# 2024 Kickoff: A vCISO's Blueprint for Cybersecurity Success

**Felicia King**

President and CISO
at QPC Security

## Why this topic?

- Achieve ROSI - return on security investment
- Stop being the chew toy; be defensible
- Where to focus efforts?
- Don’t squirrel on shiny objects

## **Felicia King** President and CISO at QPC Security

- > 50,000 hours network security architect
- > 29 years experience
- > 300 network and systems rearchitecture projects
- Consulted 15 companies with >10,000 users
- Radio show and podcast since 2004
- CISO channel on The Tech Tribe
- ASCII product advisory board
- Inventor of microsegmentation net sec hardening solutions at scale
- Inventor of school lockdown solution
- Co-inventor of safety system for U.S. manufacturing industry
- > 10 yrs as vCISO in complex environments

# Access original content not rehashed news

Articles and educational resources

https://www.qpcsecurity.com/category/educational-articles

Security podcasts and career resources

https://qpcsecurity.podbean.com/

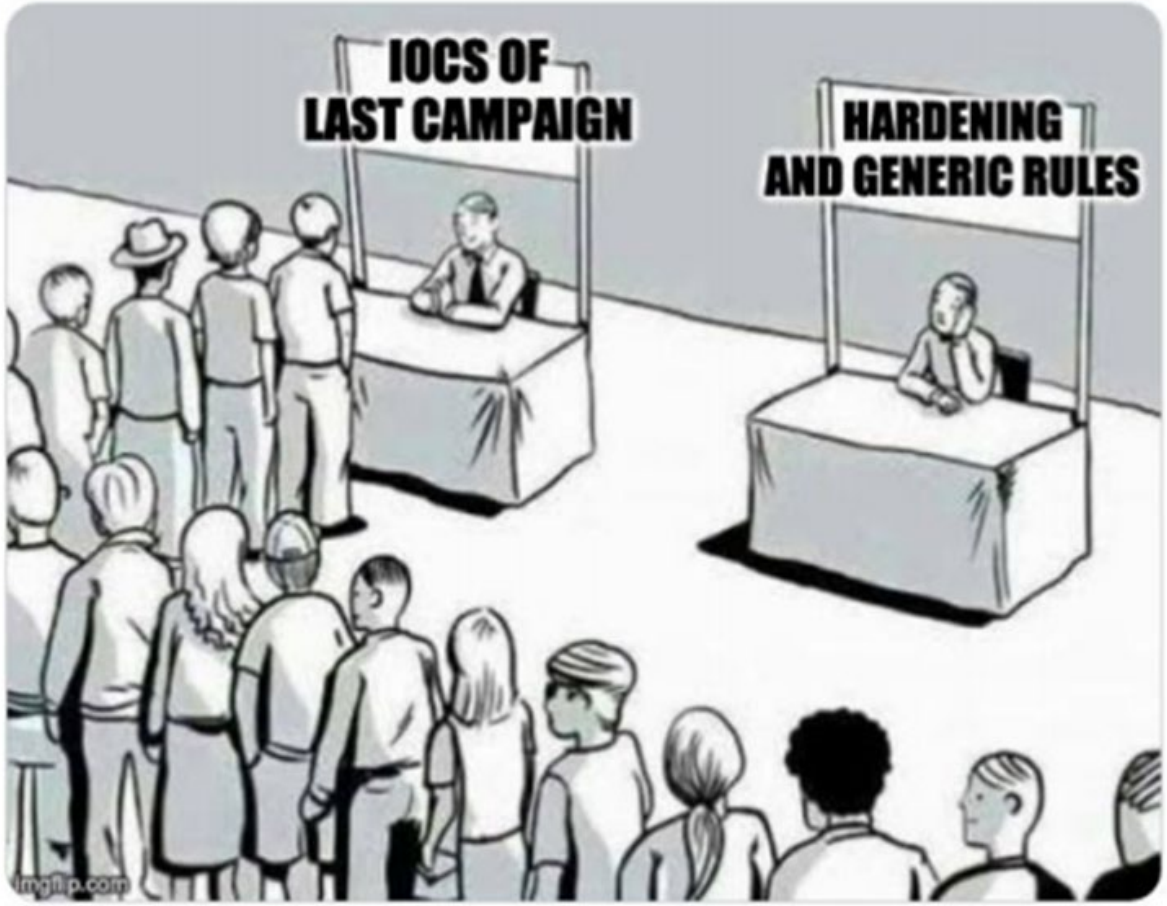
Follow

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

Other career resources

https://www.qpcsecurity.com/careers/

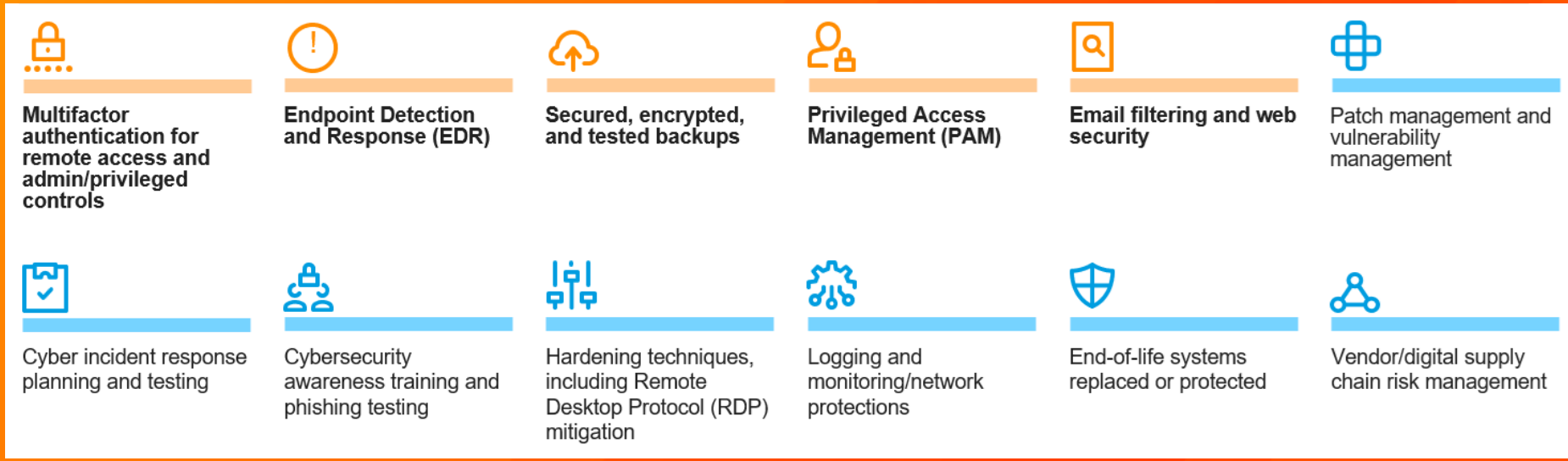
The typical approach
#Ransomware




Stop squirreling on shiny objects when the fundamentals have not been made completely rock solid.

This is where malinvestment comes from.
More tools will not solve fundamental problems.

Be legally defensible OR consequences ….
No issued policy, high premiums, denied claims.
Non-tamperable attestation proof is mandatory!
If you said it was in place PROVE IT and establish a pattern of evidence.



# Strategy

Use a framework, a risk assessment model to assess, prioritize, and communicate information security roadmap

Please do not buy $10,000 tools until you have exhausted what you can do for free.

