# CURRENT STATE OF CYBERSECURITY

# CYBER THREAT LANDSCAPE

# Today's Risk Landscape

America remains at risk from a variety of threats:

INSIDER THREAT

ACTS OF TERRORISM

CYBER ATTACKS

EXTREME WEATHER

PANDEMICS

ACCIDENTS OR TECHNICAL FAILURES

# CISA Cyber Hygiene Observations

## COMMON WEAKNESSES & THREATS:

- PHISHING SUSCEPTIBILITY
- USER/ACCOUNT PERMISSIONS
- PATCH MANAGEMENT
- UNSUPPORTED OPERATING SYSTEM & APPLICATIONS
- POTENTIALLY RISKY SERVICES
- NETWORK SEGMENTATION/CONFIGURATION

# RANSOMWARE

TLP:WHITE

- WHAT IS RANSOMWARE AND HOW DOES IT WORK?
- WHO IS AT RISK OF A RANSOMWARE ATTACK?
- HOW BIG OF A PROBLEM IS RANSOMWARE?


# RANSOMWARE

## HOW CAN YOU IMPROVE YOUR CYBERSECURITY?

- To minimize the risks of cyberattacks, follow basic cybersecurity best practices:
  - **Update** software and install patches.
  - Run up-to-date antivirus software.
  - Use **strong passwords**. A password manager can help keep track of them.
  - Change default usernames and passwords as soon as possible.
  - Implement multi-factor authentication, where you log in using a password and something else– like a code texted to your phone– to verify it's really you.
  - Install, configure, and enable a firewall.
  - Be suspicious of unexpected emails! They could be phishing to gain information, steal money, or install malware on your device.
- CISA has many resources and tips on CISA.gov, including Cyber Essentials which provides organizations with valuable information to bolster their cybersecurity.

# Misconceptions Vs. Reality

**MISCONCEPTIONS:**

- You need a BIG budget!
- A Silver Bullet Solution!
- Why would we be a target?
- There's too much to do!
- We don't own the risk!
- USG will save us!

