

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Maximizing Security:

Understanding CIS Controls[®] and CIS Benchmarks[™]

Kyle Winters, Technical Advocate
@kyle_m_winters
DEVNET-2328

CISCO *Live!*

#CiscoLiveAPJC

Cisco Webex App

Questions?

Use Cisco Webex App to chat with the speaker after the session

How

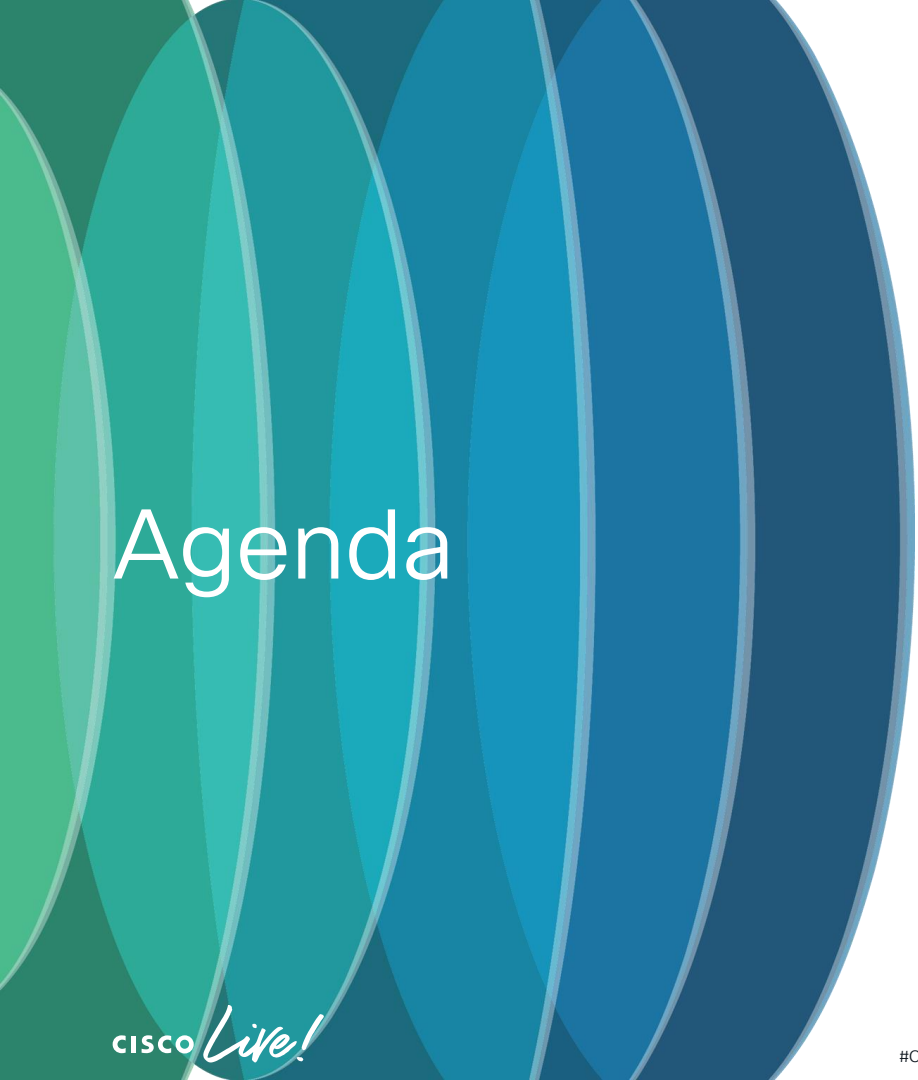
- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#DEVNET-2328>

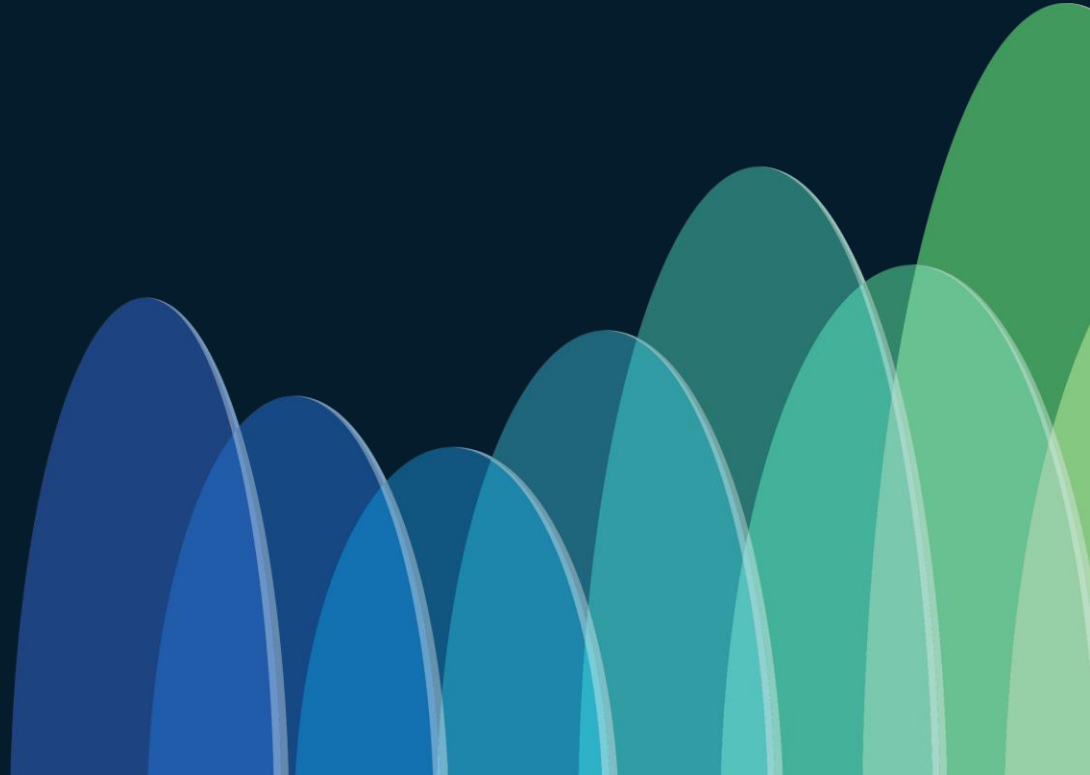




Agenda

- The Cybersecurity Landscape
- Introduction to the Center for Internet Security (CIS)
- Understanding CIS Controls®
- Understanding CIS Benchmarks™
- Conclusion

The Cybersecurity Landscape



“More than 85% of organizations will embrace a cloud-first principle by 2025 and will not be able to fully execute on their digital strategies without the use of cloud-native architectures and technologies”

Gartner

A New Application Paradigm



Agility

Can pivot to new ideas



Velocity

Bring features to market faster



Specificity

Can leverage new technologies
as new problems emerge



Visibility

Hard to track new things being
released and cleaning up old
things left behind



Scale

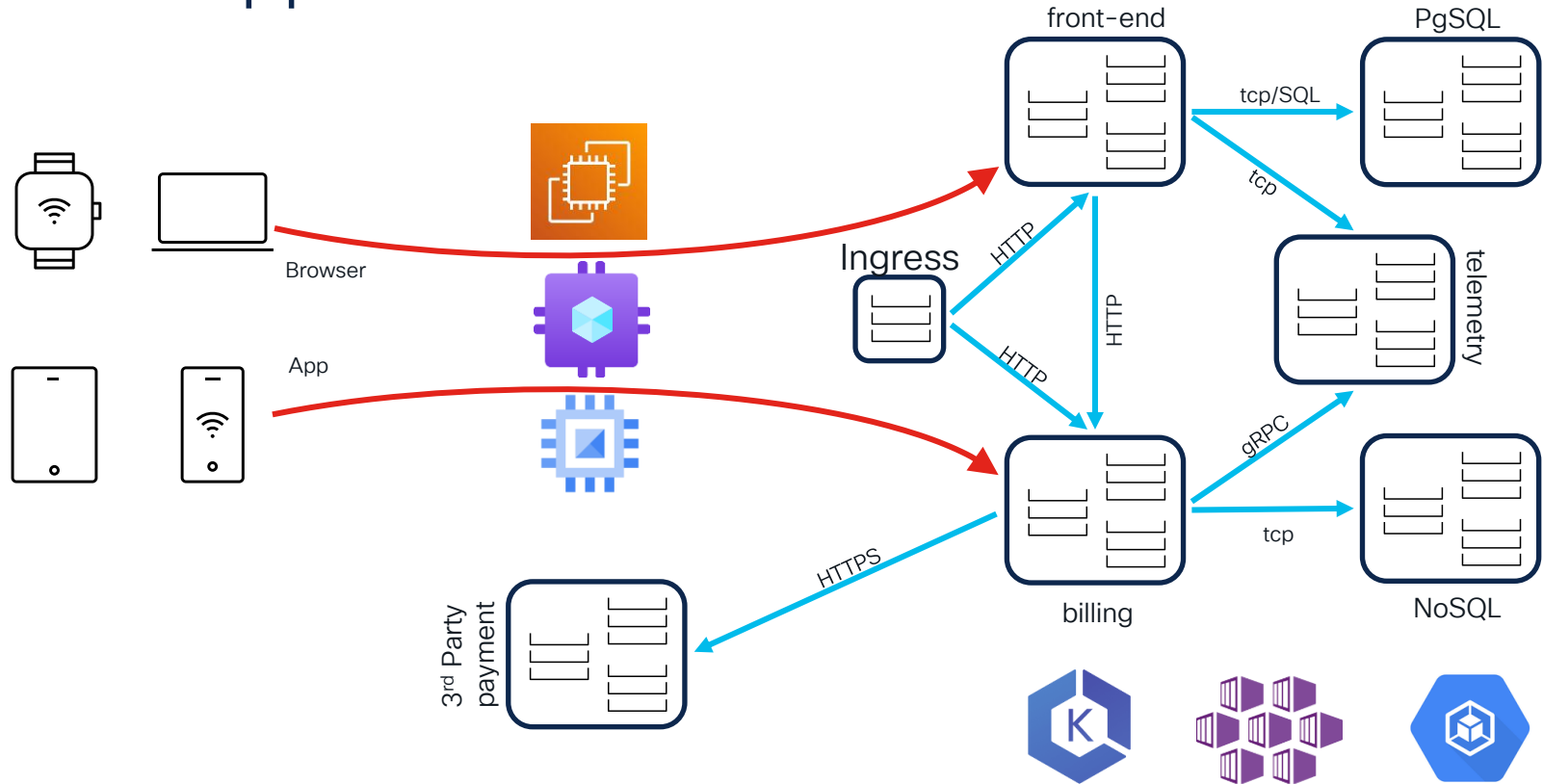
Larger attack surface as we
publish more features and
services