Assess -> Prioritize -> Fix

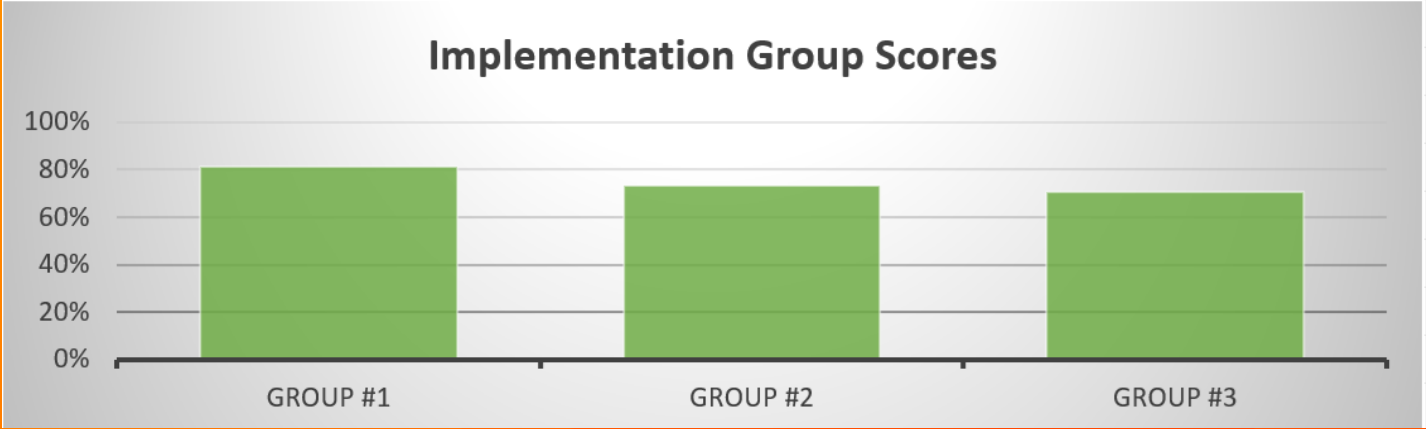
What is the current state?

What is the future state?

When will we get there?

How much will it cost?

| Implementation Group Scores | | | | | |
|---|---|---|---|---|---|
| Group #1 | 81% | Group #2 | 74% | Group #3 | 70% |




Pick a standard to start with.
Master CIS before blowing time on other frameworks of risk assessment.
Get a copy of CIS and get busy.

| Maturity level: | Description: | Score: |
|---|---|---|
| Level One | Policies Complete | 0.32 |
| Level Two | Controls 1-5 Implemented | 0.74 |
| Level Three | All Controls Implemented | 0.70 |
| Level Four | All Controls Automated | 0.73 |
| Level Five | All Controls Reported | 0.65 |
| | | |
| | Maturity Rating*: | 3.15 |
| | *Rating is on a 0-5 scale. | |

# CIS sandwich - shared responsibility

| Position | CIS area | Who |
|---|---|---|
| Foundational bottom layer bread | Approved written policy | Org leadership, CISO + Execs |
| Meat | Control implemented | Security architect & IT |
| Veggies | Control automated or technically enforced | Security architect & IT |
| Top layer of bread | Control reported to business | Compliance officer |

