RangeStorm

Marketing Strategy

Bhumi iTech

RANGESTORM

RAVI RAJ
210104082

●●● Industry Overview

$188 Billion Spent by companies on information security in 2023

$101.5 Billion of projected expenditure on service providers alone

2.72

million skilled cybersecurity workers, according to the 2021 (ISC)2 report.

3.5 Million cybersecurity job positions now open world wide.

85% of small and medium sized enterprises intend to increase expenditure on IT security until 2023 ends

+21% forecast of Compound Annual Growth for direct cyber insurance premiums until 2025

Current Cybersecurity Landscape

On-demand access to ubiquitous data and information platforms is growing

Hackers are using AI, machine learning, and other technologies to launch increasingly sophisticated attacks

Ever-growing regulatory landscape and continued gaps in resources, knowledge, and talent will outpace cybersecurity

Bhumi iTech

Envision a future of CyberSecurity professionals

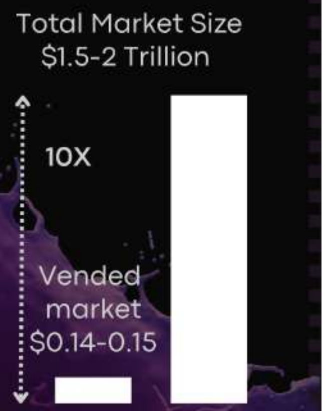
Products
- Rangestorm
- RLMS

Services
- Cloud Services
- SOC
- NOC
- Cyber Consulting

Problems Addressed

- **42%** Attacks targeted on SMBs
- Unsophisticated security tooling
- Employee training and integration of security with IT operations is Key

Value Proposition



Rangestorm

Platform to upskill employees for immediate and efficient incident response.

Combines theoretical & practical knowledge including team building.

RLMS

Learning platform for employees, teachers, learners to track & analyze their cybersecurity skill in a gamified environment.

Top Underpenetrated Markets
- Cloud security
- IoT/OT
- DevSecOps

Where Bhumi iTech comes in ?

- Rangestorm → Prioritize actions, hiring or upskilling
- SOC solutions → Realize current capabilities & solutions available
- Cyber consulting → Identify Key Risks

SWOT, Competitors, Drawbacks, Capabilities

S

- Cutting-Edge Technology: Rangestorm to practice real-world scenarios.
- Comprehensive Services Portfolio
- Real-time Monitoring
- CapEx & Subscription based pricing

W

- Complexity
- No certification offered to professionals
- No mention of AI based systems, and protection against new threats
- Missing Customer testimonials on website

O

- Holistic Cybersecurity Solution
- Mid-market pricing for SMBs
- 48% workload on Cloud platforms currently
- Partnerships with cloud service providers
- National Cyber Security Strategy 2020

T

- Competitive Landscape
- Regulatory Changes
- Ever-evolving threats might harm brand reputation
- Economic uncertainty- further lowering of security spending

cyberbit

- World's leading provider of cyber range platforms, used by organizations to train their security teams and simulate cyberattacks.
- Cyberbit has been recognized by Gartner as a "Leader" in the Magic Quadrant for Security Training Solutions.
- Partnered with Deloitte ECC to deliver greater cyber strategy services.

CROWDSTRIKE

CrowdStrike has over 6,000 customers, including some of the world's largest organizations, including Microsoft, Cisco, Palo Atlo Networks.
Leader in innovation & early mover

Growth Opportunities

Visibility Gap

Clients don't know they have a problem. Around 60 percent of buyers analyze and triage less than 40 percent of their enterprises' log data.

- Detect unauthorised access or changes to a system
- Identify malware infections
- Track suspicious activity
- Investigate security incidents
- Comply with regulations

ROI Gap

Clients want to see the ROI. Some paradigm KPIs in the industry are MTTR, MTTD, No. of incidents

- Customer value
- Business Value
- Market Value

Cybersecurity Talent Gap

With more than 3.12 million jobs in cybersecurity estimated to be unfilled in 2021, although AI has helped mend the path.

- Realize recruiting realities
- Need for full-stack solutions
- Evolving client requirements (low rate of false positives)

