aliv business

CYBER SECURITY SUMMIT 2026

CYBER RESILIENCE

DEFENDING THE DIGITAL FRONTIER

EMPOWER, PROTECT, EVOLVE

Who am I?

- Offensive Security Researcher: I love everything **Hacking**
- **Tribe of Hackers**: Blue Team 2020
- **Global Advisory Board**:
  - EC-Council for **C|TIA & C|PEN**
  - USIU-A ICT
  - Ushahidi
  - CyberSafe Foundation
- Blockchain Investigator
- Senior Technology Advisor to the Attorney General of Kenya
- **C.E.O Cyber Guard Africa**
- **Founder** of Cyber Collective, **Africahackon**
- Presented at over 420 Cyber Security conferences
- **Adjunct Professor,** Cyber Security - **Strathmore University**
- Practice Kung Fu

CYBER GUARD
AFRICA LIMITED

WHY CYBERSECURITY IS PERSONAL

IT'S NOT JUST ABOUT DEVICES, IT'S ABOUT:

- Your reputation and relationships
- Your financial security
- Your privacy and personal information
- Your professional opportunities
- Your peace of mind

UNDERSTANDING YOUR DIGITAL POSTURE

RAISE YOUR HAND IF YOU'VE;

Used the same password for multiple accounts

Connected to public WiFi without thinking twice

Clicked a link in an email or whatsapp message without verifying it

Posted something online you later regretted

Ignored a software update for weeks or months.

THE DIGITAL RISK LANDSCAPE

- Data breaches of services we use
- Password theft
- Social engineering
    - Phishing attempts (impersonation, scam emails)
- Malware and Ransomware
- Oversharing Personal information

JUST LIKE YOU LOCK YOUR FRONT DOOR, YOU NEED DIGITAL LOCKS TOO

THE AI THREAT LANDSCAPE

01

Proliferation of Conversational AI

Chatbots, AI avatars, voice assistants, video synthesis

02

Rapid Integration Across Sectors

Finance:
Voice banking

Healthcare:
AI teleconsultation

Customer Service:
automated call agents

03

Explosive Growth of Deepfake and Voice Cloning Tools

Freely accessible tools (many without accounts or payment)

Example: HEDRA and others fueling misuse

“Amateurs Hack Systems Professionals Hack People”

What do we leave out there for our lives to be targeted?

Names (both real and usernames) - you leave them everywhere

IP addresses - Browse a site and it is left there

Browser fingerprint - You accept all cookies

E-mail address - Can be retrieved everywhere

Location (exact or approximate) - What is Triangulation?

Phone numbers - The Guard book, Remember?

Date of birth (or any other PII) - Social Media posts

Stylometry - You have a pattern

Facial recognition - AI is here to stay

Hak5 Kit

DEAUTHER

FLIPPERZERO

Om.G
Cable

Crazy Radio

LIVE HACKING DEMO: How a Cyber Criminals steals your DATA

LIVE DEMONSTRATION:
A WALKTHROUGH OF A “MODERN DAY” ATTACK

Open Source Intelligence

Google, Shodan, Social Media, OSINT Industries

Email account spoofing

Exploited in the wild for Phishing

Account Compromise by a Cyber Criminal

Demonstration of how a cyber criminal takes over your life

Remediation Processes for an organization

Remediation Processes for an individual

HOW TO STAY SAFE

Credentials Protection

✓ DO'S

- ✓ Create passwords that are long and strong, using at least 8-12 characters, upper- and lowercase letters, numbers, and symbols but should be a PHRASE
- ✓ Change your password often. (General rule of thumb: Change passwords every 90 days)
- ✓ Use a password manager (MIRCOSOFT/GOOGLE PASSWORD MANAGER, DASHLANE,1PASSWORD,BITWARDEN)

✗ DON'TS

- ✗ Use information that can be easily found about you online or otherwise.
- ✗ Share passwords with others.
- ✗ Store your passwords online.
- ✗ Use any part of your Social Security Number, birth date, or other personal data when creating passwords.

Commands and Tools

1. site:ke filetype:xls salary - simple google search to find out all xls sheets that has the word 'salary' on all kenyan website
2. pimeyes.com - reverse image search to find details about where your picture has been used
3. maltego - tool for information gathering about a phone number, email or company
4. https://fakeinfo.net/fake-whatsapp-chat-generator - For generating fake information
5. https://www.metadata2go.com/ - Check metadata of files (media and all file types)
6. https://www.security.org/how-secure-is-my-password/ - check to see how strong is your password
7. https://bitwarden.com/ -- Best password manager
8. https://www.lastpass.com/ ----avoid avoid avoid
9. https://www.virustotal.com/ - check files and links for malicious content
10. https://joindeleteme.com/ or https://www.optery.com/ - Helps to delete data from the internet that has been collected by Data brokers
11. https://joindeleteme.com/ or https://incogni.com/ or https://www.optery.com/ - remove personal data from the internet and data brokers
12. https://socradar.io/blog/top-10-ai-deepfake-detection-tools-2025/ - Deepfake detection tools

SECURING YOUR DEVICES

- Use wireless networks you trust else HOTSPOT your mobile phone
- Avoid using public computers (even at friends)
- Download legitimate apps from legitimate sources.
- Use https sites
- Don’t click on links or attachments from unknown sources (especially when they are zipped with password protection, look at the email again)
- Don’t click on ad banners or websites you don’t know about or install AD Blockers (AD Block Plus)

Reduce your digital footprint

- Too much information online can be used against you
- Be very selective about the information you choose to share on social media and with whom you choose to share it. (Even the requests you receive)
- Keep personal information private (home address, phone number, and birthdate)

Extra Caution

- Back up your files to the cloud (google & Microsoft onedrive)
- Keep your computer and mobile phone updated with an AntiMalware solutions (Windows Defender, ESET etc)
- Activate 2 Step verification for all your accounts (Emails & Social Media accounts) and download the backup codes

MORE
INFO

Practical Defense Tactics

Organisational Best Practices

Employee Training & Awareness

- Regular simulation-based awareness sessions

Strong Verification Protocols

- High-value communications shouldn’t rely on casual platforms

Incident Response Planning

- Simulated drills to prepare for synthetic media breaches

Industry-Level Collaboration

Standardization & Regulation

- Governments and industry bodies need to develop formal frameworks

Cross-Industry Partnerships

- Cybersecurity in the AI age is a shared responsibility

Commands and Tools

1. site:ke filetype:xls salary - simple google search to find out all xls sheets that has the word 'salary' on all kenyan website
2. pimeyes.com - reverse image search to find details about where your picture has been used
3. maltego - tool for information gathering about a phone number, email or company
4. https://fakeinfo.net/fake-whatsapp-chat-generator - For generating fake information
5. https://www.metadata2go.com/ - Check metadata of files (media and all file types)
6. https://www.security.org/how-secure-is-my-password/ - check to see how strong is your password
7. https://bitwarden.com/ -- Best password manager
8. https://www.lastpass.com/ ----avoid avoid avoid
9. https://www.virustotal.com/ - check files and links for malicious content
10. https://joindeleteme.com/ or https://www.optery.com/ https://incogni.com/ - Helps to delete data from the internet that has been collected by Data brokers
11. https://support.google.com/websearch/answer/9673730?hl=en

INCIDENT RESPONSE PROCESS

- **Identify and report suspicious activity immediately** - unusual emails, system slowdowns, or unauthorized access attempts should be escalated to IT security without delay.

- **Follow the incident response plan** - know your organization's specific procedures, contact points, and escalation protocols before an incident occurs.

- **Preserve evidence during an incident** - avoid shutting down affected systems or deleting files until security teams can properly investigate and document the breach.

- **Implement strong password policies** - use unique, complex passwords with multi-factor authentication enabled across all accounts and systems.

- **Keep software and systems updated** - regularly install security patches and updates to prevent exploitation of known vulnerabilities.

INCIDENT RESPONSE PROCESS

- **Backup data regularly and test recovery procedures** - ensure backups are stored securely offline and verify they can be restored quickly during an incident.

- **Limit access privileges to essential functions only** - employees should only have access to systems and data necessary for their specific job responsibilities.

