbind	ident	nntp	msrpc	netbios-
192.168.18.56					ssh												rpcbind				
192.168.18.66	echo	discard	daytime	ftp	ssh	telnet	smtp	rsftp	time	domain	finger	http	hosts2-ns	kerberos-sec	pop3pw	pop3	rpcbind	ident	nntp	msrpc	netbios-
192.168.18.70					ssh												rpcbind				
192.168.18.71	echo	discard	daytime	ftp	ssh	telnet	smtp	rsftp	time	domain	finger	http	hosts2-ns	kerberos-sec	pop3pw	pop3	rpcbind	ident	nntp	msrpc	netbios-
192.168.18.75	echo	discard	daytime	ftp	ssh	telnet	smtp	rsftp	time	domain	finger	http	hosts2-ns	kerberos-sec	pop3pw	pop3	rpcbind	ident	nntp	msrpc	netbios-
192.168.18.77					ssh																
192.168.18.83	echo	discard	daytime	ftp	ssh	telnet	smtp	rsftp	time	domain	finger	http	hosts2-ns	kerberos-sec	pop3pw	pop3	rpcbind	ident	nntp	msrpc	netbios-
192.168.18.85					ssh							http									
192.168.18.90	echo	discard	daytime	ftp	ssh	telnet	smtp	rsftp	time	domain	finger	http	hosts2-ns	kerberos-sec	pop3pw	pop3	rpcbind	ident	nntp	msrpc	netbios-
192.168.18.93	echo	discard	daytime	ftp	ssh	telnet	smtp	rsftp	time	domain	finger	http	hosts2-ns	kerberos-sec	pop3pw	pop3	rpcbind	ident	nntp	msrpc	netbios-
192.168.18.97	echo	discard	daytime	ftp	ssh	telnet	smtp	rsftp	time	domain	finger	http	hosts2-ns	kerberos-sec	pop3pw	pop3	rpcbind	ident	nntp	msrpc	netbios-
192.168.18.99					ssh							http									
192.168.18.101	echo	discard	daytime	ftp	ssh	telnet	smtp	rsftp	time	domain	finger	http	hosts2-ns	kerberos-sec	pop3pw	pop3	rpcbind	ident	nntp	msrpc	netbios-
192.168.18.103	echo	discard	daytime	ftp	ssh	telnet	smtp	rsftp	time	domain	finger	http	hosts2-ns	kerberos-sec	pop3pw	pop3	rpcbind	ident	nntp	msrpc	netbios-
192.168.18.104	echo	discard	daytime	ftp	ssh	telnet	smtp	rsftp	time	domain	finger	http	hosts2-ns	kerberos-sec	pop3pw	pop3	rpcbind	ident	nntp	msrpc	netbios-
192.168.18.105	echo	discard	daytime	ftp	ssh	telnet	smtp	rsftp	time	domain	finger	http	hosts2-ns	kerberos-sec	pop3pw	pop3	rpcbind	ident	nntp	msrpc	netbios-
192.168.18.111	echo	discard	daytime	ftp	ssh	telnet	smtp	rsftp	time	domain	finger	http	hosts2-ns	kerberos-sec	pop3pw	pop3	rpcbind	ident	nntp	msrpc	netbios-
192.168.18.113	echo	discard	daytime	ftp	ssh	telnet	smtp	rsftp	time	domain	finger	http	hosts2-ns	kerberos-sec	pop3pw	pop3	rpcbind	ident	nntp	msrpc	netbios-
192.168.18.114	echo	discard	daytime	ftp	ssh	telnet	smtp	rsftp	time	domain	finger	http	hosts2-ns	kerberos-sec	pop3pw	pop3	rpcbind	ident	nntp	msrpc	netbios-
192.168.18.115					ssh																
192.168.18.116					ssh																

Figure 12 Attack surface matrix

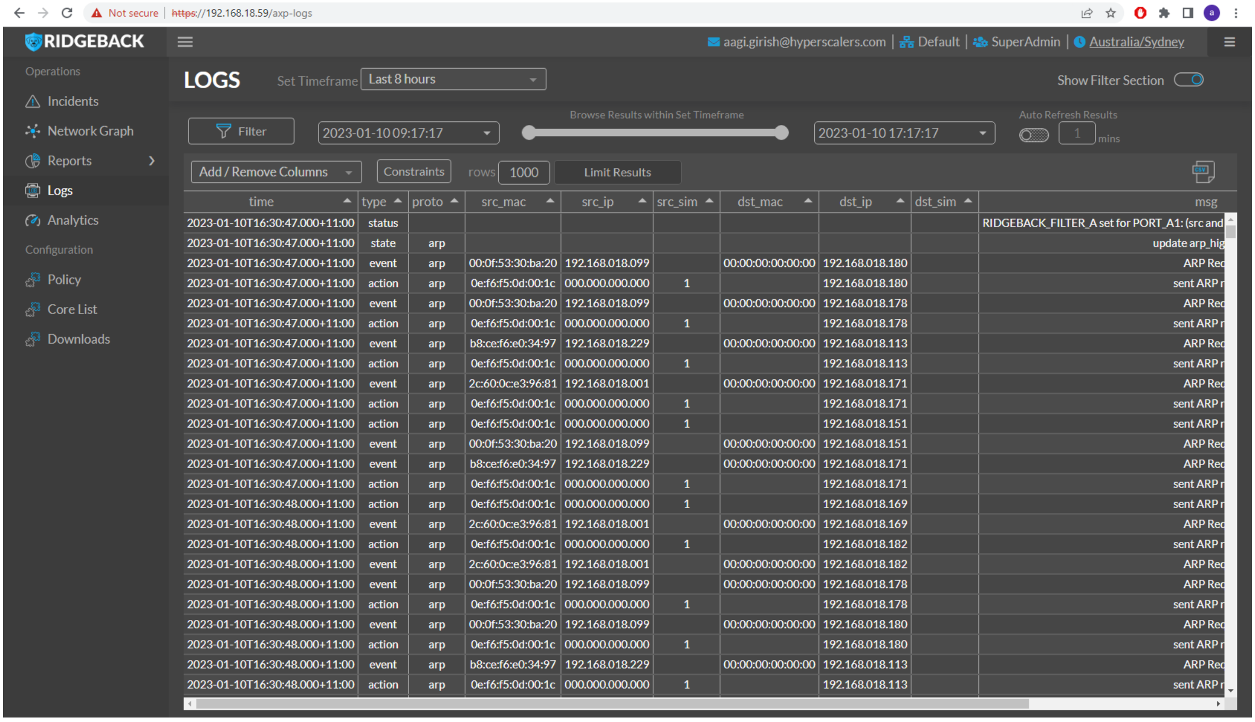
The Ridgeback asset inventory can monitor the machines in the network to ensure the normal operation in the datacentre. Any application server crash or shutdown can be identified and actioned immediately by the reporting from ridgeback.