Tech Fragmentation Gap

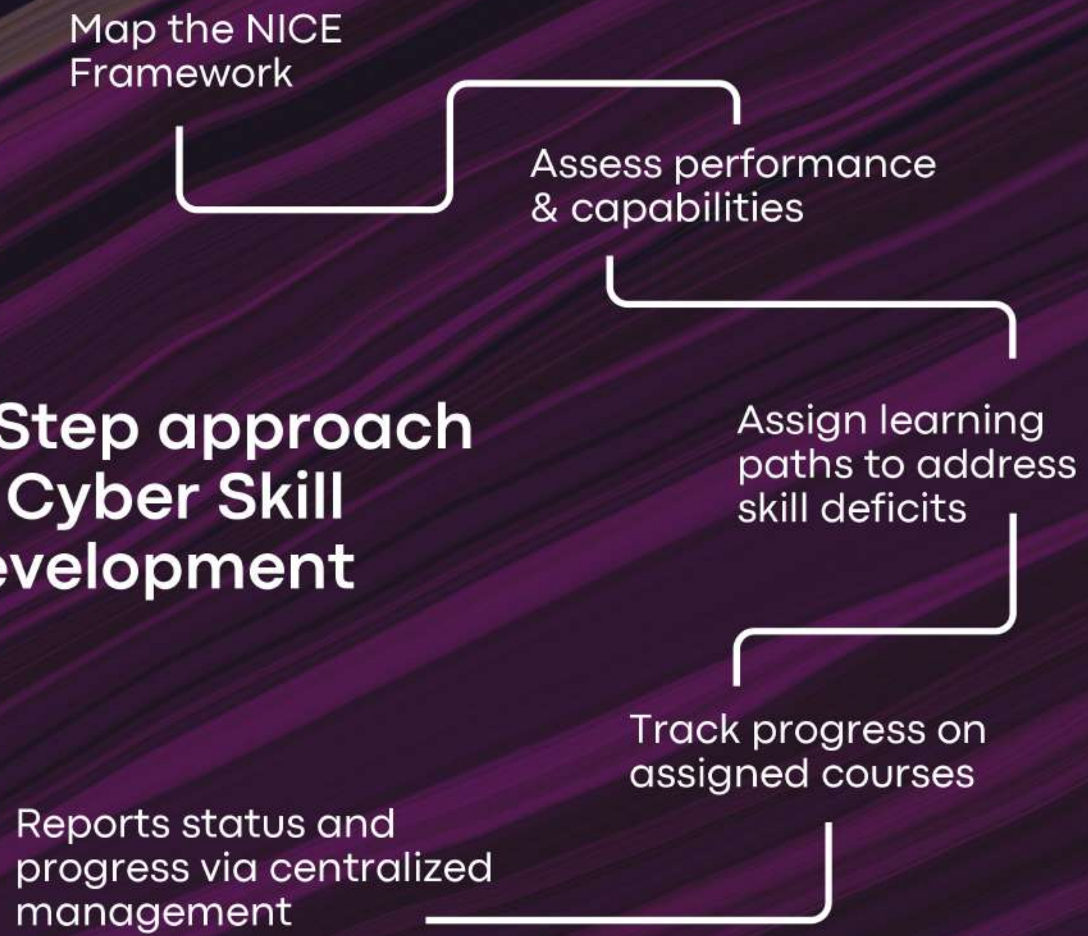
*Providers must maintain relationships with major cloud platforms

The shift to Cloud architecture makes, multi- and hybrid-cloud security critical, and CISOs will be willing to pay for increasingly hard-to-find skills (such as mainframe security) from a service provider.

NICE Framework

Establishes a common lexicon that categorizes and describes cybersecurity work and what workers need to know and be able to do to complete that work. The NICE Framework is used in both public and private sectors and across industries, in support of cybersecurity career awareness, education and training, and workforce assessment, planning, and development.

5-Step approach to Cyber Skill Development



Map the NICE Framework

Assess performance & capabilities

Assign learning paths to address skill deficits

Track progress on assigned courses

Reports status and progress via centralized management

Market Segmentation

Each of these are to be served differently & have different requirements and capabilities.

These clients can be explored through strategic partnerships with other cybersecurity companies

Large
Enterprises

- Corporations having past experience, historical data & comparison points for their cyber security needs.
- Have a dedicated department to deal with incidents

Can avail Rangestorm & RLMS for upskilling following the 3 Step model towards cybersecurity

Small & Medium
Enterprises

- MSMEs vulnerable to exploits and newer threats
- As they have rudimentary security
- Mostly outsource their services

Startups

- Limited impetus towards security
- Lack integration of security at development phase
- Fiduciary responsibility driving focus towards revenue

Highly dependent on customer data & cloud services for operations. Need personalised risk specific solutions

4 Key Areas of Focus for Bhumi iTech

Cloud technologies

Explainable AI solutions

Bundled Full-stack offerings

Mid-market pricing

Cluster Similar SMBs as per risks and potential threats, using Hierarchical Agglomerative Clustering. Then personalize offering and tech support team for each cluster.

