CISO Alliances

Nairobi Chapter

21st April 2023

ALLIANCES PROJECTS

UNITING STRENGTHS

EXPANDING OPPORTUNITIES

Alliance - ‘A union formed for mutual benefit’

Community – ‘1: a unified body of individuals: such as. A: the people with common interests living in a particular area broadly: the area itself the problems of a large community’

ALLIANCES PROJECTS

UNITING STRENGTHS

EXPANDING OPPORTUNITIES

Executive Business Exchange

DPO Alliances

CIO Alliances

CISO Alliances

CXO Alliances

CMO Alliances

CDO Alliances

CISO Alliances

Foreword

Karibu Team,

It is great to once again returning to Nairobi for todays in person CISO Alliances Nairobi.

The pandemic has naturally shifted the way of thinking, BCP and the adoption of the 'virtual' world, so I would like to firstly thank you for your continuous involvement as community members and your time investment into attending today's chapter.

As we all know the threat landscape is an ever-evolving space where we as a group of IT and Infosec leaders are either one step ahead or one step behind the threat actors. Today's agenda has been formulated around the issues highlighted by you as a group, so please do continue to influence and advise.

The CISO Alliances mantra is to ensure that these end user driven meets, are purely focused around the educational and requirement needs of everyone involved.

With you all having security and operational responsibility 'Protecting the 'Crown' Jewels', the aim of today and future programmes is to share best practice, benchmark strategies and more importantly have very open and candid debate around issues being faced.

All CISO Alliances activities operate under strict Chatham House Rule to ensure we have a trusted and confidential environment.

Without sounding like a Roman Emperor this is a 'for the people, by the people' initiative so I actively encourage open debate and opinion throughout the day.

I look forward to a very insightful day.

Asante,

Phil Manny
Regional Director – CISO Alliances Egypt | Ghana | Kenya | Nigeria

09:00

Registration and Networking

09:30

Session 1 - Group Workshop

“Open AI – Our friend or Foe?”

Session Moderator: Michael Michie

10:30

Networking Break

11:00

Session 2 - Open Forum

Strengthening Cybersecurity with Defense in Depth Approach

- Trevor Coetzee, Regional Director Sub-Saharan Africa – Palo Alto Networks
- Nikunj Haria, Pre-Sales Manager – Westcon-Comstor

12:15

Networking Lunch

13:45

Session 3 - Group Roundtable

Ransomware – What is the real impact???

14.45

Networking Break

15:00

Session 4 - End User Perspective

“MTD – Leveraging Uncertainty for Cyber Defense”

Session Moderator: Cephas Okal, ICT Manager – Sumac Microfinance Bank Ltd

Panellists:

- Samuel Kahura Wachira, CISO – CIC Insurance
- Kevin Kiereini, Regional Head of IT – East Africa – Jumia
- Geoffrey Munga, Senior Manager Cyber security – Safaricom

16:00

Interactive Discussion

Post Panel Discussion

16:45

Post Session Social

Post Alliances Networking

CISO Alliances

Chapter Agenda

CISO Alliances

Nairobi Chapter
April 2023

ALLIANCES
PROJECTS
UNITING STRENGTHS
EXPANDING OPPORTUNITIES

Use Case Partner

paloalto NETWORKS | f5

Westcon Comstor

Networking Lunch Partner

verto

Networking Partner

Pebble Africa Technologies Limited
Your IT Consulting partner

Use Case Partner

Trevor Coetzee
Regional Director - Sub Saharan Africa
Palo Alto Networks

Collins Emadau
Practice Lead
Westcon

Fiona Malmqvist
Commercial Sales Manager
Palo Alto Networks

Norbert Siteyi
Regional Sales Manager - East Africa
Westcon-Comstor

Nikunj Haria
Presales Manager
Westcon-Comstor

Westcon Comstor

paloalto NETWORKS

f5

Our tightly-aligned portfolio of Security solutions from the world's leading vendors provide the threat intelligence and advanced, end-to-end protection across the network that customers need to safeguard sensitive data, secure critical business systems and ensure business continuity.

Partner Success is what we do.