Vlan	Hostname	IP address	Mac address	Pressure	First heard	Last heard
untagged		192.168.18.1	2c:60:0c:e3:96:81	7	2023-01-10T16:30:48.000...	2023-01-10T17:15:53.000...
untagged		192.168.18.58	c0:18:50:40:69:6e	1	2023-01-10T16:32:18.000...	2023-01-10T16:41:01.000...
untagged		192.168.18.58	c0:18:50:40:69:7d	5	2023-01-10T16:31:34.000...	2023-01-10T16:31:34.000...
untagged		192.168.18.59	c2:0e:90:8d:60:10	364	2023-01-10T16:40:17.000...	2023-01-10T17:15:07.000...
untagged		192.168.18.73	c0:18:50:40:69:6e	1	2023-01-10T16:41:00.000...	2023-01-10T16:41:01.000...
untagged		192.168.18.73	c0:18:50:40:69:78	7	2023-01-10T16:45:57.000...	2023-01-10T16:55:21.000...
untagged		192.168.18.99	00:0f:53:30:ba:20	7	2023-01-10T16:31:01.000...	2023-01-10T17:15:36.000...
untagged		192.168.18.107	54:ab:3a:70:d4:ed	1	2023-01-10T17:12:56.000...	2023-01-10T17:12:56.000...
untagged		192.168.18.120	96:2d:ee:fb:04:35	6	2023-01-10T17:10:03.000...	2023-01-10T17:10:14.000...
untagged		192.168.18.225	c0:18:50:40:69:6e	7	2023-01-10T16:32:18.000...	2023-01-10T16:56:03.000...
untagged		192.168.18.226	c0:18:50:40:69:7d	1	2023-01-10T16:32:27.000...	2023-01-10T17:15:45.000...
untagged		192.168.18.229	b8:ce:f6:e0:34:97	4	2023-01-10T16:30:48.000...	2023-01-10T17:15:55.000...
untagged		192.168.18.240	c0:18:50:40:69:6e	1	2023-01-10T16:32:21.000...	2023-01-10T16:41:14.000...
untagged		192.168.18.240	c0:18:50:40:69:78	1	2023-01-10T16:41:01.000...	2023-01-10T17:15:46.000...
untagged		192.168.18.240	c0:18:50:40:69:7d	1	2023-01-10T16:41:01.000...	2023-01-10T16:45:17.000...
untagged		192.168.47.101	2c:60:0c:e3:96:81	2	2023-01-10T16:30:50.000...	2023-01-10T17:15:44.000...
untagged		192.168.47.145	2c:60:0c:e3:96:81	4	2023-01-10T16:30:55.000...	2023-01-10T17:15:58.000...
untagged		192.168.47.145	c0:18:50:40:69:6e	1	2023-01-10T17:08:23.000...	2023-01-10T17:08:23.000...
untagged		192.168.47.162	2c:60:0c:e3:96:81	1	2023-01-10T16:30:50.000...	2023-01-10T16:54:25.000...

Figure 13 Asset Inventory

All the activities in the network are logged with their corresponding timestamp and MAC address to identify the machine location and determining the way a hacker could compromise the network.

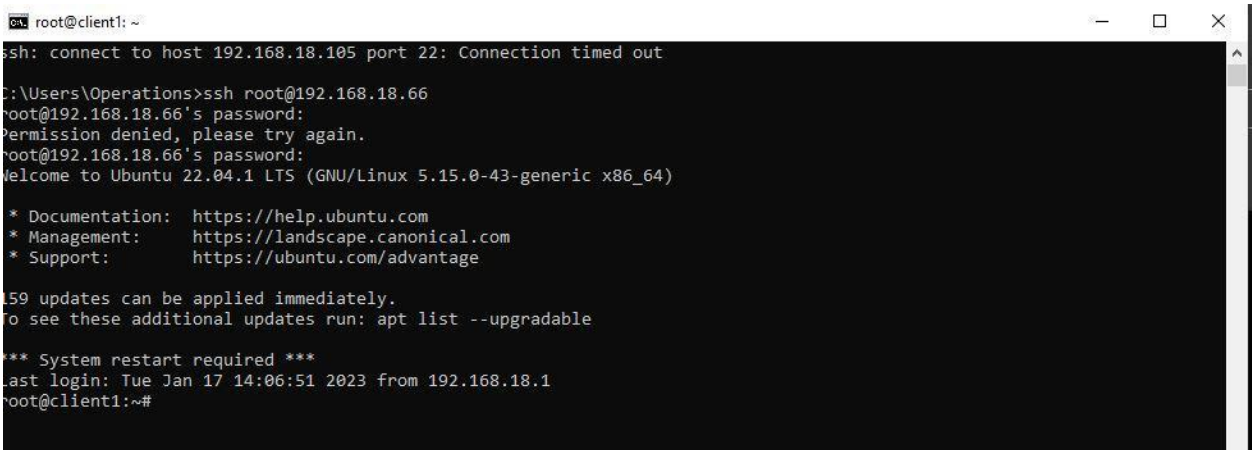


time	type	proto	src_mac	src_ip	src_sim	dst_mac	dst_ip	dst_sim	msg
2023-01-10T16:30:47.000+11:00	status								RIDGEBACK_FILTER_A set for PORT_A1: (src and
2023-01-10T16:30:47.000+11:00	state	arp							update arp_hig
2023-01-10T16:30:47.000+11:00	event	arp	00:0f:53:30:ba:20	192.168.018.099		00:00:00:00:00:00	192.168.018.180		ARP Rec
2023-01-10T16:30:47.000+11:00	action	arp	0e:f6:f5:0d:00:1c	000.000.000.000	1		192.168.018.180		sent ARP r
2023-01-10T16:30:47.000+11:00	event	arp	00:0f:53:30:ba:20	192.168.018.099		00:00:00:00:00:00	192.168.018.178		ARP Rec
2023-01-10T16:30:47.000+11:00	action	arp	0e:f6:f5:0d:00:1c	000.000.000.000	1		192.168.018.178		sent ARP r
2023-01-10T16:30:47.000+11:00	event	arp	b8:ce:f6:e0:34:97	192.168.018.229		00:00:00:00:00:00	192.168.018.113		ARP Rec
2023-01-10T16:30:47.000+11:00	action	arp	0e:f6:f5:0d:00:1c	000.000.000.000	1		192.168.018.113		sent ARP r
2023-01-10T16:30:47.000+11:00	event	arp	2c:60:0c:e3:96:81	192.168.018.001		00:00:00:00:00:00	192.168.018.171		ARP Rec
2023-01-10T16:30:47.000+11:00	action	arp	0e:f6:f5:0d:00:1c	000.000.000.000	1		192.168.018.171		sent ARP r
2023-01-10T16:30:47.000+11:00	action	arp	0e:f6:f5:0d:00:1c	000.000.000.000	1		192.168.018.151		sent ARP r
2023-01-10T16:30:47.000+11:00	event	arp	00:0f:53:30:ba:20	192.168.018.099		00:00:00:00:00:00	192.168.018.151		ARP Rec
2023-01-10T16:30:47.000+11:00	event	arp	b8:ce:f6:e0:34:97	192.168.018.229		00:00:00:00:00:00	192.168.018.171		ARP Rec
2023-01-10T16:30:47.000+11:00	action	arp	0e:f6:f5:0d:00:1c	000.000.000.000	1		192.168.018.171		sent ARP r
2023-01-10T16:30:48.000+11:00	action	arp	0e:f6:f5:0d:00:1c	000.000.000.000	1		192.168.018.169		sent ARP r
2023-01-10T16:30:48.000+11:00	event	arp	2c:60:0c:e3:96:81	192.168.018.001		00:00:00:00:00:00	192.168.018.169		ARP Rec
2023-01-10T16:30:48.000+11:00	action	arp	0e:f6:f5:0d:00:1c	000.000.000.000	1		192.168.018.182		sent ARP r
2023-01-10T16:30:48.000+11:00	event	arp	2c:60:0c:e3:96:81	192.168.018.001		00:00:00:00:00:00	192.168.018.182		ARP Rec
2023-01-10T16:30:48.000+11:00	event	arp	00:0f:53:30:ba:20	192.168.018.099		00:00:00:00:00:00	192.168.018.178		ARP Rec
2023-01-10T16:30:48.000+11:00	action	arp	0e:f6:f5:0d:00:1c	000.000.000.000	1		192.168.018.178		sent ARP r
2023-01-10T16:30:48.000+11:00	event	arp	00:0f:53:30:ba:20	192.168.018.099		00:00:00:00:00:00	192.168.018.180		ARP Rec
2023-01-10T16:30:48.000+11:00	action	arp	0e:f6:f5:0d:00:1c	000.000.000.000	1		192.168.018.180		sent ARP r
2023-01-10T16:30:48.000+11:00	event	arp	b8:ce:f6:e0:34:97	192.168.018.229		00:00:00:00:00:00	192.168.018.113		ARP Rec
2023-01-10T16:30:48.000+11:00	action	arp	0e:f6:f5:0d:00:1c	000.000.000.000	1		192.168.018.113		sent ARP r