- **Staff to recognize social engineering attacks** - phishing emails, pretexting calls, and other manipulation tactics are common entry points for cybercriminals.

- **Monitor network traffic and system logs continuously** - early detection of anomalous activity can prevent minor incidents from becoming major breaches.

- **Establish clear communication protocols during incidents** - designate who communicates with stakeholders, media, and regulatory bodies to ensure consistent messaging and legal compliance.

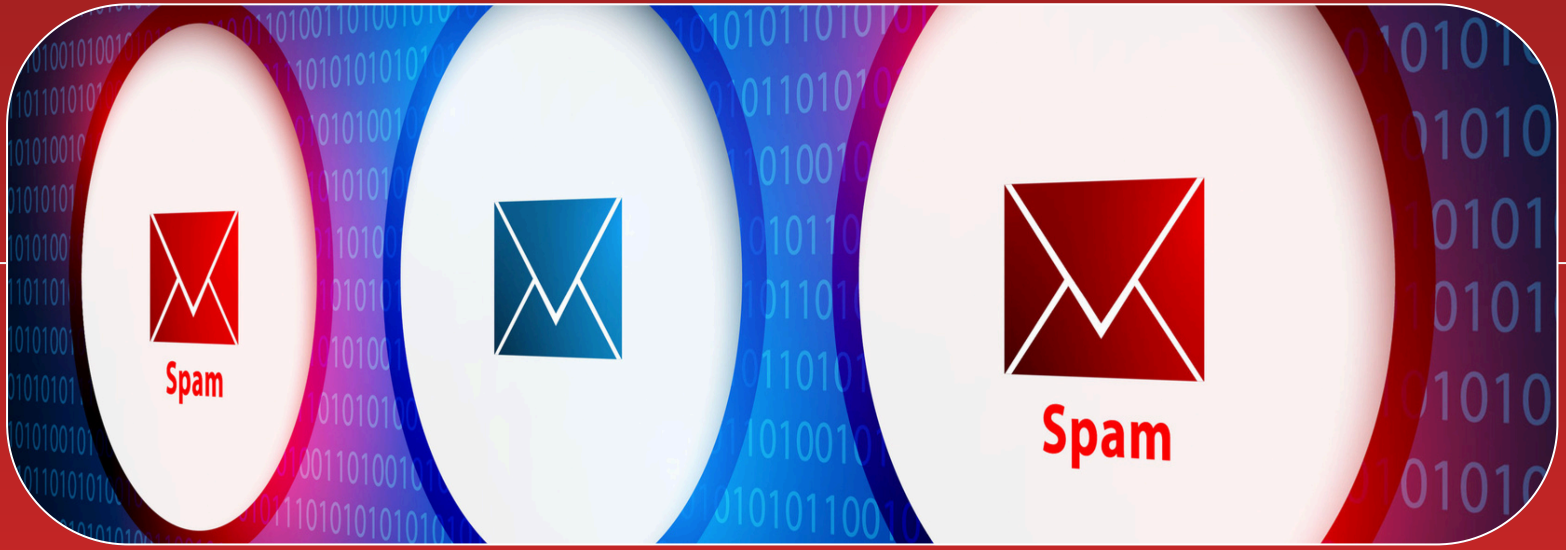
Call to Action

Authentication & Access Control

Use strong, unique passwords with multi-factor authentication enabled. Only access systems necessary for your role and never share login credentials.

Email & Communication Security

Verify sender authenticity before clicking links or downloading attachments. Use approved company channels for sensitive information and encrypt data when required.



Device & Network Safety

Keep devices updated with security patches and antivirus software. Lock your workstation when away and avoid public Wi-Fi for company business. Report lost devices immediately.

Call to Action

Data Handling & Storage

Store sensitive information only in approved locations with regular backups. Dispose of confidential documents securely and never use personal devices or cloud services for company data.

Incident Response

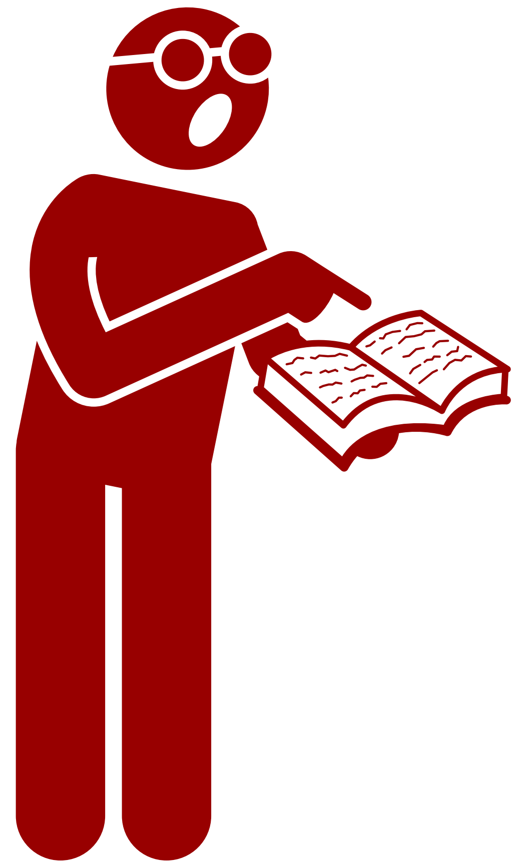
Report suspicious activity, potential breaches, or unusual system behavior immediately to IT security. Early reporting prevents minor issues from becoming major incidents.

Regular Updates & Training

Stay current with security training and policy updates. Cybersecurity threats evolve constantly, making ongoing awareness essential for data protection.

AFRICAHACKON

Redefining Threat Intelligence and Incident Response for the Organizational Future



CYBER GUARD AFRICA LIMITED

Threat Monitoring

Threat Intelligence

Ransomware

Modern Architecture Re-Definition

Asset inventories are foundational to almost any activity.

Whether you're **assessing risk**, **detecting threats**, or **responding to incidents**, It all begins with **knowing** what you're defending

Your architecture should answer three questions:

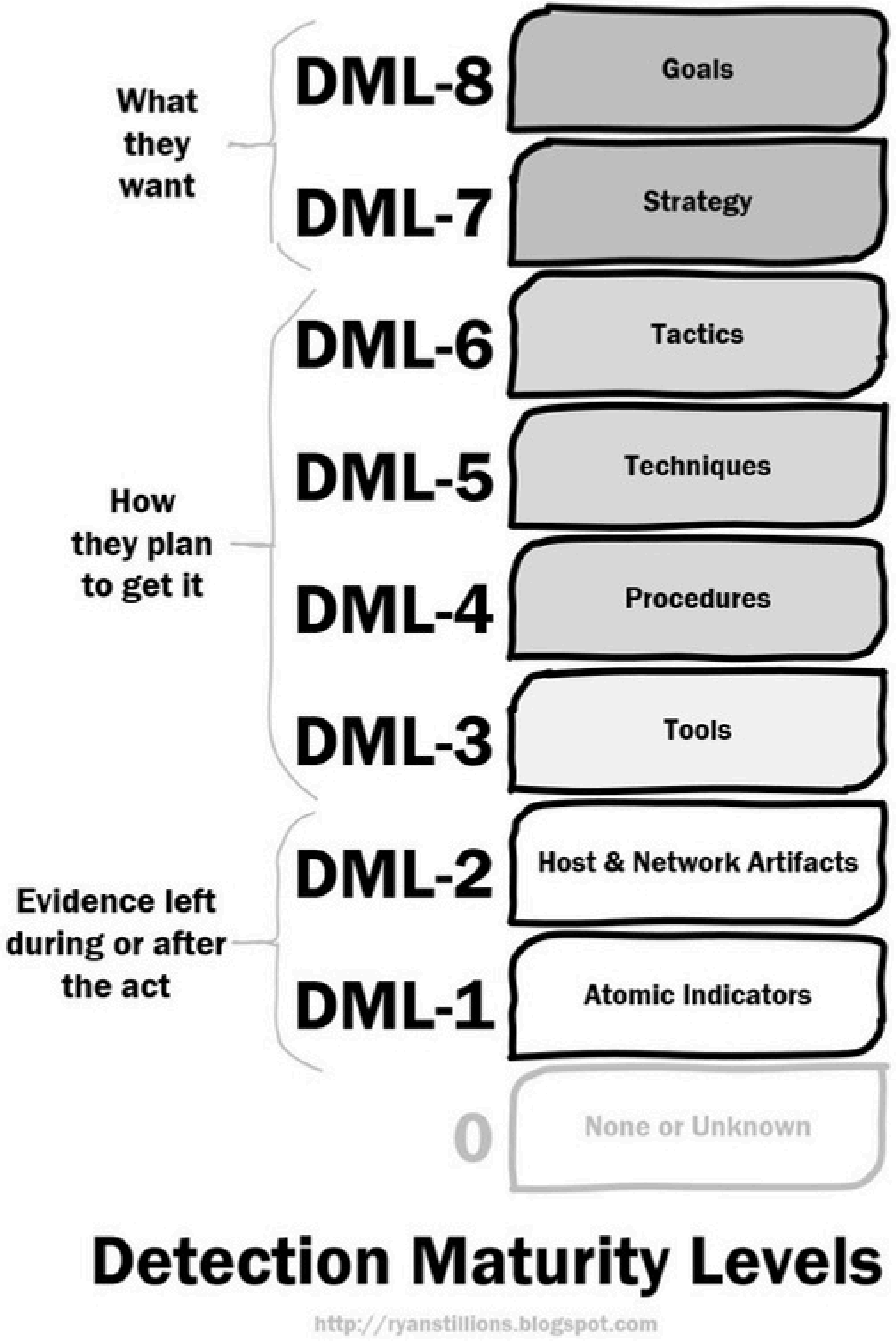
- What are we protecting?
- What are we detecting?
- What happens when something breaks?

