Security Applications Open Discussion

HIPAA One

CROWDSTRIKE

AIRLOCK DIGITAL CROWDSTRIKE

Cyber CPR
A Logically Secure Product

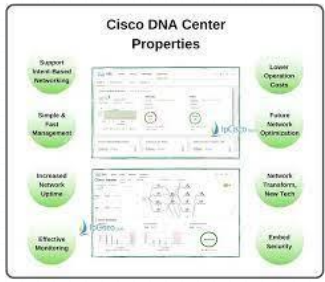
BITSIGHT
The Standard in SECURITY RATINGS

netskope

DUO

KEEPER
Cybersecurity Starts Here

Milton Kabia
ISSO/IT Security Director ANTHC
mkabia@anthc.org



CITRIX
Citrix NetScaler

RAPID7
insightVM

SECURELINK

01: Inventory and Control of Enterprise Assets

- **01: Inventory and Control of Enterprise Assets:** enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments.

Organization	Application

Application Type – General, business, or custom-made

Application Service Owner:

02: Inventory and Control of Software Assets

- 02: Inventory and Control of Software Assets: Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution

Organization	Application

Application Type – General, business, or custom-made
Application Service Owner:

03: Data Protection

- **03: Data Protection:** Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

Organization	Application

Application Type – General, business, or custom-made

Application Service Owner:

04: Secure Configuration of Enterprise Assets and Software

- **04: Secure Configuration of Enterprise Assets and Software:** Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

Organization	Application

Application Type – General, business, or custom-made

Application Service Owner:

05: Account Management:

- **05: Account Management:** Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

Organization	Application

Application Type – General, business, or custom-made

Application Service Owner:

06: Access Control Management

- **06: Access Control Management:** Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

Organization	Application

Application Type – General, business, or custom-made

Application Service Owner:

07: Continuous Vulnerability Management:

- **07: Continuous Vulnerability Management:** Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers.

Organization	Application

Application Type – General, business, or custom-made

Application Service Owner:

08: Audit Log Management:

- **08: Audit Log Management:** Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

Organization	Application

Application Type – General, business, or custom-made

Application Service Owner:

09: Email and Web Browser Protection:

- **09: Email and Web Browser Protection:** Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.

Organization	Application

Application Type – General, business, or custom-made

Application Service Owner:

10: Malware Defense:

- **10: Malware Defense:** Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

Organization	Application

Application Type – General, business, or custom-made

Application Service Owner:

11: Data Recovery:

- **11: Data Recovery:** Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

Organization	Application

Application Type – General, business, or custom-made

Application Service Owner:

12: Network Infrastructure Management:

- 12: Network Infrastructure Management: Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.

Organization	Application

Application Type – General, business, or custom-made

Application Service Owner:

13: Network Monitoring and Defense:

- **13: Network Monitoring and Defense:** Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.

Organization	Application

Application Type – General, business, or custom-made

Application Service Owner:

14: Security Awareness and Skills Training:

- **14: Security Awareness and Skills Training:** Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

Organization	Application

Application Type – General, business, or custom-made

Application Service Owner:

15: Service Provider Management:

- 15: Service Provider Management: Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.

Organization	Application

Application Type – General, business, or custom-made
Application Service Owner:

16: Application Software Security:

- **16: Application Software Security:** Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.

Organization	Application

Application Type – General, business, or custom-made

Application Service Owner:

17 Incident Response Management:

- **17 Incident Response Management:** Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

Organization	Application

Application Type – General, business, or custom-made

Application Service Owner:

18: Penetration Testing:

- 18: Penetration Testing: Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker

Organization	Application

Application Type – General, business, or custom-made

Application Service Owner:

Others

Risk Assessment Tools/Programs

Organization	Application

Application Type – General, business, or custom-made
Application Service Owner:

Others

Wireless Vulnerabilities
Assessment Tools/Applications

Organization	Application

Application Type – General, business, or custom-made
Application Service Owner:

Others

Border/DMZ/Firewall Security Applications

Organization	Application

Application Type – General, business, or custom-made
Application Service Owner:

CROWDSTRIKE

BITSIGHT
The Standard in SECURITY RATINGS

netskope

Milton Kabia
ISSO/IT Security Director ANTHC
mkabia@anthc.org