RidgeBot Telecom Use Case

Business Needs

A major cybersecurity challenge faced by telecommunications providers is a rapidly growing threat surface area that is driven by the expansion of very large, interconnected networks. In this use case, we'll focus on a large global telecommunications provider that services businesses and consumers in the Asia-Pacific region with mobile, fixed line, broadband internet services, high-quality video, and Over-The-Top applications.

To deliver their services with an optimal customer experience, the telecom provider relies heavily on web applications, servers, and highspeed internet connections. To support its large and diverse customers, the provider has developed and deployed thousands of web applications and servers to support mobile and wired devices.

The telecom provider is very aware that telecommunications providers are primary targets for cyberattacks and that they must ensure that their web applications and servers are adequately protected. Additionally, compliance requirements for telecommunications providers mandate that providers conduct regular cybersecurity risk assessments and reviews. Often this requires penetration testing to be performed on all new applications and components prior to becoming operational, and regularly while operational.

Because of the importance of penetration testing, the telecom provider sought a solution to pentest its vast array of web applications and servers. The provider's main goal was for a solution that was cost effective and didn't need additional resources. They also wanted a penetration testing solution that is automated and requires little human intervention. Lastly, the solution must be able to support both development and operational environments and can be scheduled in as needed.

The telecom provider selected RidgeBot from Ridge Security, to deliver penetration testing to these essential use cases:

1. To perform penetration testing on its web servers and other internal production servers and devices on a regular basis to achieve complete coverage of the provider's infrastructure.
2. To perform web application penetration testing on a regular basis.
3. To use RidgeBot to scan the subnet for "unauthorized" server.
4. To use RidgeBot to scan for weak passwords on the servers.
5. To use RidgeBot to look for Ransomware vulnerabilities.
6. To use RidgeBot as the ethical red team with their security monitor tool to validate certain suspicious activities.
7. To use RidgeBot's automated reporting to meet compliance requirements.
8. To use RidgeBot to reduce the need for other security tools

How RidgeBot was deployed and is used

RidgeBot was installed in the Telecom Provider's development test beds and used to penetration test new application during their DevSecOps processes. Jira tickets are generated to record any follow-on remediation and corrective actions needed to resolve verified security gaps.

For penetration testing of production servers and websites, RidgeBot is deployed in the subnet with full access to the target servers. Tasks are setup for specific penetration testing scenarios appropriate for web assets. The provider schedules RidgeBot to run the task at regular quarterly intervals to meet compliance requirements.

The telecom provider's red team reviews RidgeBot's automatically generated reports to determine the security posture of the web assets and identify any vulnerabilities or potential exploits that may pose a risk.

To look for an "unauthorized" server, the telecom provider runs an Attack Surface Discovery report that assesses an asset's TCP/IP ports, websites, and URLS. RidgeBot will scan multiple subnets and identify all active servers with their open ports. The provider's red team uses RidgeBot's Asset Management feature to automatically identify all assets and take appropriate actions on the "unauthorized" server.

Similarly, the telecom provider's red team can run the weak credential exploit scenario to make sure the active servers or web applications do not have generic and test password in production environments.

The provider's red team also uses RidgeBot's extensive API capability to integrate RidgeBot with their security monitoring tool. The security monitoring tool will use RidgeBot's API to initiate a RidgeBot task to simulate an attack on a web asset.

The Telecom provider's red team and compliance organization use Ridgebot's automatically generated reports to serve as the bases for security risk assessments and to confirm the quarterly penetration test are being performed with documented results.

RidgeBot® Benefits

In this use case, the telecom provider realized many benefits and advantages of RidgeBot over manual penetration testing methods and tools:

1. **The ability to do penetration testing on all its web assets (applications and servers) in development and production environments.**
   This capability far exceeded the provider's expectations, and they have complete coverage of their assets.

2. **The ability to perform automated penetration testing on assets anytime or at a regular set schedule i.e., doing multiple penetration testing on assets weekly, quarterly, or yearly – whenever needed.**
   This enables the telecom provider to meet and exceed compliance requirements for penetration testing.

3. **RidgeBot automatically generates detailed reports are tasks are completed.**
   Detailed reporting is crucial to visibility of testing results, analysis, and verification that penetration testing has been performed. The reports are easily stored and used for historic trending over time.

4 **RidgeBot integrates with the Telecom provider's existing security monitoring tools.** This greatly improves efficiencies across security monitoring and red teams.

5 **RidgeBot augments the telecom provider's red team to perform penetration testing on thousands of servers regularly without additional resources or budget.** RidgeBot delivers a cost-effective penetration solution to the provider.

6 **The telecom provider was able to eliminate the need for several open-source security tools by using RidgeBot to scan, test, and analyze internal servers.** This reduced the customer's supply chain risk and resources needed to support these tools.

Example of metric between RidgeBot vs manual Penetration testing (from RSCS presentation).

	Old Manual Practice	Assisted by RidgeBot
IT Asset Coverage	~100 critical severs and 2 websites	All ~1000 IP devices and 2 websites
IT Asset Not Covered	~900 IT devices not tested	0
Test Frequency	4/Year (Quarterly)	15/Year (Monthly and On-demand)
Man-hour for Single Test	320 (2 engineers, 3 weeks testing, 1 week report)	24 (1 engineer, 3 days)
Estimated Man-hour for Single Test (estimated if to cover all IT assets)	~1000 (estimated by the team if to cover all IT assets)	24 (1 engineer, 3 days)
Man-hour needed for 15 Tests/Year	4,800 $96,000 (assume $20 hourly rate)	360 $7,200 (assume $20 hourly rate)
Man-hour needed for 15 Tests/Year (estimated if to cover all IT assets)	15,000 $300,000 (assume $20 hourly rate)	360 $7,200 (assume $20 hourly rate)
Number of Tools Used	6	1 (RidgeBot)

RidgeBot's Proven Effectiveness

Since RidgeBot was deployed, it has repeatedly proved itself to be extremely valuable to this telecom provider by testing and validating the security posture of the provider's numerous web applications, servers, and infrastructure components.

It is routinely used by the provider's red team and other organizations, enabling them to achieve their objective to manage the cybersecurity risks of all IT assets. RidgeBot greatly improved the efficiencies of its red team and security operations teams by reducing the number of security tools they needed to support.

RidgeBot not only quickly detects vulnerabilities within assets, but it also verifies their exploitability along with providing remediation guidance, making it one of the telecom provider's most used security tools.