Threat Detection Maturity Level (DML)

Detection Maturity Level (DML) model helps to assess how mature your detection capabilities are beyond just ingesting threat intel feeds.

Ryan Stillions makes a strong case for moving detection up the stack, from fundamental indicators to Tools and TTPs, and even understanding why an adversary is in your network.

- Detection without context = noise
- Prevention alone isn't enough (and fails eventually)
- Mature programs detect behavior, not just signatures
- Great detection adds value before the breach escalates



What they want

- DML-8 Goals
- DML-7 Strategy

How they plan to get it

- DML-6 Tactics
- DML-5 Techniques
- DML-4 Procedures
- DML-3 Tools

Evidence left during or after the act

- DML-2 Host & Network Artifacts
- DML-1 Atomic Indicators

0 None or Unknown

Detection Maturity Levels

http://ryanstillions.blogspot.com

Earth Kasha Campaign - New TTPs

INITIAL ACCESS

- Spear phishing emails sent from compromised legitimate accounts.
- Emails contain OneDrive links pointing to ZIP archives.
- These ZIPs include malicious Excel files with filenames such as: Revised_Resume[.]xlsm and Taiwan_Japan_Cooperation_Report[.]xlsm

EXECUTION OF ROAMINGMOUSE DROPPER

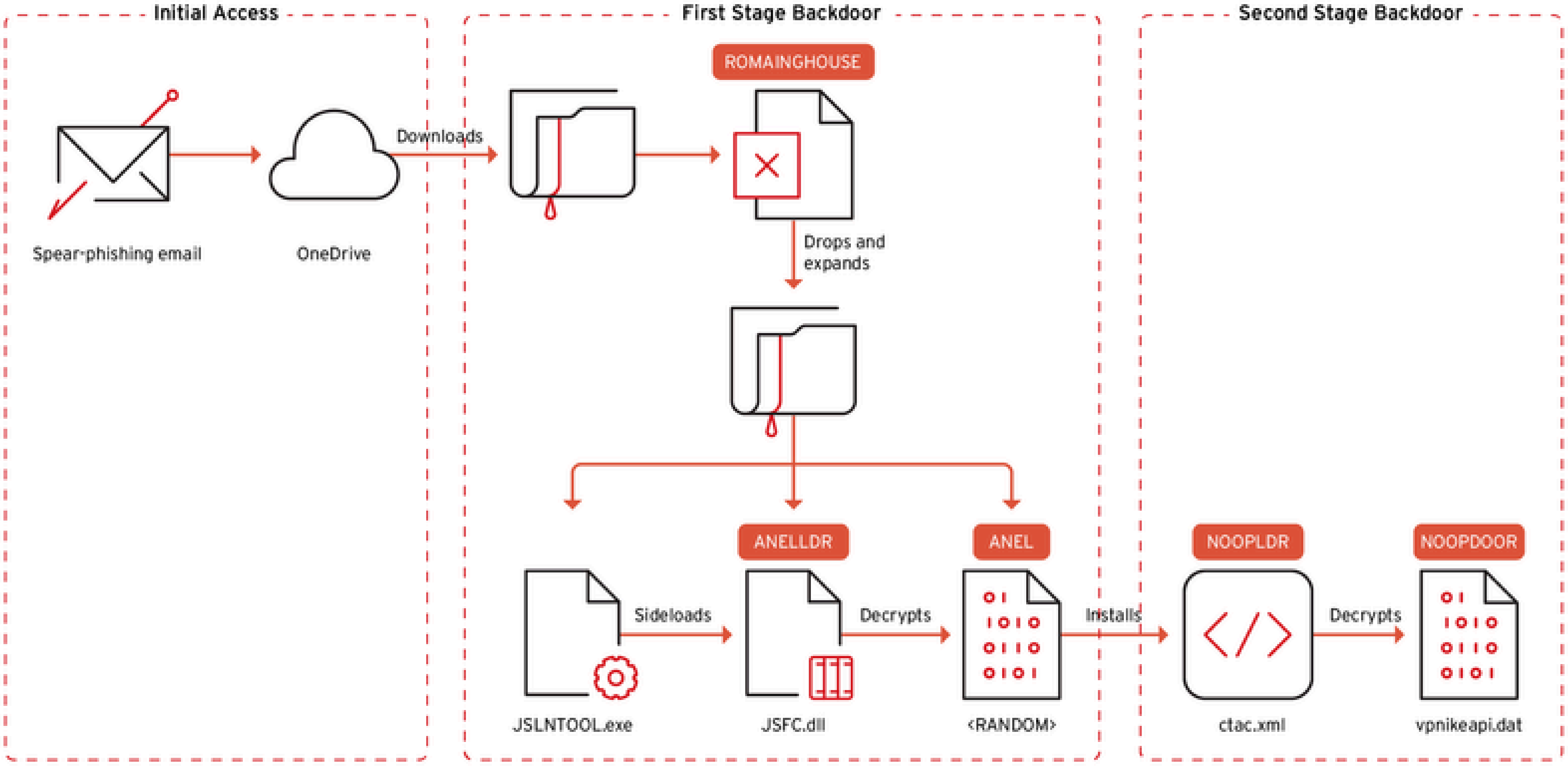
- The Excel file contains VBA macros that trigger only after user interaction (e.g., clicking a cell), allowing the malware to evade sandbox analysis.
- Upon activation, it drops and executes a malicious routine named ROAMINGMOUSE.

PAYLOAD EXTRACTION

- ROAMINGMOUSE decodes a Base64-encoded ZIP file embedded within itself. The ZIP archive contains:
  - Signed legitimate executables from vendors (e.g., JustSystems Inc.).
  - A malicious DLL (JSFC[.]dll) called ANELLDR.
  - An encrypted backdoor payload known as ANEL.

BACKDOOR DEPLOYMENT: ANEL

- The ANELLDR DLL is side-loaded by the legitimate executable.
- It decrypts the ANEL backdoor using AES-256-CBC + LZO compression, then executes it in-memory.
- ANEL establishes communication with C2 servers, allowing the threat actor to:
  - Remotely control the compromised system.
  - Execute commands.
  - Maintain persistence.



