ALLIANCES PROJECTS

UNITING STRENGTHS

EXPANDING OPPORTUNITIES

SECURITY METRICS

Q&A with Chris Gatsi

A CISO's JOURNEY
ALLIANCES PROJECT

ALLIANCES INSIGHTS

www.alliances.global

Introduction to Insights from the Security Metrics Q&A Digital Chapter with Chris Gatsi

DESCRIPTION

Join us for an informative webinar featuring Chris Gatsi, Divisional IT Audit Manager at Bidvest South Africa, as he delves into the essential metrics for measuring the success of your cybersecurity program. In this engaging Q&A session, Chris covers:

- The importance of defining clear objectives for cybersecurity metrics.
- Strategies for identifying, collecting, and analysing data to measure cybersecurity effectiveness.
- Common cybersecurity metrics such as Mean Time to Resolve (MTTR), incident management, asset compliance, and vulnerability management.
- Practical insights on how to report metrics to different stakeholders, including the board and risk committees.
- The role of user awareness training and how to measure its impact on reducing phishing incidents.
- The challenges and solutions in creating dynamic and effective cybersecurity metrics.

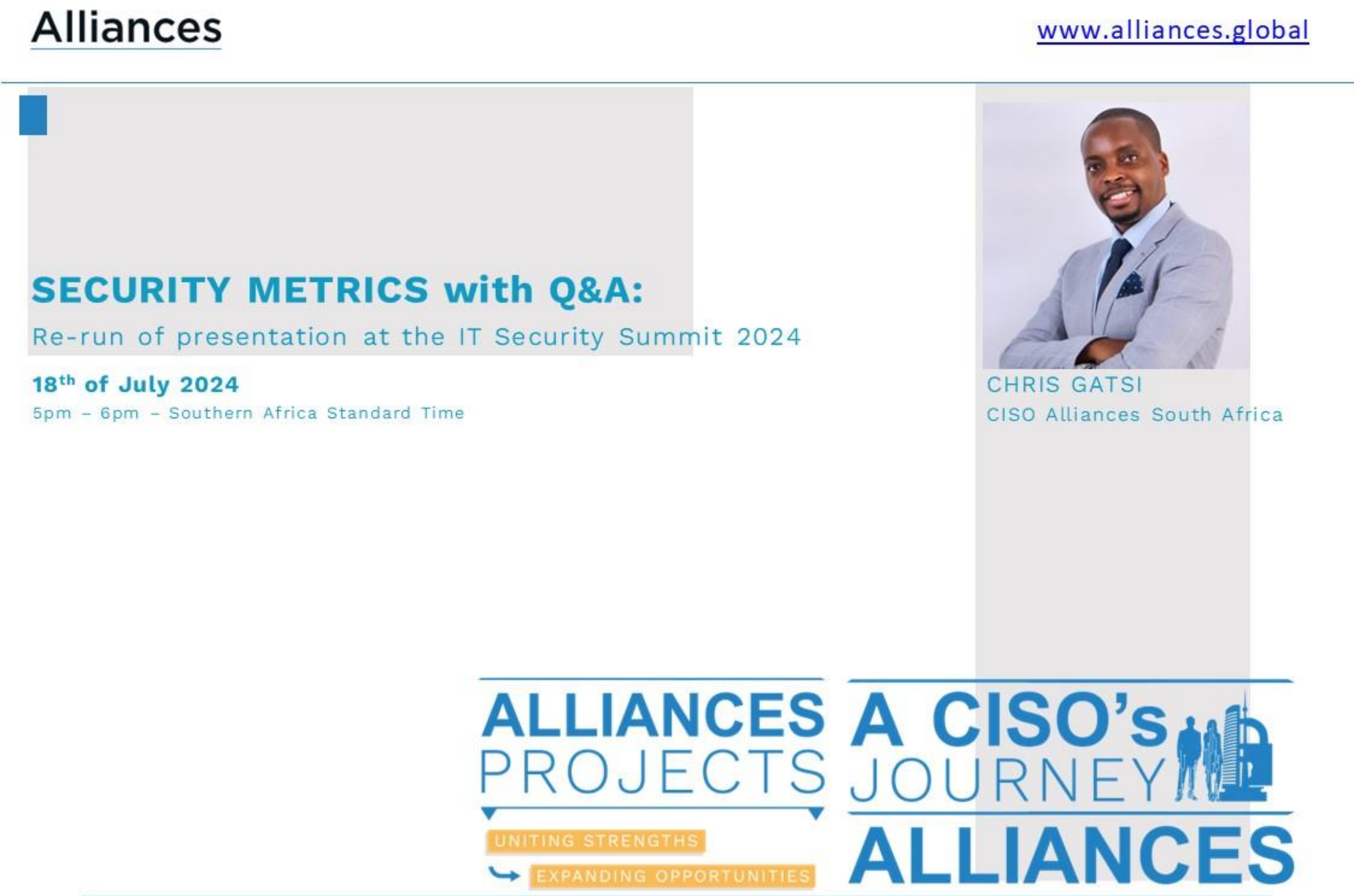
Whether you're a CISO, CIO, or an IT professional looking to enhance your cybersecurity measurement framework, this webinar offers valuable knowledge and practical tips to help you succeed. Don't miss out on this opportunity to learn from an industry expert and improve your organization's cybersecurity posture.

DESCRIPTION

The Importance of Defining Clear Objectives for Cybersecurity Metrics

In the webinar, Chris Gatsi emphasized the critical need for cybersecurity professionals to start with a clear understanding of their end goals. Drawing inspiration from Stephen Covey’s "7 Habits of Highly Effective People," he highlighted that beginning with the end in mind allows cybersecurity teams to establish meaningful and outcome-based metrics. By clearly defining what they intend to achieve, professionals can align their cybersecurity efforts with broader business objectives, ensuring that every metric tracked provides actionable insights into the program's success and areas for improvement. Clear objectives help in setting realistic goals, fostering a results-oriented approach, and enabling effective communication with stakeholders.

A CISO’s
JOURNEY
ALLIANCES PROJECT



Alliances www.alliances.global

SECURITY METRICS with Q&A:

Re-run of presentation at the IT Security Summit 2024

18th of July 2024

5pm – 6pm – Southern Africa Standard Time

CHRIS GATSI
CISO Alliances South Africa

ALLIANCES PROJECTS

UNITING STRENGTHS
EXPANDING OPPORTUNITIES

A CISO's JOURNEY
ALLIANCES

A CISO's JOURNEY
ALLIANCES PROJECT

Strategies for Identifying, Collecting, and Analysing Data to Measure Cybersecurity Effectiveness

Chris discussed a structured approach to measuring cybersecurity effectiveness, starting with understanding the business and its cyber landscape. He outlined a high-level methodology that includes:

1.Understanding Business Objectives: Aligning cybersecurity goals with the overall business strategy.

2.Identifying Risks: Recognizing and quantifying potential risks to the organization.

3.Establishing Metrics: Setting specific, measurable, achievable, relevant, and time-bound (SMART) metrics.

4.Data Collection: Determining sources of data, which can include firewalls, switches, network monitoring tools, and reports from various departments.

5.Benchmarking: Comparing metrics against industry standards to gauge performance.

6.Continuous Monitoring and Evaluation: Regularly reviewing metrics to identify trends, measure progress, and make necessary adjustments.

7.Reporting and Improvement: Communicating findings to stakeholders and implementing improvements based on lessons learned.

Common Cybersecurity Metrics

Chris highlighted several key metrics that are essential for monitoring and improving cybersecurity:

- Mean Time to Resolve (MTTR): Measures the average time taken to resolve cybersecurity incidents, reflecting the efficiency of incident response processes.

- Incident Management: Includes metrics such as the number of incidents thwarted, mean time to acknowledge incidents, and mean time between failures.

- Asset Compliance: Tracks the compliance of devices with security standards, the discovery of rogue devices, and the ratio of asset value to security control costs.

- Vulnerability Management: Metrics such as the mean time to patch vulnerabilities, the percentage of high to medium vulnerabilities resolved within a specified time, and the number of repeat vulnerabilities.

Practical Insights on Reporting Metrics to Different Stakeholders

Chris emphasized the importance of tailoring reports to the audience, ensuring that the information is relevant and understandable. For instance, while technical details might be crucial for IT teams, board members and risk committees are more interested in high-level summaries that focus on risk management, return on investment, and compliance. He suggested:

- **Visualizing Data**: Using charts and graphs to make complex data more accessible.

- **Contextualizing Metrics**: Explaining what the metrics mean in terms of business impact.

- **Regular Updates**: Providing consistent and timely updates to keep stakeholders informed of progress and issues.

- **Storytelling**: Crafting a narrative around the data to highlight achievements and areas needing attention.

The Role of User Awareness Training and Its Impact on Reducing Phishing Incidents

User awareness training is a crucial element of cybersecurity strategy. Chris discussed metrics related to training, such as the percentage of users who have completed training and behavior change analytics. These metrics help organizations understand how well their training programs are working and identify areas for improvement. He noted the importance of:

- **Tracking Training Completion**: Ensuring that all employees complete mandatory cybersecurity training.
- **Behaviour Change Metrics**: Monitoring changes in user behaviour, such as a reduction in phishing proneness.
- **Continuous Improvement**: Using metrics to refine and enhance training programs, making them more effective over time.

Challenges and Solutions in Creating Dynamic and Effective Cybersecurity Metrics

Chris acknowledged several challenges in creating effective cybersecurity metrics:

- **Dynamic Nature of Threats**: Cyber threats evolve rapidly, requiring metrics that can adapt to new risks.

- **Data Collection**: Identifying reliable sources of data and ensuring continuous data flow can be difficult.

- **Stakeholder Communication**: Translating technical metrics into business-relevant information requires skill and understanding.

- **Resource Constraints**: Limited budgets and resources can hinder the development and tracking of comprehensive metrics.

ADVICE TO ADDRESS THESE CHALLENGES

Adapting Metrics: Regularly reviewing and updating metrics to reflect the current threat landscape and business priorities.

Automation: Leveraging automation tools to streamline data collection and analysis.

Benchmarking and Industry Standards: Using benchmarks to validate metrics and ensure they are relevant and effective.

Cross-Functional Collaboration: Engaging stakeholders from different departments to ensure metrics align with overall business goals and receive the necessary support.

A CISO's JOURNEY

ALLIANCES PROJECT

ABOUT THE ALLIANCES

Always has been and will continue to be *a union formed for mutual benefit*

THANK YOU