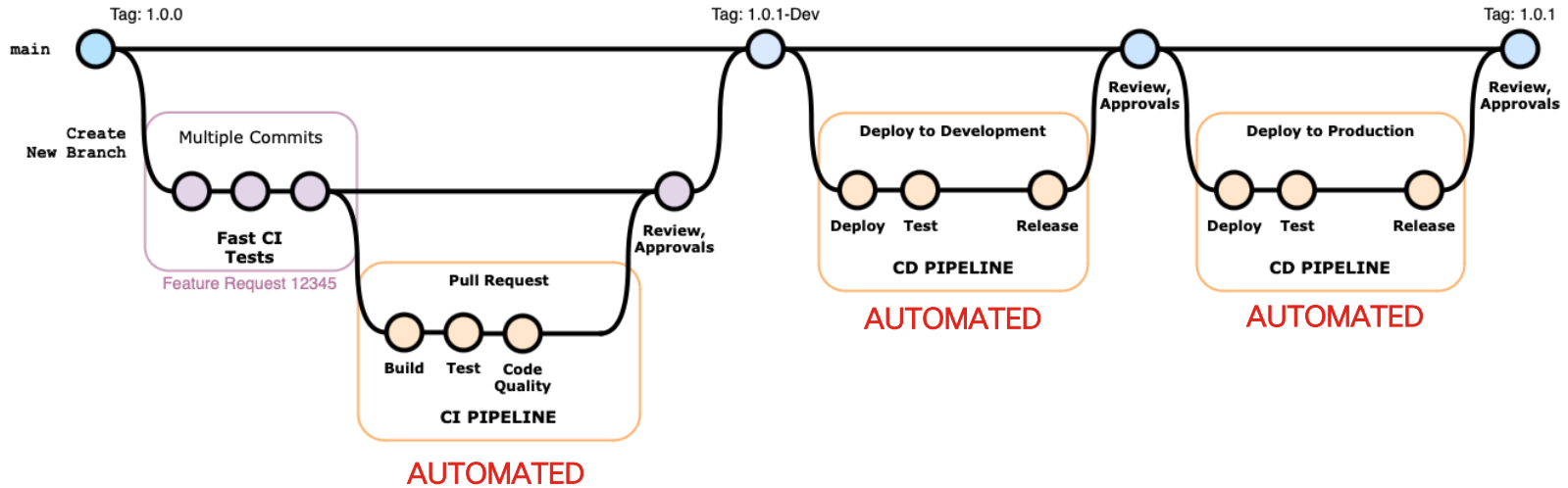
Complexity

New attack vectors emerge
based on new technology

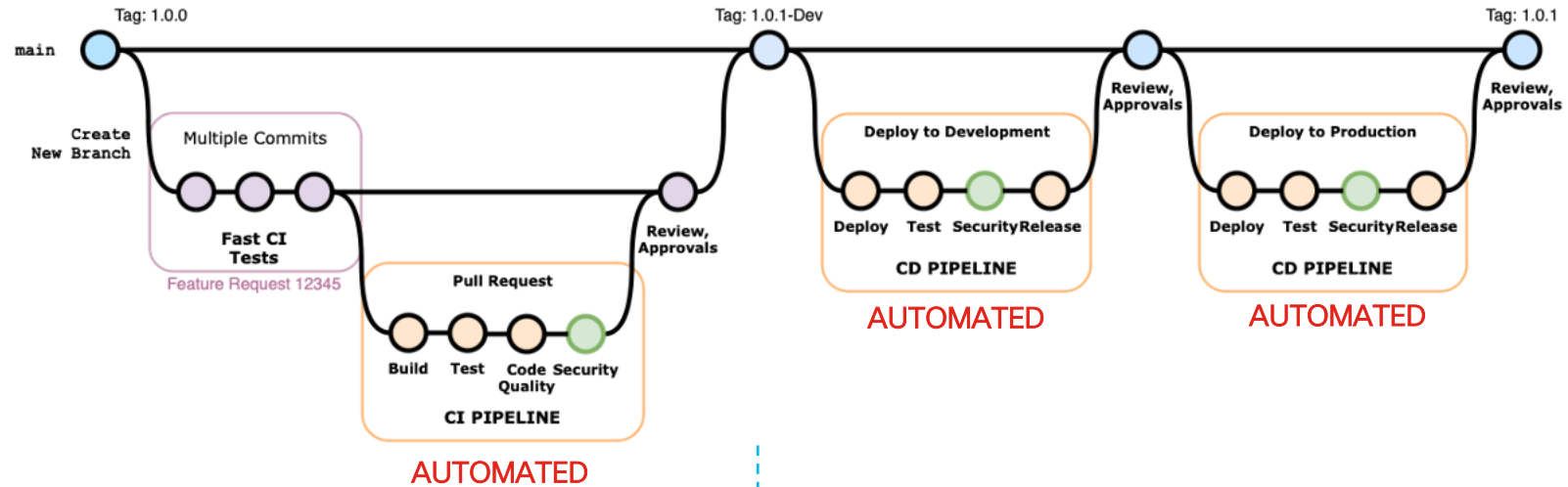
A New Application Architecture



A New Application Development Process



A New Application Security Process

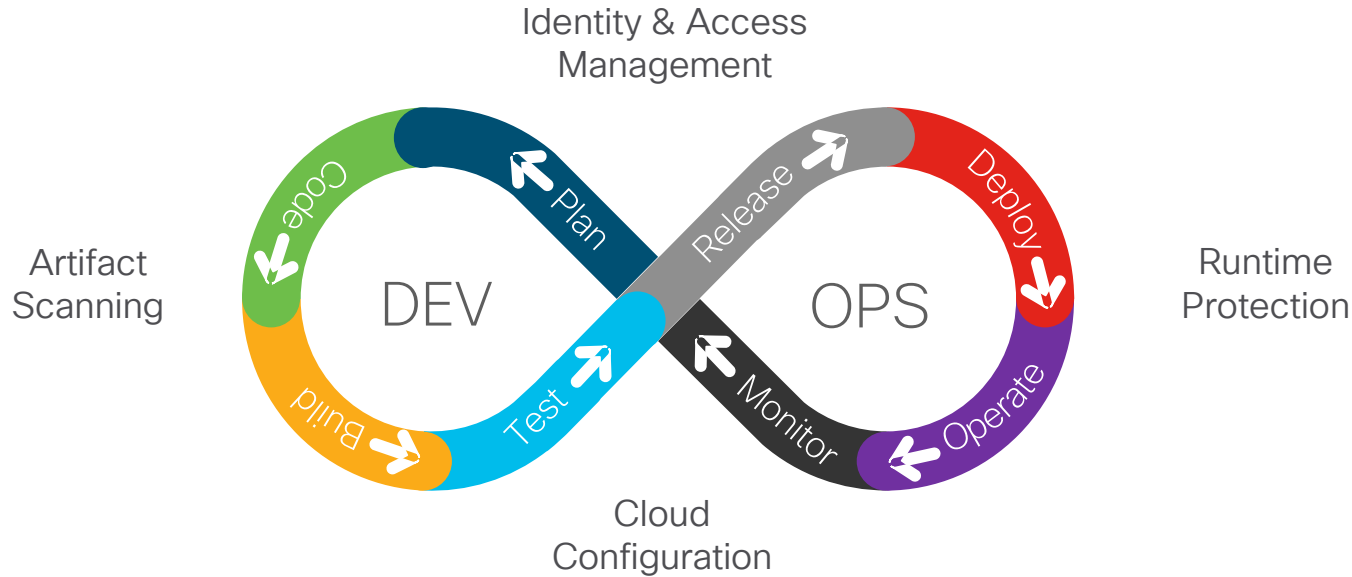


Apply Security Before *Any* Integration

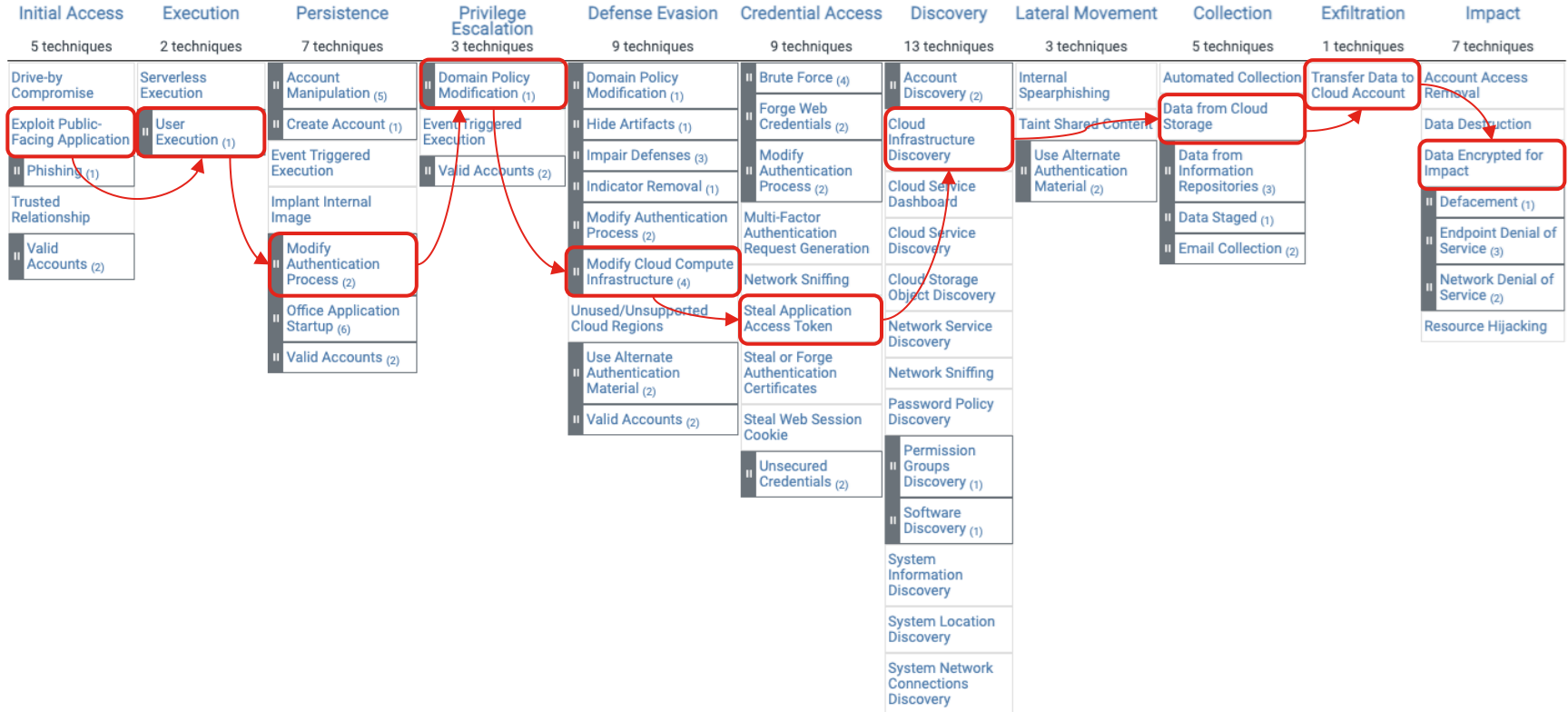
Apply Security Before *Every* Deployment

Shifting Security to the Left

Protecting Apps from Development to Runtime



Threats Are Becoming More Complex



Time is Money and it's Expensive



\$4.4M

Global average cost of
a breach in 2023



\$9.8M

Average cost of a
breach
in the US in 2023



\$10.9M

Average cost of a
healthcare breach in
the US in 2023



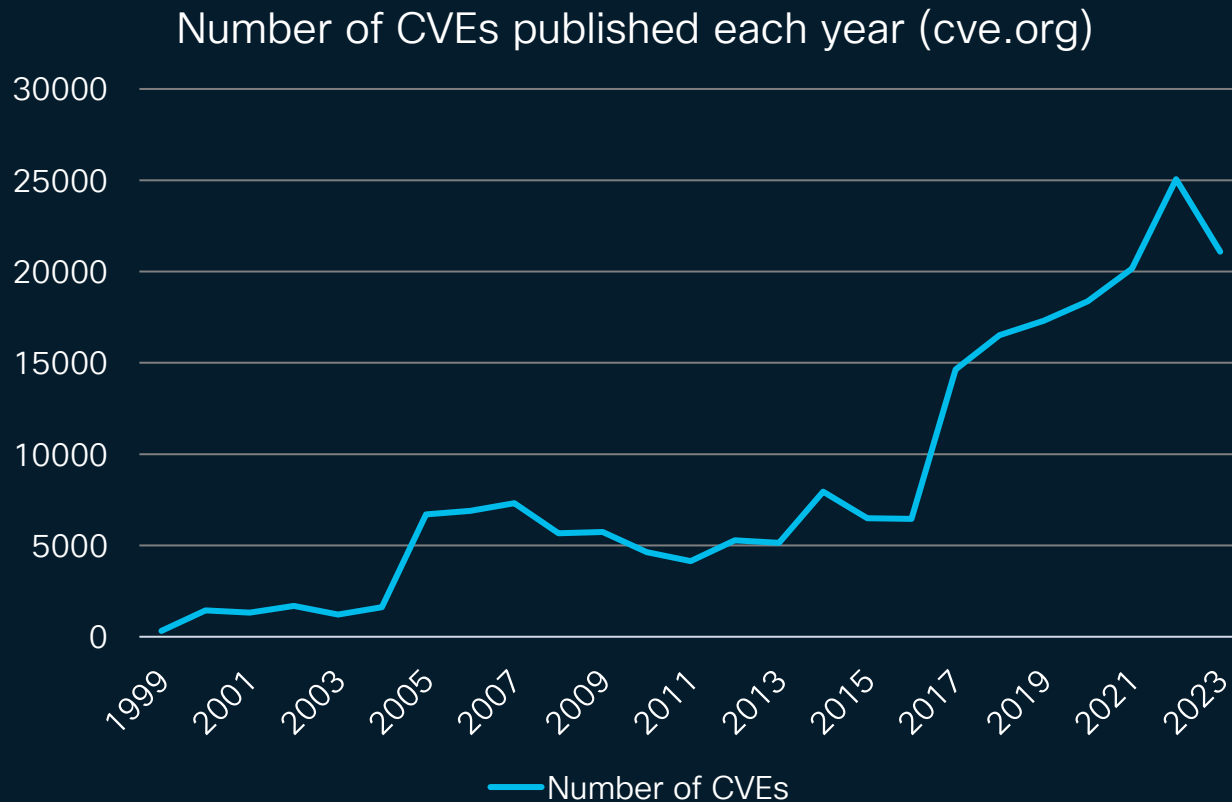
\$10.5T

Forecast of global
costs in cybercrime
by 2025

CISCO *Live!*



Hundreds of New Vulnerabilities Discovered Weekly



Threats Are Becoming More Expensive



21 mins

Average time from
credential discovery to
attack initiation



\$4.4M

Global average cost of a