Westcon Comstor

Community Attendees

Andy Chadwick
Head of Africa Cyber Network
FCDO

Anthony Nthiwa
IT Infrastructure Manager
CMC MOTORS

Cephas Okal
ICT Manager
Sumac Microfinance Bank Ltd

Chumari Wachaga
Group Head of IT /CIO
AutoXpress Group

Cyrus Kamau
Deputy Director and Chief Analyst,
Infrastructure and ICT
NATIONAL COMMISSION FOR
SCIENCE, TECHNOLOGY AND
INNOVATION. (NACOSTI)

David Kitonga
Global IS Manager
Oxfam

Dennis Rono
Manager - IT Operations
AutoXpress Limited

Emily Muragari
Consultant, Information Security
Transunion Bank

Emmanuel Mose
ICT Specialist
AERC

Community Attendees

Eric Ngei
Senior Manager, Cybersecurity
KCB Bank Group

Ferdinand Ragot
IT Manager
Inchcape Kenya

Fredrick Endeki
Regional Head of ICT
Ministry of Health, KMTC

Geoffrey Munga
Senior Manager Cyber security
Safaricom

Godfrey Machio
Data Protection Officer
Family Bank

James Tindi
ICT Infrastructure and Security Lead
Sumac Microfinance Bank

Joseph Okumu
Manager-ICT
Kenya Association of Manufacturers

Julius Caragu
Information Security Officer
Madison Group Kenya

Kevin Kiereini
Regional Head of IT - East Africa
Jumia

Community Attendees

Laban Nyarera
CISO
Family Bank

Lewis Mwiti
Group Systems Admin
Madison Group Kenya

Michael Michie
CISO Alliances Member

Michael Etale
Cyber Security Manager
ABSA Bank Kenya

Oscar Ashihundu
IT Risk Officer
Co-operative Bank

Rakesh Ravindran
CISO
Diamond Trust Bank

Samuel Kahura Wachira
CISO
CIC Insurance

Stanley Githae
Head IT
Chai Sacco Society Ltd

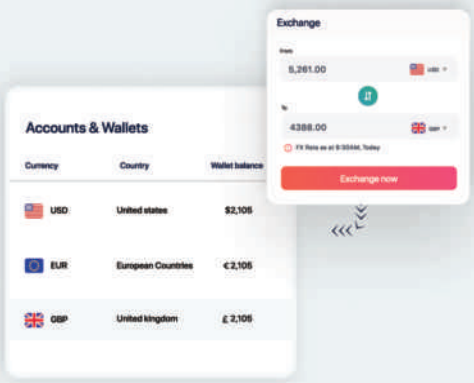
Timothy Were
Deputy Director ICT
Govt. of Kenya

verto

Simplifying cross-border payments for businesses

Collect

Collect payments in up to 25 currencies



Convert

Convert up to 51 currencies

Pay

Payout globally to 190+ countries

www.vertofx.com

Workshop

09.30 - Session 1

“Open AI – Our friend or Foe?”

Session Leader
Michael Michie, CISO Alliances Member

Session Overview and Synopsis:

Unfortunately, AI can be used by criminals for a variety of illegal activities. As with any technology, AI has both positive and negative applications, depending on how it is used.

We will kick start the day with a group workshop where we divide into sub-groups and debate:

1. Cyberattacks: Criminals can use AI to develop sophisticated malware that can bypass security measures and infiltrate computer systems.
2. Fraud: AI can be used to create realistic fake identities, which can be used to commit identity theft and financial fraud.
3. Social engineering: Criminals can use AI-powered chatbots to engage with potential victims and trick them into revealing sensitive information or performing actions that benefit the criminal.
4. Deepfakes: Criminals can use AI to create convincing deepfake videos and images that can be used to blackmail or extort individuals.

Session Outcome:

- A collective response of perspectives

Takeaways

During the session Michael introduced the discussion and observations around the rapidly evolving AI landscape and the debate of "Open AI – Our Friend or Foe?"

"Our newest employee without a contract…"
"Good but needs hand holding"

This was followed by a group workshop activity splitting the attendees into 7 teams in order to debate the following 5 questions and present back findings and gain a collective response.

Question 1

What are we doing to safeguard our organisations again public facing AI?

Findings/Debates:

- **Monitoring of AI as a new concept – Good and bad traffic**
- **We cannot block it so there is a need to sanitise and educate**
- **Define access policy - Risk appetite should be included in process**
- **Implementing of administrative control, technical controls and monitoring**
- **"This is a tough questions as there are so many AI tools and many use the likes of Chat GPT for their job – the only action is to create awareness**
- **Define awareness before policy – For technical departments awareness needs to go deeper**
- **Structure DLP accordingly**
- **Knowledge at present is limited so a lot of research is needed to allow for best advice**

Question 2

What are some of the steps and precautions do you feel should have for best practice?