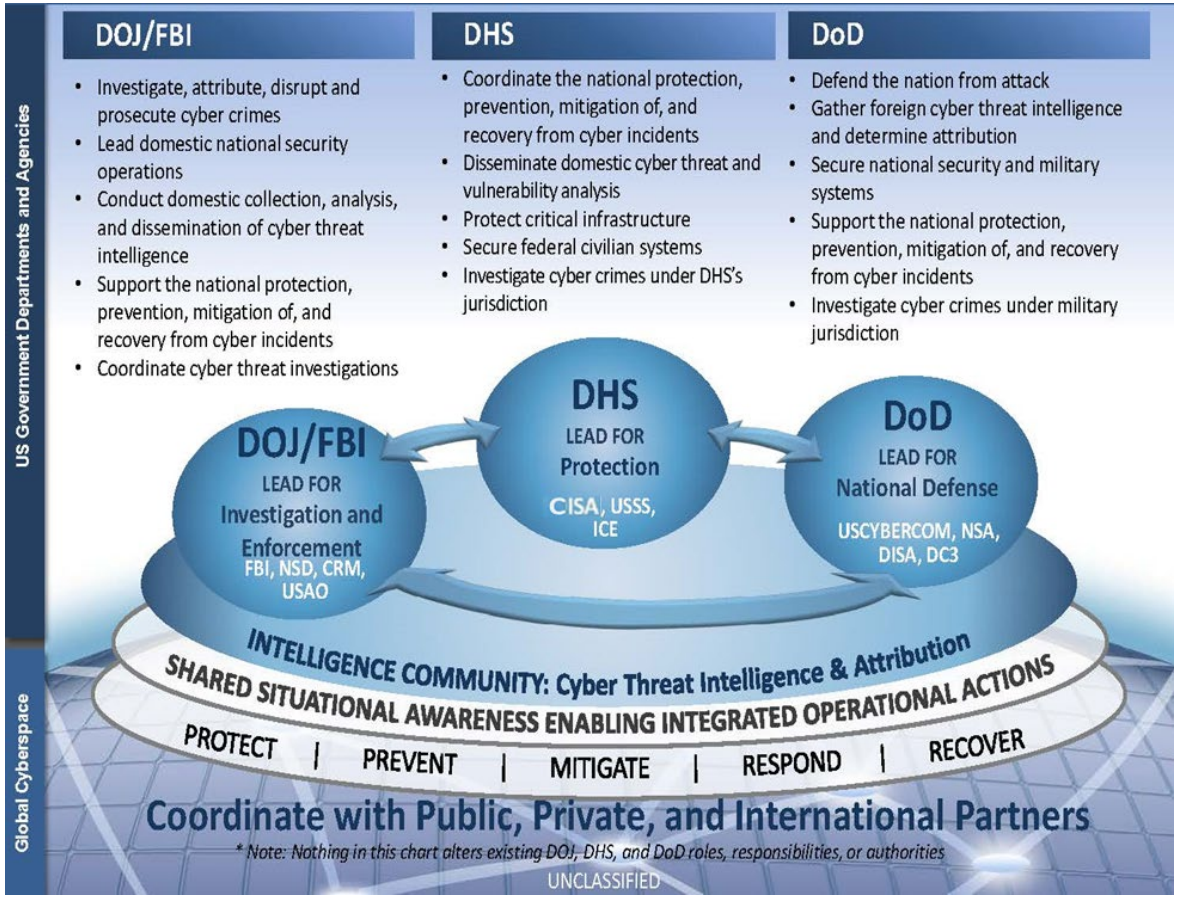
**REALITY:**

- Crawl-Walk-Run
- Get the "101" stuff in order
- You need good asset inventory
- Research the solutions!
- You own the risk!
- Partner-up!

# Federal Cybersecurity

## Whole of Government Response (DOJ/FBI, DHS/CISA, DoD)

- Presidential Directives
  - HSPD 5 — Domestic Incidents
  - PPD 8 — National Preparedness
  - PPD 21 — Critical Infrastructure Security & Resilience
  - PPD 41 — US Cyber Incident Coord Activities Defined
- Disseminates Domestic Cyber Threat Information
- Protects Critical Infrastructure
- Secures Federal Civilian Executive Branch Systems
- Directives are implemented through doctrine, policy, plans
  - National Cyber Strategy
  - National Preparedness System
  - National Infrastructure Protection Plan (NIPP)
  - National Cyber Incident Response Plan (NCIRP)



# From the Guidance

*Whether the applicant has implemented, or begun implementing, any Education Department or Cybersecurity and Infrastructure Security Agency (CISA) best practices recommendations (answered on a yes/no basis), a description of any Education Department or CISA free or low-cost cybersecurity resources that an applicant currently utilizes or plans to utilize, or an explanation of what is preventing an applicant from utilizing these available resources.*

# CISA Cybersecurity Offerings

TLP:WHITE

## Local CSA Provided

- **Preparedness Activities**
  - Information/Threat Indicator Sharing
  - Cybersecurity Training and Awareness
  - Cyber Exercises and “Playbooks”
  - National Cyber Awareness System
  - Vulnerability Notes Database
  - Information Products and Recommended Practices / MS-ISAC – EI-ISAC
  - **Cybersecurity Service Offerings**
    - Cyber Resilience Reviews (**CRR**)
    - External Dependency Management (**EDM**)
    - Cyber Infrastructure Surveys (**C-IST**)
    - Cyber Security Evaluation Tool (**CSET**)

## CISA HQ Response Assistance

- Remote / On-Site Assistance
- Malware Analysis
- Hunt and Incident Response Teams
- Incident Coordination

## Cybersecurity Advisors (CSA)

- Assessments
- Working group collaboration
- Resiliency Workshops
- Best Practices private-public
- Incident assistance coordination

## Protective Security Advisors

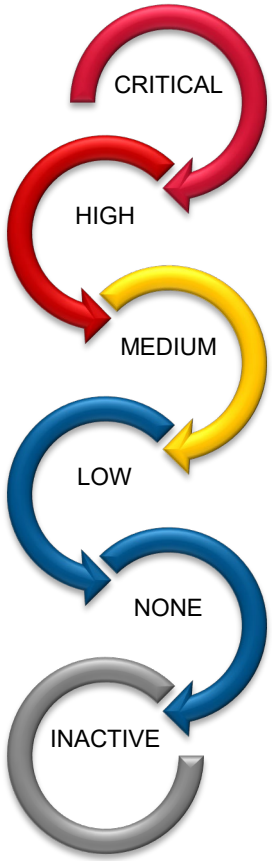
- Physical Security Assessments
- Incident liaisons between government and private sector for CI protection
- Support for National Special Security Events

## Delivered by CISA Vulnerability Mgt Team

- Cyber Hygiene Scanning (CyHy)
- Web Application Scanning (WAS)
- Remote Penetration Testing (RPT)
- Risk & Vulnerability Assessment (RVA)
- Red Team Assessment (RTA)
- Validated Architecture Design (VADR)
- Critical Product Evaluation (CPE)
- CISA Qualification Initiative (CQI)

# CyHy: Cyber Hygiene Scanning

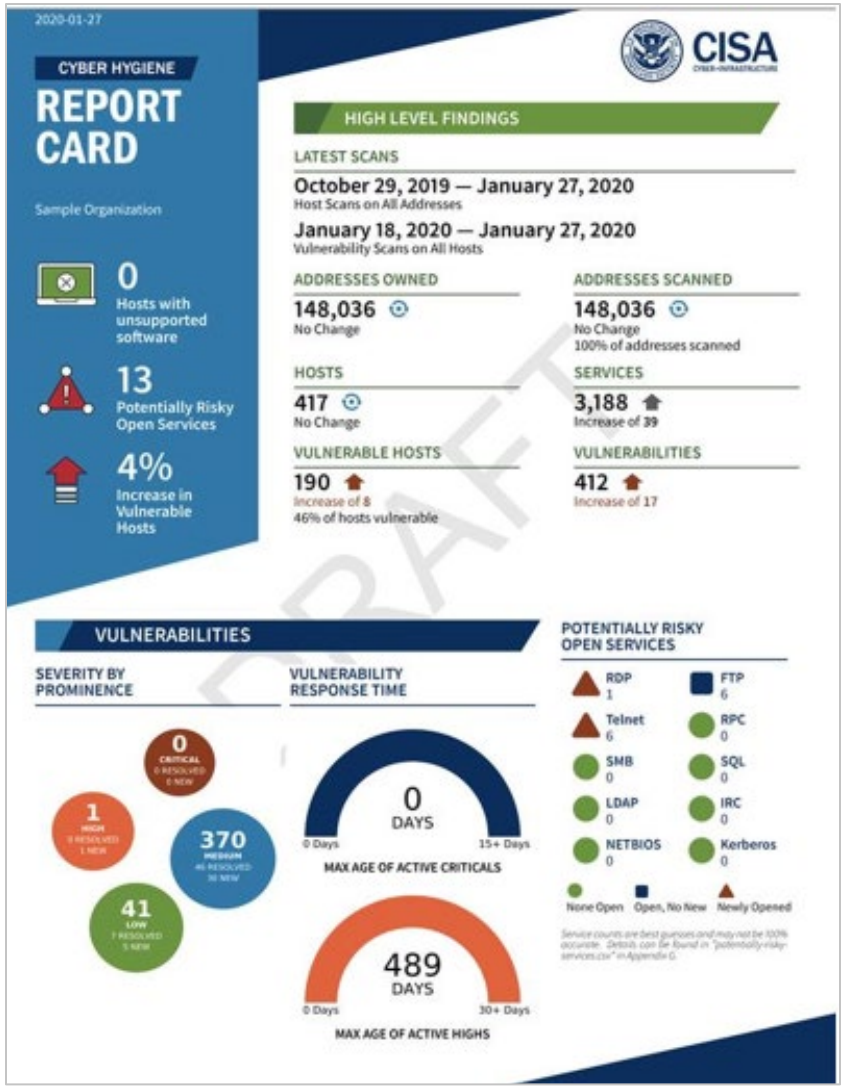
## System & Application Vulnerability Scanning