©2025 TREND MICRO

Detection Mechanisms:
3 Layers of the Modern SOC

The Data Layer: Ingest and Route Security Telemetry

This is the entry point into the SOC.
It handles data ingestion and routing from sources like:

- EDR systems
- Network Detection tools
- Cloud security logs
- Identity platforms and more

The Detection and Analytics Layer: Store, Detect, and Analyze

This layer is responsible for:

- Storing security data
- Powering rule-based detections
- Running analytics at scale

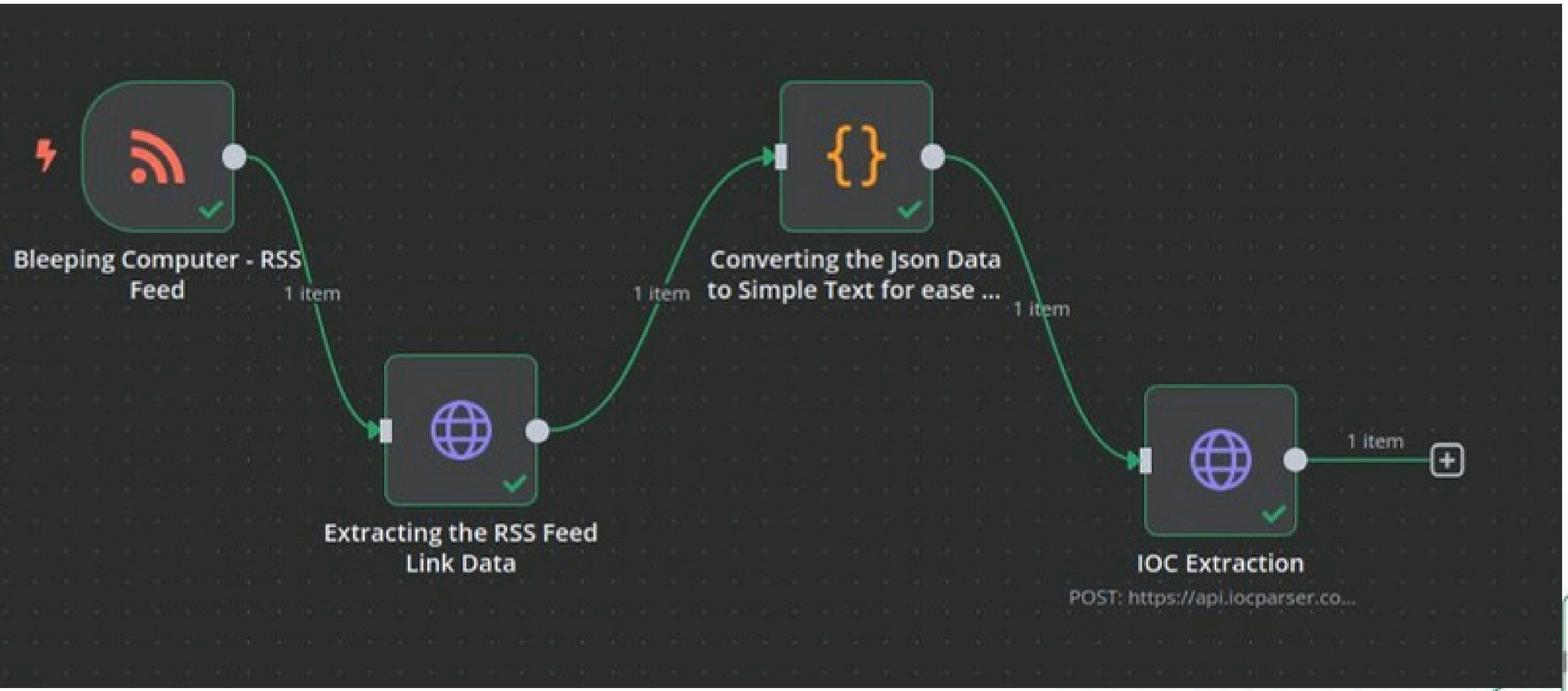
It spans across SIEMs, data platforms, and XDRs.
But the value of this layer depends on upstream data quality.

The Response and Decision Layer: Augment and Automate

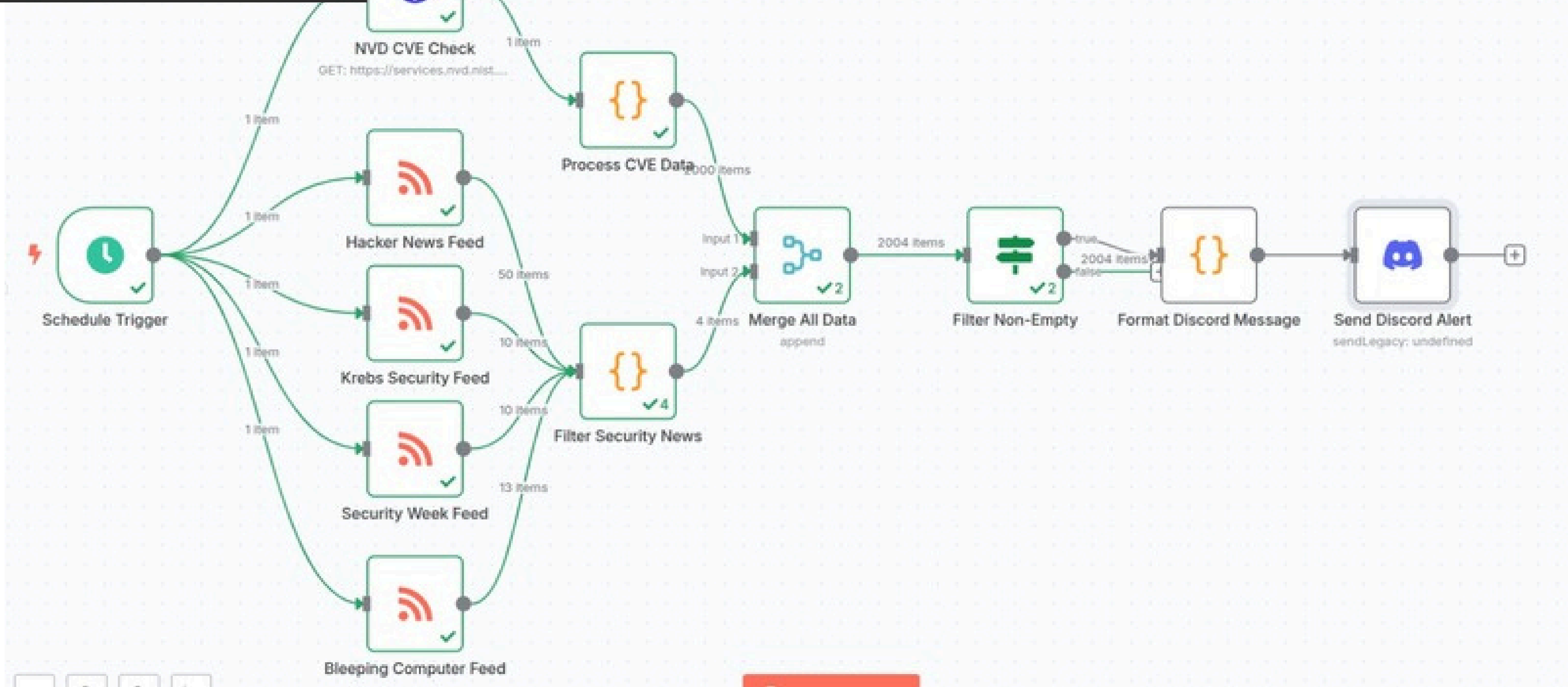
- This is the AI-augmented layer that enables:
- Triage and alert enrichment
- Automation of low-level tasks
- Faster decision-making for SOC teams

As incident volume grows, this layer is becoming
the key to reducing analyst fatigue and accelerating response.

