strobes™

Cybersecurity Masterclass

Continuous Threat Exposure Management for GRC

By Akhil Reni

strobes™

Get To Know Us

strobes

Strobes is one of the first Continuous Threat Exposure Management (CTEM) companies that enables enterprises to do Attack surface management and Risk-based vulnerability management at scale.

Akhil Reni
CTO & Co-Founder
Strobes

I am a hacker turned CTO with over 10 years of experience in offensive security, and vulnerability management. I lead product development at Strobes and do bug bounty programs once in a blue moon.

strobes™

Research

Hacking Zomato's Order System to Order Food For Free!
https://hackerone.com/reports/403783

Scaling Strobes With Multi-Region & Multi Tenancy
https://medium.com/@hungry.soul/engineering-multi-tenancy-multi-region-at-strobes-28446b7e3d46

Automating Inside Sales
https://medium.com/@hungry.soul/automating-inside-sales-part-1-find-any-email-address-a848ffba8078

Ranking #4 On X's (Twitter) Hacker Leaderboard
https://hackerone.com/X

Acknowledged By

PayPal

50 more

strobes™

Agenda

Overview Of Continuous Threat Exposure Management (CTEM)

Asset Management
- Importance of comprehensive asset management
- Identifying gaps in threat coverage
- Strategies to achieve 100% coverage

Understanding Threat Exposure
- Definition of threat exposure and attack surface
- Sources of vulnerabilities and misconfigurations
- Challenges in managing threat exposure effectively

Vulnerability Aggregation and Prioritization
- Techniques for aggregating vulnerabilities from multiple sources
- Prioritizing vulnerabilities based on risk and impact
- Aligning vulnerability management with organizational risk goals

Implementing a CTEM Program
- Key steps in CTEM
- Streamlining processes and reducing chaos

Meeting Governance & Compliance Goals
- Aligning CTEM with organizational governance objectives
- Demonstrating due diligence and regulatory compliance
- Enhancing transparency and accountability in threat management

Q & A?

strobes™

Intro

CTEM
Continuous Threat Exposure Management

It is a proactive approach to cybersecurity that focuses on continuously identifying, assessing, prioritizing, and mitigating an organization's exposure to cyber threats. It involves the ongoing process of discovering and managing vulnerabilities, misconfigurations, and other security weaknesses across an organization's entire attack surface.

strobes™

Intro

Understanding Threat Exposure

Think of the threat surface as the sum total of all the potential ways an attacker could penetrate your organization's defenses. The larger and more complex the attack surface, the greater the threat exposure.

01 Vulnerabilities and weaknesses

Vulnerabilities are flaws or gaps in an organization's systems, networks, or applications that attackers can exploit to gain unauthorized access or perform malicious activities. Weaknesses can include misconfigurations, unpatched software, weak passwords, or lack of proper security controls.

02 Attack surface complexity

The attack surface encompasses all potential entry points an attacker could use to penetrate an organization's defenses, including servers, endpoints, cloud services, and user accounts.

03 Potential impact on the organization

Successful cyber attacks can lead to data breaches, financial losses, reputational damage, legal and regulatory issues, and disruption of business operations. The potential impact of a cyber attack depends on factors such as the sensitivity of the data involved, the criticality of affected systems, and the attacker's intentions.

strobes™

Source Of Vulnerabilities & Weaknesses

Container Images & Runtime

Software Code

OSS Packages & Dependecies

Cloud Environments

Networks

Applications

Endpoints

Self-Managed Data Centres

strobes™

Ways We Use To Uncover Them

SAST	DAST	Netwok & Infra
SCA & SBOM	Secret Security	CSPM/CNAPP
DAST	SAST	ASM
Internal Pentests	External Pentests	Bug Bounty

strobes™

Challenges

- No Unified Approach
- No Correlation
- No Prioritization

strobes™

Challenges

- Everything in Silos
- Coverage
- Slower Compliance

strobes™

CTEM
Key steps in Continuous Threat Exposure Management

strobes™

Continuous Threat Exposure Management

1 Scoping

- Centeralized Asset Inventory
- Attack Surface Discovery
- Comprehensive Asset Management

2 Discovery

- Discover CVEs, Misconfigurations, Weakness across Environment
- Unified Vulnerability Management
- Achieve 100% Coverage

3 Prioritization

- Map threats to sensitivity of the Asset
- Check vulnerability context, like code execution, threat context like does it have an active exploit?

4 Validation

- Validate attack paths - Can a compromised cloud resource with IAM attached can give root to entire cloud account?
- Verify the exploits if available

5 Mobilization

- Identify Asset Owners & Stakeholders
- Sync the information with tools like Servicenow or Jira
- Coordinate the teams to patch the risks and re-validate them

strobes™

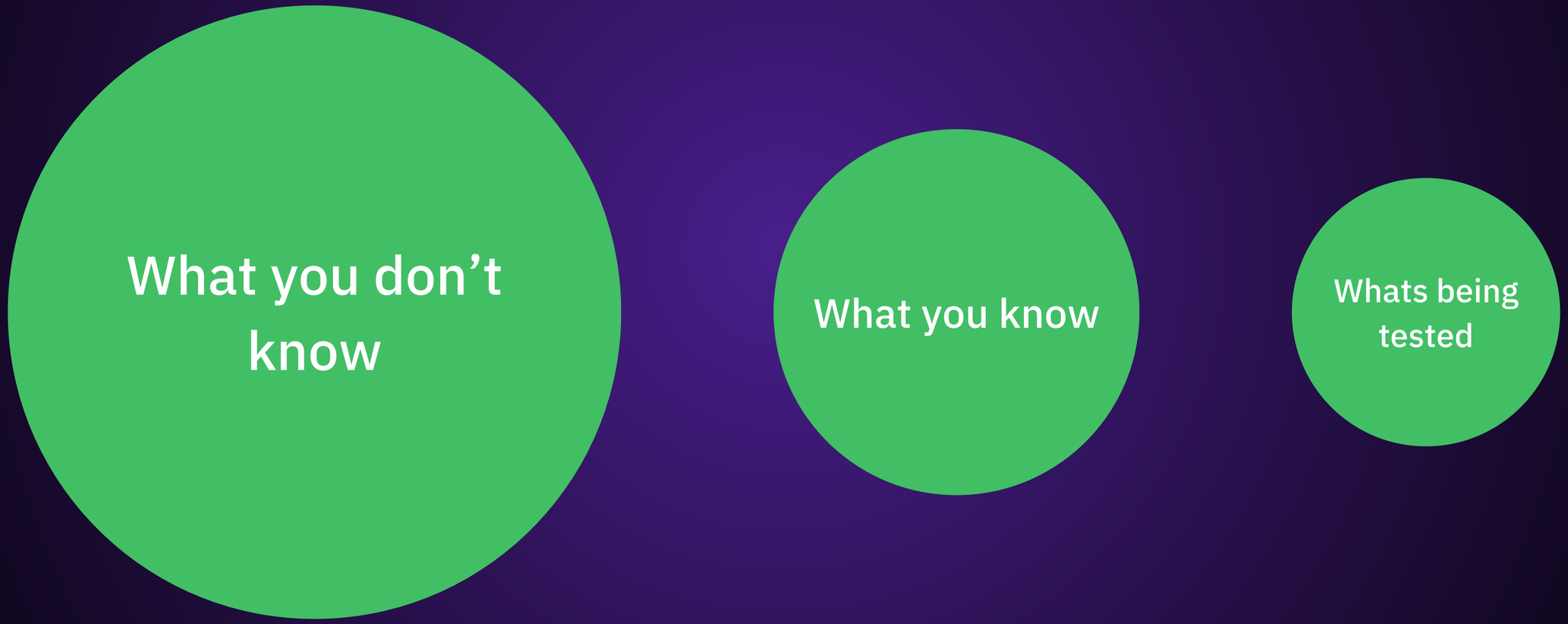
Asset Management

Attack Surface Layers

Managed Assets	Endpoints	Servers	Networks	Mobile	Websites	IoT
Unknown Assets	Shadow IT	Cloud Stores	Test Data	Code Repositories	Unused Credentials	
NTH - Party Assets	Contractors	Hosted Data	Java Scripts	Cloud Services	APIs	
Ephemeral Assets	Virtual Environments	Development Environments	Short-lived Cloud Assets	BYOD		

strobes™

Asset Management & It’s Coverage



strobes™

Asset Management & It's Coverage

- Are You Sure All Your Endpoints Have AV, EDR, etc Installed?
- All External Facing Applications Have Firewall Enabled?
- All Endpoints, Servers, Applications, Networks, Cloud Were Scanned For Vulnerabilities?
- And much more...

strobes™

Asset Management & It's Coverage

A classical example, someone got their application live but was missed going through WAF coverage

Hello Akhil,

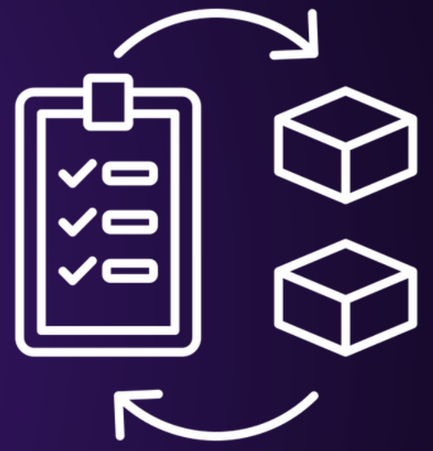
We wanted the required information so that we could analyse traffic on our WAF and identify why such payload was not blocked on WAF.

Also, the website x.com was made live only last week, on 17th April. So, we are perplexed regarding the date of exposure.

strobes™

Current challenges with asset management?

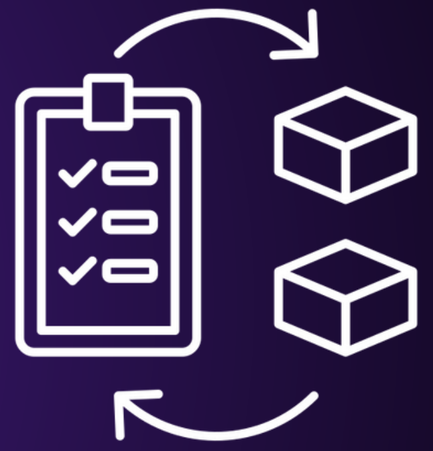
- Excel sheets
- Not Comprehensive
- Data not correlated from multiple sources
- Who owns the asset?
- Automatic onboarding of newer assets
- Automatic offboarding of dead assets?
- No Unified Solution
- Still do not cover modern APIs, Applications, Cloud and more



strobes™

How to build Asset Inventory?

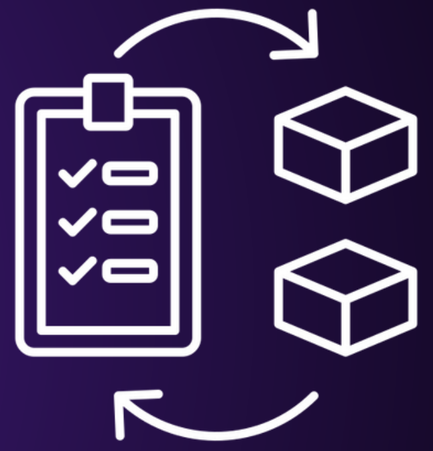
- Move away from Excel sheets
- Have a centralized solution for asset inventory
- Integrate with all teams and technologies
- Leverage cloud inventory tools
- Track ownership
- SBOM
- Add as many attributes as possible
  - Sensitivity
  - Exposure (behind a firewall? internal? external?)
  - AV installed?
  - EDR installed?



strobes™

What all attributes can be tracked?

- Falls under PCI Scope
- Falls under GDPR?
- Vulnerability Scanned
- Last Scanned
- Business unit
- Region



What can be tracked (and not limited to)

- CIDRs, IPs, Endpoints, Servers, etc.
- Web Application URLs and Mobile Applications (published + internal)
- API Endpoints (OpenAPI, Swagger, Postman collections)
- Everything on Cloud (all cloud resources)
- Container Images
- OSS Software, Dependencies (SBOM)

strobes™

Achieve 100% Coverage

A robust and comprehensive asset inventory is the first step to achieve 100% threat coverage

Rule #1

Centralized Inventory Solution

- Move away from dispersed Excel sheets
- Implement a unified, centralized system for tracking all assets
- Integrate asset data from all teams and technologies into one place

Rule #2

Comprehensive Asset Tracking

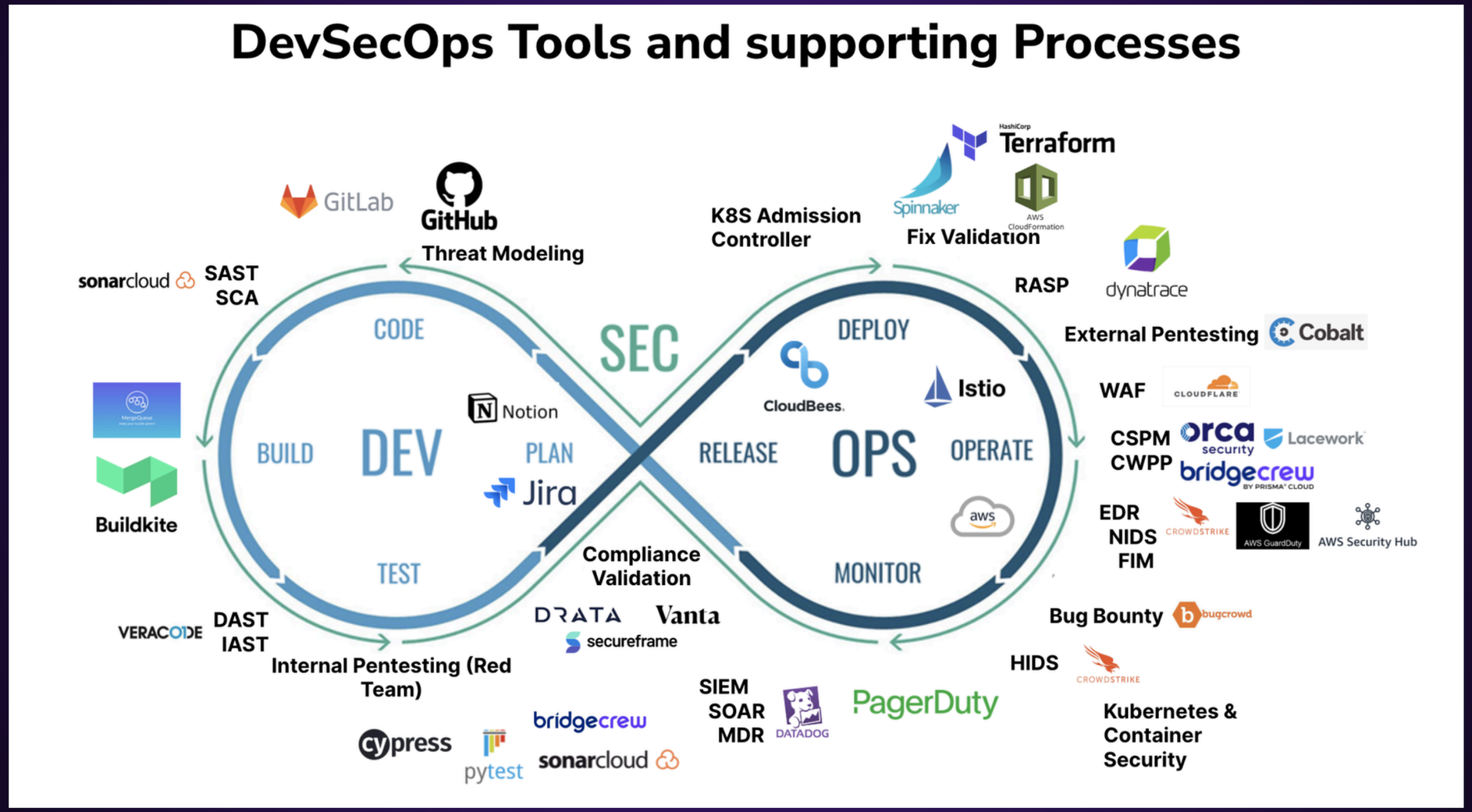
- Track a wide range of attributes for each asset (sensitivity, exposure, owner, etc.)
- Go beyond basic fields to capture all information that makes assets unique
- Include on-prem, cloud, container, and application-level assets

Rule #3

Automation and Integration

- Leverage tools to automate asset discovery and stay up-to-date
- Integrate with existing systems (CMDB, scanners, cloud APIs, etc.)
- Automate ongoing asset updates to replace manual, error-prone processes

Vulnerabilities & Risks Aggregation



Reference: https://www.linkedin.com/pulse/my-dev-sec-ops-mindmap-sangram-dash

strobes™

Vulnerabilities & Risks Aggregation

- Excel sheets
- Multiple Dashboards to Login
- No Correlation
- No Enrichment with Threat Intelligence
- Improper or No Taxonomy & Compliance Mappings
- Tough to Align with Governance Goals

strobes™

Vulnerabilities & Risks Aggregation

SAST	DAST	Netwok & Infra
SCA & SBOM	Secret Security	CSPM/CNAPP
DAST	SAST	ASM
Internal Pentests	External Pentests	Bug Bounty

→ Unified Solution

strobes™

Vulnerabilities & Risks Aggregation

Managed Assets	Endpoints	Servers	Networks	Mobile	Websites	IoT
Unknown Assets	Shadow IT	Cloud Stores	Test Data	Code Repositories	Unused Credentials	
NTH - Party Assets	Contractors	Hosted Data	Java Scripts	Cloud Services	APIs	
Ephemeral Assets	Virtual Environments	Development Environments	Short-lived Cloud Assets	BYOD		

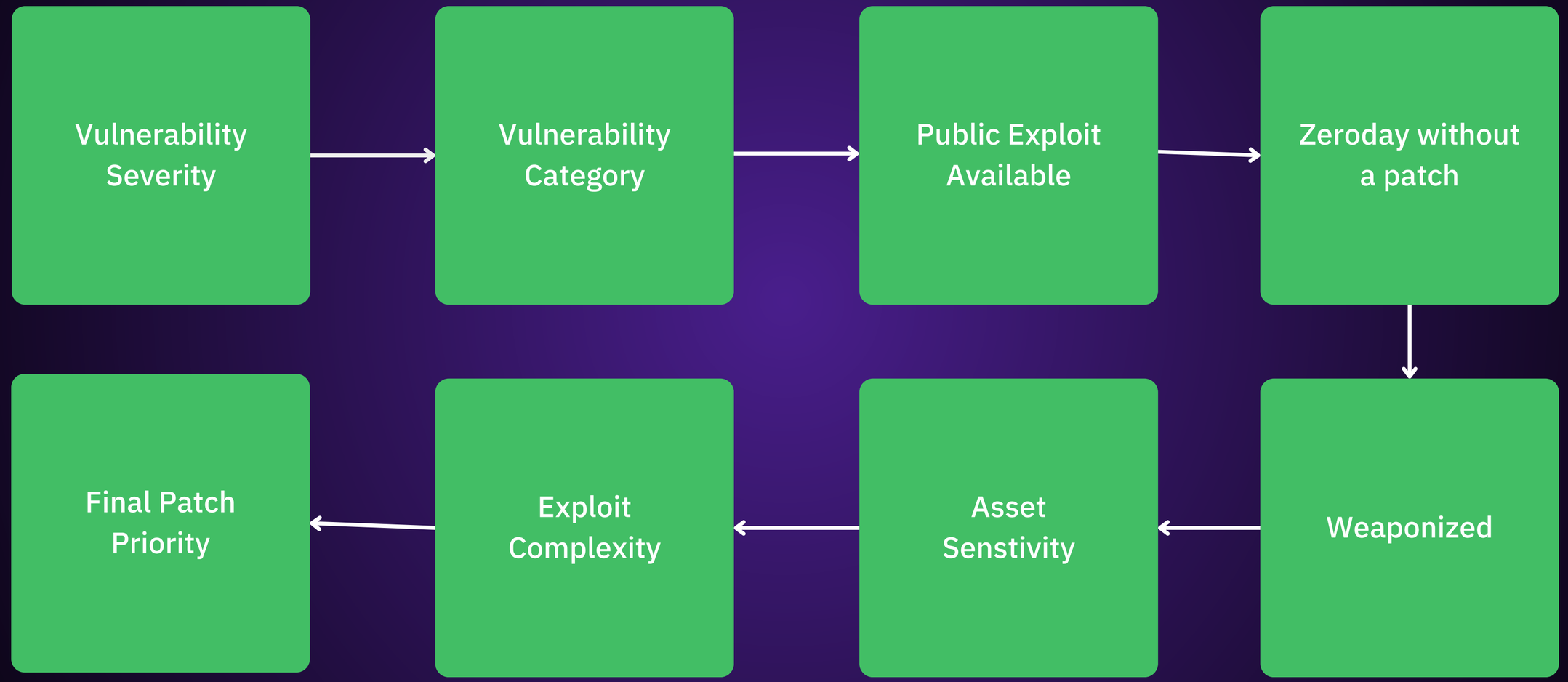
SAST	DAST	Netwok & Infra
SCA & SBOM	Secret Security	CSPM/CNAPP
DAST	SAST	ASM
Internal Pentests	External Pentests	Bug Bounty

Unified Solution

- Patch Management
- Incident Management
- Ticketing
- SIEM

strobes™

Risk Prioritization



Download Whitepaper At: https://strobes.co/vulnerability-prioritzation/

GRC Goals In CTEM

1. Policy Development

Establishing clear policies that define roles, responsibilities, and expectations for managing cyber threats and vulnerabilities. This includes policies for asset management, vulnerability assessment, patch management, and incident response.

2. Risk Management Framework

Implementing a risk-based approach to prioritize the most critical assets and vulnerabilities based on their potential impact to the business. This involves defining risk criteria, conducting regular risk assessments, and making informed decisions on risk treatment.

3. Oversight and Accountability

Assigning ownership and accountability for various aspects of the CTEM. This includes defining clear roles for asset owners, vulnerability managers, and executive sponsors, and establishing oversight mechanisms such as regular reporting and performance metrics.

GRC Goals In CTEM

4. Compliance and Standards Alignment

Ensuring that the organization's CTEM practices align with relevant industry standards, regulations, and best practices (such as NIST, ISO, or PCI-DSS). This helps maintain compliance, demonstrate due diligence, and benchmark performance.

5. Integration and Collaboration

Establishing processes to integrate CTEM and RBVM activities with other cybersecurity and IT functions, such as incident response, change management, and project planning. Fostering collaboration between security, IT, and business teams is crucial for effective governance.

6. Continuous Improvement

Regularly reviewing and improving the governance framework based on lessons learned, industry developments, and changing business needs. This includes updating policies, refining processes, and investing in new tools and skills as needed.

strobes™

Quantifying GRC Goals

Asset Discovery & Coverage

- Percentages of assets being scanned using vulnerability scanners
- A number of assets have EDR, AV, Firewall, etc installed.
- Frequency or Timestamps for vulnerability, configuration, compliance scans
- Asset discovery for IOT, Cloud, On-prem, APIs, Application, etc.

strobes™

Quantifying GRC Goals

Vulnerability Identification and Assessment

- Combined view of all vulnerabilities divided by
  - Severity
  - Status
  - Priority
  - Assets
  - Owners

strobes™

Quantifying GRC Goals

Patch & Remediation Performance

- Mean time to remediate (MTTR)
- Number of vulnerabilities not compliant with your SLA policies

strobes™

Quantifying GRC Goals

Risk Quantification

- Current overall risk score
- Risk scores per business unit, asset groups, owners, etc.
- History of risk scores

strobes™

Quantifying GRC Goals

Compliance & Policy Adherence

- Percentage of assets and vulnerabilities in compliance with policies
- Number of policy violations or exceptions identified and addressed
- Audit and assessment results against industry standards (NIST, ISO, CIS, PCI DSS, etc.)

strobes™

Quantifying GRC Goals

Stakeholder Engagement and Communication

- Frequency and effectiveness of risk communication to executives
  - Number of tickets raised & patched
- Percentage of business units actively participating in CTEM
- Feedback and satisfaction scores from asset owners and stakeholders

strobes

Thank you for joining

Akhil Reni
CTO & Co-Founder
Strobes

https://twitter.com/akhilreni_hs

https://github.com/akhil-reni

https://www.linkedin.com/in/akhilreni/