breach in 2023



\$1.02M

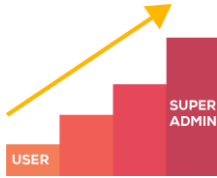
Cost savings for
breaches discovered in
less than 200 days



\$1.44M

Increased costs when
security system
complexity is high

Complex Threats Built Upon Avoidable Mistakes



80%

of security breaches
involve privileged
credentials



78%

of identified attack paths
use known vulnerabilities
(CVEs) as an initial
access attack vector



3

the average number of
steps in an attack path
to reach a crown jewel
asset

How serious are misconfigurations?



of cloud breaches will have a
root cause of a preventable
misconfiguration

Complex Threats Built Upon Avoidable Mistakes



70%

of organizations have a
Kubernetes API server that is
publicly accessible



72%

of organizations have at
least one S3 bucket that
allows public “read”
access



36%

of organizations keep
unencrypted secrets and
personally identifiable information
(PII) in these cloud services

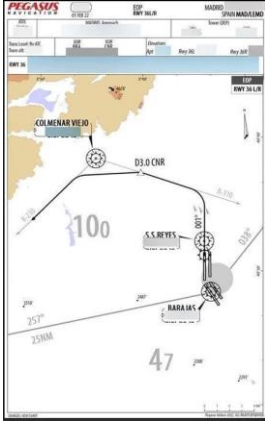
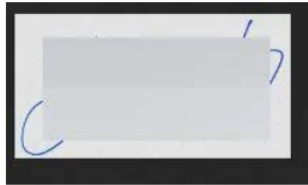
Pegasus Airlines Breach



