Maximizing Cybersecurity with Limited Resources:

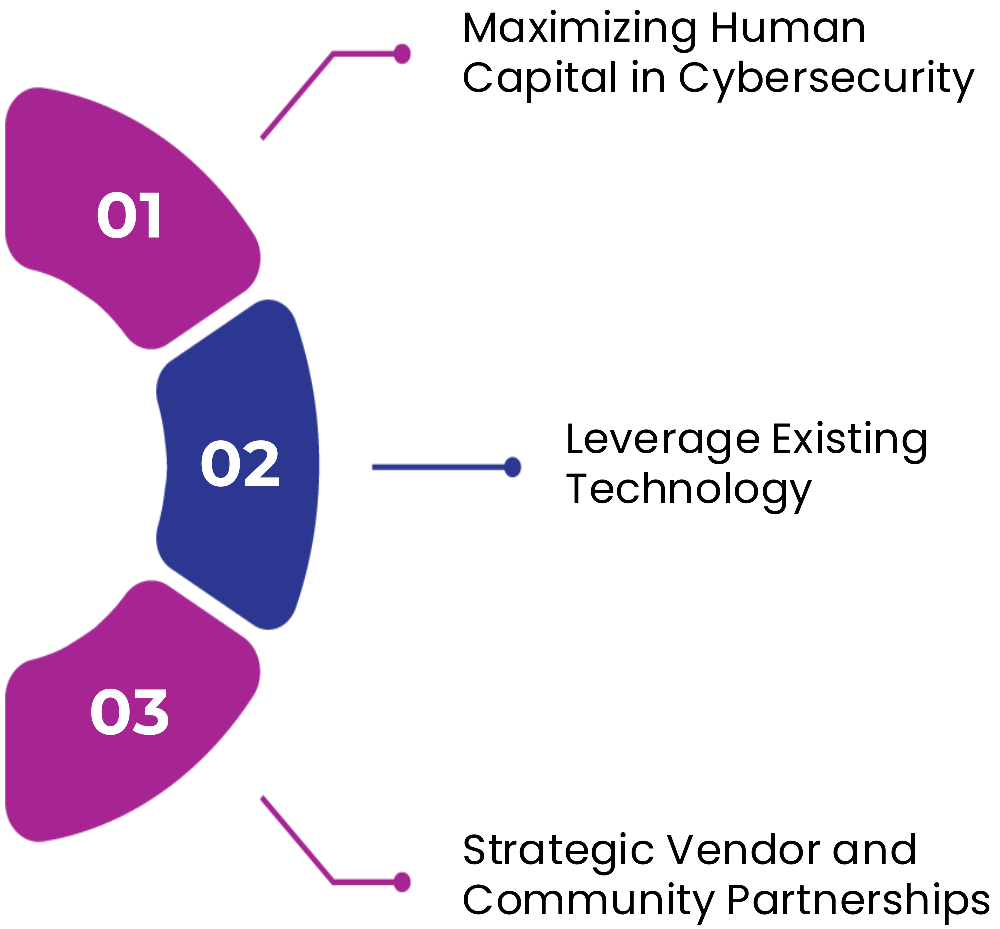
Strategic Approaches for Leaders

Introduction

Safi Raza
Head of Cybersecurity @ Fusion Risk Management

- 20 Years in Technology (12 Years in Information Security)
- CISSP | CCSP Certified
- B.S. Computer Science – Florida Atlantic University
- M.S. Cybersecurity – Georgia Tech (in progress)