- Automated scanning of Internet accessible systems (Top 1000 Ports / NMAP & NESSUS)
- Weekly report card that include current scan results, historic trends, and result comparisons to the national average
- Helps individual customers understand their exposure
- Informs national risk management efforts
- Federal agencies must mitigate critical vulnerabilities within 30 days of detection
- Scans can start within 72 hours!
- Unlimited capacity of subscribers

# CyHy: Cyber Hygiene Scanning Report Card

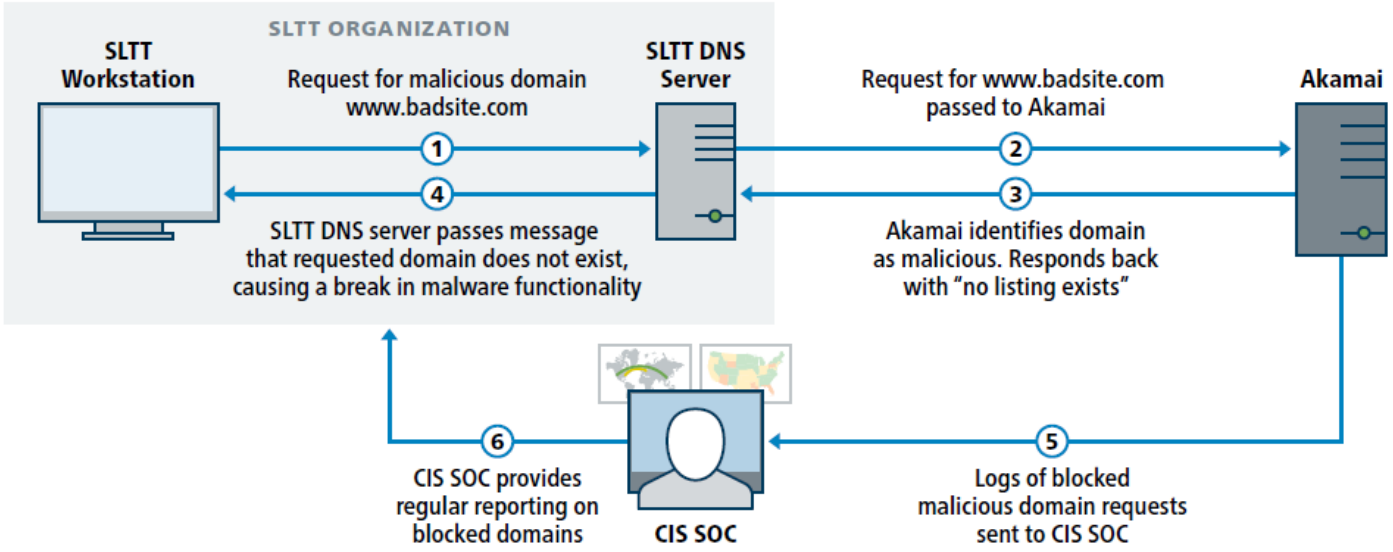
TLP:WHITE



# MS-ISAC's Malicious Domain Blocking and Reporting

- MDBR technology prevents IT systems from connecting to harmful web domains, helping limit infections related to known malware, ransomware, phishing, and other cyber threats. This capability can block the vast majority of ransomware infections just by preventing the initial outreach to a ransomware delivery domain.