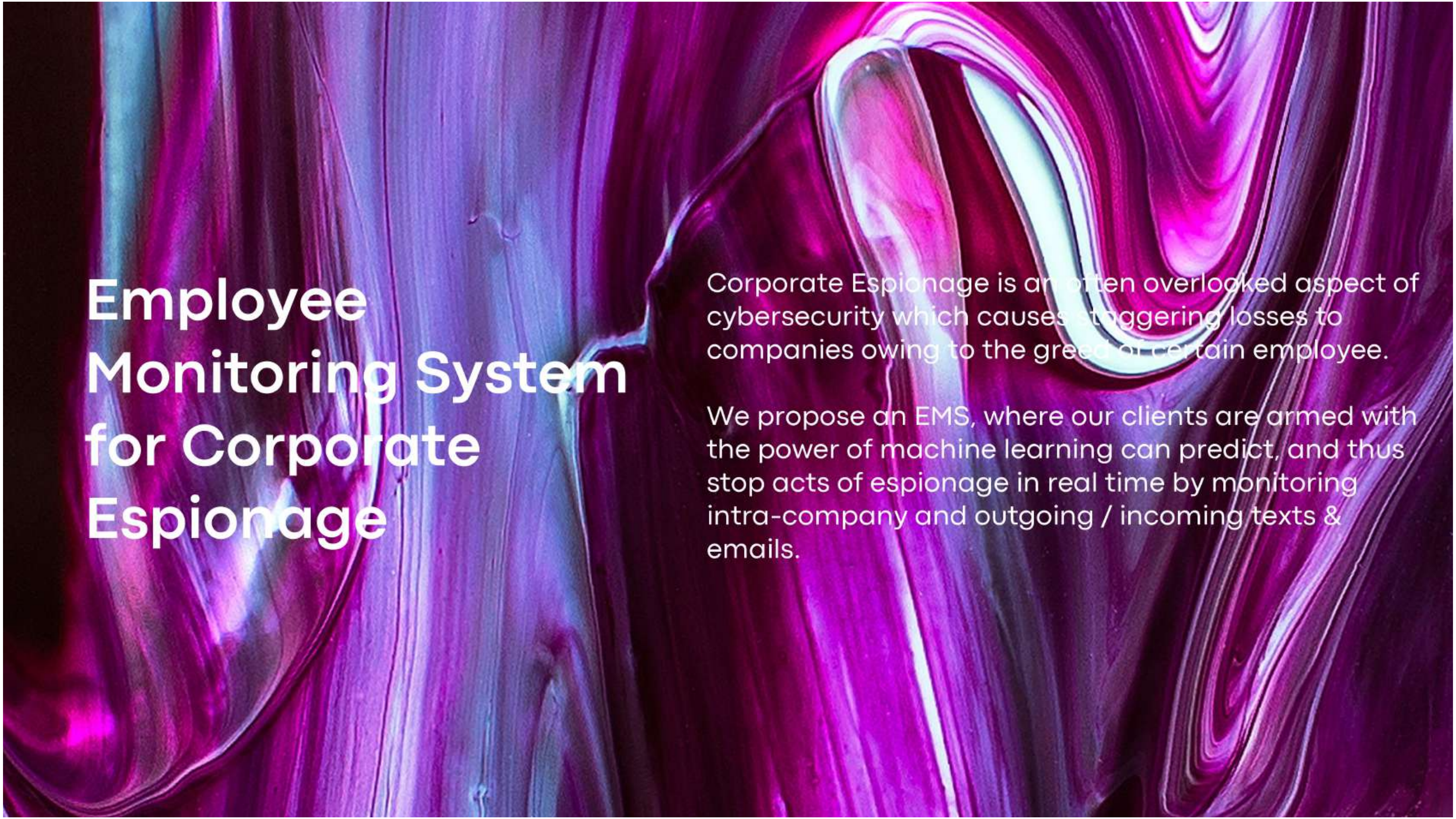
- Operational Cost reduction
- Upgraded Capabilities
- Affordability
- Customized as per risks

“Reverse Bug Bounty”

Conduct contests called reverse bug bounties where companies participate and our team of hackers try to infiltrate their systems is a company if a company’s infrastructure is successfully able to fend off any cyberattacks from our team, then they get discounted access to our premium software and training.

These companies being already good at cyber defence, are usually a good addition to our portfolio of clients.

In contrast, companies that we successfully breach / social engineer will generally be more inclined to use our software, which we present according to the type of cyber threat that they are most vulnerable to.



Employee Monitoring System for Corporate Espionage

Corporate Espionage is an often overlooked aspect of cybersecurity which causes staggering losses to companies owing to the greed of certain employee.

We propose an EMS, where our clients are armed with the power of machine learning can predict, and thus stop acts of espionage in real time by monitoring intra-company and outgoing / incoming texts & emails.

Proposed partner: Trendmicro

Bhumi iTech

Enhanced Cybersecurity Solutions

Innovation and Agility of smaller company

Research and Development Opportunities:

Resource sharing & diversification

Access to Smaller Business Segment

Access to Global Threat Data

Complimentary services & market differentiation

Access to new clients through partner