Findings/Debates:

- **Ensure code is secure**
- **How to prevent abuse?**
- **Remember AI in insentient i.e. Chat GPT has been used to create malware**
- **Data should not be balanced – Unconscious bias**
- **Range of considerations for security control:**
- **Build audit trails**
- **Privacy of data of feeding into tools**
- **Constantly review tools - as adaptable**
- **Data validation and privacy should be at the forefront**
- **Platform Security**
- **Option of blocking or training for users as well as builders (implement malicious intent intelligence)**
- **Quality of data – We should start working on it now so when we need it, it is cleansed.**
- **The element of consent and permission**
- **How do we test and trial?**

Takeaways

Question 3

Regulations – Should AI be regulated?

Findings/Debates

- **It definitely should be, however regulations should be proactive as opposed to reactive**
- **Who is responsible for regulating and how will we do it?**
- **What will be the regulation parameters?**
- **How can it work for you?**
- **Should we regulate ourselves?**
- **The process will need to be controlled**
- **Does a regulation need to be by own organisation, country or industry?**
- **How would regulation work with other languages?**
- **How to regulated harmful AI**

Question 4

How much autonomy should you allow for AI?

Findings/Debates

- **Autonomy should be allowed**
- **It needs to controlled within organisations, ensuring limitations and adequate reviews**
- **We need to factor in the issues or morals and ethics**
- **Autonomy should NOT be allowed just yet**
- **Autonomy need to related and flexible in line with specific verticals**
- **Autonomy should be used a much as possible but with built in safeguards**

Question 5

Is AI our Friend of Foe?

Findings/Debates

- **Both – It depends on how it is used and the intention**
- **50/50 – Intention is the driver**
- **It is our friend**
- **Like any intelligent solution (weapon) in the wrong hands it will be abused**

Takeaways


CISO Alliances
Nairobi Chapter
21st April 2023
Use Case Partner
paloalto
Westcon Comstor
Networking Partner
Pebble Africa Technologies Limited
Radisson BLU
HOTEL & RESIDENCE

Open Forum

11.00 - Session 2

Session Overview and Synopsis: Zero Trust Principles – Best Practices & Real-World Applications

Zero trust and layered security are two different concepts but are often used together to improve the overall security posture of an organization.

Zero trust is a security concept that assumes that all users, devices, and applications, both inside and outside of an organization's network, are untrusted until they are verified and authenticated. This means that zero trust security operates on the principle of "never trust, always verify." In practice, this means that access to resources is restricted to only those users and devices that have been verified and authorized to access them.

Layered security, on the other hand, is a strategy that involves implementing multiple layers of security controls to protect an organization's assets. This approach recognizes that no single security measure can provide complete protection against all types of threats. Instead, multiple layers of security are implemented, with each layer designed to detect and prevent different types of threats. This approach also ensures that if one layer of security is breached, there are other layers in place to provide additional protection.

Session Outcome:

- How combining zero trust and layered security can create a comprehensive security strategy that provides multiple layers of protection while also ensuring that only verified and authorized users and devices are allowed to access sensitive resources.
- How this approach can help organizations reduce their overall risk and improve their ability to detect and respond to security incidents.

Takeaways

Presentation focused on;

1. **The benefits and challenges of implementing a Zero Trust security model and its importance in today's threat landscape**
2. **The key principles of Zero Trust, including identity verification, access control, and continuous monitoring**
3. **The key principles of Zero Trust, including identity verification, access control, and continuous monitoring**
4. **The challenges of implementing Zero Trust, such as the need for cultural change, legacy systems, and complex environments.**
5. **The best practices for implementing Zero Trust, including collaboration across departments, continuous testing, and automation.**
6. **The importance of network segmentation and micro-segmentation in Zero Trust**
7. **The use of advanced analytics and threat intelligence in Zero Trust security**
8. **The impact of Zero Trust on compliance and regulatory requirements**

It was noted of importance the need to foster cultural change in implementing Zero Trust, with emphasis on the need to shift the organizational mindset from a perimeter-based security approach to a Zero Trust approach that assumes all access requests are potential threats.

Key takeaway was the importance of a phased approach to implementation. Starting with a pilot project, identify the most critical assets and applications, and gradually expand the Zero Trust model to the entire organization.

Overall, the Zero Trust roundtable discussions provide a valuable opportunity to share knowledge, collaborate, and advance the implementation of Zero Trust security strategies. It was unanimously agreed by working together, organizations can improve their security posture and better protect themselves against advanced cyber threats.

Takeaways

Group Roundtable

13.45 - Session 3

Ransomware – What is the real impact???

Session Overview and Synopsis:

The impact of ransomware can be significant and far-reaching, both for individuals and organizations.

These include:

- Financial impact:
- Operational impact:
- Security impact:
- Psychological impact:

During the group discussion we will address the above impacts and explore the proactive measure needed to prevent such attacks.

We will conclude with a 'Quiz' to include prizes for the team with the best score.