Three Approaches



01 Maximizing Human Capital in Cybersecurity

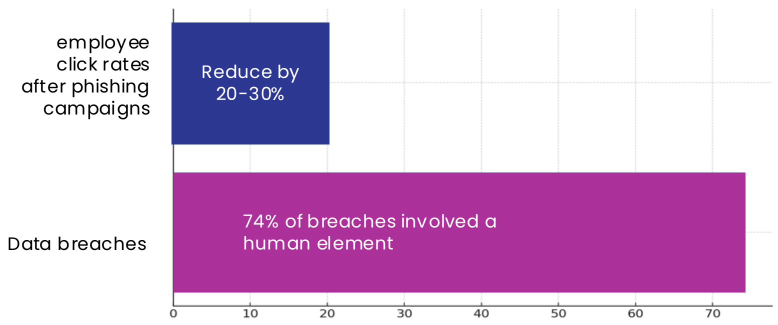
02 Leverage Existing Technology

03 Strategic Vendor and Community Partnerships

Maximizing Human Capital In Cybersecurity

01 Ongoing Phishing Campaigns

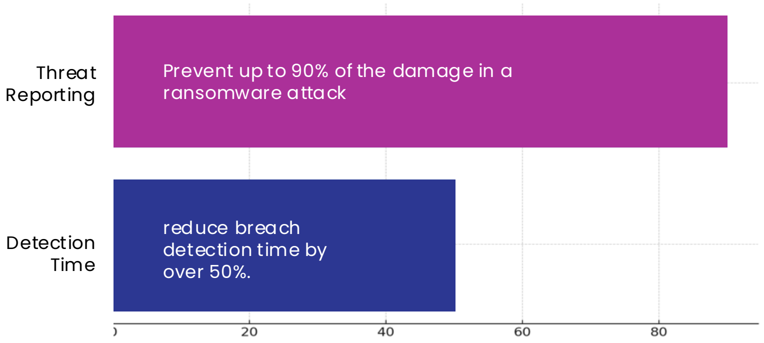
Shift from periodic phishing tests to continuous campaigns, keeping employees vigilant against evolving threats.



Verizon 2023 Data Breach Investigations Report

02 Incentivize Threat Reporting

Reward employees for reporting real threats and use these examples to create more realistic phishing simulations.



(IBM Security 2022).

03

Share Key Metrics

Share engaging cybersecurity metrics (e.g., "Most Targeted User of the Month") with employees to increase awareness and interest.

04

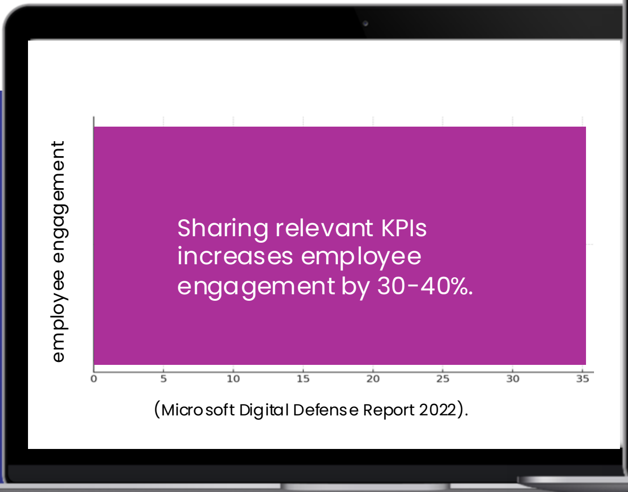
Share Incident and Pentest Results

Share the results of social engineering tests and incidents to raise employee awareness and preparedness.

05

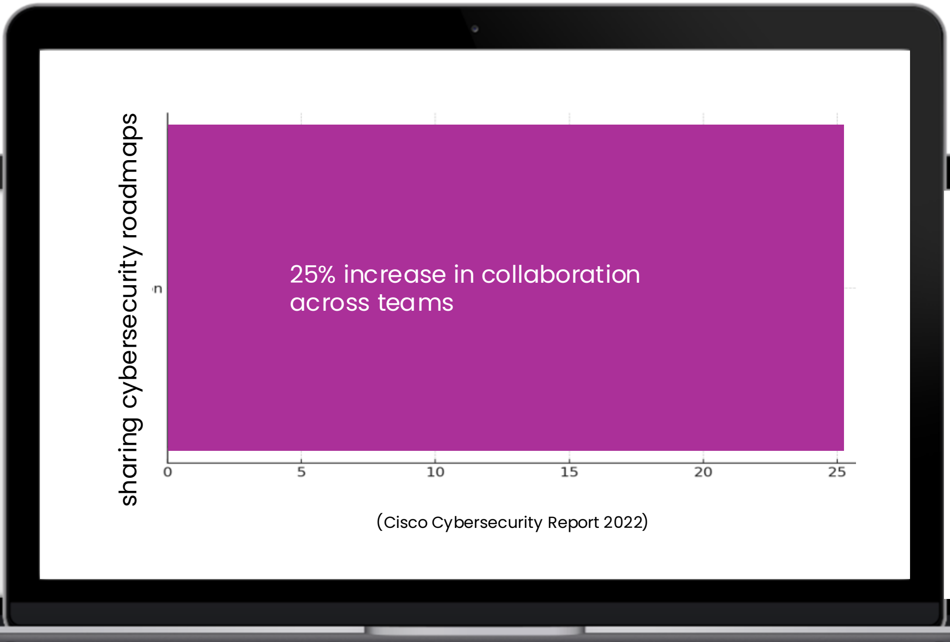
Shadow a SOC Analyst

Allow employees to shadow SOC analysts to gain firsthand exposure to how cybersecurity threats are managed.