Figure 14 Ridgeback protection logs

4 Testing the Appliance

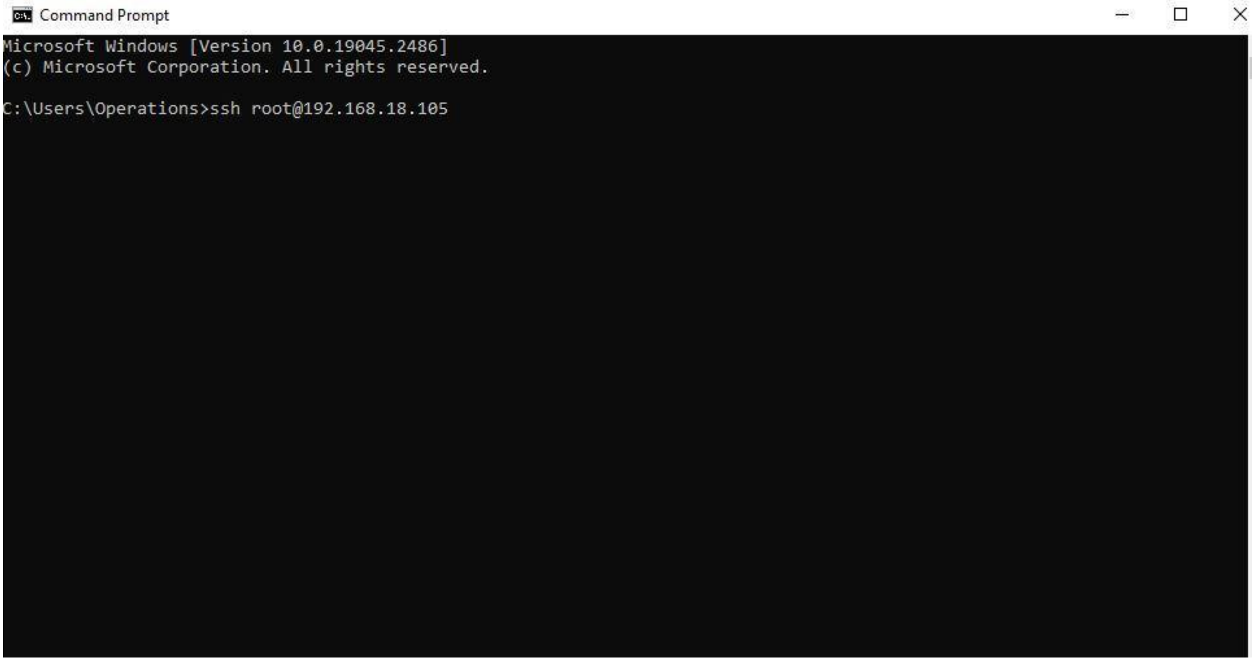
To test the appliance that we have deployed using the above steps can be tested by simulating a kind of Nmap network scan or ssh over list of unknown IPs.



```
ssh: connect to host 192.168.18.105 port 22: Connection timed out

:\Users\Operations>ssh root@192.168.18.66
root@192.168.18.66's password:
Permission denied, please try again.
root@192.168.18.66's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-43-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

159 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

*** System restart required ***
Last login: Tue Jan 17 14:06:51 2023 from 192.168.18.1
root@client1:~#
```

Figure 15 Logging into the system

Here we can see user logging into a known Ip address using SSH and password can get access into the whole system.



```
Microsoft Windows [Version 10.0.19045.2486]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Operations>ssh root@192.168.18.105
```

Figure 16 First random ping with the unknown Ip address

After logging into the system with the known IP address, then they try to access the other devices connected to the same network. In this above figure, it can do be done with individual IP address Or Nmap scan which is done in next steps.

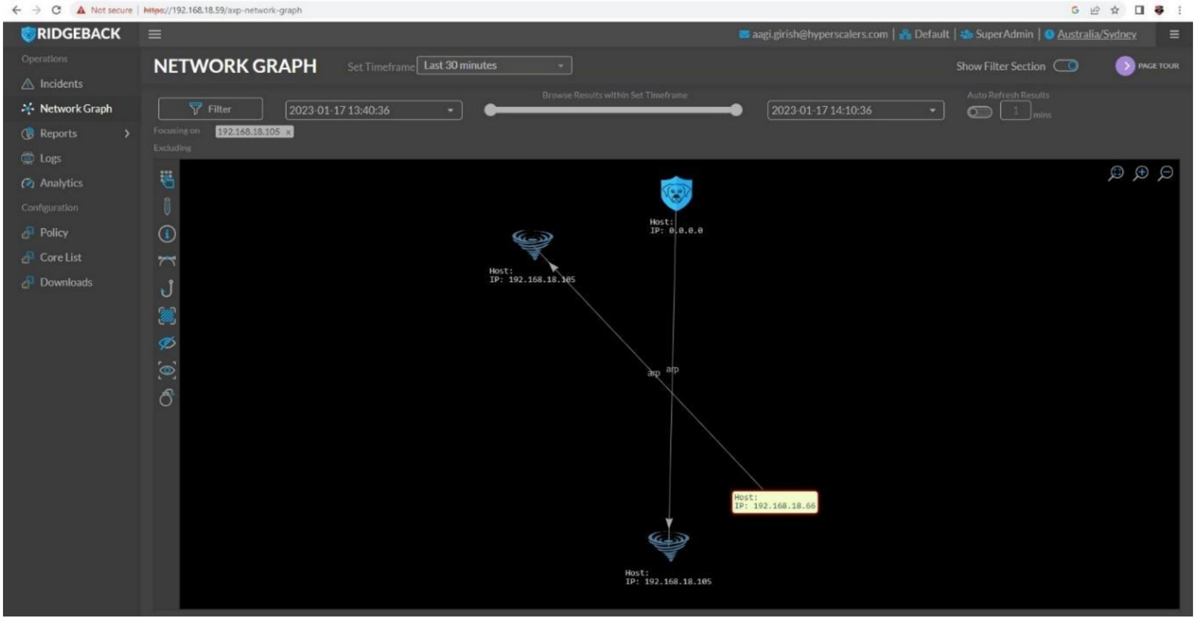
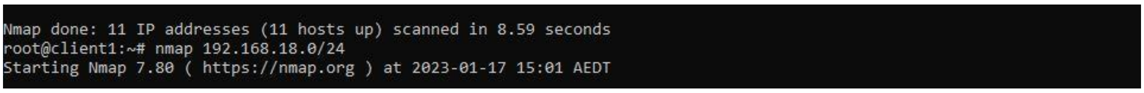


Figure 17 Ridgeback Network graph showing the IP address

We can now saw the unknown IP address in the ridgeback Network Graph keeping in a phantom and ready for TCP communication but leave on the phantom.



```
Nmap done: 11 IP addresses (11 hosts up) scanned in 8.59 seconds
root@client1:~# nmap 192.168.18.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-01-17 15:01 AEDT
```

Figure 18 Nmap scan

Here we have done the Nmap scan for large number IPs in a short period which helps to scan accordingly.