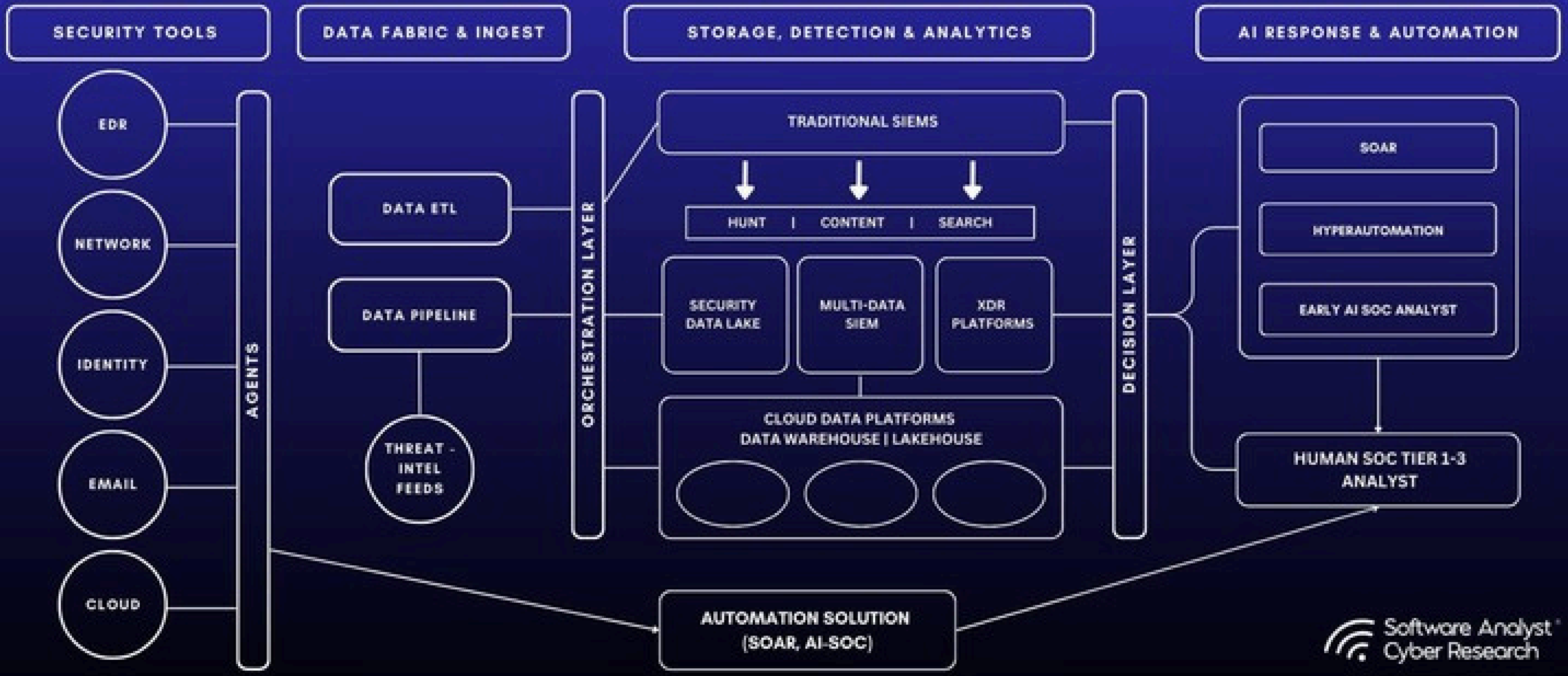
Move from Alerts to Automation and Action



Bleeping Computer - RSS Feed
1 item
Extracting the RSS Feed Link Data
1 item
Converting the Json Data to Simple Text for ease ...
1 item
IOC Extraction
POST: https://api.iocparser.co...
1 item



FUTURE SOC ARCHITECTURE



SECURITY TOOLS

DATA FABRIC & INGEST

STORAGE, DETECTION & ANALYTICS

AI RESPONSE & AUTOMATION

EDR

NETWORK

IDENTITY

EMAIL

CLOUD

AGENTS

DATA ETL

DATA PIPELINE

THREAT - INTEL FEEDS

ORCHESTRATION LAYER

TRADITIONAL SIEMS

HUNT | CONTENT | SEARCH

SECURITY DATA LAKE

MULTI-DATA SIEM

XDR PLATFORMS

CLOUD DATA PLATFORMS
DATA WAREHOUSE | LAKEHOUSE

DECISION LAYER

SOAR

HYPERAUTOMATION

EARLY AI SOC ANALYST

HUMAN SOC TIER 1-3 ANALYST

AUTOMATION SOLUTION
(SOAR, AI-SOC)

Software Analyst Cyber Research

Incidence Response

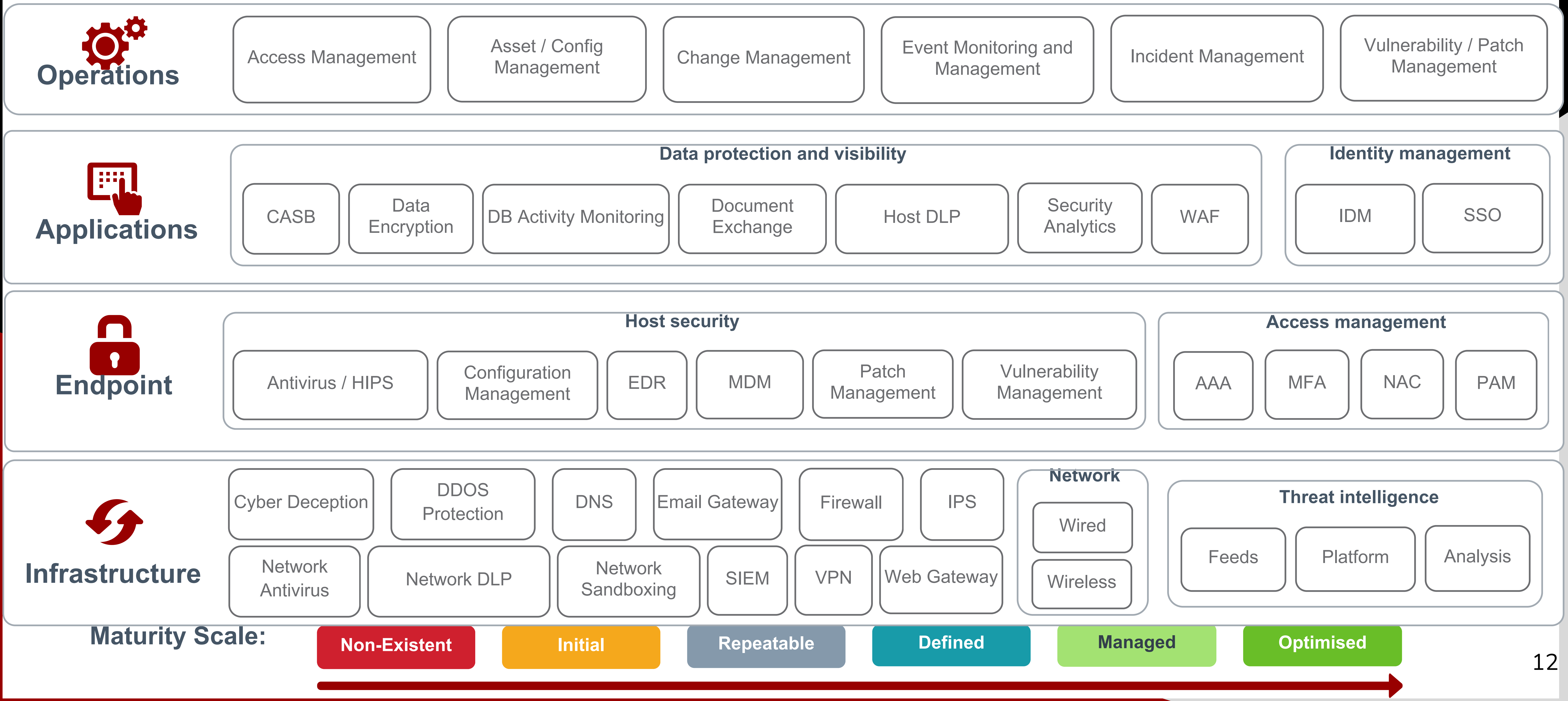
Maturity and capability levels

Level of Maturity:	Non-Existent	Initial	Repeatable	Defined	Managed	Optimised
Process	No process exists	Ad-hoc and informal	Some basic templates or checklists exist	Formally documented processes are consistent	Formal and integrated workflows	Mature and automated workflows
Metrics	No metric exists	Ad-hoc reporting	Basic metrics, informal reporting	Formally documented metrics, manual reporting	Advanced metrics and semi-automated reporting	Fully automated reporting
Tools	No technology control exists	Planning underway	Basic functionality implemented with only elemental capabilities	Functionality implemented and aligned to policies	Integrated logging, manual correlation	Integrated platform, automated correlation