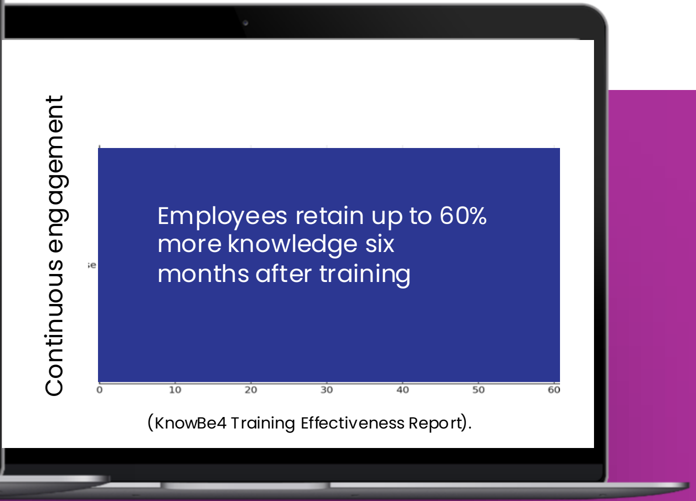
Sharing relevant KPIs increases employee engagement by 30-40%.

(Microsoft Digital Defense Report 2022).



25% increase in collaboration across teams

(Cisco Cybersecurity Report 2022)



Employees retain up to 60% more knowledge six months after training

(KnowBe4 Training Effectiveness Report).

06

Leverage Interns | Assist NFP

Partner with internship programs and organizations supporting underprivileged students for cybersecurity tasks, helping with essential work while providing valuable experience.

07

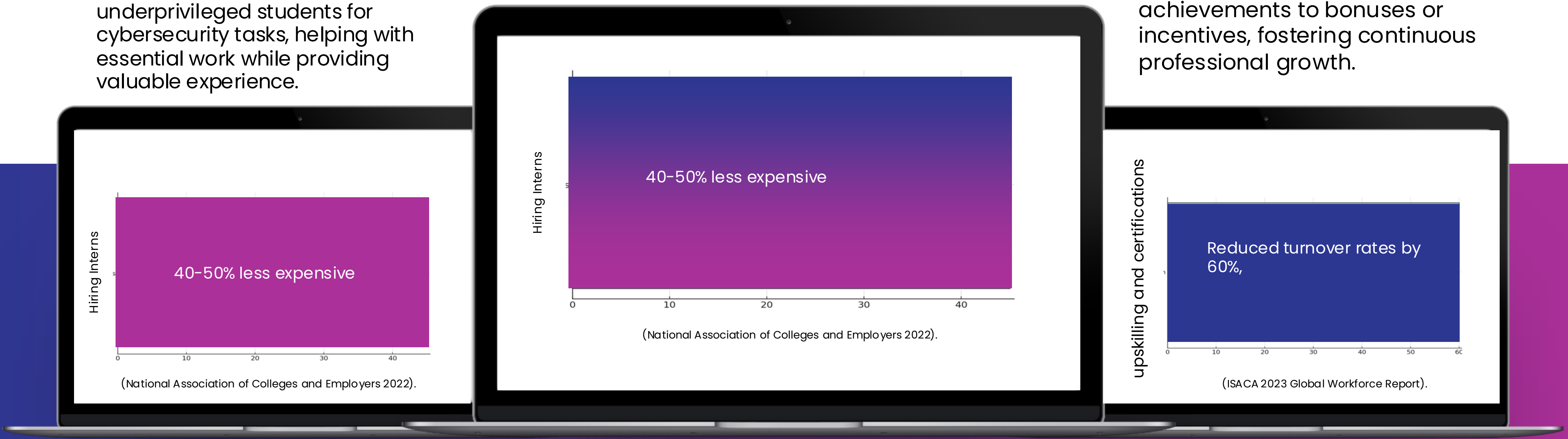
Invest in Freshly Certified Talent

Hire newly certified professionals who bring fresh skills at a lower cost, providing opportunities for growth within the organization.