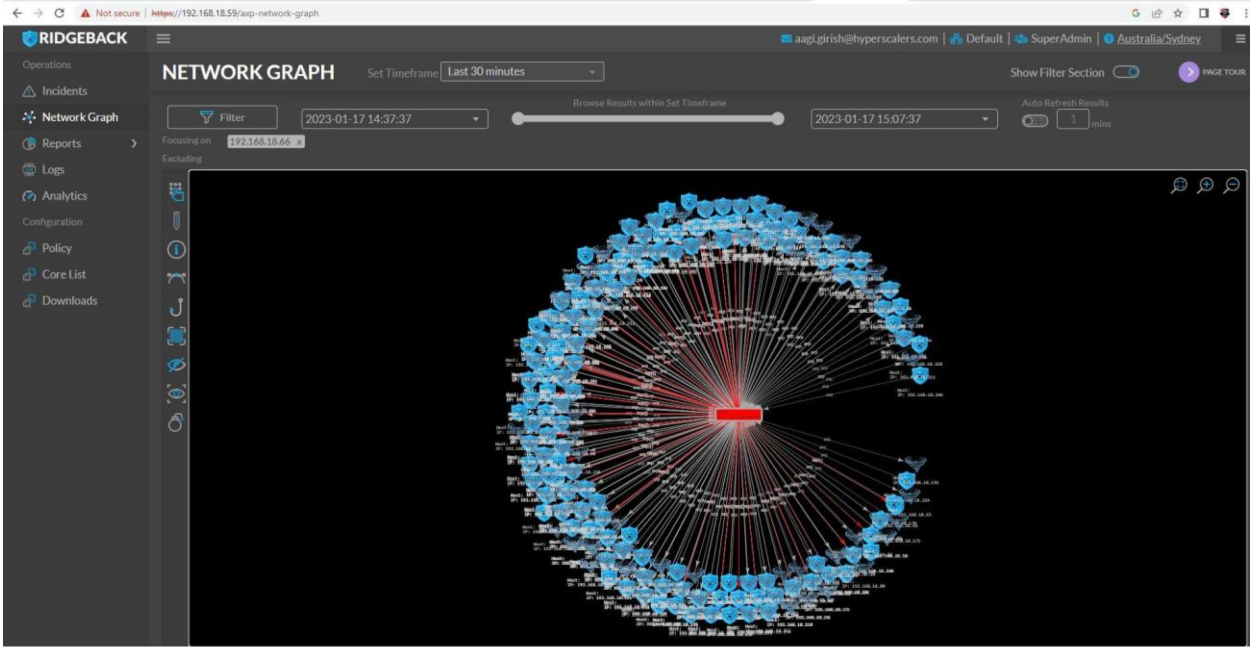
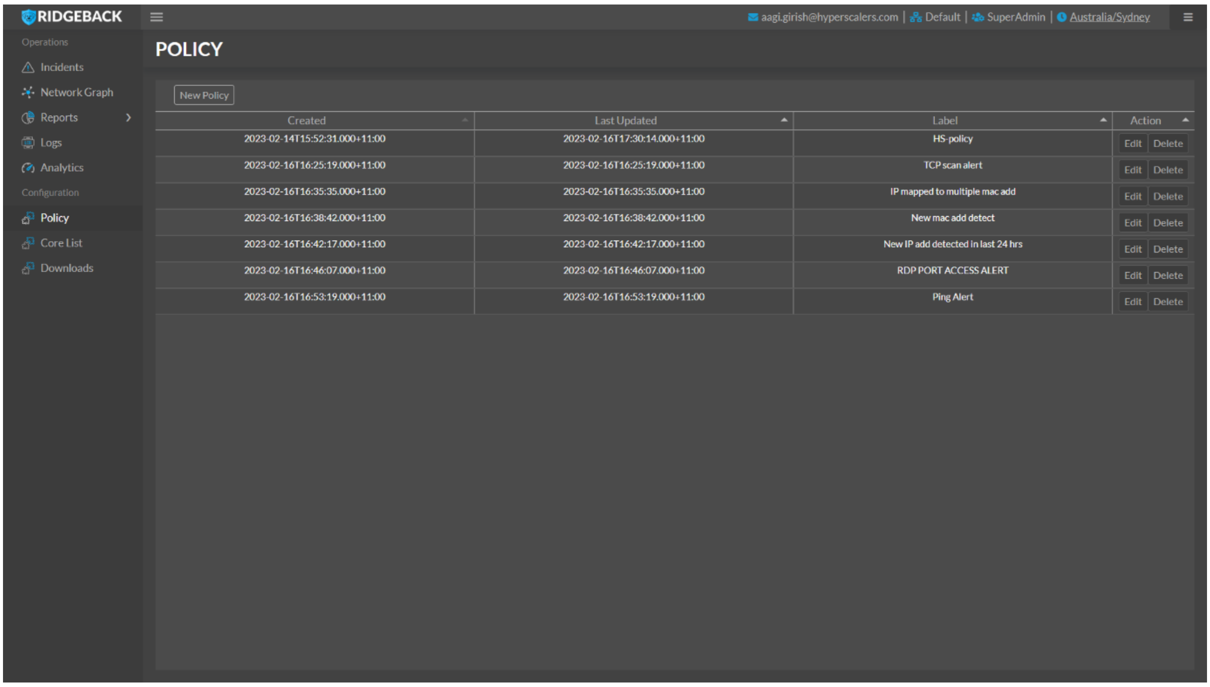


Figure 19 Ridgeback Network graph showing pinned Nmap IP address

Policy

Below given picture shows about the policy that we have assigned to Ridgeback Network Defences. The Policy that we have assigned are listed below:

- HS-policy
- TCP Scan alert
- IP mapped to multiple Mac addresses.
- New mac address detection
- New IP detected in last 24 hours.
- RDP port access alert
- Ping alert



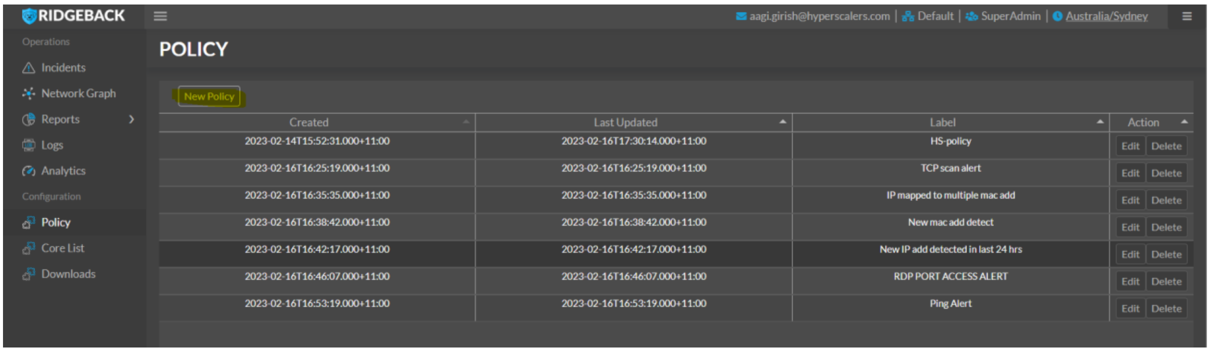
POLICY

Created	Last Updated	Label	Action
2023-02-14T15:52:31.000+11:00	2023-02-16T17:30:14.000+11:00	HS-policy	Edit Delete
2023-02-16T16:25:19.000+11:00	2023-02-16T16:25:19.000+11:00	TCP scan alert	Edit Delete
2023-02-16T16:35:35.000+11:00	2023-02-16T16:35:35.000+11:00	IP mapped to multiple mac add	Edit Delete
2023-02-16T16:38:42.000+11:00	2023-02-16T16:38:42.000+11:00	New mac add detect	Edit Delete
2023-02-16T16:42:17.000+11:00	2023-02-16T16:42:17.000+11:00	New IP add detected in last 24 hrs	Edit Delete
2023-02-16T16:46:07.000+11:00	2023-02-16T16:46:07.000+11:00	RDP PORT ACCESS ALERT	Edit Delete
2023-02-16T16:53:19.000+11:00	2023-02-16T16:53:19.000+11:00	Ping Alert	Edit Delete

Figure 20 Ridgeback Network Defences Policy

Creating New Policy

To create a new policy for Ridgeback Network Defences, go to the policy and click on new policy and follow the steps.