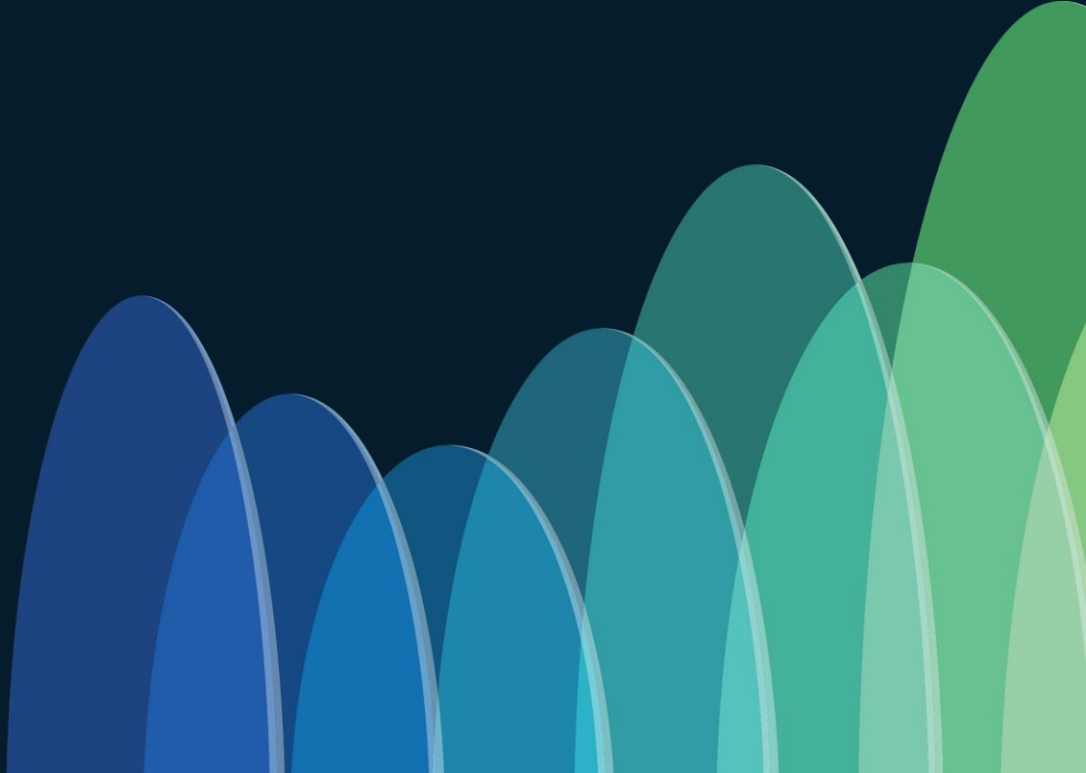
An unsecured AWS S3 bucket exposed 23 million files – or 6.5 terabytes of sensitive data, which included:

- Crew member Personal Identifiable Information (PII) such as photos and signatures
- Source code including additional plain text passwords
- Flight charts
- Airport runway maps and refueling information
- Takeoff and landing procedures

Exposure of this highly-sensitive information put Pegasus crew and passengers at risk



Introduction to the Center for Internet Security (CIS)



What is the Center for Internet Security (CIS)?

Mission:

- To make the connected world a safer place by developing, validating, and promoting timely best practice solutions that help people, businesses, and governments protect themselves against pervasive cyber threats.

Vision:

- Leading the global community to secure our ever-changing connected world.

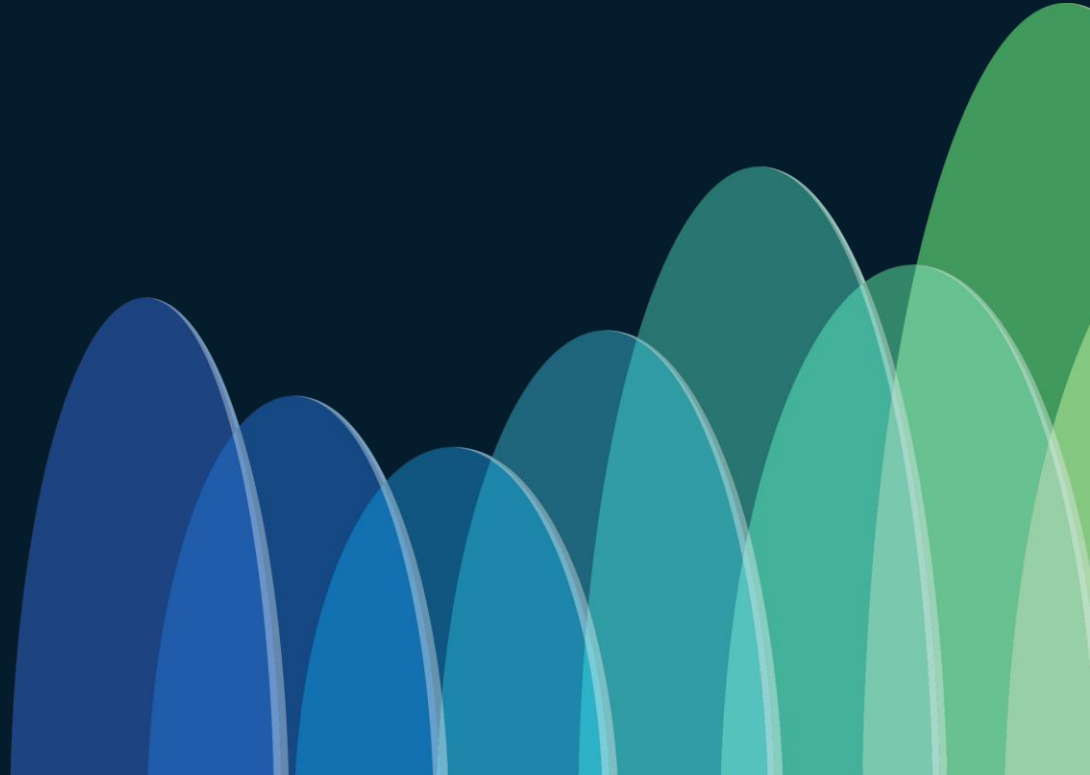


What is the Center for Internet Security (CIS)?

- A community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™.
- Develop and promote consensus-based, internationally recognized security best practices.
- Facilitate collaboration among industry experts, government agencies, and academia to address emerging cyber threats.



Understanding CIS Controls®



What are CIS Controls™ ?

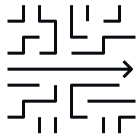
- The CIS Critical Security Controls (CIS Controls®) are a prescriptive, prioritized, and simplified set of best practices that you can use to strengthen your cybersecurity posture.
- The CIS Controls® consist of 18 overarching measures that help strengthen your cybersecurity posture. They prioritize activities over roles and device ownership.
- Today, thousands of cybersecurity practitioners from around the world use the CIS Controls® and/or contribute to their development via a community consensus process.

“The CIS Controls® take the background and knowledge of cybersecurity experts literally around the world and help focus efforts on things that are of most value. Directly impacting the adversaries and challenges we face today on our networks.”

Harley Parkes

Director, ACD (Integrated Adaptive Cyber Defense)

With CIS Controls®, You Can...



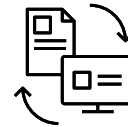
Simplify Your
Approach to
Threat Protection



Comply with
Industry
Regulations



Achieve
Essential Cyber
Hygiene



Translate
Information into
Action



Abide by the
Law

Comply With Industry & Government Regulations

Australian Signals Directorate
Essential Eight

FFIEC-CAT

MITRE ATT&CK v8.2

PCI DSS

CISA Cybersecurity
Performance Goals (CPGs)

GSMA FS 31 Baseline
Security Controls

NERC-CIP

NYS Department of Financial
Services 23 NYCRR Part 500

CMMC

HIPAA

New Zealand Information
Security Manual v3.5

SOC 2

Criminal Justice Information
Services (CJIS)

ISACA COBIT 19

NIST CSF 1.0

TSA Security Defense
Directive Pipeline

CSA Cloud Controls
Matrix v4

ISO 27001:2022

NIST CSF 2.0

UK Cyber Essentials

Cyber Risk Institute (CRI)
Profile v1.2

ISO/IEC 27002:2022

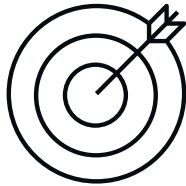
NIST SP 800-53 R5

UK National Cyber Security
Centre (NCSC) Cyber
Assessment v3.1

Microsoft Cloud
Security Benchmark

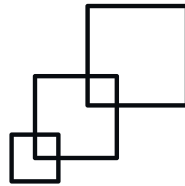
NIST SP 800-171

The Importance of CIS Controls®



Risk-Based Approach

CIS Controls® are designed to be implemented in a risk-based, prioritized manner, ensuring that organizations focus on the most critical actions first.



Scalability

The tiered structure of the Implementation Groups allows organizations to scale their cybersecurity efforts based on their size, complexity, and risk profile.



Measurable Outcomes

Implementing CIS Controls® provides measurable security improvements, making it easier for organizations to track their progress and demonstrate compliance with industry standards.

“We use the CIS Controls® to help our clients achieve compliance with state and federal cybersecurity regulations. The CIS 18 are prioritized, easy to understand, and extremely cost-effective for small to mid-size organizations looking to prove they are secure enough to do business in today’s marketplace. I highly recommend starting with CIS in building your cybersecurity program.”