08

Certifications and Incentives

Encourage team members to pursue cybersecurity certifications by tying achievements to bonuses or incentives, fostering continuous professional growth.



(National Association of Colleges and Employers 2022).

(National Association of Colleges and Employers 2022).

(ISACA 2023 Global Workforce Report).

09 Self-Development Time

Allocate dedicated time for cybersecurity staff to enhance their skills, contributing to a more resilient team.

10 Cyber Hour (Open Forum)

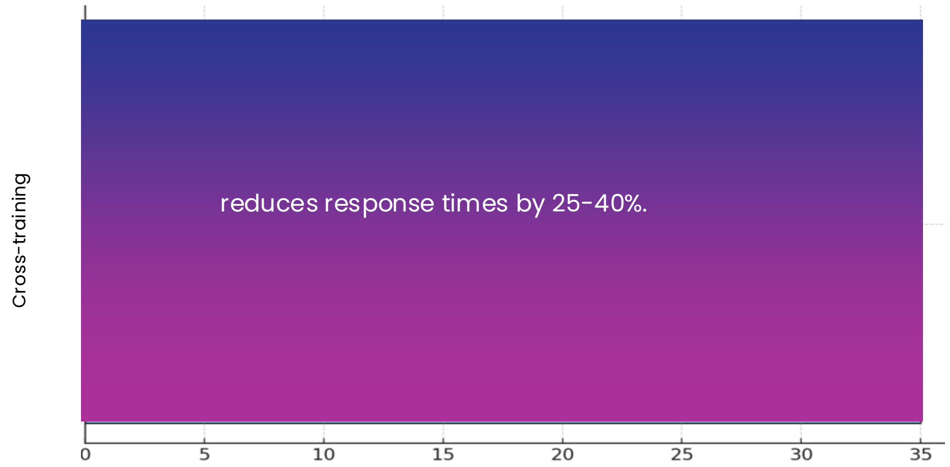
Host regular open sessions where employees can ask cybersecurity questions, fostering transparency and engagement.

11 Cyber Ambassador Program

Empower non-technical staff to advocate for cybersecurity within their departments, enhancing overall security culture.

12 Cross-training

Cross-train team members in areas like incident response, threat hunting, and risk management, creating a versatile and resilient cybersecurity team.



(Gartner Cybersecurity Survey 2023).

13 Upskilling and Study Groups

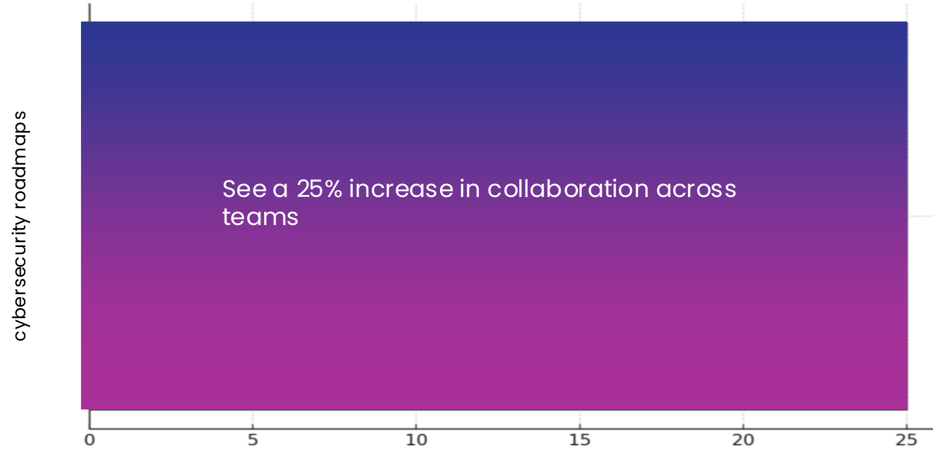
Facilitate upskilling by encouraging the formation of study groups focused on certifications and knowledge sharing.

14 Recognition of Achievements

Regularly celebrate employee achievements, such as certifications, to boost morale and motivation.

15 Cybersecurity Roadmap Transparency

Share the organization's cybersecurity roadmap with employees to foster alignment and collaboration.



(Cisco Cybersecurity Report 2022).

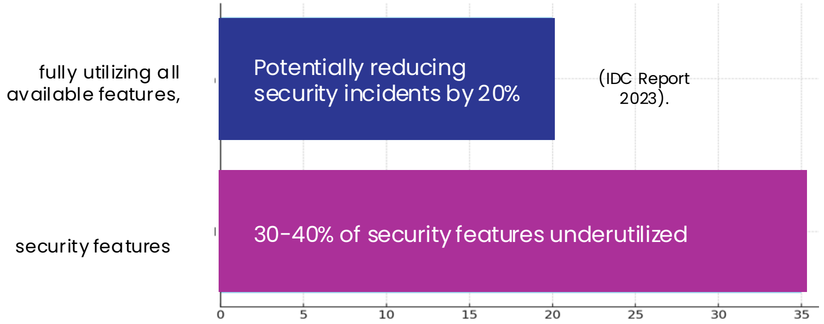
16 Lunch & Learn Sessions

Organize informal "Lunch & Learn" sessions where employees can engage with cybersecurity topics in an accessible and relaxed environment.

Leverage Existing Technology

01 Maximize Existing Tools:

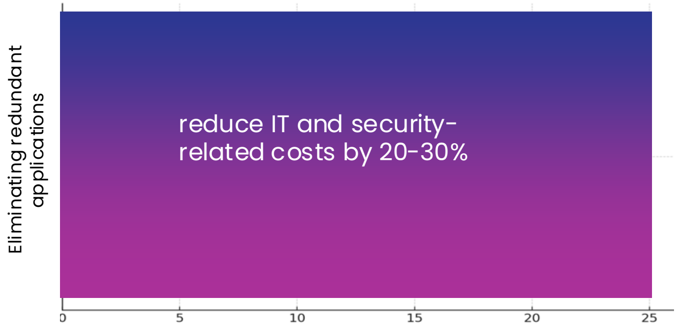
Fully utilize all features in your current security tools to enhance their effectiveness and value.



(Gartner 2022).

02 Consolidate Redundant

Applications: Eliminate duplicate apps that provide similar functions to reduce risks, streamline operations, and lower costs.



(Forrester Research 2022).

03 Optimize License Utilization:

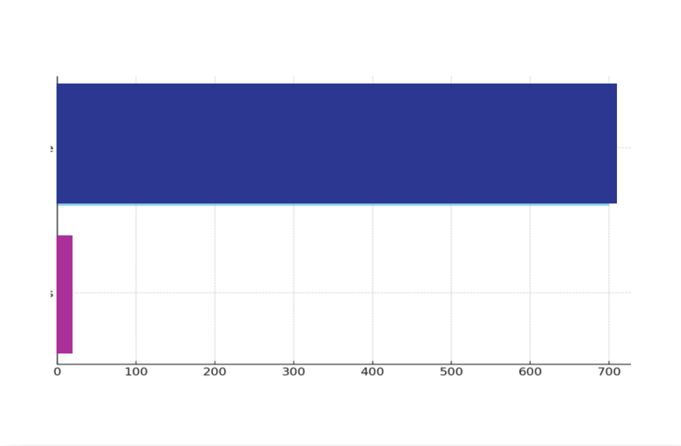
Regularly monitor and manage application licenses to ensure efficient use and eliminate unused or underutilized licenses.

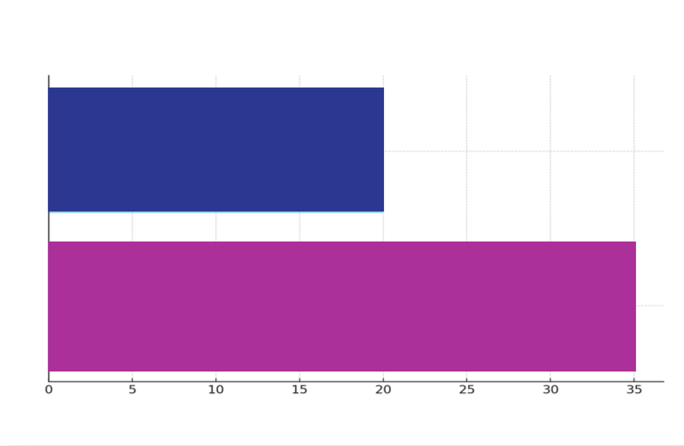
04 Automate Security Processes:

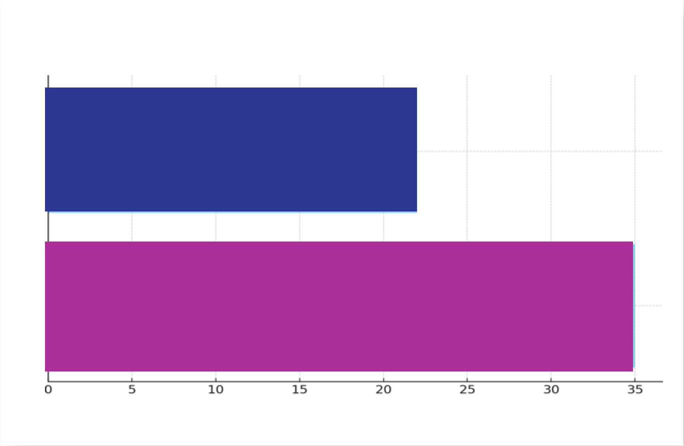
Automate routine tasks such as log reviews, patching, and reporting using SOAR platforms and custom scripts to reduce manual workload.

05 Leverage Cloud-native Security:

Use integrated security tools from cloud providers (e.g., Azure, AWS) to achieve cost-effective and scalable security management.



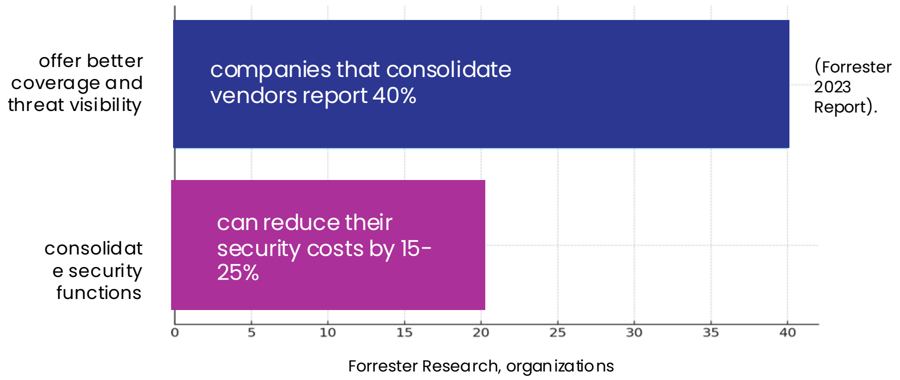




Strategic Vendor and Community Partnerships

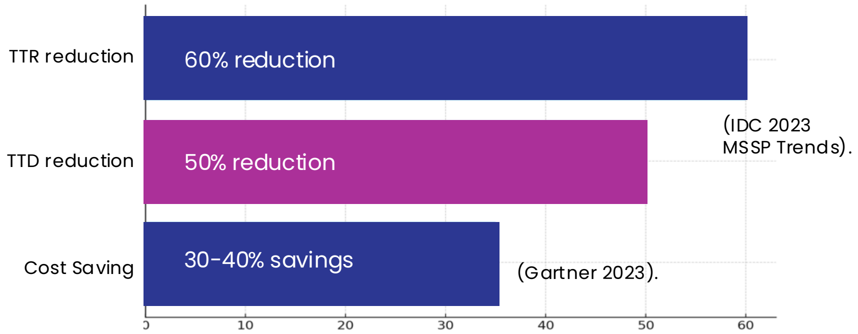
01 Vendor Consolidation:

Work with vendors to consolidate security functions (e.g., EDR, SIEM) into one solution, reducing complexity and cost.



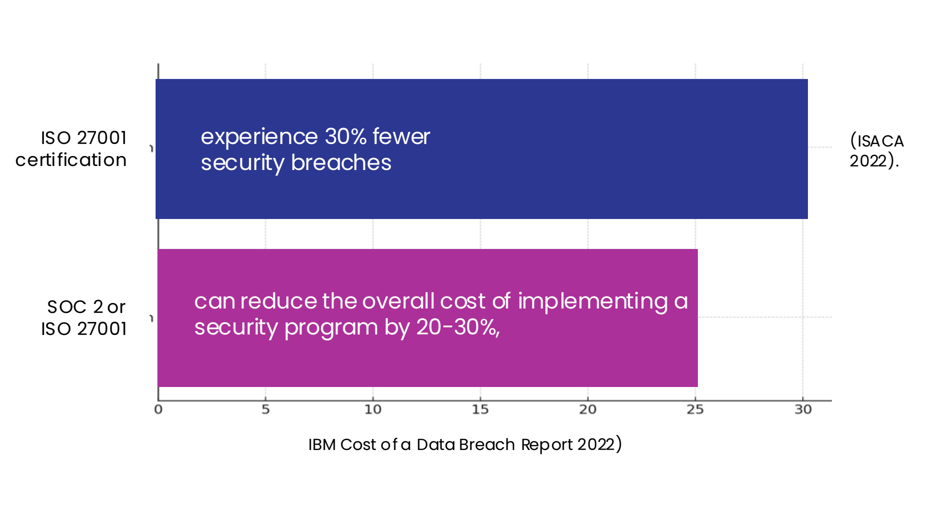
02 MSSPs:

Outsource functions like 24/7 SOC monitoring or threat intelligence to Managed Security Service Providers for cost-effective security management.



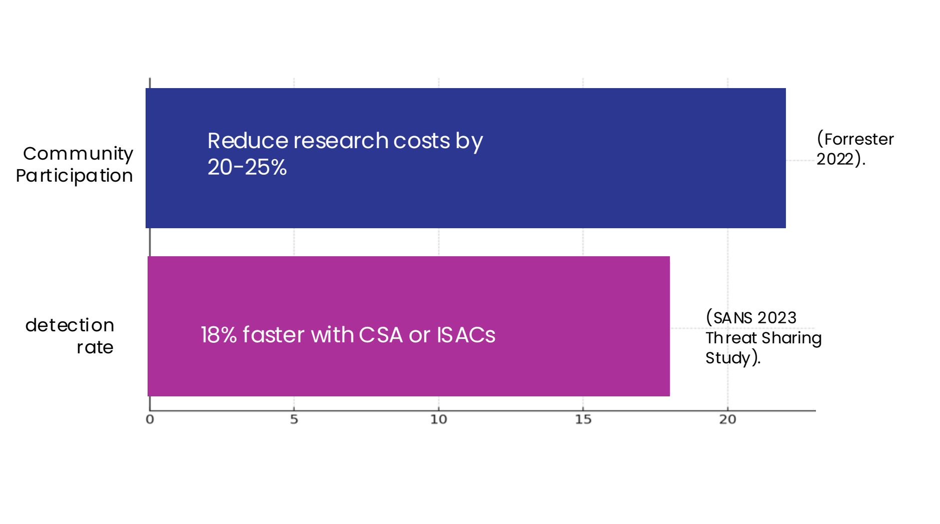
03 Leverage Regulatory Compliance:

Align your security initiatives with compliance requirements (SOC 2, ISO 27001) to streamline efforts and save on duplication.

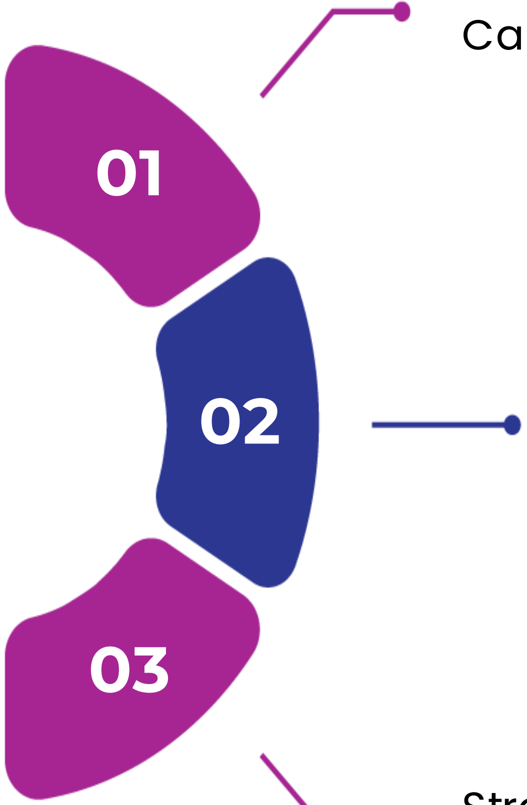


04 Collaborate with Peers and Communities:

Share threat intelligence and resources through platforms like CSA (Cloud Security Alliance) and ISACs, reducing costs and benefiting from collective knowledge.



3 Approaches



01 Maximizing Human Capital in Cybersecurity

02 Leverage Existing Technology

03 Strategic Vendor and Community Partnerships

Q&A | Connect with me on LinkedIn

Safi Raza

Senior Director of Cyber Security at Fusion Risk Management