MDBR proactively blocks network traffic from an organization to known harmful web domains, helping protect IT systems against cybersecurity threats. Once an organization points its domain name system (DNS) requests to the Akamai's DNS server IP addresses, every DNS lookup will be compared against a list of known and suspected malicious domains. Attempts to access known malicious domains such as those associated with malware, phishing, and ransomware, among other threats, will be blocked and logged. CIS will then provide reporting that includes log information for all blocked requests and assist in remediation if needed.




https://www.cisecurity.org/ms-isac/services

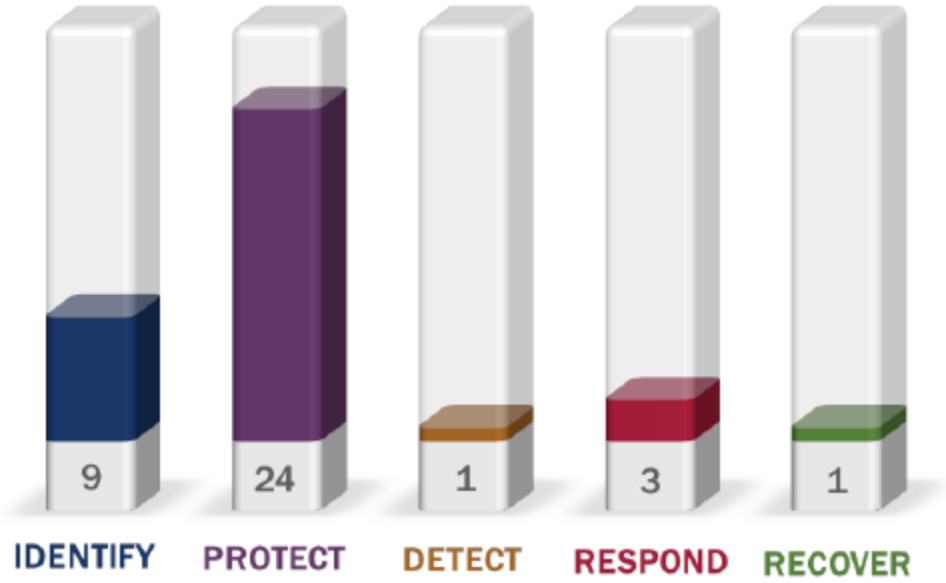
# CROSS-SECTOR CYBERSECURITY PERFORMANCE GOALS

