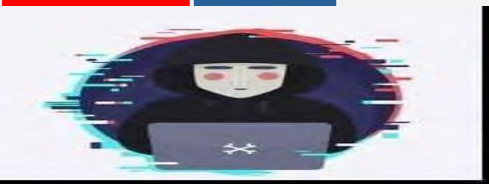

CYESEC TECH
CYBER SECURITY & ESOLUTIONS

Lead Faculty and CEO, **Red & Blue Team overall Lead**, Certified Profesional in Offensive and Defensive Security HND || BSC || CCNA || CEH || CCSA || CPENT || CDFA || Cyber Security & Forensic Analyst



RED TEAM VS BLUE TEAM

TWO DIFFERENT ROLES IN HACKING

follow @thehardsecurity

Which team you'll join? Comment!

RED TEAM

- Offensive Approach
- Exploit vulnerabilities
- Do Social Engineering
- Performs Pentesting
- Ethical Hacking
- Web App Hacking

BLUE TEAM

- Defensive Approach
- Damage Control
- Threat protection
- Incident Response
- Infrastructure security
- Digital Forensics

PROACTIVE CYBERSECURITY STRATEGIES AND EVOLVING CYBERSECURITY TOOLS FOR ATTACK PREVENTION

Introduction: Proactive Cybersecurity Strategies is an essential survival guide for security leaders and organizations. Some evolving cybersecurity tool for prevention are continuation focus to develop more cyber awareness in this case, through key insights from leaders in the field and help close the cyber skills gap by exposing more women to the industry. The result is a collaborative team effort involving many diverse cyber leaders and experts from government and the private sector.

New threats are emerging regularly; estimations show 300,000 new types of malware being identified daily. The cost of carrying out a cyber attack is decreasing, and the number of incidents is building up. The average cost of just one of these attacks is over $380,000. Small-and-medium-sized businesses spend an average of $1.2 million following cybersecurity incidents while 60% of these small businesses were forced to close within six months of the attack because of the huge financial toll as well as the damages associated with staff laziness and greed to cyber-attacks exposure within workspace.

The good news is, these attacks can be relatively predictable with a strong security posture installed, such enterprises can address security threats reliably.

WHY YOU NEED TO TAKE A PROACTIVE APPROACH TO CYBERSECURITY

Alongside the development of the world,organizations have started to interface more of their processes to cyberspace.

A company’s reputation, intellectual property (IP), staff, and customers are at risk of being compromised if not the properly protect their assets, enterprise data and businesses image with need to a solid cybersecurity strategy installed.

