CORELOGIC TECHNOLOGIES

Top 12 Cybersecurity Best Practices for 2024

Exploring the top 12 cybersecurity best practices that businesses and individuals should adopt in 2024 to protect against evolving threats.

Cybersecurity Policy

- **DEFINE CLEAR ROLES AND RESPONSIBILITIES**

  Clearly outline the roles and responsibilities of different stakeholders, from IT teams to business leaders, to ensure accountability and seamless implementation.

- **ESTABLISH SECURITY STANDARDS AND CONTROLS**

  Develop and implement robust security standards, policies, and controls to safeguard your organization's information assets and critical systems.

- **FOSTER A CULTURE OF CYBERSECURITY AWARENESS**

  Implement comprehensive training and awareness programs to educate employees on security best practices and their role in maintaining a secure environment.

- **IMPLEMENT ROBUST INCIDENT RESPONSE PLAN**

  Develop a comprehensive incident response plan to ensure your organization can effectively detect, respond to, and recover from cybersecurity incidents.

- **ENSURE CONTINUOUS MONITORING AND IMPROVEMENT**

  Regularly review and update the cybersecurity policy to address evolving threats, incorporate lessons learned, and continuously improve the organization's security posture.

Secure Perimeter and IoT Connections

IMPLEMENT FIREWALLS

Deploy robust firewalls at the network perimeter to control and monitor inbound and outbound traffic, blocking unauthorized access attempts.

SECURE IOT DEVICES

Ensure IoT devices are configured with strong passwords, updated firmware, and secure communication protocols to prevent unauthorized access and data breaches.

UTILIZE VPNS

Establish virtual private network (VPN) connections for remote users and IoT devices to encrypt data transmission and provide an additional layer of security.

MONITOR NETWORK ACTIVITY

Implement network monitoring and intrusion detection systems to identify and respond to suspicious activities, such as unauthorized access attempts or unusual traffic patterns.

REGULARLY PATCH AND UPDATE

Maintain a robust patch management process to keep all systems, including IoT devices, up-to-date with the latest security patches and firmware updates to address vulnerabilities.

People-Centric Security Approach

Strengthening cybersecurity defenses starts with a people-centric approach. By focusing on educating and raising awareness among employees, organizations can create a strong human firewall against cyber threats. This approach emphasizes the critical role that employees play in safeguarding an organization's digital assets.

Access Control

- **IMPLEMENT ROLE-BASED ACCESS CONTROL (RBAC)**

  Assign the minimum set of permissions required for users to perform their job functions, granting access on a need-to-know basis.

- **ENFORCE SEPARATION OF DUTIES (SOD)**

  Ensure that critical tasks are divided among multiple individuals to prevent a single person from abusing their privileges.

- **IMPLEMENT STRONG AUTHENTICATION**

  Require multi-factor authentication, such as a combination of passwords, biometrics, and security tokens, to verify user identity and prevent unauthorized access.

- **REGULARLY REVIEW AND AUDIT ACCESS**

  Periodically review user access rights and revoke unnecessary permissions to minimize the risk of insider threats and unauthorized access.

- **IMPLEMENT LEAST PRIVILEGE ON SYSTEMS AND APPLICATIONS**

  Restrict user and application permissions to the minimum required to perform their intended functions, reducing the attack surface and the potential impact of a breach.

Password Management

USE STRONG PASSWORDS

Require employees to create complex passwords that are at least 12 characters long, include a mix of uppercase, lowercase, numbers, and special characters.

IMPLEMENT MULTI-FACTOR AUTHENTICATION

Require employees to use two or more forms of authentication, such as a password and a one-time code sent to their mobile device, to access sensitive systems and applications.

EDUCATE EMPLOYEES ON PASSWORD BEST PRACTICES

Train employees on how to create and manage secure passwords, spot phishing attempts, and report any suspicious activity.

REGULARLY REVIEW AND UPDATE PASSWORDS

Implement a password rotation policy that requires employees to change their passwords every 90 days, and revoke access for terminated employees immediately.

USE A PASSWORD MANAGER

Provide employees with a secure password manager to store and generate complex passwords, reducing the risk of password reuse and making it easier to manage multiple credentials.

