sectona

One of the world's largest mobile operators implements Sectona to adhere to compliance regulations.

Background

As the world adapts to the ever-changing digital evolution, cyberattacks have been increasing in number and sophistication. Continuously working to ensure end-end security for businesses from threats internal and external to their organization, the mobile operator has introduced its Secure Intelligence Center – a Security Operations Centre (SOC) based out of India. The SOC uses SOAR, Artificial Intelligence, and Machine Learning. This orchestrated platform helps proactively monitor and prevent attacks on its customers from the rapidly evolving cybersecurity threat landscape.

Industry
Telecom

Challenge

The emphasis has been on strengthening the security of the Secure Intelligence Centre Infrastructure from internal and external threats to the organization while demonstrating security and audit compliance to its customers. As part of its security framework, the organization needed a solution that can address the following:

1. A solution that supports & integrates with cloud environments like AWS, and Azure to cater to the growing customer presence on the cloud.
2. A scalable solution that enables easy-to-extend capabilities & scales as per use.
3. A solution that can deliver seamless and secure access to internal teams and customers from anywhere consistently with the least possible friction.
4. A solution supporting a multi-tenancy approach for developing PAM as a Service Proposition.

Solution

Sectona Security Platform, a light, integrated approach to privileged access management, leverages cross-platform capabilities to secure every privileged session across the infrastructure by isolating the endpoints, securing passwords, SSH Keys, and secrets in the solution's purpose built-vault. It helps in providing simplified access anywhere while also enabling a unique model for SOC service providers to help their customers adopt PAM security objectives. The Secure Intelligence Centre initially deployed the PAM solution internally as a pilot program. Realizing the value that PAM adds, the mobile operator decided to roll out the solution across their SOC team. The SOC team underwent necessary hands-on and support training on the PAM solution for proposing PAM-as-a-service to its portfolio of customers.

Benefits

- Securing privileged user access across the entire gamut of IT (servers, databases, network devices).
- Manage and monitor each privileged session while isolating the sessions from unsecured endpoints.
- Storing credentials in a tamper-proof hardened built-in password vault.
- Achieving multi-tenancy capabilities with a logical separation of customer instances for easily providing PAM as a service.
- Flexible deployment options to either - deploy PAM on customer premise, thereby providing a managed PAM offering - or - deploy in SOC, thereby providing PAM as a service via a centralized master PAM instance.

CISO Says:

"Looking for a solution that can enable seamless and secured access to the SOC Infrastructure without having to worry about credential compromise. We were on the lookout for a mechanism through which the credentials are encrypted and stored in a purpose-built vault, inaccessible to any authorized user." He continues, "With Sectona Security Platform, we are able to achieve this and more. With the reports and dashboards, we also ensure that we adhere to compliance regulations by unlocking the solution's full potential."

sectona

Sectona with its light, integrated approach provides a single console for securing passwords & secrets in embedded vault, secure access with cross-platform access technology & manage privileges over endpoints.
For more information, visit www.sectona.com and follow @SectonaTech on X (Twitter) or @Sectona on linkedin