Minimum Proposed Targets		Repeatable	Defined	Managed	Optimised
Specific System / Application **Easier**			Retail, Manufacture Construction, Prof. Services	Tech, Education, Legal, Healthcare, Media	Govt agencies, FSI, Security MSP, Energy
Across Entire Organisation **Harder**		Retail, Manufacture Construction, Prof. Services	Tech, Education, Legal, Healthcare, Media	Govt agencies, FSI, Energy, Service Providers (MSP)	Intelligence / Defence agencies, Security MSP

Security Architecture Reference Model

CYBER GUARD AFRICA LIMITED



Operations

- Access Management
- Asset / Config Management
- Change Management
- Event Monitoring and Management
- Incident Management
- Vulnerability / Patch Management

Applications

Data protection and visibility

- CASB
- Data Encryption
- DB Activity Monitoring
- Document Exchange
- Host DLP
- Security Analytics
- WAF

Identity management

- IDM
- SSO

Endpoint

Host security

- Antivirus / HIPS
- Configuration Management
- EDR
- MDM
- Patch Management
- Vulnerability Management

Access management

- AAA
- MFA
- NAC
- PAM

Infrastructure

- Cyber Deception
- DDOS Protection
- DNS
- Email Gateway
- Firewall
- IPS
- Network Antivirus
- Network DLP
- Network Sandboxing
- SIEM
- VPN
- Web Gateway

Network

- Wired
- Wireless

Threat intelligence

- Feeds
- Platform
- Analysis

Maturity Scale: Non-Existent → Initial → Repeatable → Defined → Managed → Optimised

KPI - Incident Response

1. Mean Time to Detect (MTTD): Avg. time taken to identify an incident.
2. Mean Time to Respond (MTTR): Avg. time between detection and first mitigation action.
3. Mean Time to Contain (MTTC): Avg. time to stop the incident from spreading.
4. Mean Time to Resolve (MTTRv): Avg. time to fully fix and close the incident.
5. Number of Incidents Detected: Total incidents identified in a time period.
6. Percentage of Incidents by Severity Level: Distribution of incidents by criticality.
7. First Response Time: Time from detection to initial analyst response.
8. Number of Reopened Incidents: Count of incidents reopened after closure.
9. False Positive Rate: Percentage of alerts flagged as incidents that weren’t real.
10. Detection Accuracy: Ratio of true positives to total alerts.

KPI - Incident Response

CYBER GUARD
AFRICA LIMITED

11. SLA Compliance Rate: % of incidents resolved within agreed SLA timelines.
12. Incident Recurrence Rate: Rate at which similar incidents reoccur.
13. User-Reported vs. System-Detected Incidents: Comparison of manually vs. automatically detected issues.
14. Cost per Incident: Average financial impact of each incident.
15. Time to Escalation: Time from detection to escalation to a higher tier/team.
16. Incident Closure Rate: % of incidents resolved within a defined period.
17. Incident Root Cause Categories: Classification of underlying causes.
18. Volume of Phishing/Malware/Ransomware Incidents: Count of incidents by type.
19. Percentage of Automated vs. Manual Responses: Share of responses handled automatically.
20. Resolution SLA Breach Rate: % of incidents resolved after SLA deadlines.

Incidence Response Process

1. Detection and Analysis

- Identify and confirm the breach
- Assess the scope and impact
- Gather initial evidence

2. Containment

- Isolate affected systems
- Prevent further unauthorized access
- Preserve evidence for forensic analysis

3. Eradication

- Remove the threat (malware, unauthorized accounts, etc.)
- Address vulnerabilities that led to the breach

4. Recovery

- Restore systems and data from clean backups
- Implement additional security measures
- Return to normal operations

5. Post-Incident Activities

- Conduct a thorough investigation
- Document the incident and response
- Update security policies and procedures
- Provide training based on lessons learned

6. Notification and Reporting

- Inform stakeholders (employees, customers, partners)
- Report to relevant authorities if required by law
- Prepare for potential legal or regulatory consequences

Case Study

CYBER GUARD
AFRICA LIMITED

Company Background

InsureTech Solutions is a large insurance company with 850 employees and annual revenue of $500 million. They offer multiple insurance products including life, health, auto, and property insurance. Their operations are fully cloud-based, utilizing various SaaS and PaaS solutions.

The Incident

On a Thursday afternoon, InsureTech's Security Operations Center (SOC) detected anomalous activity in their claims processing system.

Further investigation revealed unauthorized access to policyholder data, potentially compromising sensitive information of over 1 million customers across various insurance products.

This was established that it was a successful phishing to one of the administrators that was not detected by all internal solutions.

The account details was then used to retrieve all information of customers

Incidence Response Process cont…

1. Detection and Analysis

- The SOC(security operation centre) confirmed the breach within 90 minutes of the initial alert.
- They discovered that the attacker exploited a misconfigured Identity and Access Management (IAM) policy in their cloud environment.
- Initial assessment showed that customer names, addresses, social security numbers, and policy details were accessed.

2. Containment

- Access to the compromised cloud services was immediately restricted.
- All API keys and access tokens were revoked and regenerated.
- Cloud network segmentation was enhanced to isolate affected systems.
- Snapshots of affected cloud instances were taken for forensic analysis.

Incidence Response Process cont...

3. Eradication

- The security team corrected the IAM policy misconfigurations.
- They conducted a thorough review of all cloud service configurations to identify and remediate any similar vulnerabilities.
- Automated tools were deployed to continuously monitor for unauthorized changes in cloud configurations.

4. Recovery

- Access to the compromised cloud services was immediately restricted.
- All API keys and access tokens were revoked and regenerated.
- Cloud network segmentation was enhanced to isolate affected systems.
- Snapshots of affected cloud instances were taken for forensic analysis.

Post-Incident Activities

- A detailed cloud forensics analysis revealed that the attacker had intermittent access for approximately 5 days.
- The incident response team documented the entire event, including timeline and actions taken.
- InsureTech hired a specialized cloud security firm to conduct a comprehensive audit of their multi-cloud environment.
- Based on the findings, they updated their cloud governance policies and implemented more robust encryption for data at rest and in transit.

Notification and Reporting

- The CEO personally notified major corporate clients and partners within 36 hours of confirming the breach via a structured messaging through the communications department.
- A public statement was released within 72 hours, demonstrating transparency and outlining steps taken to protect customers.
- InsureTech reported the incident to relevant insurance regulatory bodies and data protection authorities as required by law.
- They offered two years of free identity theft protection and credit monitoring to affected customers.
- The board was also notified about the breach and the extent of damage to the company as well as the repercussions.

Financial Impact

- Immediate costs: $2 million for incident response, forensic services, and cloud security experts
- Long-term costs: $10 million for security upgrades, customer protection services, and enhanced cloud monitoring tools
- Estimated revenue loss due to reputational damage: $25 million over the next two years
- Potential regulatory fines: Up to $50 million (pending investigation)

Key Lessons for C-Suite

1. Invest in cloud-specific security measures and regular configuration audits.
2. Consider outsourcing security assessments through a third-party organization to identify security gaps
3. Ensure cloud governance policies are robust and consistently enforced across all services.
4. Implement a comprehensive cloud security posture management strategy.
5. Prioritize employee training on cloud security best practices.
6. Develop and regularly test an incident response plan specifically for cloud-based incidents.
7. Consider specialized cyber insurance for cloud environments to mitigate financial risks. Maintain transparent communication with stakeholders, emphasizing the company's commitment to data protection.

Building an Environment to Support Threat Hunting Simulations

Know Yourself

- Knowing your environment better than any **INSIDER THREAT** or **EXTERNAL THREAT** actors.

- If you **REALLY** want to protect your environment, you **REALLY** have to know your environment better than anyone.