Jim Long

Managing Partner – The Long Law Firm, PLLC

Structure of the CIS Controls®

Overview:

A brief description of the intent of the Control and its utility as a defensive action

Why is this Control critical?:

A description of the importance of this Control in blocking, mitigating, or identifying attacks, and an explanation of how attackers actively exploit the absence of this Control

Procedures and tools:

A more technical description of the processes and technologies that enable implementation and automation of this Control

Safeguard descriptions:

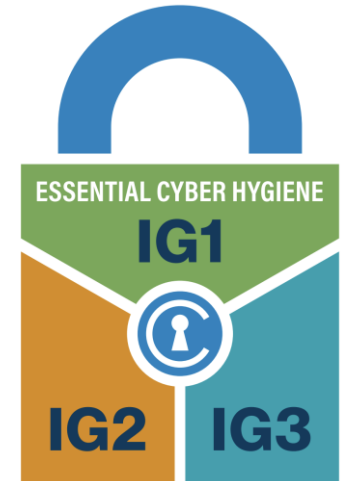
A table of the specific actions that enterprises should take to implement the Control. Typically a single action each, for simplicity.

Implementation Groups Guide Your Efforts

The number of Safeguards an enterprise is expected to implement increases based on which group the enterprise falls into.

153
Total Safeguards

IG1 (Basic)	Essential cyber hygiene practices suitable for small to medium-sized organizations with limited resources.	56 Safeguards
IG2 (Foundational)	Additional safeguards for organizations that handle sensitive information and have moderate cybersecurity needs.	74 Safeguards
IG3 (Organizational)	Advanced controls for organizations with significant cybersecurity requirements and high-value assets.	23 Safeguards



The 18 CIS Critical Security Controls

The CIS Controls® consist of 18 overarching measures that help strengthen your cybersecurity posture. They prioritize activities over roles and device ownership. That way, you can implement the CIS Controls® in a way that works for you.



Sample CIS Control

CONTROL

06

Access Control Management

8 Safeguards

IG1 5/8

IG2 7/8

IG3 8/8

CONTROL 6

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.

Safeguard 6.1: Establish an Access Granting Process

Asset Type: Documentation Security Function: Govern IG1 IG2 IG3

Establish and follow a documented process, preferably automated, for granting access to enterprise assets upon new hire or role change of a user.

Safeguard 6.2: Establish an Access Revoking Process

Asset Type: Documentation Security Function: Govern IG1 IG2 IG3

Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.

Safeguard 6.3: Require MFA for Externally-Exposed Applications

Asset Type: Users Security Function: Protect IG1 IG2 IG3

Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.

Safeguard 6.4: Require MFA for Remote Network Access

Asset Type: Users Security Function: Protect IG1 IG2 IG3

Require MFA for remote network access.

Safeguard 6.5: Require MFA for Administrative Access

Asset Type: Users Security Function: Protect IG1 IG2 IG3

Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a service provider.

Safeguard 6.6: Establish and Maintain an Inventory of Authentication and Authorization Systems

Asset Type: Software Security Function: Identify IG2 IG3

Establish and maintain an inventory of the enterprise's authentication and authorization systems, including those hosted on-site or at a remote service provider. Review and update the inventory, at a minimum, annually, or more frequently.

Safeguard 6.7: Centralize Access Control

Asset Type: Users Security Function: Protect IG2 IG3

Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.

Safeguard 6.8: Define and Maintain Role-Based Access Control

Asset Type: Users Security Function: Govern IG3

Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.

Sample CIS Control

CONTROL

06

Access Control Management

8 Safeguards

IG1 5/8

IG2 7/8

IG3 8/8

CONTROL 6

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.

Safeguard 6.1: Establish an Access Granting Process

Asset Type: Documentation Security Function: Govern IG1 IG2 IG3

Establish and follow a documented process, preferably automated, for granting access to enterprise assets upon new hire or role change of a user.

Safeguard 6.2: Establish an Access Revoking Process

Asset Type: Documentation Security Function: Govern IG1 IG2 IG3

Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.

Safeguard 6.3: Require MFA for Externally-Exposed Applications

Asset Type: Users Security Function: Protect IG1 IG2 IG3

Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.

Safeguard 6.4: Require MFA for Remote Network Access

Asset Type: Users Security Function: Protect IG1 IG2 IG3

Require MFA for remote network access.

Safeguard 6.5: Require MFA for Administrative Access

Asset Type: Users Security Function: Protect IG1 IG2 IG3

Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a service provider.

Safeguard 6.6: Establish and Maintain an Inventory of Authentication and Authorization Systems

Asset Type: Software Security Function: Identify IG2 IG3

Establish and maintain an inventory of the enterprise's authentication and authorization systems, including those hosted on-site or at a remote service provider. Review and update the inventory, at a minimum, annually, or more frequently.

Safeguard 6.7: Centralize Access Control

Asset Type: Users Security Function: Protect IG2 IG3

Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.

Safeguard 6.8: Define and Maintain Role-Based Access Control

Asset Type: Users Security Function: Govern IG3

Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.

Sample CIS Control

CONTROL

06

Access Control Management

8 Safeguards

IG1 5/8

IG2 7/8

IG3 8/8

CONTROL 6 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.

Safeguard 6.1: Establish an Access Granting Process

Asset Type: Documentation Security Function: Govern IG1 IG2 IG3

Establish and follow a documented process, preferably automated, for granting access to enterprise assets upon new hire or role change of a user.

Safeguard 6.2: Establish an Access Revoking Process

Asset Type: Documentation Security Function: Govern IG1 IG2 IG3

Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.

Safeguard 6.3: Require MFA for Externally-Exposed Applications

Asset Type: Users Security Function: Protect IG1 IG2 IG3

Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.

Safeguard 6.4: Require MFA for Remote Network Access

Asset Type: Users Security Function: Protect IG1 IG2 IG3

Require MFA for remote network access.

Safeguard 6.5: Require MFA for Administrative Access

Asset Type: Users Security Function: Protect IG1 IG2 IG3

Safeguard 6.3: Require MFA for Externally-Exposed Applications

Asset Type: Users

Security Function: Protect

IG1

IG2

IG3

Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.

IG1 vs. IG2 vs. IG3



Safeguard 3.6: Encrypt Data on End-User Devices

Asset Type: Data

Security Function: Protect

IG1

IG2

IG3

Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.

Safeguard 3.10: Encrypt Sensitive Data in Transit

Asset Type: Data

Security Function: Protect

IG2

IG3

Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).

Safeguard 3.13: Deploy a Data Loss Prevention Solution

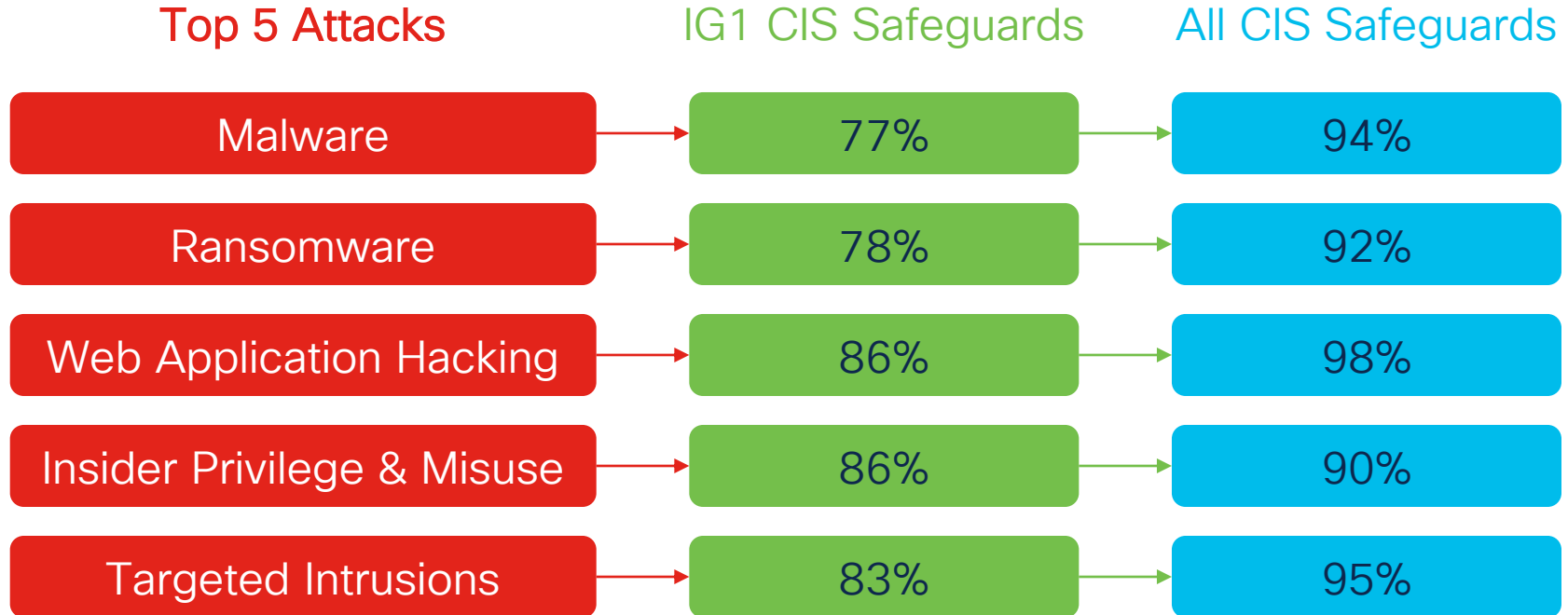
Asset Type: Data

Security Function: Protect

IG3

Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's data inventory.