PROACTIVE VS REACTIVE CYBERSECURITY

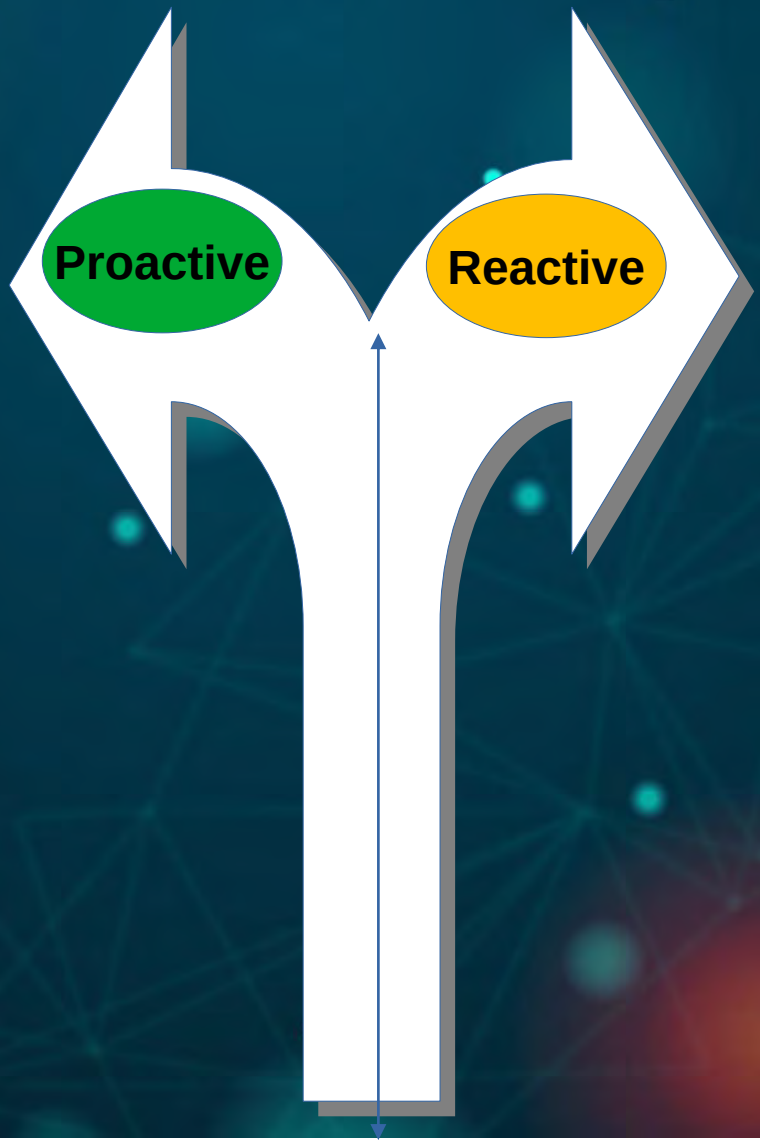
Proactive cybersecurity involves preemptively identifying and addressing security weaknesses and threats before an attack occurs. n the other hand, reactive cybersecurity involves responding to cidents that have already happened.

while there is no replacement for a solid, reactive, cybersecurity defense strategy that focuses on the core est practices of patch management.

Once a security incident has occurred, the damage is already done. The data loss, cost and time to fix the impact and the potential downtime of any system have already caused financial reputation, or other losses to e client and business.

Majority of today’s cybersecurity practices are reactive.
Most organizations are not adequately prepared against cybersecurity incidents until it is too late; they wait for cybersecurity incident to happen before they take action.
However, having a proactive approach to security rather than reacting to every new threat can be time-saving and cost effective.

A proactive approach to cybersecurity defensive measures is the best approach to make sure there is little to no room for attackers to exploit the network.



THE NECESSITY OF A PROACTIVE APPROACH TO CYBERSECURITY

Even though businesses have taking a more proactive approach to cybersecurity, they are still far behind in cybersecurity preparedness. An IBM study revealed that 48 ercent of surveyed IT security practitioners reported a data breach that resulted in the loss or theft of more than 1,000 records that contained sensitive or information.

The reactive approach may save clients initially, but eventually, it will increase costs and ultimately result in a damaged reputation. The cost of responding to a single public vulnerability is almost more than being originally prepared for one. Furthermore,harsher regulatory penalties are eing doled out for not properly securing third-party data and igital information.

On the other hand, a proactive approach will help organizations define a baseline level of cybersecurity; this will engage any security team with guide against threats and notify the heads on available countermeasures to deploy before corrective action in real-time.

The level of specificity and actionable intelligence that accompanies critical alerts helps cybersecurity experts pinpoint and remediate a problem so much faster through proactive awareness training programs, workshops, practical approached and essential usability of the state of act toolkits to combat cybercrime and deployed countermeasures.

National Cybersecurity Policy And Strategy 2021

In all it chapters, chapter 9 ASSURANCE MONITORING AND EVALUATION

9.1 Standard and Good Practices

9.2 Quality Control and Security Processes

DEFENCE-IN-DEPTH TO DEFENCE-IN-CONCERT.

Defence-in-depth is no longer fit for purpose. A new approach of defence-in-concert is your best chance to stop threats.

HOW

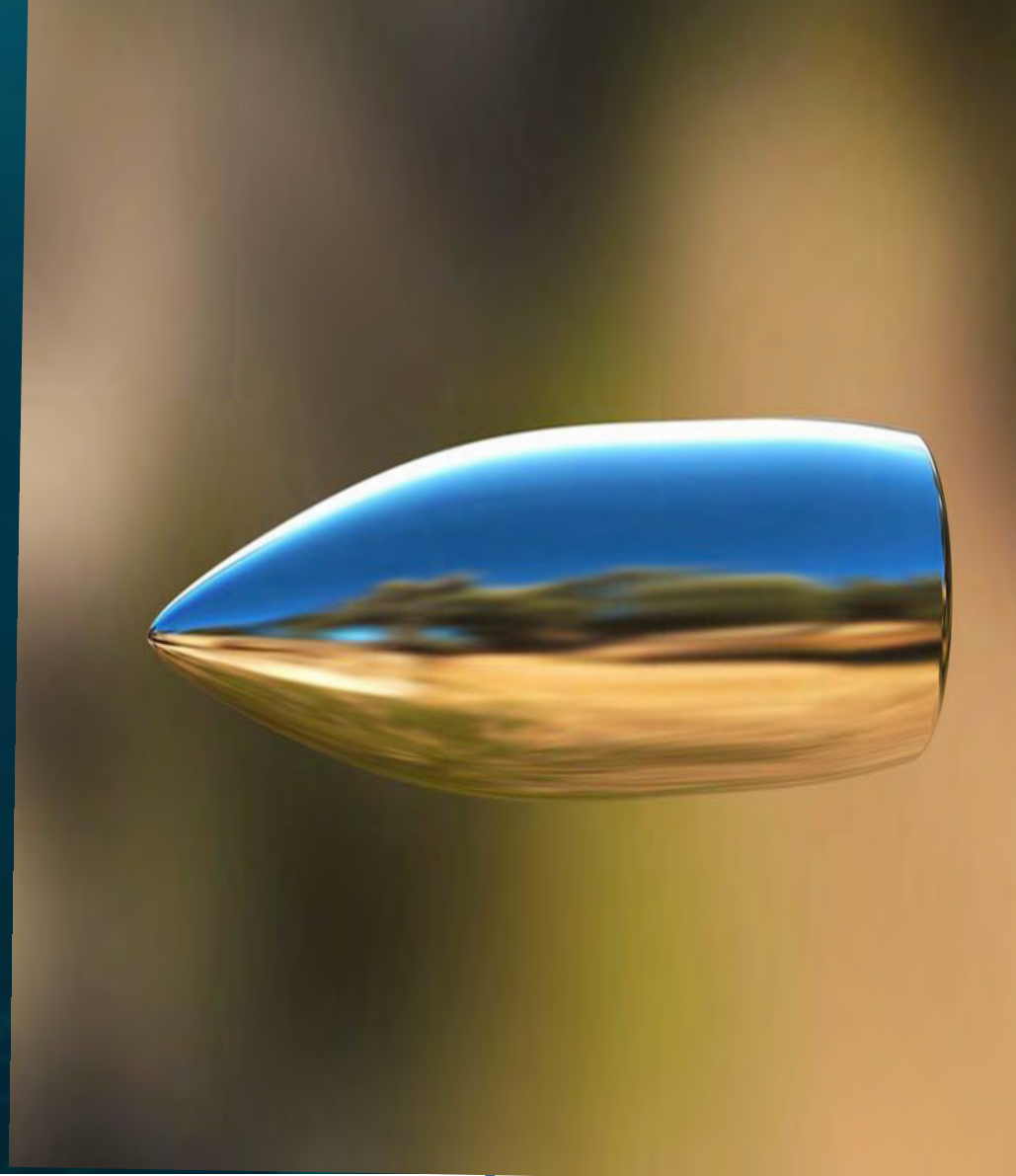
The Defence-in-Depth approach (DiD) refers to an information security approach in which series of security mechanisms and controls are thoughtfully layered throughout a computer etwork to protect the confidentiality, integrity, and availability of the network and the ata within an organization.

An effective DiD strategy may include these (and other) security best practices, tools and policies.

Network Segmentation,
Endpoint detection and Response(EDR)
Patch Management,
Intrusion Prevention or Detection System (IDS/IPS)
Firewall and Password

WHY DOES IT MATTER?

There is no silver bullet in cybersecurity, however, a DiD strategy ensures network security is redundant, preventing any single point of failure.
DiD strategy significantly increases the time and complexity required to successfully compromise a network, which further drains the resources of engaged cyber threat actors and increases the chances that an active attack is identified and mitigated before completion.



A DiD approach is routinely practiced in physical security when trying to protect valuable equipment or other material assets. For example, election offices often have a chain of custody logs, security cameras, and locks within the physical elections environment to protect elections equipment and associated infrastructure. In the banking world, security cameras,ballistic glass,and vaults are used to protect assets and personnel.

N/B: The question now is who cares about those staff members how are sacked because of one mistakes or the other?

WHAT YOU CAN DO!

The idea behind defense in depth is to manage risk with diverse defensive strategies, so that if one layer of defense turns out to be inadequate, another layer of defense will hopefully prevent a full breach. This principle is well known, even beyond the security community; for example, it is a famous principle for programming language design: Defense in Depth: Have a series of defenses so that if an error isn't caught by one, it will probably be caught by another.

Defense-In-Concert is a strategic approach to cybersecurity that drives collaboration and contextualization of security data within infrastructure.

Defense-In-Concert can also be a strategic approach to provides an holistic to support corporate initiatives without compromising corporate security architectural infrastructure, Instead of adding more layers, Defense-in- Concert means making sure your existing security tools are all speaking the same language and working in concert.

This approach unifies security tools to deliver comprehensive visibility, leading to a faster, more effective detection and response. Contrast this to point solutions which are often unable to integrate data and drown security team to an overwhelming complex unidentified number of security alerts.

SIGNIFICANT OF DEFENSE-IN-CONCERT

Enables you to:

1,Track threats across your entire ecosystem

2,Validate the severity of alerts through increased context

3, Identify attacks and attackers links by carrying out logical operation and behavior of a directory if it has been compromised or infected by malware files

REALIZING DEFENSE-IN-CONCERT WITH OPEN XDR

Extended detection and response or XDR is a new approach to threat detection and response that provides holistic protection against cyberattacks, unauthorized access and misuse.

1

XDR analyzes security data as a whole, it also enhances threat detection and eliminate the hustle files that can lead to frustration around integrated links and soled point solutions. Though an open cloud-native platform cloud help an organizations benefit from open XDR with improved visibility, enabled by high-fidelity alerts across endpoint, network and cloud environments.

2

Open XDR empowers analysts with a centralized user interface and built-in automation to improve productivity. The simplicity and context of relevant activity in XDR environment allows even junior analysts to achieve more in finding out and reporting the level of SQL injection in the network

3

Open XDR is the shiny new toy that everyone seems to be talking about. Gartner is a management consulting company recently listed XDR as one of the “Top 10 Security Projects for 2021 and 2022.” ESG research revealed that 70% of organizations expressed that they are already using or considering XDR.

EVOLVING CYBERSECURITY TOOLS FOR ATTACK PREVENTION.

XDR TOOL

Network security Monitoring tool

Graphite.

Prometheus.

Zabbix.

Nagios Core.

Monitorix.

Icinga.

Cacti.

Libre NMS.

XDR Features

Encryption Tools: Encryption Protect data by scrambling text so that it is unreadable to unauthorized users , examples of tools including Tor, Keepass, veracrypt, Nocrdlocker, Axcrypt and truecrypt.

Web Vulnerability Scanning Tools : These tool scan web application to identify cross-scripting, SQL injection and path traversal, example of tools including Burpsuite, Nikto, Paros proxy and SQLMap.

Pen Testing Tool
&
Antivirus Software

Network Intrusion Detection (IDS) monitors network and system traffic from unusual or suspicious activity and notifies the administrator if potential threat is detected. Example of tools includes: snort, security onion, solawind security event manager, kisnet and zeek

Packet sniffer

&

Firewall Tools: are Tufin, Algo sec, Firemon and Redseal

PREVENTIVE MEASURES

What is a Zero-Day Exploit?

Zero-day exploits are techniques used by malicious actors to attack a system that has a vulnerability, while the users and developers of the system are still unaware of the vulnerability.

The term “ zero day attack ” refers to the fact that the vulnerability is new and has been known for zero days, or in other words, unknown. Malicious actors, or other parties, might discover a vulnerability and wait to use it strategically, or sell it to others who have the ability to exploit it. Zero day vulnerabilities are extremely dangerous because, by definition, no measures have been taken to remediate or protect against the vulnerability.

4 STRATEGIES FOR DETECTING ZERO-DAY EXPLOITS

Zero-day exploits cannot be identified by traditional signature-based anti-malware systems. However, there are a few ways to identify suspicious behavior that might indicate a zero-day exploit:

1

Statistics-based monitoring—anti-malware vendors provide statistics on exploits they previously detected. Organizations can feed these data points into a machine learning system to identify current attacks. This type of detection has limitations when discovering new threats as it can be predisposed to false negatives and false positives.

2

Signature-based variant detection—all exploits have a digital signature. Organizations can feed digital signatures into machine learning algorithms and artificial intelligence systems to identify variants of prior attacks.

3

Behavior-based monitoring—malicious software uses procedures to probe a system. Behavior-based detection creates alerts when it identifies suspicious scanning and traffic on the network. Rather than analyzing in-memory or signatures activity, behavior-based detection discovers malware by looking at how it interacts with devices.

4

Hybrid detection—a hybrid detection approach uses all three methods mentioned above. It can use all three monitoring and identification approaches to be more efficient at discovering zero-day malware.

When drafting your plan, follow the SANS Institute's six stages of incident response. the plan should specify

I. 1, Preparation
II. 2, Identification
III. 3,Containment
IV. 4, Eradication
V. 5, Recovery
VI. 6, Lessons Learned

Conclusion

Organizations are finding themselves under the pressure of being forced to react quickly to the dynamically increasing number of cybersecurity threats. Since attackers have been using an attack life cycle, organizations have also been forced to come up with a vulnerability management life cycle.
The vulnerability management life cycle is designed to counter the efforts made by attackers in the quickest and most effective way.

As a multi-certified cybersecurity expert with 15 years of field experiential,the vulnerability management life cycle is designed to counter the efforts made by attackers in the quickest and most effective way. We can discussed the vulnerability management life cycle through a practical approached.

Organizations around the globe are realizing how important it is to continually invest in cybersecurity training programs. This investment will ensure that a company remains competitive in the market. Failure to properly secure their assets could lead to irreparable damage, and in some circumstances could lead to bankruptcy. Due to the current threat landscape, investing in protection alone isn't enough. Organizations must enhance their overall security posture. This means that the investments in protection, detection, and response must be aligned.

THANKS

There is no real end in sight, as long as there are cyber criminals, warriors and attacks! The future is 100% CYBER WARFARE in all of its forms I shall continue to hack!

“Dont be my victim I will not expose you but hack you”

RC 1779309

CYESEC TECHNOLOGIES

(CYBERSECURITY & ESOLUTIONS)

New Address: Suite 10, Coffee Shops Complex
National Defense College Permanent Site
Bill Clinton Boulevard, Piwoyi, Abuja

Training Center Address:
Nigerian Army Resource Center Abuja.
Opposite KASCO Market, Mambilla Barracks
Junction, Asokoro, Abuja

cyesec.com.ng cyesec-technologies Cyesec-Technologies
emma_okoi@cyesec.com.ng +2347036740799, +2348168508433

FACULTY/ CEO

EMMANUEL OKOI, HND, BSC, CCNA,CHE, CCSA,CPENT, CDFA

CYBERSECURITY & FORENSIC ANALYST

Website: https://cyesec.com.ng/

+2347036740799