POLICY

Created	Last Updated	Label	Action
2023-02-14T15:52:31.000+11:00	2023-02-16T17:30:14.000+11:00	HS-policy	Edit Delete
2023-02-16T16:25:19.000+11:00	2023-02-16T16:25:19.000+11:00	TCP scan alert	Edit Delete
2023-02-16T16:35:35.000+11:00	2023-02-16T16:35:35.000+11:00	IP mapped to multiple mac add	Edit Delete
2023-02-16T16:38:42.000+11:00	2023-02-16T16:38:42.000+11:00	New mac add detect	Edit Delete
2023-02-16T16:42:17.000+11:00	2023-02-16T16:42:17.000+11:00	New IP add detected in last 24 hrs	Edit Delete
2023-02-16T16:46:07.000+11:00	2023-02-16T16:46:07.000+11:00	RDP PORT ACCESS ALERT	Edit Delete
2023-02-16T16:53:19.000+11:00	2023-02-16T16:53:19.000+11:00	Ping Alert	Edit Delete

Figure 21 Creating New Policy

First, we need to add Time Windows

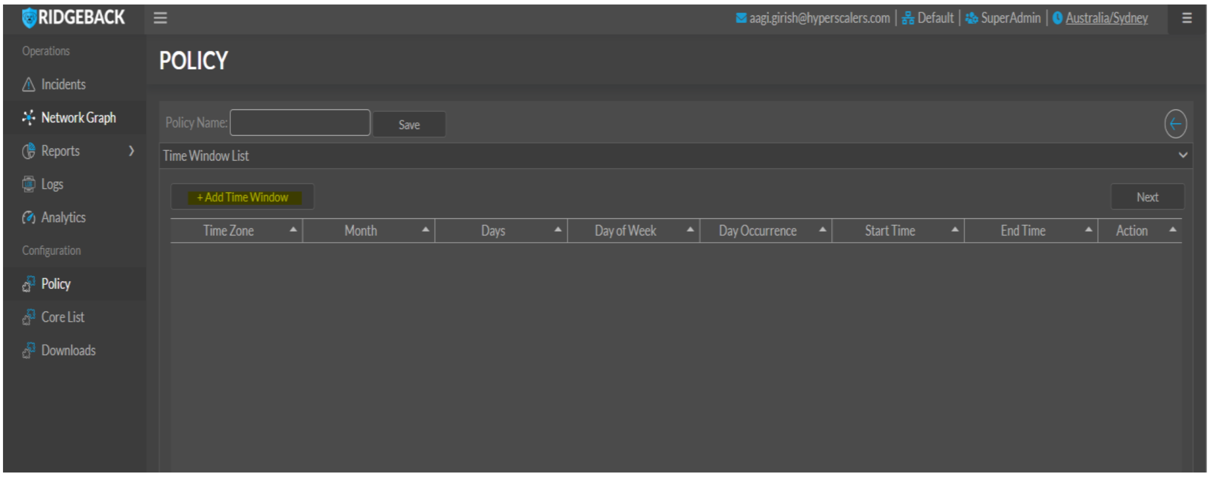
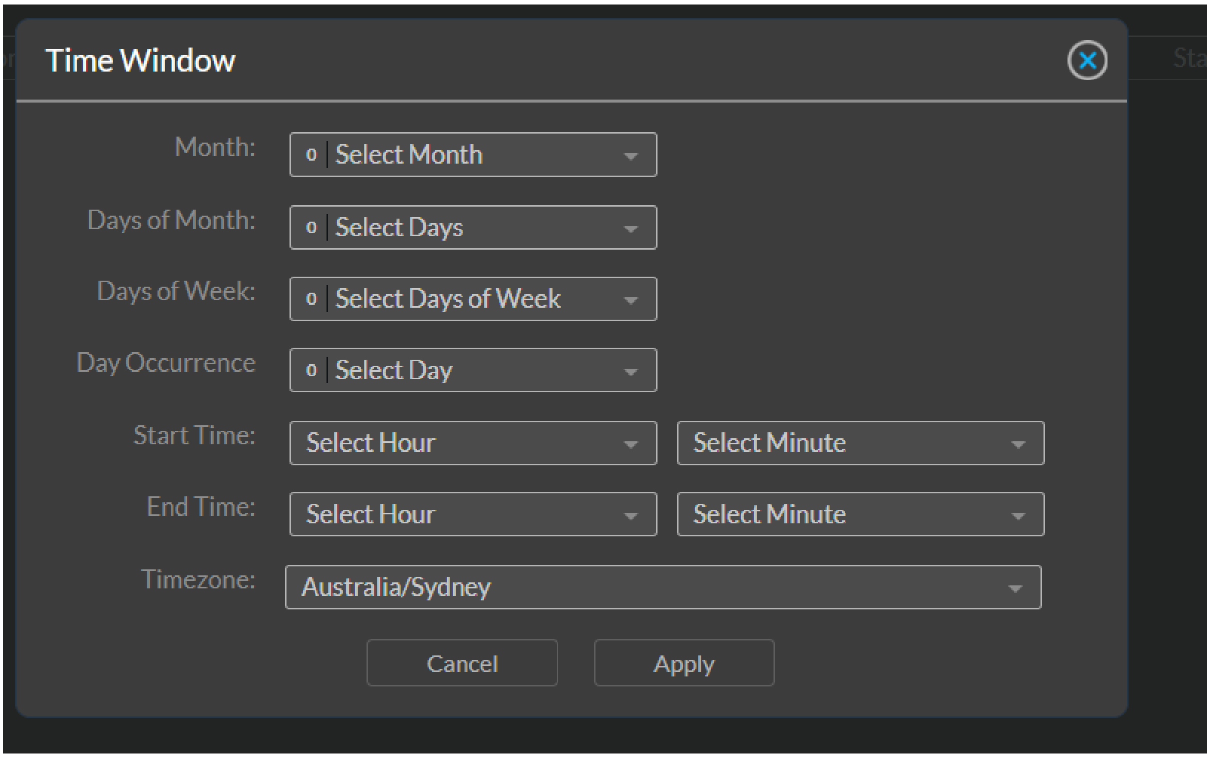


Figure 22 Add Time Window (1)