Success Against Common Attack Techniques

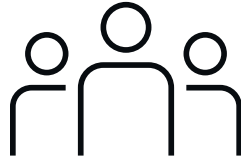


Steps for Implementing CIS Controls®



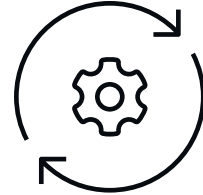
Assessment & Planning

Identify gaps and prioritize CIS Controls® based on your organization's risk profile and resources



Resource Allocation

Allocate necessary resources, including budget, tools, and personnel, to support the implementation process



Incremental Implementation

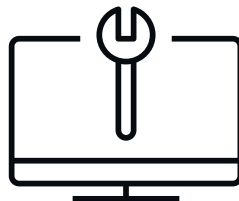
Focus on high-impact controls first to maximize immediate security benefits

Tools and Resources for Effective Implementation



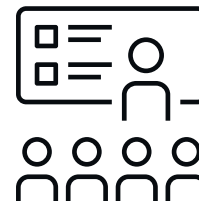
Documentation & Guidelines

Refer to CIS's detailed documentation and guidelines for each control to understand best practices and implementation steps



Automated Tools

Leverage endpoint protection, vulnerability management, and configuration management tools to streamline implementation



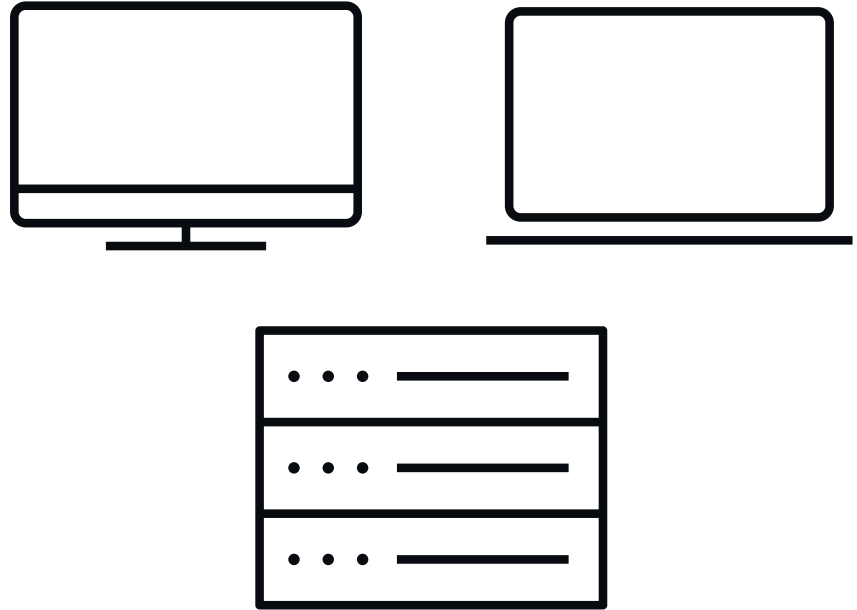
Training & Awareness

Foster a culture of continuous learning and improvement to keep up with evolving cybersecurity threats and practices

Understanding CIS Benchmarks™

The Problem with Default Configurations

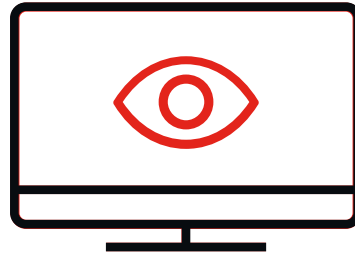
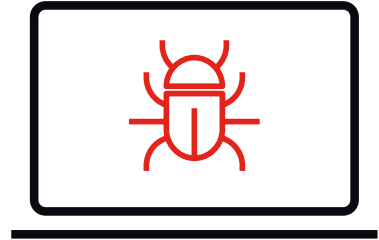
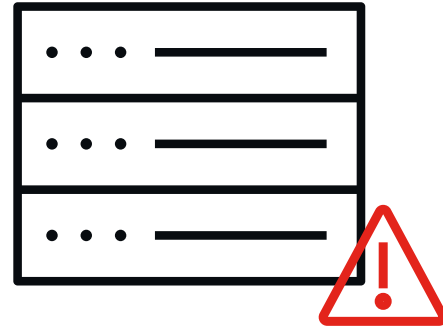
Many systems ship out with default configurations designed for ease of use and deployment over security



The Problem with Default Configurations

Many systems ship out with default configurations designed for ease of use and deployment over security.

Unless you change these configurations with security in mind, you could leave your systems vulnerable to cyber threat actors.



What are CIS Benchmarks™ ?

- The CIS Benchmarks™ are community-developed secure configuration recommendations for hardening organizations' technologies against cyber attacks.
- Mapped to the 18 CIS Controls®, the CIS Benchmarks™ elevate the security defenses for cloud provider platforms and cloud services, containers, databases, desktop software, server software, mobile devices, network devices, and operating systems.



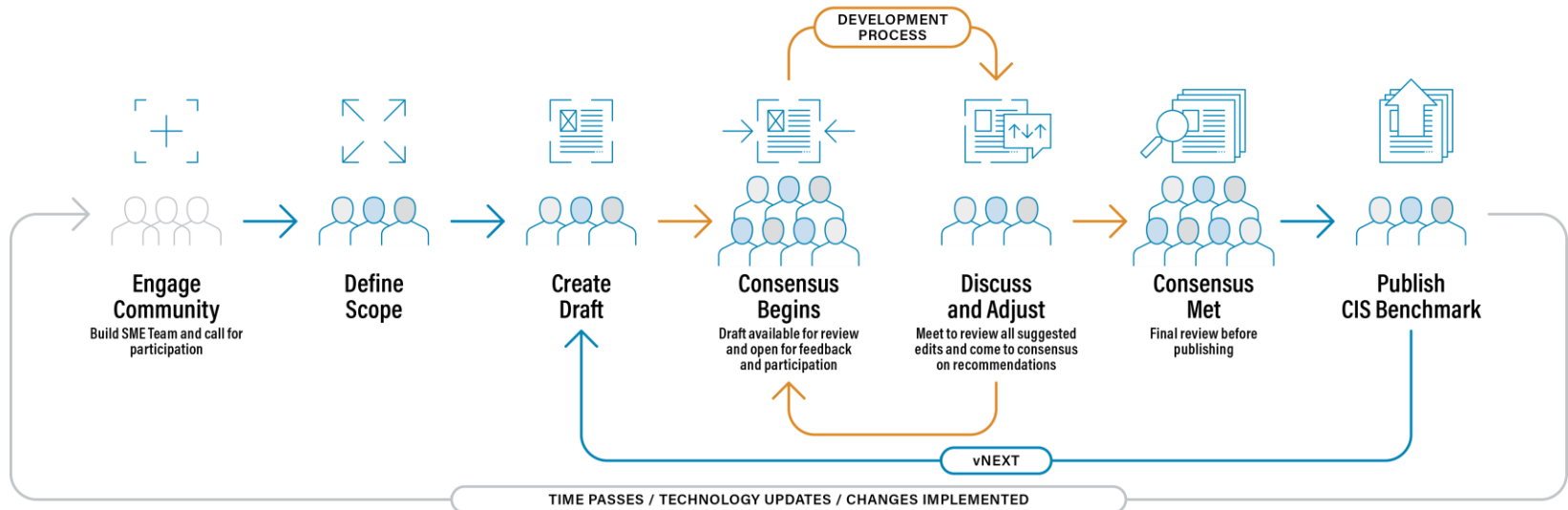
“Without this resource, the hardening of our devices would have taken a lot longer and required many meetings between IT and Security to debate which configuration settings to change and the impact they could have. The CIS Benchmarks™ provided the necessary information to alleviate many of the fears IT may have had with changing specific settings.”

Adam

Banking Information Security Engineer

A Consensus Development Process

The CIS Benchmarks™ are different from other secure configuration guides because they are the product of an ongoing consensus process. Subject matter experts (SMEs), technology vendors, public and private community members, and academics from different industries come together in this process to debate use cases and agree upon secure recommendations.



Structure of the CIS Benchmarks™

- Description:
 - Summarizes the recommendation
- Rationale:
 - Discusses the importance of the recommendation
- Impact:
 - Frames the security benefit of implementing the recommendation
- Audit:
 - Identifies how you can prove you've implemented the recommendation for an audit
- Remediation:
 - Goes through the actual steps of implementing the recommendation

How to Use a CIS Benchmarks™

- Use a PDF:
 - Anyone can download them free of charge in PDF format for non-commercial use.
- Through CIS SecureSuite Membership:
 - CIS SecureSuite Members can download the Benchmarks in additional formats such as Word, Excel, and XML via CIS WorkBench; They can also use the CIS Build Kits to automate their hardening efforts across Windows, macOS, and select Linux systems to CIS Benchmarks™ standards.
- Launch a CIS Hardened Image:
 - These virtual machine images are hardened in accordance with the CIS Benchmarks™.
- Deploy the Tools of Certified Product Vendors:
 - CIS SecureSuite Product Vendor Member tools provide certified offerings for configuration, assessment, and remediation of CIS Benchmarks™ content.

