



Alliances

CISO Alliances Nairobi
Dec 16th 2020



In Partnership with

FOOD FOR THOUGHT /TOPICS DISCUSSED



The December session involved a 2 part approach:

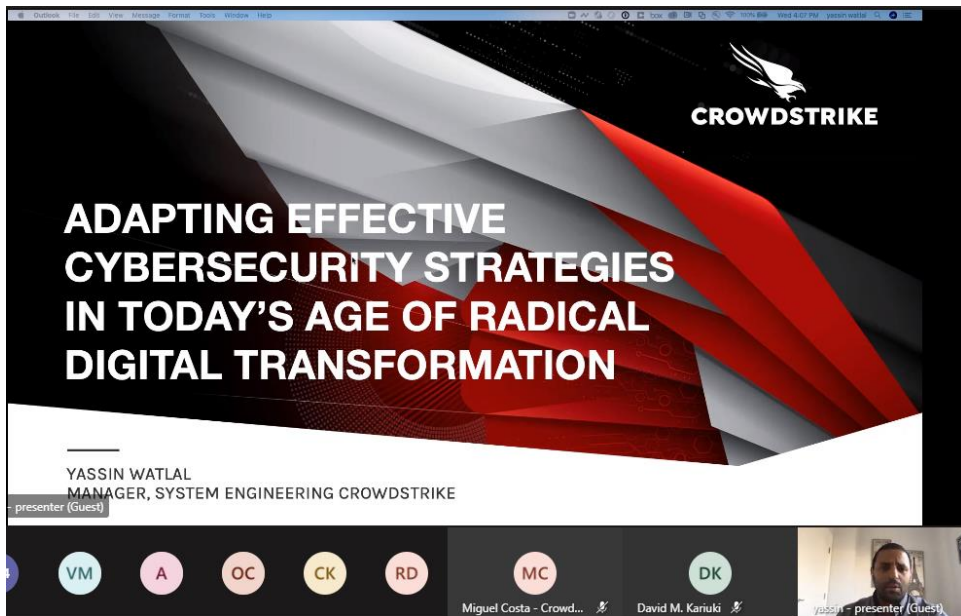
- 1) Presentation by Yassin Watlal, Manager System Engineering - CrowdStrike META
- 2) Panel Discussion featuring:



- Roland Daccache, Team Leader Sales Engineering - CrowdStrike META
- Karan Challa, IT Security Manager - SBM Bank
- Anthony Muiyuro, Associate Director, Cybersecurity, Privacy & Trusted Technology - EY
- Cynthia Karago, CISO - GE Africa



- 1) Presentation



During the Presentation Yassin Watlal covered:



- Understanding digital transformation & what is its effect on cybersecurity in organisations
- Key cyber security trends you should plan for
- Why is it critical for organisations of all sizes to have a cybersecurity strategy that adapts rapidly
- What strategy can help reduce the risk of a breach as a companies pivot to the cloud and embrace remote work

FOOD FOR THOUGHT /TOPICS DISCUSSED



- A review of Computing Revolution (1st, 2nd and 3rd Platform)
- 'Digital Native' example of scale & agility
- 'Digital Native' Business Technology & Security enjoy Agility, Elasticity and Scale



- Public Cloud Option (2 Type): SAS Basis
Cloud & Scalable



Trends & Challenges



- Macro trends affecting customers (Economy, Geo-Politics, AI, The New Normal, Cyber Security)
- Customer Security Trends (Increased Complexity, End Points, Legacy Cyber Security needs to go, New Attack and New Approach Needed, Talent Challenges continue)



- 2019 CrowdStrike Global Threat Report Trends
- Importance of Survival of the Fastest - MITRE ATTACK PHASE EXAMPLE



- The Endpoint Under Sustained Attack
- Collaboration & Leveraging Intelligence



RECOMMENDATIONS

▪ **Hygiene**

- User Awareness
- Asset & Vulnerability Management
- Multi Factor Authentication

▪ **Look beyond malware**

- Get visibility into assets and activity as a whole
- Utilize endpoint telemetry to respond more quickly and get proactive
- Focus on security outcomes over feature comparisons

▪ **Accept the 1 - 10 - 60 cybersecurity metrics challenge**

- Leverage your resources



FOOD FOR THOUGHT /TOPICS DISCUSSED

2) Panel Discussion



The banner features the CrowdStrike logo on the left and the DigitalAlliances logo on the right with the tagline 'continue collaboration'. Below the logos, it says 'In partnership with'. Four speakers are listed with their photos and titles: Roland Daccache (Team Leader - Sales Engineering CrowdStrike META), Karan Challa (IT Security Manager SBM Bank), Anthony Muiyuro (Associate Director, Cybersecurity, Privacy & Trusted Technology - EY East Africa), and Cynthia Karago (Moderator, CISO, GE Africa). The event title is 'Nairobi - Panel Discussion' on 'Wed 16th of December 15.00-16.30 (EAT)'. Registration details are provided: 'To register: phil@alliances.global' and 'www.alliances.global'. A quote from the moderator asks, 'Adapting effective cybersecurity strategies in today's age of radical digital transformation?'. The CISO Alliances logo is in the bottom right corner.

Sub Topics

- Aligning Security Strategy to Business
- Emerging Threats
- Securing the Remote Workforce
- Back to Basics

Takeaways:

- Security is like a custom recipe and dependent on individual organisation
- 'Dance' between business and key security requirement
- Balancing business and security hats important
- What is the language of the business?
- Security is there if the business is there - Need to understand what the business is doing
- Today's world is digitally connected, so important to identify threat level, criticality to decide what technology of security to deploy
- CIA Triangle - All are interlinked



FOOD FOR THOUGHT /TOPICS DISCUSSED



- Cyber Security is a big enable to the business - Board Agenda
- Phishing potential with WFH outside of protected environment
- 1st half of 2020 saw more than whole of 2019 with 41,000 attempted intrusions, mainly financially motivated



- Challenges of building human firewall - Psychology surrounding emotions heightened
- Ensuring that security is replicated across all systems and end points
- End points haven't changed so correct deployment paramount
- Solution Simplicity - 95% of attack should be absorbed by end point with threat intelligence in place to support gap



- Exploring more modern/adaptive solutions that are not confined to data centre - Becoming more pre-emptive
- Indication of Compromise (IOC) - Ability to publish threat on a global basis within minutes



Questions & Audience Comments



- "Movement to cloud compromised by local laws , and regulations"
- Hacking v/s cracking - Can you clarify the difference?
- What are your views on OT and implementation of new technology to legacy systems?



- On the stages of hacking, is it possible many organisations are experiencing reconnaissance and scanning phases without their consent?
- "I'm interested in the panellists views on the recent Google outage in light of increased attention to and dependence on cloud."



- How does NIST help , considering technology?
- Would you consider "scaring" your business execs and users a strategy for cyber security awareness . Basically painting a doomsday scenario of a cyber attack



- "Design to influence behaviour ...the attacker are becoming tougher"
- "Over and above security awareness training, we should also implement tools to help prevent common SE attacks e.g URL scanners, anti-phishing tools to scan input forms etc"



- "Monitoring using endpoints is the best option to mitigate hacking(ransomware)"
- "Message to execs is using business language -customer impact if systems are unavailable, financial loss should a breach occur including penalties from regulator (this can be used to counter the budget for security), etc.



- Todays modern eCrime and ransomware threats are cruising through the traditional security stack. What is the most reliable and cost-efficient approach to combat these sophisticated attacks?



- What are the benefits of your cloud focused approach as CrowdStrike?
- "Criminals are collaboration, we as industry professionals must do the same to stay ahead of the curve"