Takeaways

The impact of ransomware can be significant and far-reaching, both for individuals and organizations.

These include:

- **Financial impact:**
- **Operational impact:**
- **Security impact:**
- **Psychological impact:**

During the session we conducted an exercise of gamification splitting the attendees into 2 teams to compete for the opportunity to win some prizes.

The aim was explore the real impacts and proactive measures needed to protect.

- **Team 1 named themselves - "The Winning Team" (Confidence was high)**
- **Team 2 names themselves – "D2G – Data Guardian Guild"**

Outcomes

Financial impact

Direct

- **Payment of ransom**
- **Legal litigation**
- **Fines**
- **Recovery cost**
- **Share price impact**
- **Increased cyber security insurance costs**
- **Incident response cost - Security investment**
- **People**
- **Technology**
- **Panic buys / hires**

Indirect

- **Loss of revenue**
- **Reputational loss**
- **Loss of stakeholder confidence**

Operational impact

- **System downtime**
- **Data loss for organisations**
- **Denial of service to both staff and customers**
- **Reallocation of resources away from other projects and core functions**
- **Risk of being re-attacked at the point of rebuilding**
- **Reduced operational capacity**
- **Time investment in demonstrating the attack to regulators**
- **Idle staff resources**
- **Process flaws or gaps e.g Department silos**

Takeaways

Security Impact

- Data loss (availability, confidentiality, encryption release
- IP theft
- Security overload
- Repeat and persistent attacks
- National Incidents
- Opens up avenues for internal fraud to the system

Psychological Impact

- Investor Confidence
- Personal confidence
- Emotional stress
- Litigation process
- Potential job loss
- 'Blame Game' around loopholes leading to incident
- Undermining of staff and skill set - Many may be:
  - Looking for other employment
  - Be paranoid
  - Suspicious of the work environment

Measures to be considered?

- Awareness training – Inclusive of staff and board level education (Building the human firewall)
- Implementation of zero trust framework
- Air gapped backups
- BCP Test
- Attack simulation test /table top simulation
- Incident response plans
- Crisis management plans – policies & procedures
- Managed defence – extended defance & response
- Layered security approach – controls on top of other controls to develop defence in depth
- Monitoring IOC (indicators of compromise)
- Getting cyber security insurance
- Patch absolutely everything
- Security assessment for 3rd party vendors
- Resource development and skilling up of team

Takeaways

CISO Alliances

CISO Alliances Chapter

21st April 2023

www.alliances.global

ALLIANCES PROJECTS

End User Perspective

15.00 - Session 4

“MTD – Leveraging Uncertainty for Cyber Defense”

Session Leader

Cephas Okal, ICT Manager – Sumac Microfinance Bank Ltd

Session Overview and Synopsis:

Moving Target Defense (MTD) is the concept of controlling change across multiple system dimensions in order to increase uncertainty and apparent complexity for attackers, reduce their window of opportunity and increase the costs of their probing and attack efforts. Moving target defense (MTD) has emerged as one of the game-changing themes to alter the asymmetric situation between attacks and defenses in cyber-security. MTD is distinguished from the traditional reactive defense by the fact that it can move one or more system attributes continually. The ability of MTD can be implemented in one of the three layers (software, running platform, and physical network) or more.

Touch Points:

- How MTD reduces the need for threat detection
- How MTD enables us to create, analyze, evaluate, and deploy mechanisms and strategies that are diverse and that continually shift and change over time to increase complexity and cost for attackers
- How MTD can limit the exposure of vulnerabilities and opportunities for attack
- How MTD can increase system resiliency

Takeaways

Moving Target Defense (MTD) is a dynamic cybersecurity strategy that aims to proactively protect computer systems, networks, and data by constantly changing their attack surface.

By employing techniques such as randomization, diversification, and adaptation, MTD confounds attackers by making it difficult for them to gain a foothold and exploit system vulnerabilities.

This approach is in stark contrast to the traditional, static nature of security measures that rely on fixed configurations and predictable patterns.

MTD disrupts the asymmetric advantage that attackers often hold, as it forces them to deal with a constantly evolving and compromised target, increasing the complexity and cost of an attack, and ultimately enhancing the overall security of the operating system and the defended system.

How Does Moving Target Defense Work?

MTD introduces unpredictability, uncertainty and complexity to the system, disrupting the attacker's ability to gain control of a foothold and maintain a stable connection with their target. The key principles of MTD are randomization, diversification, and adaptation. Here's an overview of how MTD works in practice:

1. **Randomization: MTD uses randomization techniques to introduce uncertainty and variability into the system. For example, it may randomly change IP addresses, port numbers, or memory locations, making it difficult for attackers to predict the system's configuration.**
2. **Diversification: MTD employs diversification to create heterogeneous environments, reducing the chances of a single vulnerability being exploited across multiple systems. This can involve using different software versions, operating systems, or hardware components to minimize the potential impact of an attack.**
3. **Adaptation: MTD continuously adapts and reconfigures the target environment in response to threats or changes in the system's state. This dynamic behavior makes it challenging for attackers to maintain a persistent presence within the system and increases the time and effort required for them to execute a successful attack.**
4. **Monitoring and Analytics: MTD relies on monitoring and analytics to detect anomalies and potential threats in real-time. By analyzing system behavior and network traffic, MTD can identify indicators of compromise and quickly adapt the system to counter the identified threats.**
5. **Integration with existing security measures: MTD works alongside traditional security measures, such as firewalls, intrusion detection systems, and antivirus software, to create a more comprehensive and resilient cybersecurity strategy. By combining MTD with these established security measures, organizations can better protect their systems, networks, and data from evolving threats.**

Takeaways

Case Study Example:

An organisation who static security solutions:

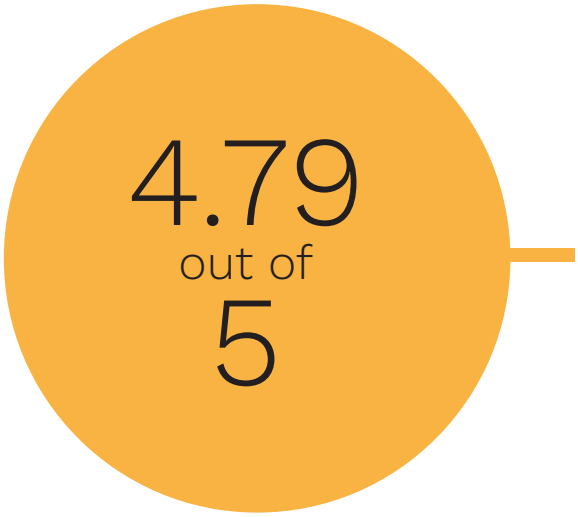
- **Network Security**
- **Server Security**
- **Application Security**
- **End user security**

The system is in place including a perimeter firewall; however, modules are segregated to allow for several 'roadblocks' to stop attackers.

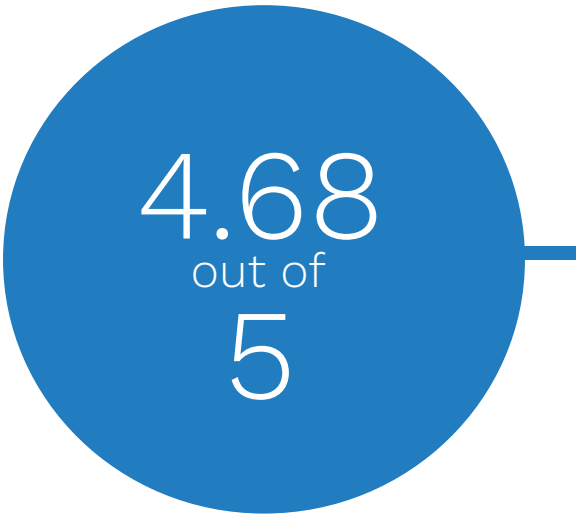
The example discussed the issue and problems around patching. 80% generally use MS in their environment which notoriously uses quick fixes. Therefore, it is important to run a test on patches as the questions lies – Do you have time or the correct environment to deal with a multi-attack scenario?

Curative suggestions were based on having a security solution that offers virtual patching and can be immediately deployed without fear of breaking or causing any regression issues as is synonymous at present.

Chapter Scores



Chapter Overall Experience Scored by the Community



Chapter Format Scored by the Community

WHAT TO EXPECT

Alliances - A union formed for mutual benefit
Everyone is expected to contribute

Access to a community of peers to benchmark, support and debate

Non-discriminatory community on race, gender, age, vertical experience

Community First, Commercials Last

An opportunity to engage on the Chat forum, Digital Alliances Chapter and Physical Chapters

WHAT WE EXPECT

This is a supportive environment for progression and growth

You do not directly benefit from topics being raised but, have experience within the topic:
1 - Share your knowledge
2 - Bring forward themes / topics that matter to you and your business objectives

Suggest and recommend peers to broaden the perspectives within the group

Constructive comments rather than opinionated are provided. Back up your opinion

If there is a potential eventuality of commercial gain for the organisation you work for, you will be expected to pay to play to help sustain the Alliances and their activities.

THANK YOU
WE HOPE YOU ARE ENJOYING THE JOURNEY