100+ CIS Benchmarks™ across 25+ vendors

- Cloud Providers
 - Alibaba Cloud
 - Amazon Web Services
 - Google Cloud Computing Platform
 - Google Workspace
 - IBM Cloud Foundations
 - Microsoft 365
 - Microsoft Azure
 - Microsoft Dynamics 365 Power Platform
 - Oracle Cloud Infrastructure
- Desktop Software
 - Microsoft Exchange Server
 - Microsoft Office
 - Zoom
 - Google Chrome
 - Microsoft Web Browser
 - Mozilla Firefox
 - Safari Browser
- DevSecOps Tools
 - Software Supply Chain Security
- Mobile Devices
 - Apple iOS
 - Google Android
- Multi Function Print Devices
 - Print Devices
- Network Devices
 - Check Point Firewall
 - Cisco
 - F5
 - Fortinet
 - Juniper
 - Palo Alto Networks
 - pfSense Firewall
 - Sophos
- Operating Systems
 - IBM i
 - IBM Z System
 - Aliyun Linux
 - AlmaLinux OS
 - Amazon Linux
 - Bottlerocket
 - CentOS Linux
 - Debian Family Linux
 - Debian Linux
 - Distribution Independent Linux
 - Fedora Family Linux
 - LXDE
 - Oracle Linux
 - Red Hat Enterprise Linux
 - Robot Operating System (ROS)
 - Rocky Linux
 - SUSE Linux Enterprise Server
- Server Software
 - Ubuntu Linux
 - Microsoft Intune for Windows
 - Microsoft Windows Desktop
 - Microsoft Windows Server
 - Apple macOS
 - IBM AIX
 - Oracle Solaris

CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0

1 - Initial Setup

- 1.1 - Filesystem
- 1.2 - Package Management
- 1.3 - Mandatory Access Control
- 1.4 - Configure Bootloader
- 1.5 - Configure Additional Process Hardening
- 1.6 - Configure Command Line Warning Banners
- 1.7 - Configure GNOME Display Manager

2 - Services

- 2.1 - Configure Server Services
- 2.2 - Configure Client Services
- 2.3 - Configure Time Synchronization
- 2.4 - Job Schedulers

3 - Network

- 3.1 - Configure Network Devices
- 3.2 - Configure Network Kernel Modules
- 3.3 - Configure Network Kernel Parameters

4 - Host Based Firewall

- 4.1 - Configure a single firewall utility
- 4.2 - Configure Uncomplicated Firewall
- 4.3 - Configure nftables
- 4.4 - Configure iptables

5 - Access Control

- 5.1 - Configure SSH Server
- 5.2 - Configure privilege escalation
- 5.3 - Pluggable Authentication Modules
- 5.4 - User Accounts and Environment

6 - Logging and Auditing

- 6.1 - System Logging
- 6.2 - System Auditing
- 6.3 - Configure Integrity Checking

7 - System Maintenance

- 7.1 - System File Permissions
- 7.2 - Local User and Group Settings

CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0

• 5.1 Configure SSH Server

- 5.1.1 Ensure permissions on /etc/ssh/sshd_config are configured
- 5.1.2 Ensure permissions on SSH private host key files are configured
- 5.1.3 Ensure permissions on SSH public host key files are configured
- 5.1.4 Ensure sshd access is configured
- 5.1.5 Ensure sshd Banner is configured
- 5.1.6 Ensure sshd Ciphers are configured
- 5.1.7 Ensure sshd ClientAliveInterval and ClientAliveCountMax are configured
- 5.1.8 Ensure sshd DisableForwarding is enabled
- 5.1.9 Ensure sshd GSSAPIAuthentication is disabled
- 5.1.10 Ensure sshd HostbasedAuthentication is disabled
- 5.1.11 Ensure sshd IgnoreRhosts is enabled
- 5.1.12 Ensure sshd KexAlgorithms is configured
- 5.1.13 Ensure sshd LoginGraceTime is configured
- 5.1.14 Ensure sshd LogLevel is configured
- 5.1.15 Ensure sshd MACs are configured
- 5.1.16 Ensure sshd MaxAuthTries is configured
- 5.1.17 Ensure sshd MaxSessions is configured
- 5.1.18 Ensure sshd MaxStartups is configured
- 5.1.19 Ensure sshd PermitEmptyPasswords is disabled
- 5.1.20 Ensure sshd PermitRootLogin is disabled
- 5.1.21 Ensure sshd PermitUserEnvironment is disabled
- 5.1.22 Ensure sshd UsePAM is enabled

CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0

5.1.20 Ensure sshd PermitRootLogin is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `PermitRootLogin` parameter specifies if the root user can log in using SSH. The default is `prohibit-password`.

Rationale:

Disallowing `root` logins over SSH requires system admins to authenticate using their own individual account, then escalating to `root`. This limits opportunity for non-repudiation and provides a clear audit trail in the event of a security incident.

CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0

Audit:

Run the following command to verify **PermitRootLogin** is set to **no**:

```
# sshd -T | grep permitrootlogin  
  
permitrootlogin no
```

- **IF - Match** set statements are used in your environment, specify the connection parameters to use for the **-T** extended test mode and run the audit to verify the setting is not incorrectly configured in a match block

*Example additional audit needed for a match block for the user **sshuser**:*

```
# sshd -T -C user=sshuser | grep permitrootlogin
```

Note: If provided, any Match directives in the configuration file that would apply are applied before the configuration is written to standard output. The connection parameters are supplied as keyword=value pairs and may be supplied in any order, either with multiple **-C** options or as a comma-separated list. The keywords are **addr** (source address), **user** (user), **host** (resolved source host name), **laddr** (local address), **lport** (local port number), and **rdomain** (routing domain)

CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the `PermitRootLogin` parameter to `no` above any `Include` and `Match` entries as follows:

```
PermitRootLogin no
```

Note: First occurrence of an option takes precedence, `Match` set statements withstanding. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in `Include` location.

CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			
v7	<u>4.3 Ensure the Use of Dedicated Administrative Accounts</u> Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1021	TA0008	M1042

CIS Benchmarks™ for Cisco Technologies

- Cisco ASA 9.x Firewall (1.1.0)
- Cisco IOS XE 16.x (2.1.0)
- Cisco IOS XE 17.x (2.1.0)
- Cisco NX-OS (1.1.0)
- Cisco Wireless LAN Controller 7 (1.1.0)
- Cisco IOS 15 (4.1.1)
- Cisco IOS 12 (4.0.0)
- Cisco Firepower Threat Defense (1.0.0)
- Cisco Firewall (4.1.0)
- Cisco Firewall v8.x (4.2.0)
- Cisco IOS XR 7.x (1.0.0)
- Cisco IOS 17.x (2.0.0)
- Cisco IOS 16 (2.0.0)

“Since we switched over to a standardized CIS Benchmark, it’s easy for us to give the auditor the data and say: We’re using CIS, and these devices are going to be compliant with that because we implement the CIS Benchmarks™ through group policy. If we fall in alignment with these configuration standards, it just clearly makes sense that it could really lighten the workload on the team of the State of Minnesota. I’m really impressed [by] the value you get with CIS. It’s huge.”

Terry Seiple

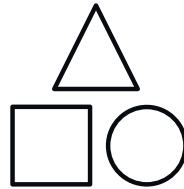
State of Minnesota Security Architect

Steps for Adopting CIS Benchmarks™



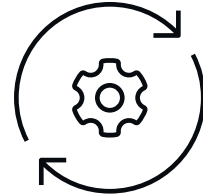
Assessment & Selection

Select appropriate benchmarks based on your specific IT environment (e.g., operating systems, cloud services, applications)



Customization

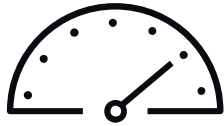
Customize the benchmarks to align with your organization's policies and operational requirements



Implementation

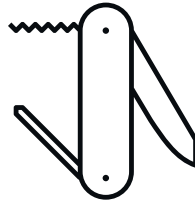
Apply the recommended configurations to your systems using automated tools where possible

Tools & Resources for Configuration Management



CIS-CAT Pro

A tool provided by CIS for automating the assessment and implementation of CIS Benchmarks™



Configuration Management Tools

Utilize tools like Ansible, Chef, and Puppet to automate the deployment and management of secure configurations