Time Window

Month: 0 Select Month

Days of Month: 0 Select Days

Days of Week: 0 Select Days of Week

Day Occurrence 0 Select Day

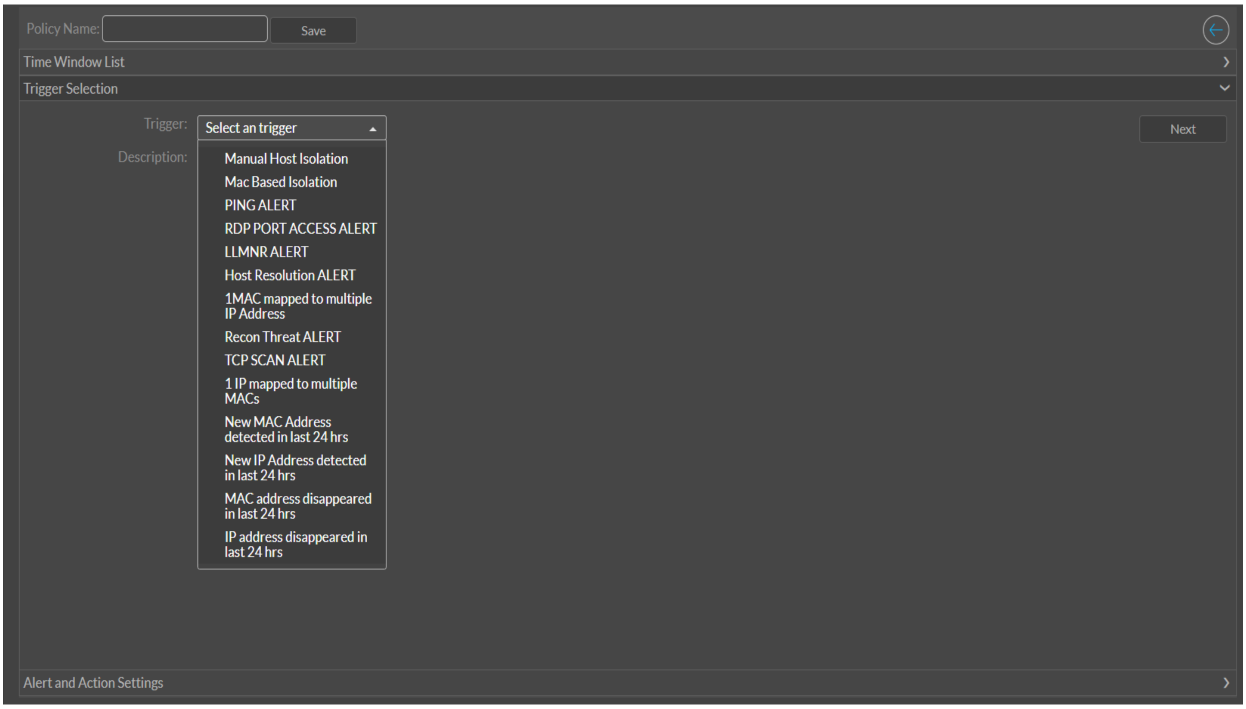
Start Time: Select Hour Select Minute

End Time: Select Hour Select Minute

Timezone: Australia/Sydney

Figure 23 Add Time Window (2)

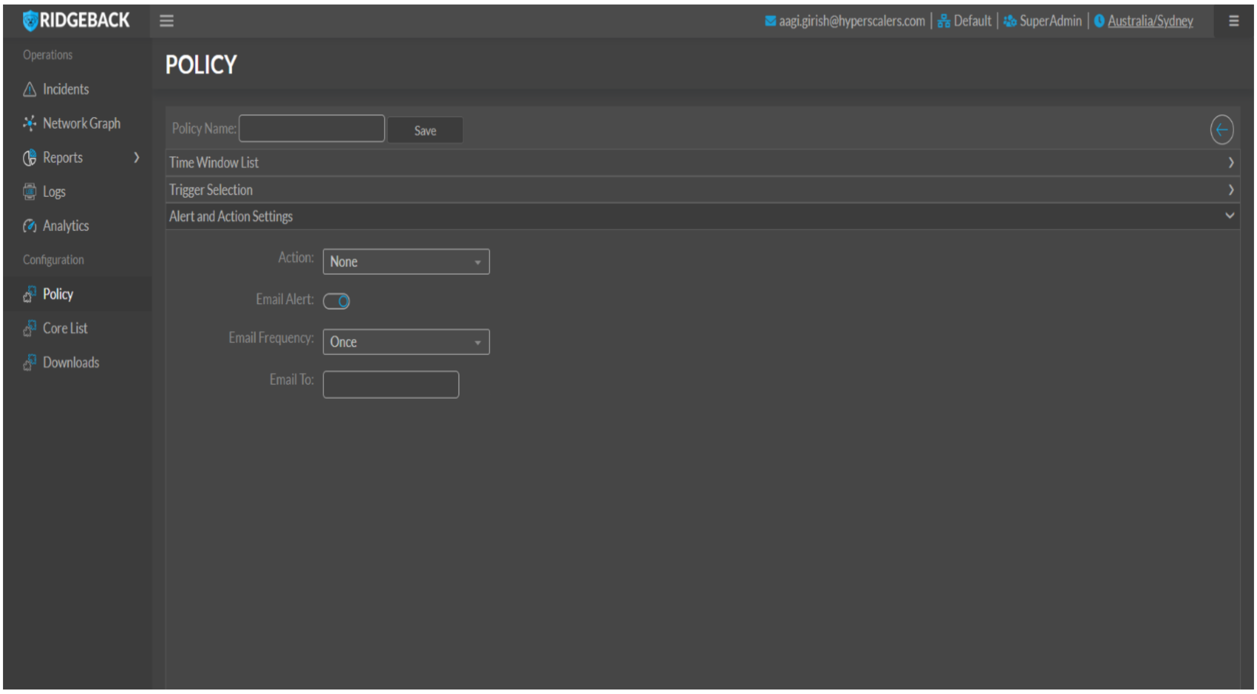
Second, we need to Trigger Selection



Policy Name:
Save
Time Window List
Trigger Selection
Trigger:
Select an trigger
Description:
Manual Host Isolation
Mac Based Isolation
PING ALERT
RDP PORT ACCESS ALERT
LLMNR ALERT
Host Resolution ALERT
1MAC mapped to multiple IP Address
Recon Threat ALERT
TCP SCAN ALERT
1 IP mapped to multiple MACs
New MAC Address detected in last 24 hrs
New IP Address detected in last 24 hrs
MAC address disappeared in last 24 hrs
IP address disappeared in last 24 hrs
Next
Alert and Action Settings

Figure 24 Trigger Selection

Third we need to add alert and action settings.



Action: None

Email Alert:

Email Frequency: Once

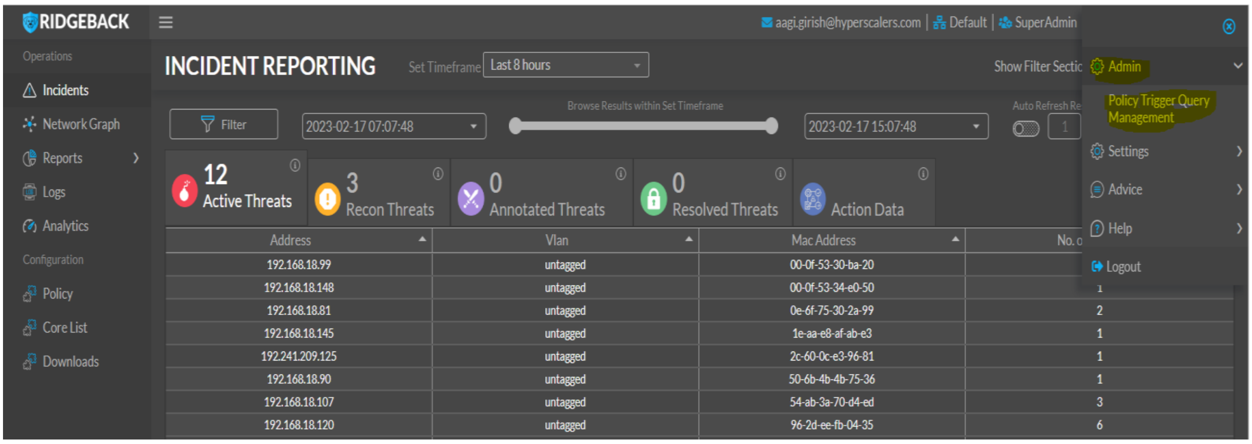
Email To:

Figure 25 Alert and Action Settings

Policy Trigger Query Management

In Policy Trigger Query Management, we can create our own trigger query for that we need to have knowledge of SQL. To create Policy Trigger Query, follow the below steps.

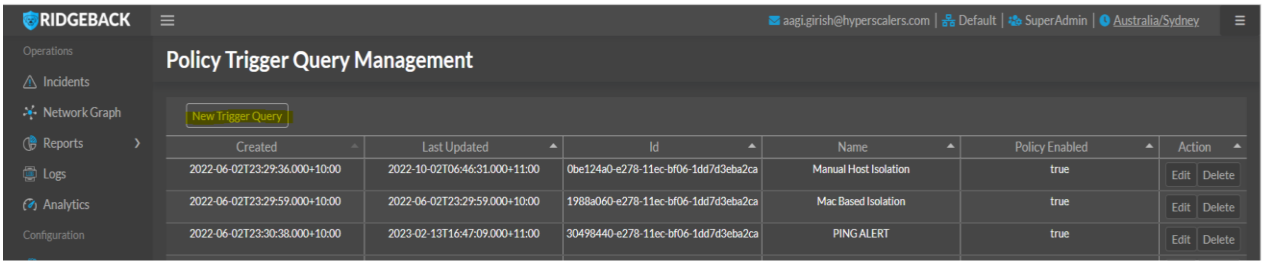
- Go to admin and choose policy trigger query management.