Realize that it all starts with policy and ends with validation / attestation

IT gets authority and support for technical controls from POLICY

CIS Community Defense Model

https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0

# What are the top 6 things you can do in order to get ROSI?

**Table 6.** CIS Safeguards that had the highest number of mapped ATT&CK (sub-)techniques

| RANK | CIS SAFEGUARD | CIS SAFEGUARD TITLE | NUMBER OF ATT&CK (SUB-) TECHNIQUES DEFENDED BY A CIS SAFEGUARD | IG1 | IG2 | IG3 |
|---|---|---|---|---|---|---|
| 1 | 4.1 | Establish and Maintain a Secure Configuration Process | 342 | ✓ | ✓ | ✓ |
| 2 | 6.1 | Establish an Access Granting Process | 217 | ✓ | ✓ | ✓ |
| 3 | 6.2 | Establish an Access Revoking Process | 217 | ✓ | ✓ | ✓ |
| 4 | 18.3 | Remediate Penetration Test Findings | 214 | | ✓ | ✓ |
| 5 | 6.8 | Define and Maintain Role-Based Access Control | 206 | | | ✓ |
| 6 | 4.7 | Manage Default Accounts on Enterprise Assets and Software | 188 | ✓ | ✓ | ✓ |
| 7 | 18.5 | Perform Periodic Internal Penetration Tests | 187 | | | ✓ |
| 8 | 5.4 | Restrict Administrator Privileges to Dedicated Administrator Accounts | 164 | ✓ | ✓ | ✓ |
| 9 | 5.3 | Disable Dormant Accounts | 155 | ✓ | ✓ | ✓ |
| 10 | 2.5 | Allowlist Authorized Software | 101 | | ✓ | ✓ |
| 11 | 2.7 | Allowlist Authorized Scripts | 81 | | | ✓ |
| 12 | 3.3 | Configure Data Access Control Lists | 75 | ✓ | ✓ | ✓ |
| 13 | 4.2 | Establish and Maintain a Secure Configuration Process for Network Infrastructure | 73 | ✓ | ✓ | ✓ |
| 14 | 2.3 | Address Unauthorized Software | 67 | ✓ | ✓ | ✓ |
| 15 | 4.4 | Implement and Manage a Firewall on Servers | 60 | ✓ | ✓ | ✓ |
| 16 | 4.8 | Uninstall or Disable Unnecessary Services on Enterprise Assets and Software | 54 | | ✓ | ✓ |
| 17 | 13.8 | Deploy a Network Intrusion Prevention Solution | 53 | | | ✓ |
| 18 | 13.3 | Deploy a Network Intrusion Detection Solution | 53 | | ✓ | ✓ |
| 19 | 12.2 | Establish and Maintain a Secure Network Architecture | 51 | | ✓ | ✓ |
| 20 | 5.2 | Use Unique Passwords | 47 | ✓ | ✓ | ✓ |

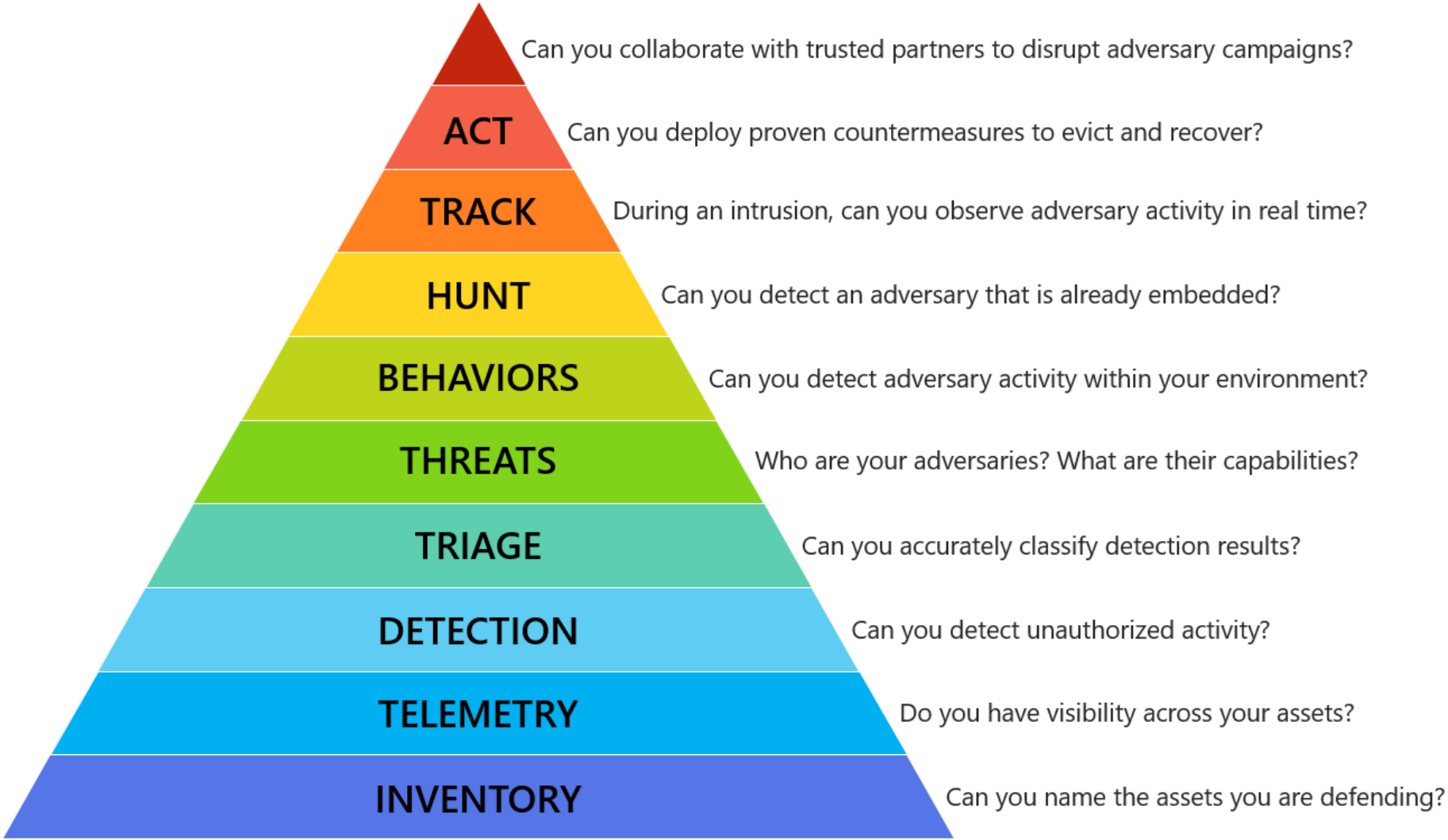
# Vuln mgmt - Are you doing at least this?

- GPO central store
- Software and asset reconciliation monthly
- EOL/EOS removal
- Continuous vuln assessment internal/external
- Assess CIS gaps compliance
- iDrac, bios, firmware, drivers, OMSA, DSU, DCU
- Unique bios admin and local admin
- SQL
- Full disk encryption
- Websites
- Browser config management
- Business line apps - no patch automation
- SSRS hardening
- NTLM disable, LLMNR, samRPC, SMB ver control
- PowerShell upgrade and disable old versions
- Krbtgt roll
- Tiered access control
- PAWs and microsegmentation
- PBX, cams, door controllers, speakers, NAS
- Hypervisor, backup software

# 10 Best Practices - Cyber Hygiene InfoSec rabbit approved

- Run continuous IT asset scans and monitor hardware and software
  Use an asset management platform!
- Perform vulnerability scans every day, assess detected vulnerabilities, and remediate them
- Patch all software and firmware, especially critical vulnerabilities in accordance with the vulnerability management policy
- Ensure endpoint protection software is installed and updated regularly
- Impose strict password policies and prevent users from setting weak passwords
- Identify deviated system settings and harden endpoints to meet security compliance standards
- Evaluate system health, user login credentials, services, and processes regularly
- Analyze software usage, blacklist rogue assets, and manage license violations
- Block rogue applications and unwanted USB devices that pose security threats
- Detect and respond to indications of attacks and compromise immediately

**Make Whiskers happy with good cyber hygiene practices**


Can you collaborate with trusted partners to disrupt adversary campaigns?
ACT
Can you deploy proven countermeasures to evict and recover?
TRACK
During an intrusion, can you observe adversary activity in real time?
HUNT
Can you detect an adversary that is already embedded?
BEHAVIORS
Can you detect adversary activity within your environment?
THREATS
Who are your adversaries? What are their capabilities?
TRIAGE
Can you accurately classify detection results?
DETECTION
Can you detect unauthorized activity?
TELEMETRY
Do you have visibility across your assets?
INVENTORY
Can you name the assets you are defending?

# Vulnerability management deep dive

- Stop calling it patch management. It’s not about patches, it is about multi-layered vulnerability management. Paradigm shift!
- https://qpcsecurity.podbean.com/e/vulnerability-management-part-1/
- https://qpcsecurity.podbean.com/e/vulnerability-management-with-felicia-and-dan-part-2/