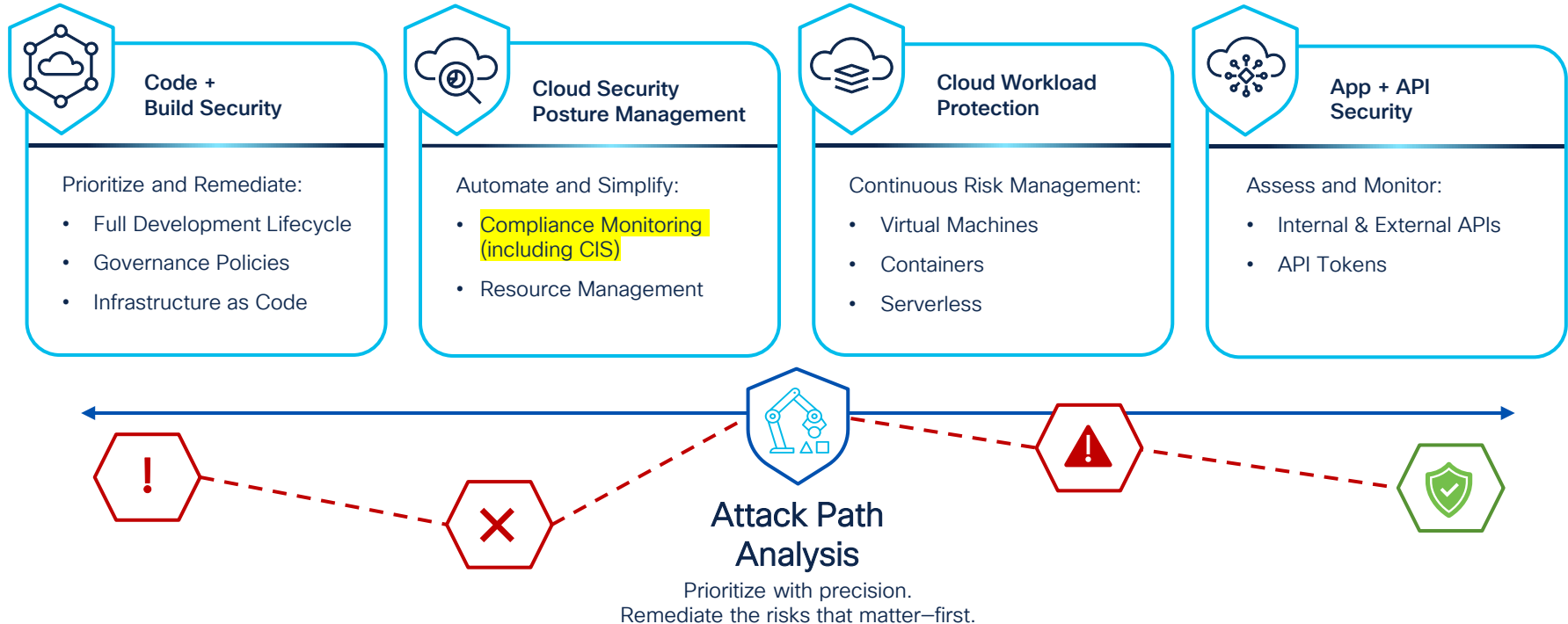


Documentation & Support

Leverage the detailed documentation provided by CIS for each benchmark to understand the rationale and implementation steps

Cisco Panoptica

Comprehensive Code to Cloud Security



CIS Compliance Tracking in Panoptica

- Each framework provides a scorecard approach to CIS compliance
- Requirements that can automatically verify are scored and their results presented
- Manual controls are also included in the framework to provide a complete view with ability for users to indicate pass/fail

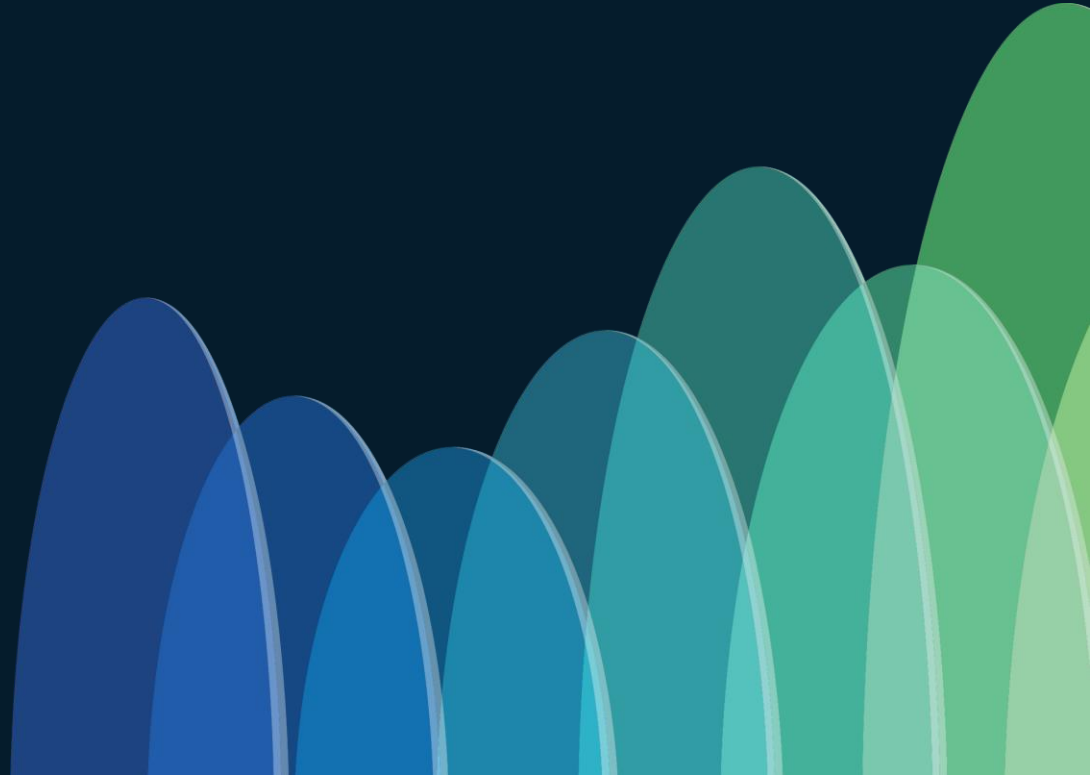
The screenshot displays the Panoptica interface for the AWS CIS v1.3 compliance framework. The left sidebar shows navigation options: Dashboard, THREATS & VULNERABILITIES (Attack Path Analysis, External Attack Surface, Vulnerability Management), POSTURE MANAGEMENT (Cloud Inventory, Security Posture, Compliance Frameworks), WORKLOADS & DATA (API Security), BUILD & APPLICATIONS (CI/CD), and MANAGEMENT (Integrations, Settings). The main content area shows the 'Compliance Framework' section for 'AWS CIS v1.3'. It displays a scorecard with 48.44% compliance, 1 account, 55 total rules, and 10 completed rules. Below this, a table lists 5 controls: Identity and Access Management (22 sub-controls, 54% progress), Storage (3 sub-controls, 0% progress), Logging (11 sub-controls, 50% progress), Monitoring (15 sub-controls, N/A progress), and Networking (4 sub-controls, 59% progress). The 'Networking' control is expanded, showing a table of sub-controls. Sub-control 5.2 is highlighted as 'Failed'. Below this, a table of rules is shown, with rule 5.2 highlighted as 'Failed'.

Control	Sub Controls	Description	Progress
Identity and Access Management	22	This section contains recommendations for configuring identity and access manage...	54%
Storage	3	This section contains recommendations for configuring S3 and EC2 services to secu...	0%
Logging	11	This section contains recommendations for configuring AWS's account logging featur...	50%
Monitoring	15	This section contains recommendations for configuring AWS to assist with monitorin...	N/A
Networking	4	This section contains recommendations for configuring security-related aspects of th...	59%

Number	Compliant	Sub Control	Check Type	Compliance Progress
5.1	Passed	Ensure no Network ACLs allow ingress from 0.0.0.0/0 to remote server administrati...	Automated	100%
5.2	Failed	Ensure no security groups allow ingress from 0.0.0.0/0 to remote server administrati...	Automated	88%

Rule	Type	Matches		
Verify that no security groups allow ingress from 0.0.0.0/0 to remote server administration ports	Security Group	Assets: 4 Failed 32 Passed		
5.3	Failed	Ensure the default security group of every VPC restricts all traffic	Automated	48%
5.4	Failed	Ensure routing tables for VPC peering are "least access"	Manual	0%

Conclusion



Summary

- The Center for Internet Security (CIS) is a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™
- The CIS Critical Security Controls (CIS Controls®) are a prescriptive, prioritized, and simplified set of best practices that you can use to strengthen your cybersecurity posture.
- The CIS Controls® consist of 18 overarching measures that help strengthen your cybersecurity posture. They prioritize activities over roles and device ownership.
- The CIS Benchmarks™ are community-developed secure configuration recommendations for hardening organizations' technologies against cyber attacks.
- Mapped to the 18 CIS Controls®, the CIS Benchmarks™ elevate the security defenses for cloud provider platforms and cloud services, containers, databases, desktop software, server software, mobile devices, network devices, and operating systems.

Next Steps

- Visit the [CIS website](#) and become a member
- Begin implementing [CIS Controls®](#) and [CIS Benchmarks™](#)
- Sign up for [Cisco U.](#) (it's free!)
- Check out [Cisco Panoptica](#) and get a free demo

Keynote Deep Dives

Wednesday
10:30am – 11:30am



Experiences Amplified:
How AI Can Fuel
Better Employee
and Customer
Experiences

Level 1
Room 106



Smart, Secure,
Seamless:
Transforming
Experiences with
Next-Generation
Networking

Level 2
Room 204



Harness a Bold
New Era:
Transform Data
Centre and
Service Provider
Connectivity

Level 2
Room 203



Securing User to
Application and
Everything in
Between

Level 2
Melbourne Room 2



Unlocking
Digital Resilience
through Unified
Observability

The HUB
Centre Stage

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



Complete your surveys in the **Cisco Live mobile app**.



Continue your education

- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: kywinter@cisco.com



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC