Intelligence Solutions for ~~Cybercrime~~ Management

A session at the Nigeria
Computer Society Cybersecurity
Forum and Workshop

June 2024

Hamzat Lateef

Founder / COO, CyberPlural.

Intelligence Solutions for ~~Cybercrime~~ Management

- Cybersecurity vs Cybercrime vs Cyber Posture Management
- Importance of intelligence-driven cybersecurity in the face of evolving cybercrime threats.
- Prevention – Logging & Protection - Detection & Response – Automation (SOAR / AI/ ML*)
- Overview of common cyber threats, including malware, phishing, ransomware, and advanced persistent threats (APTs)
- Role of threat intelligence in proactive defense and effective cyber posture management
- Little Rants* / Hard Talk -

Threat Intelligence for Cyber Posture Management

Gathering and analyzing data from various sources, such as security alerts, incident reports, dark web forums, and open-source intelligence.

Gathering and analyzing data from various sources

Identifying emerging threats, attack patterns, and adversary tactics, techniques, and procedures (TTPs)

Identifying emerging threats.

Providing actionable insights to security teams, enabling them to make informed decisions and implement appropriate countermeasures.

Providing actionable insights to security teams

Threat Modeling and Risk Assessment

1

Assessing the organization's threat landscape, considering both internal and external factors

Assessing the organization

2

Identifying critical assets, such as sensitive data, mission-critical systems, and key infrastructure

Identifying critical assets

3

Analyzing vulnerabilities and weaknesses that could be exploited by cybercriminals

Analyzing vulnerabilities

4

Prioritizing risks based on the likelihood of occurrence and potential impact

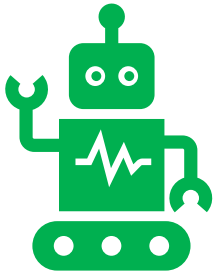
Prioritizing risks

5

Implementing appropriate security controls and countermeasures to mitigate identified risks

Implementing appropriate security controls

Automated Threat Hunting and Analysis



Leveraging AI and ML Algorithms

Leveraging AI and machine learning algorithms to continuously monitor and analyze security events and indicators of compromise (IoCs).

Correlate Security Data

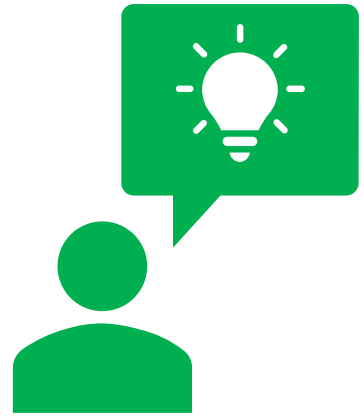
Correlating security data from multiple sources to detect anomalies and identify potential threats

Automate Incident Response

Automating incident response and mitigation processes, reducing the time to detect, investigate, and respond to cyber incidents

Collaborative Intelligence Sharing

Participating in trusted threat intelligence communities, such as Information Sharing and Analysis Centers (ISACs) and industry-specific forums



Enhancing collective defense against cybercriminals by leveraging the collective knowledge and experiences of the security community

Sharing indicators of compromise, attack patterns, and best practices with other organizations

By the Numbers

10 BANKING & FINANCE

9 GOVERNMENT

7 EDUCATION

6 TELECOMMUNICATION

3 INFORMATION TECH.

1 NEW MEDIA

1 CONSTRUCTION

1 TRANSPORTATION

The vast majority of disclosure activities are centered on identifying and addressing vulnerabilities that ultimately lead to unauthorized access to Personally Identifiable Information (PII)

Note **–** Addressing ongoing findings, some affected parties have been unresponsive.

whitehat.ng

https://www.linkedin.com/feed/update/urn:li:activity:7145760289865596928

By the Numbers

7 RANSOMWARE

2 DEFACEMENT

2 PONZI SCHEME CRASHES OFF

2 BREACH & STOLEN FUND

2 PHISHING / DATA COLLECTION

1 DDOS

1 INSIDER THREAT

1 INFO STEALER MALWARE CAMPAIGN

It's evident that ransomware posed a significant threat, while a variety of other cyber incidents also made an impact throughout the year.

whitehat.ng

https://www.linkedin.com/feed/update/urn:li:activity:7145760289865596928

Key Takeaways

Intelligent solutions, including threat intelligence, threat modeling, and automated threat hunting, are crucial for effective cyber posture management

Threat intelligence enables proactive and adaptive security measures, allowing organizations to stay ahead of evolving cyber threats

Collaborative intelligence sharing strengthens the overall cybersecurity posture by facilitating the exchange of valuable information and best practices

Implementing a comprehensive, intelligence-driven cybersecurity strategy is essential for organizations to combat the growing threat of cyber attacks.

Little rants*/ HARD TALK

- Focus on awareness, less of technical implementation [basics are missing], jumping into automation……..
- Products/ Technology other than the basic is NOT a strength going forward….
- People truly are shamed of how most of the cyber incidents happened…..
- Conferences and workshops that should ignite collaboration in real time have also been turned to checklist marking (and LinkedIn Aspire to Perspire)….
- No ONE currently assume (practical and beyond paper) position of authority to galvanize these support that will bring stakeholders together beyond photo ops objective…..
- We want to copy standard; we don't want be the STANDARD.
- The brain drain thing is already happening in Cyber because people are under paid here, no training, just hire people to fulfill compliance objective…….

Questions and Answers

Extra Resources

- https://blog.cyberplural.com/the-tale-of-a-persistent-threat-actor-monitoring-ops/
- https://www.linkedin.com/feed/update/urn:li:activity:7145760289865596928
- https://blog.cyberplural.com/cyberplural-annual-cybersecurity-report-2023-key-insights-and-trends/
- https://github.com/ngwhitehat
- Report using - incident@cert.gov.ng , cert@projectwhitehat.ng cert@nitda.gov.ng
- https://github.com/ngwhitehat/Nigeria-Cyber-Incidents