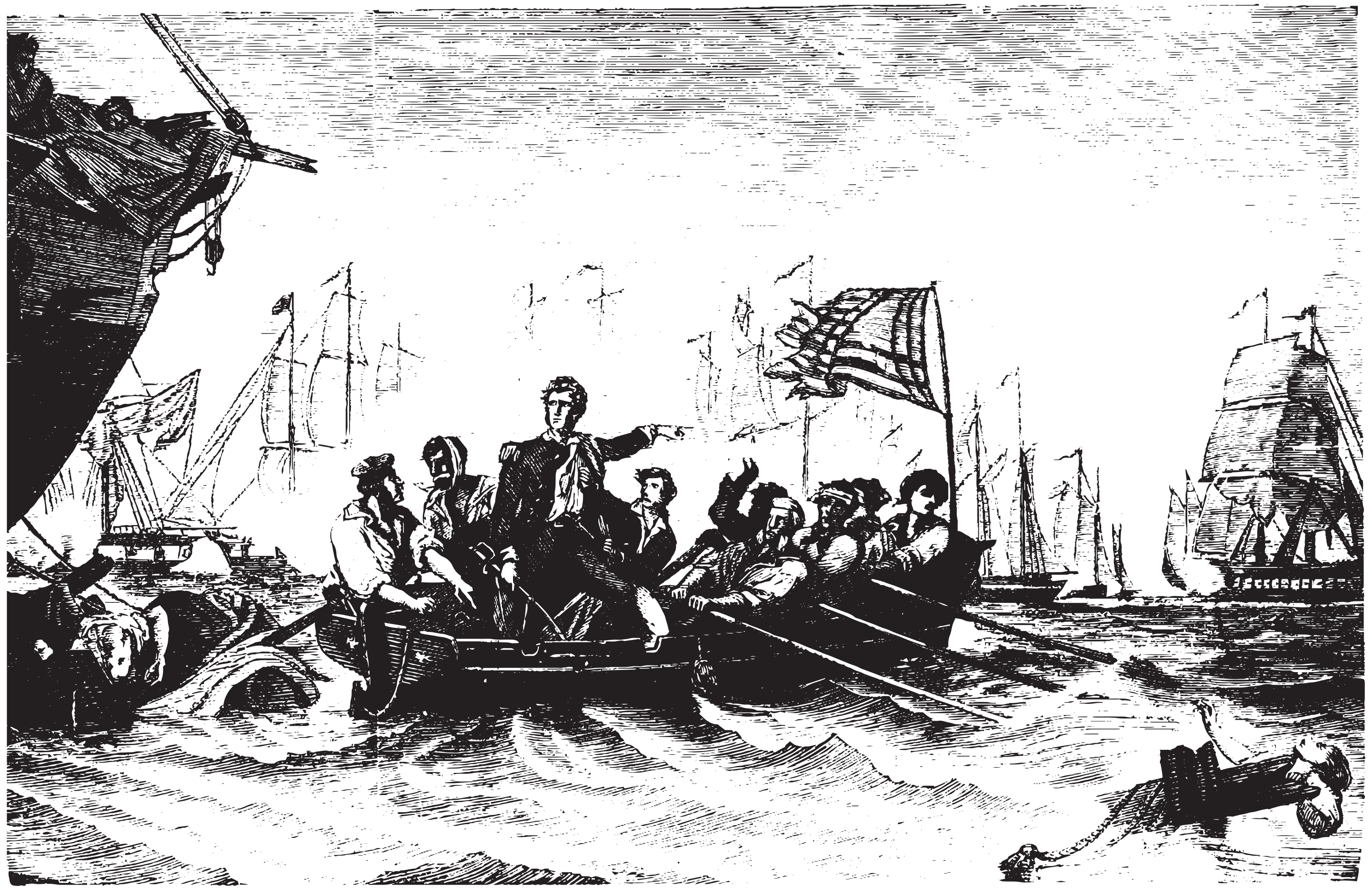
Know Your Enemy

- Define your enemies, are they internal, external or both
- What is their capability? What motivates them?, What do they target?

Know Your Battles

CYBER GUARD AFRICA LIMITED

- Why will they target us? How can they impact our vision, mission?
- What will they target ? What are our crown jewels?
- How will they target? Have we seen attempts before?
- Where are we exposed? How does our attack surface reflect?



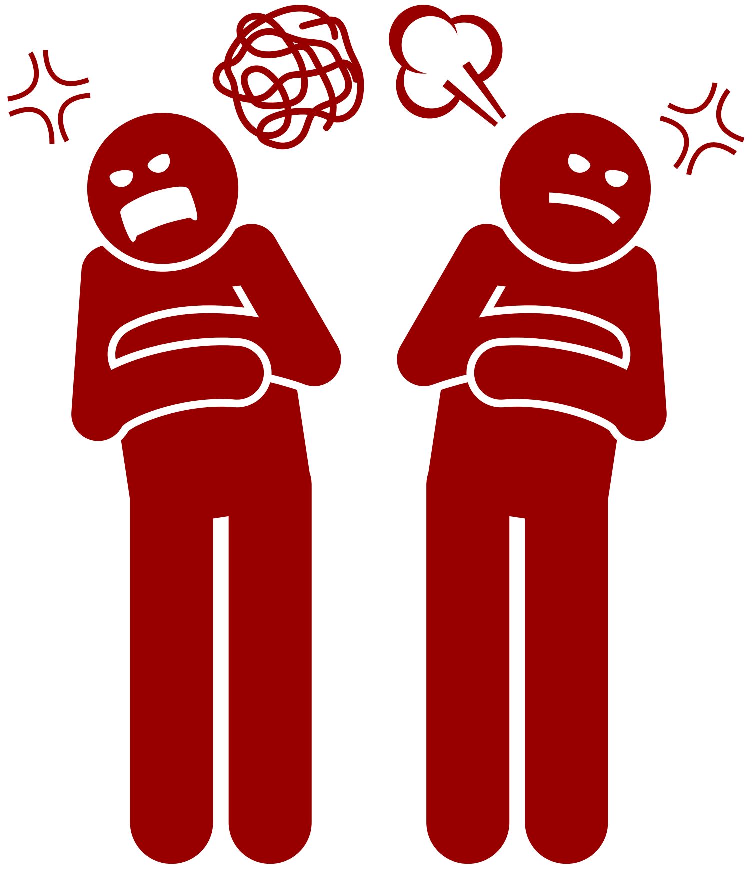
Threat Hunting Simulation with the 3K’s

Know Yourself

- Consistently run hunt exercises and how often they'll be carried out to accurately understand your environment.
- Define your hunt mission name: e.g Understanding our Critical Assets
- Define your hunt description

Know Your Enemy

- Identify attackers activities you would like to hunt for in your environment



Know Your Battles

- Identify the attack path the attackers will follow to target your critical assets
- Identify opportunities to detect attacker activity through your hunts
- Network Traffic Hunting
  - Failed traffic analysis
  - Abnormal traffic patterns
  - Abnormal protocol usage
- Endpoint Activity Hunting
  - Abnormal process hunting
  - Remote Access Anomalies
  - Windows Services Anomalies
  - Suspicious Executables Anomalies

Defensible Security Architecture Lifecycle to Support Threat Hunting Simulations

Design

Re-design

Implement

Operate

Monitoring

DRIOM

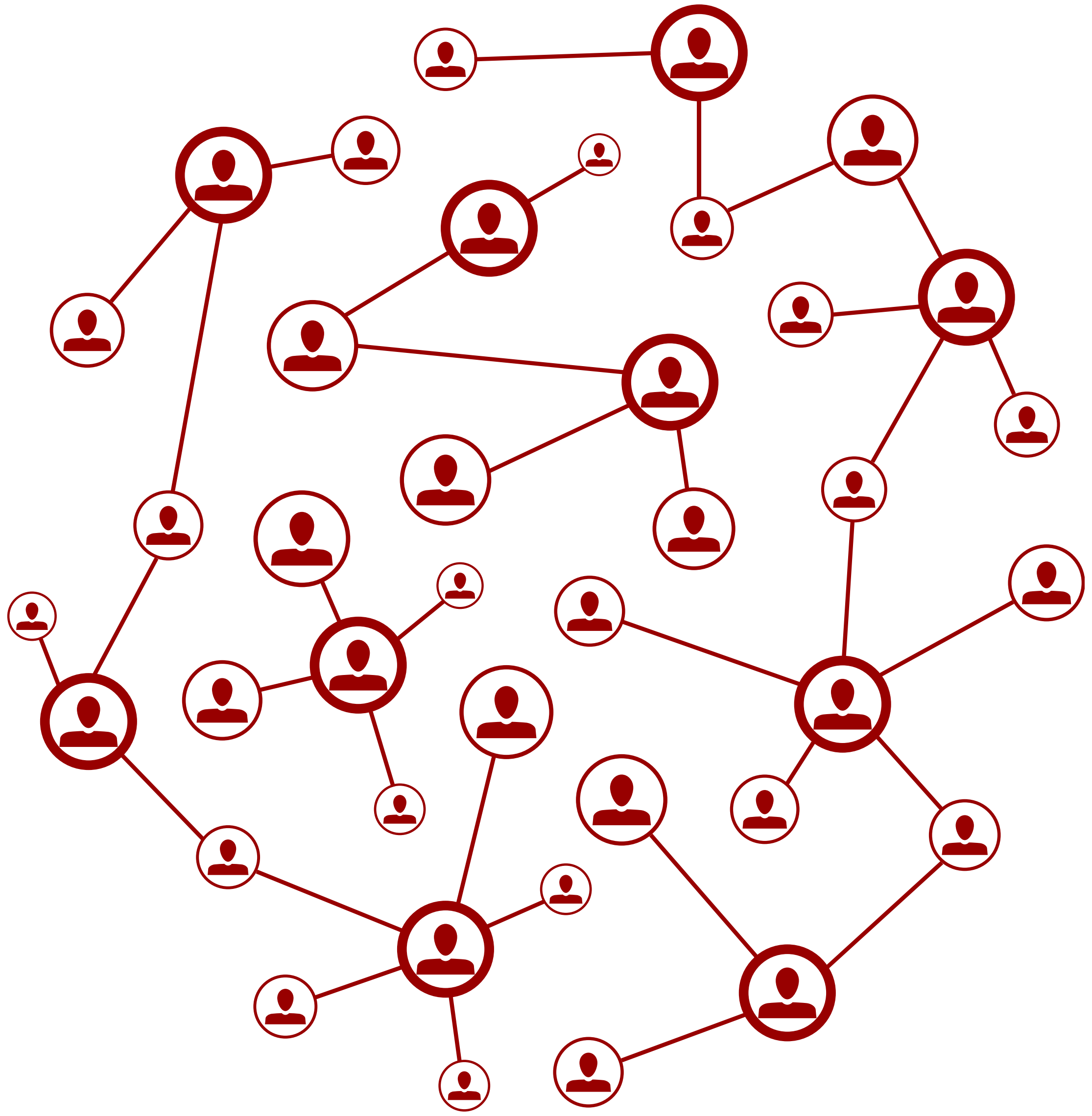
1. Discover & Assess

- Identify requirements, business & regulatory – i.e. HIPAA, PCI, SOX, GDPR, etc. Leverage BCP & GRC documentation
- Identify assets in scope and crown jewels
- Understand business and risk appetite
- Identify resources available: tools, budget, personnel, skills, time
- Practical threat modeling and risk analysis
- Attack surface analysis, network attack surface, data egress analysis, network visibility analysis and protocol visibility analysis
- Red teaming: impact analysis (think offensive), realistic scenarios based on attacker's TTP's

2. Re-Design

- Identify desired state, determine the gap (current vs. desired) and roadmap
- Architectural decisions
- Threat focused, covering protection, detection and reaction
- Risk mitigation
    - People
    - Processes
    - Technology
    - Controls

- Documentation
- Some of the documentation needed here is:
    - Business rules regarding the handling of data/information assets
    - Written and published security policy
    - Codified data/information asset ownership and custody
    - Risk analysis documentation
    - Data classification policy documentation



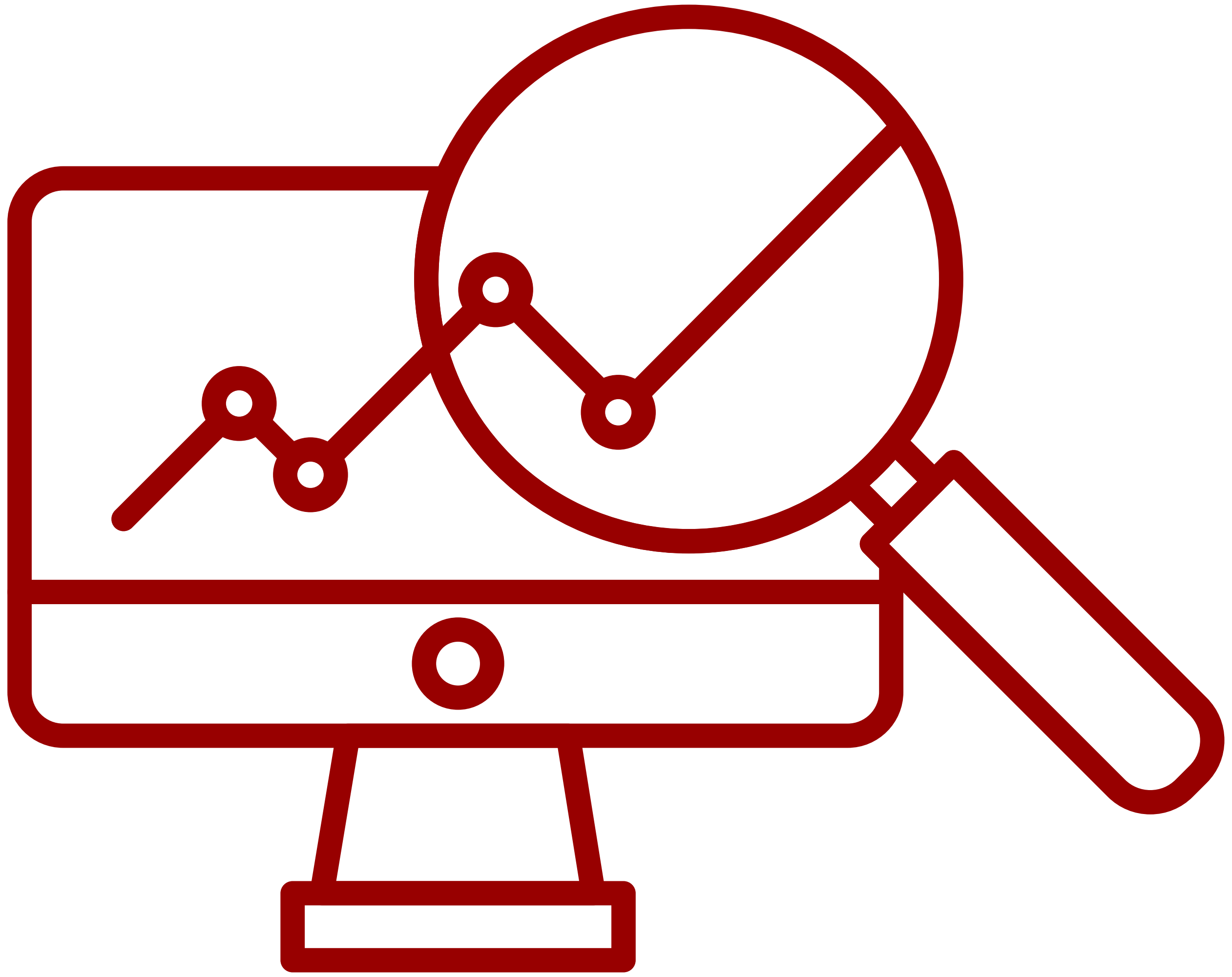
3. Implement

- Implement based on security architecture design
- Harden at each layer
- Network-centric
- Data-centric
- Enable logging for monitoring
- Determine baseline
- Device configurations and traffic flows
- Validate implementation

CYBER GUARD AFRICA LIMITED

4. Operate & Monitor

- Continuous security monitoring
- Data at rest: registry keys, windows event logs, DNS, etc.
- Network Security Monitoring
- Data in motion: NetFlow, transactional, pcaps
- Continue creating awareness, maintaining threat focused operations and augmenting visibility based on threat intel and IR lessons learned



THANK YOU

WWW.CYBERGUARDAFRICA.COM
WWW.BRIGHTZEED.COM
BRIGHT.GAMELI@CYBERGUARDAFRICA.COM
+254712421951