Address	Vlan	Mac Address	No. o
192.168.18.99	untagged	00-0f-53-30-ba-20	
192.168.18.148	untagged	00-0f-53-34-e0-50	1
192.168.18.81	untagged	0e-6f-75-30-2a-99	2
192.168.18.145	untagged	1e-aa-e8-af-ab-e3	1
192.241.209.125	untagged	2c-60-0c-e3-96-81	1
192.168.18.90	untagged	50-6b-4b-4b-75-36	1
192.168.18.107	untagged	54-ab-3a-70-d4-ed	3
192.168.18.120	untagged	96-2d-ee-fb-04-35	6

Figure 26 Policy Trigger Query Management

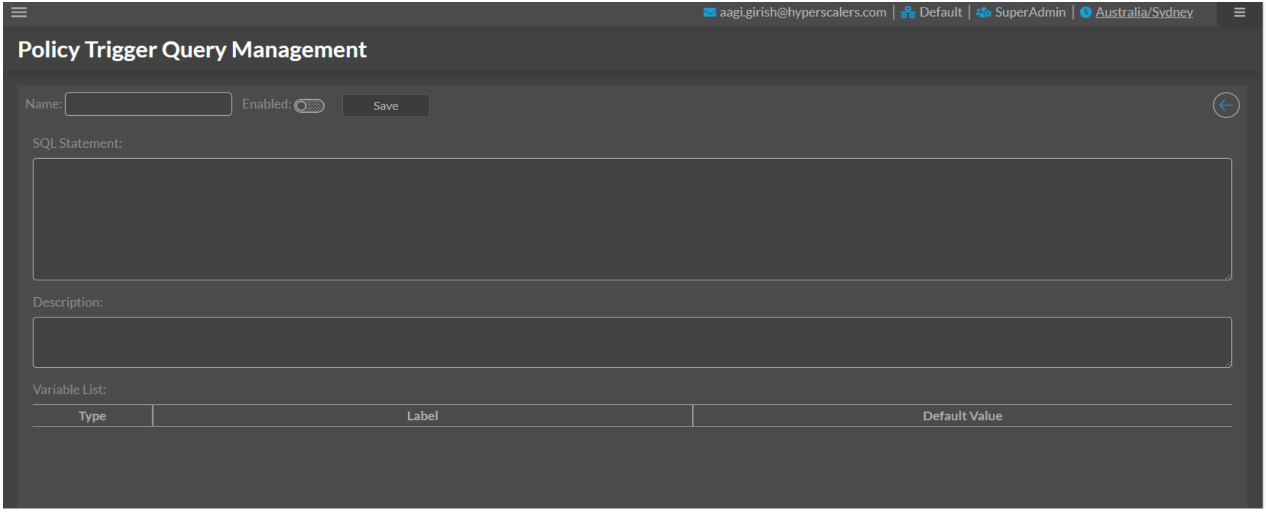
- Click on policy trigger query management and again click on New Trigger Query


RIDGEBACK
aagi.girish@hyperscalers.com | Default | SuperAdmin | Australia/Sydney
Operations
Incidents
Network Graph
Reports
Logs
Analytics
Configuration
Policy Trigger Query Management
New Trigger Query

Created	Last Updated	Id	Name	Policy Enabled	Action
2022-06-02T23:29:36.000+10:00	2022-10-02T06:46:31.000+11:00	0be124a0-e278-11ec-bf06-1dd7d3eba2ca	Manual Host Isolation	true	Edit Delete
2022-06-02T23:29:59.000+10:00	2022-06-02T23:29:59.000+10:00	1988a060-e278-11ec-bf06-1dd7d3eba2ca	Mac Based Isolation	true	Edit Delete
2022-06-02T23:30:38.000+10:00	2023-02-13T16:47:09.000+11:00	30498440-e278-11ec-bf06-1dd7d3eba2ca	PING ALERT	true	Edit Delete

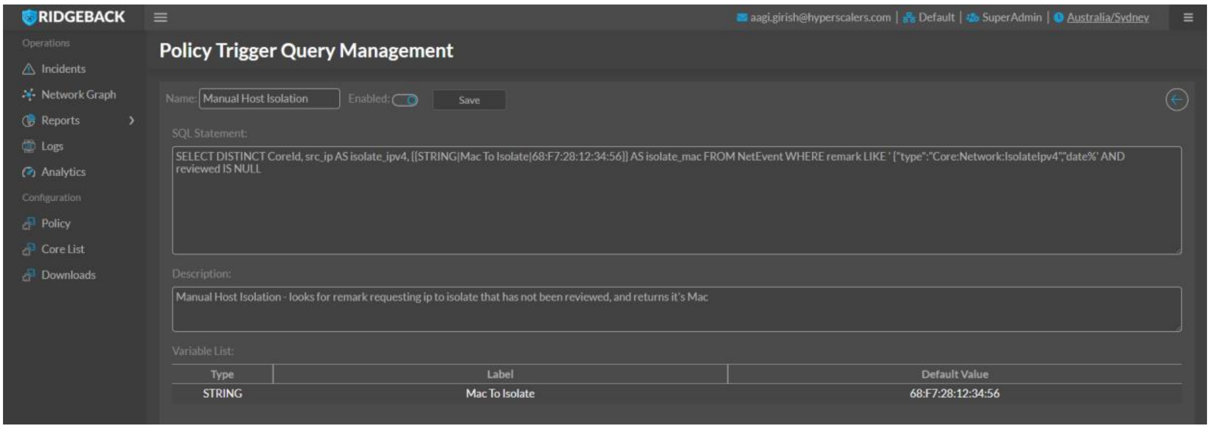
Figure 27 New Trigger Query

- In this page, we can create our own Trigger Query using SQL statements.


aagi.girish@hyperscalers.com | Default | SuperAdmin | Australia/Sydney
Policy Trigger Query Management
Name:
Enabled:
Save
SQL Statement:
Description:
Variable List:

Type	Label	Default Value

Figure 28 Create Policy Trigger Query Management (1)



Policy Trigger Query Management

Name: Manual Host Isolation Enabled:

SQL Statement:

```
SELECT DISTINCT CoreId, src_ip AS isolate_ipv4, {{STRING|Mac To Isolate|68:F7:28:12:34:56}} AS isolate_mac FROM NetEvent WHERE remark LIKE ' {"type":"Core:Network:IsolateIpv4","date%' AND
reviewed IS NULL
```

Description:

Manual Host Isolation - looks for remark requesting ip to isolate that has not been reviewed, and returns it's Mac

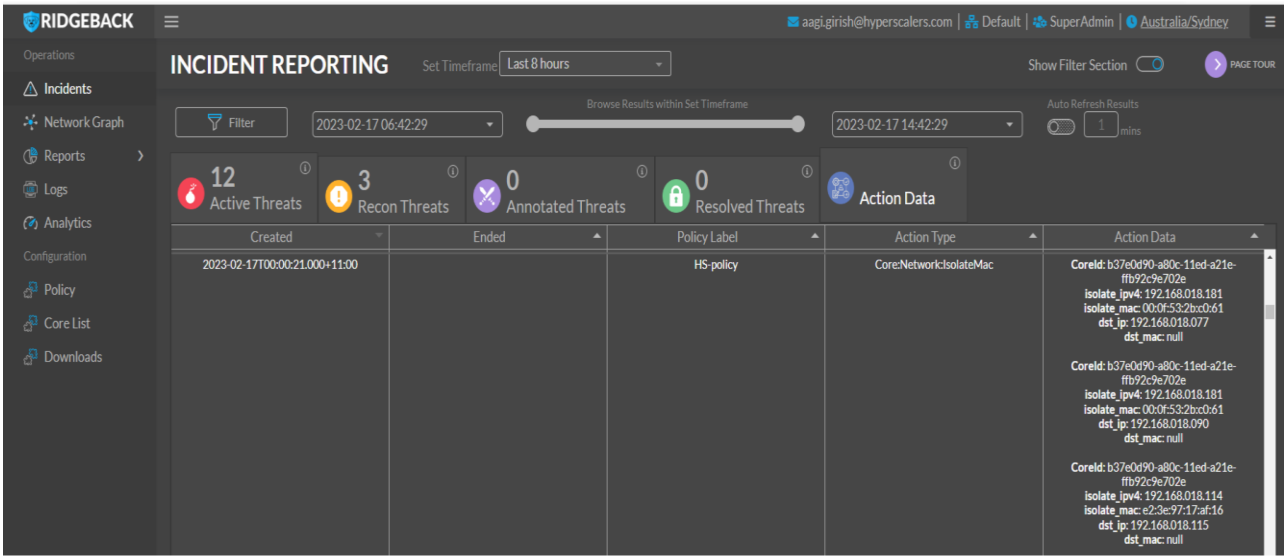
Variable List:

Type	Label	Default Value
STRING	Mac To Isolate	68:F7:28:12:34:56

Figure 29 SQL Statement Policy Trigger Query Management (2)

HS-Policy

Under HS-Policy we have applied Recon threat alert policy which looks for ARP threats, even that don't have TCP or ICMP threats. Below given picture shows the list of isolated Mac address that Ridgeback Network defences picked up inside the network. When Isolate Mac action alert setting is activated it will isolate all the Mac address and IP address within network and send alert in email when the policy is activated.



INCIDENT REPORTING

Set Timeframe: Last 8 hours

2023-02-17 06:42:29 — 2023-02-17 14:42:29

Auto Refresh Results: 1 mins

12 Active Threats | 3 Recon Threats | 0 Annotated Threats | 0 Resolved Threats | Action Data

Created	Ended	Policy Label	Action Type	Action Data
2023-02-17T00:00:21.000+11:00		HS-policy	Core:Network:IsolateMac	**CoreId:** b37e0d90-a80c-11ed-a21e-ffb92c9e702e **isolate_ipv4:** 192.168.018.181 **isolate_mac:** 00:0f:53:2b:c0:61 **dst_ip:** 192.168.018.077 **dst_mac:** null **CoreId:** b37e0d90-a80c-11ed-a21e-ffb92c9e702e **isolate_ipv4:** 192.168.018.181 **isolate_mac:** 00:0f:53:2b:c0:61 **dst_ip:** 192.168.018.090 **dst_mac:** null **CoreId:** b37e0d90-a80c-11ed-a21e-ffb92c9e702e **isolate_ipv4:** 192.168.018.114 **isolate_mac:** e2:3e:97:17:af:16 **dst_ip:** 192.168.018.115 **dst_mac:** null

Figure 26 HS-Policy

5 ADDENDUM

```
###############################################
#
# RIDGEBACK CORE CONFIGURATION
# Support email: support@ridgebacknet.com
#
###############################################

# Remote server address
RC_SERVER=192.168.18.59
# Remote server port
RC_PORT=19444
# Remote server key
RC_KEY=11223344556677
# Organization identifier (UUID)
RC_ORGID=00000000-0000-0000-0000-000000000000
# Core identifier (UUID)
RC_COREID=f23cd800-66de-11ed-99ba-ab01031b8332

###################################
# PORT_A1
# Set this option to be the ethernet port for your endpoint.
# Examples:
# PORT_A1=eth0
# PORT_A1=en0
PORT_A1=rpcap://\Device\NPF_{3D03C7E0-990B-40FA-82AB-05BFE0B2AEAC}
# PORT_A1={{NETWORK_ADAPTER}}

###################################
# BOGUS_MAC_ADDR
# Ridgeback Hunter on wireless requires a bogus MAC address.
# Ridgeback Hunter on wired normally does not require a bogus MAC.
# Ridgeback Hunter on a wired with network access control requires a MAC.
# Set this option to your endpoint's MAC address, if MAC is needed.
# Multiple MAC addresses are supported by using multiple key=value lines.
# Example:
# BOGUS_MAC_ADDR=ff:ff:ff:ff:ff:ff
# BOGUS_MAC_ADDR=ff:ff:ff:ff:ff:ff
BOGUS_MAC_ADDR=0E-6F-75-30-2A-99

##################################
# LIVE
# Have Ridgeback assume, at startup, that one or more addresses are
# live endpoints.
# LIVE=192.168.1.1
# LIVE=192.168.1.2
# etc.

##################################
# DECOY_BLACKLIST
# Ridgeback will not deploy decoys on the listed IP addresses.
# DECOY_BLACKLIST=192.168.1.1
# DECOY_BLACKLIST=192.168.1.2
# etc.
# DECOY_BLACKLIST=127.0.0.1
DECOY_BLACKLIST=192.168.18.81

##################################
# ADMIN
# Ridgeback will refuse to inspect traffic from or to the listed IP addresses.
ADMIN=192.168.18.1
ADMIN=192.168.18.59
ADMIN=192.168.18.124
ADMIN=0.0.0.0
ADMIN=192.168.18.99
ADMIN=192.168.18.105
ADMIN=192.168.18.56
ADMIN=192.168.18.102
```

```
ADMIN=192.168.18.225
ADMIN=192.168.18.73
ADMIN=192.168.18.57
ADMIN=192.168.18.226
ADMIN=192.168.18.240
# etc.
# ADMIN=127.0.0.1
ADMIN=192.168.18.81

##################################
# If Ridgeback Hunter is being run on a single interface system (which
# is not recommended), then foreign (non-local) traffic can bleed in and
# fill the segment table. To prevent foreign traffic from bleeding into
# the segment table is to use an explicit FILTER_A configuration.
# Include 224.0.0.252 if you wish to support LLMNR.
# Examples:
# FILTER_A=(src and dst net 192.168) or (src or dst 224.0.0.252)
# FILTER_A=(not src host 192.168.0.10)
# FILTER_A=(not src host 127.0.0.1)
FILTER_A=(src and dst net 192.0.0.0/8) or (src or dst 224.0.0.252)

##################################
# LICENSE
# Licensing is now handled by server components.

##################################
# LOCAL LOGGING
# If RC_SERVER is not set, the core will log here:
# /var/opt/ridgeback/ridgeback.log

###############################################################
# DANGER - DANGER - DANGER
###############################################################
# Do not modify the options below without
# guidance from Ridgeback developers.
#
# Reporting options
# By default, status files are not written.
SUBNET_REPORT_DELAY=0
TABLES_REPORT_DELAY=0
INTEREST_REPORT_DELAY=0
#
# Out-of-the-box, Ridgeback will aggressively deploy decoys.
# For some DHCP networks, you may want to set ARP_HIGH_PRESSURE to
# a value 2 or greater.
ARP_HIGH_PRESSURE=3
#
# Do not set ARP_LIVE_HIGH_PRESSURE without consulting both Ridgeback
# support and a network engineer who monitors your network.
# ARP_LIVE_HIGH_PRESSURE=
#
# Display ARP information
ARP_INFO=1
# Default Plugins
PLUGIN_ARP_RESPONDER=1
PLUGIN_ICMP_RESPONDER=1
PLUGIN_TCP_RESPONDER=1
PLUGIN_UDP_RESPONDER=1
```

2 Copyright and Licensing

6 REFERENCES

1. Ridgeback Network Defense, I. (no date) *Ridgeback - 2023 reviews, pricing, features, Ridgeback - 2023 Reviews, Pricing, Features*. Available at: https://www3.technologyevaluation.com/solutions/54883/ridgeback (Accessed: January 30, 2023).

2. *Solving it's complexity* (no date) *Solving IT's Complexity*. Available at: https://www.hyperscalers.com/ (Accessed: January 30, 2023).

3. *We stop lateral movement* (no date) *Ridgeback Network Defense*. Available at: https://www.ridgebacknet.com/ (Accessed: January 30, 2023).