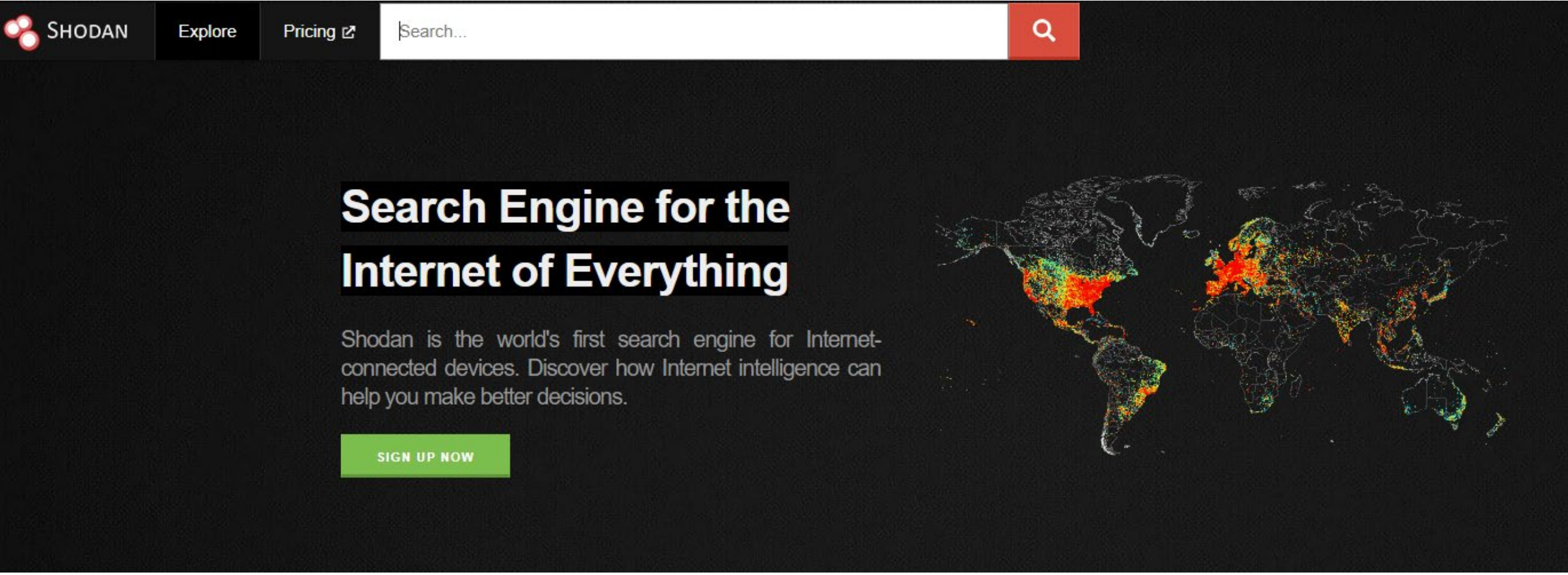
TLP:CLEAR

Adobe Acrobat Document

## CPGs BY CATEGORY

Total # of CPGs: 38






Shodan (www.shodan.io) is a web-based search platform for Internet connected devices. This tool can be used not only to identify Internet connected computers and Internet of Things/Industrial Internet of Things (IoT/IIoT), but also Internet connected Industrial Control Systems (ICS) and platforms.

# Stuff Off Search

| Shodan | Censys | Thingful |
|---|---|---|
| Shodan is a web-based search platform for internet connected devices.<br><br>Key features:<br>• Identify Internet connected devices, Internet of Things/Industrial Internet of Things (IoT/IIoT), and industrial control systems (ICS).<br>• Potential exploits.<br>• Default passwords.<br>• Integrations with vulnerability tools, logging aggregators and ticketing systems allow Shodan to be seamlessly integrated into an enterprise.<br><br>https://www.shodan.io | Censys is a web-based risk management tool that helps identify publicly accessible assets —even if they can't be scanned by a vulnerability management tool.<br><br>Key features:<br>• Home network risk identifier (HNRI), allowing employers to anonymously monitor staff's home network infrastructure for vulnerabilities that may pose a risk to the company.<br>• Exposed routers.<br>• Default credentials.<br>• Popular vectors for ransomware.<br><br>https://www.censys.io | Thingful is a search engine for the Internet of Things (IoT).<br><br>Key features:<br>• Searchable index of public and private connected objects and sensors around the world.<br>• Monitors IoT networks and infrastructures including energy, radiation, weather, and air quality devices.<br>• Reports seismographs, iBeacons, vehicles, ships, aircraft and animal trackers. The tool assists with response by enabling end users to create watchlists and publications on public/private IoT resources.<br><br>https://www.thingful.net/ |

# STEPS YOU SHOULD TAKE

1. ESTABLISH OR CHECK YOUR BACKUPS
   3-2-1 RULE
2. MFA EVERYTHING
3. PATCH THE KNOWN EXPLOITED VULNERABILITIES

# How to Reach Us

## Contact Information


**Colin Glover**
**Kentucky Cybersecurity State Coordinator/**
colin.glover@cisa.dhs.gov
(202) 380-5741 (Cell)

**Ryan Lewis**
**Kentucky Cybersecurity Advisor**
ryan.lewis@cisa.dhs.gov
(202) 975-9453 (Cell)