Privileged and Third-Party Users

DETECT UNAUTHORIZED ACCESS ATTEMPTS

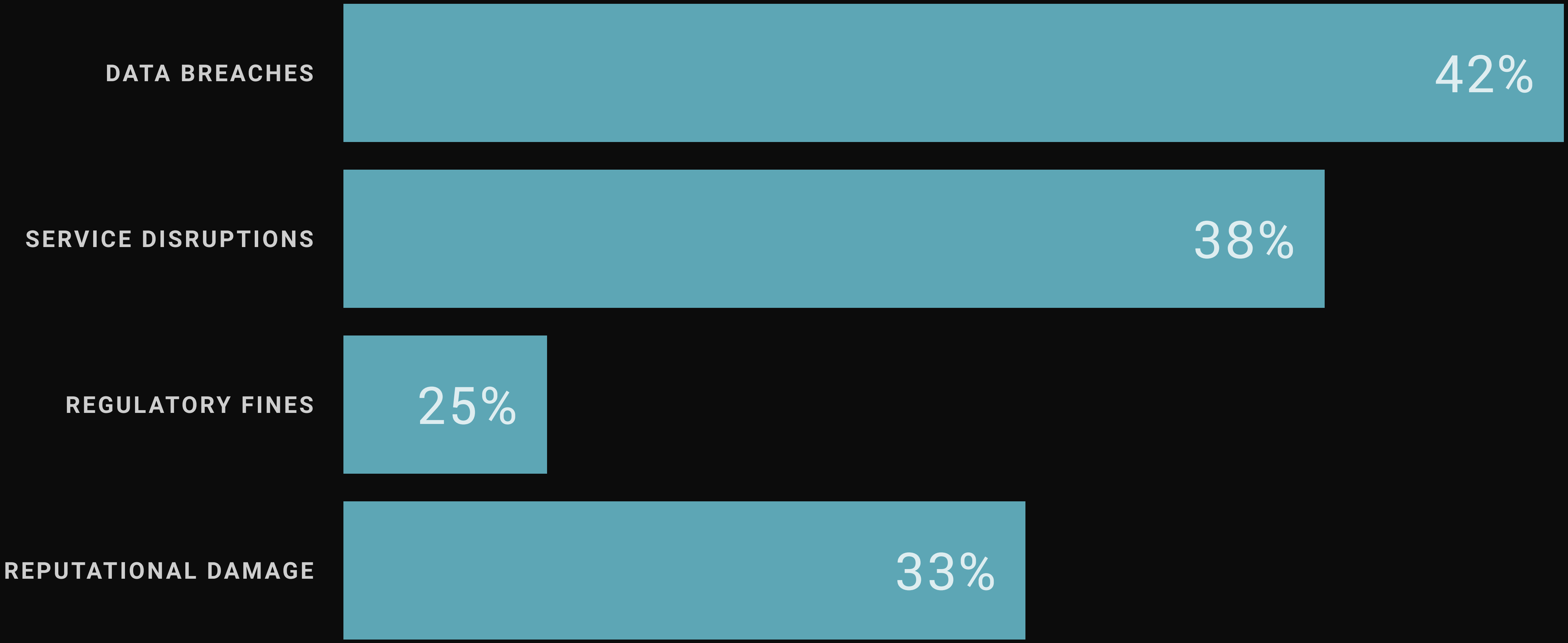
MONITOR USER BEHAVIOR ANOMALIES

TRIGGER ALERTS FOR SUSPICIOUS ACTIVITIES

GENERATE DETAILED AUDIT TRAILS

Supply Chain Risk Management

Percentage of risk exposure from various vendor-related vulnerabilities



Data Protection and Management

Policy Recommendation	Description
Data Encryption	Implement strong encryption protocols to protect sensitive business data during collection, processing, storage, and transmission.
Access Controls	Establish role-based access controls and multi-factor authentication to limit access to business data based on user permissions.

*Data adapted from the NIST Cybersecurity Framework (https://www.nist.gov/cyberframework)

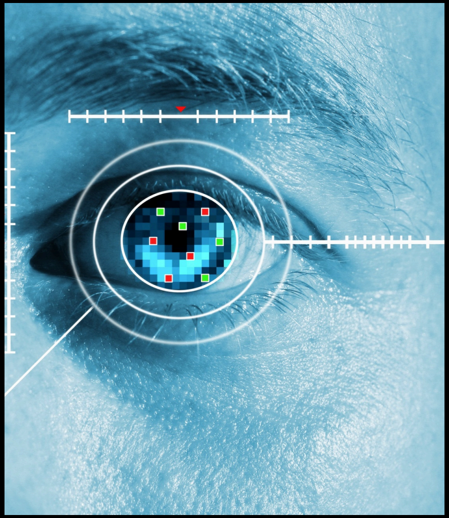
Biometric Security

FINGERPRINT SCANNER

A fingerprint scanner is a biometric device that uses a person's unique fingerprint pattern to authenticate their identity for secure access.

FACIAL RECOGNITION CAMERA

A facial recognition camera captures an individual's facial features and compares them to a stored database to verify their identity for multi-factor authentication.



IRIS SCANNER

An iris scanner uses the unique patterns in a person's iris to identify and authenticate them for secure access, providing an additional layer of biometric security.

HANDPRINT SCANNER

A handprint scanner captures the unique shape and size of a person's hand to confirm their identity, offering a reliable biometric solution for access control.

VOICE RECOGNITION

Voice recognition technology uses a person's unique voice characteristics to verify their identity, adding an extra layer of biometric security to authentication processes.

Multi-Factor Authentication

WHAT IS MFA?

Multi-Factor Authentication (MFA) is a security process that requires users to provide additional verification beyond a password to access an account or system.

HOW DOES MFA WORK?

MFA requires users to provide two or more pieces of evidence to verify their identity, such as a password, a one-time code sent to their phone, or a biometric feature like a fingerprint or facial recognition.

BENEFITS OF MFA

MFA adds an extra layer of security to prevent unauthorized access even if a password is compromised, making it much harder for attackers to gain access to sensitive information or accounts.

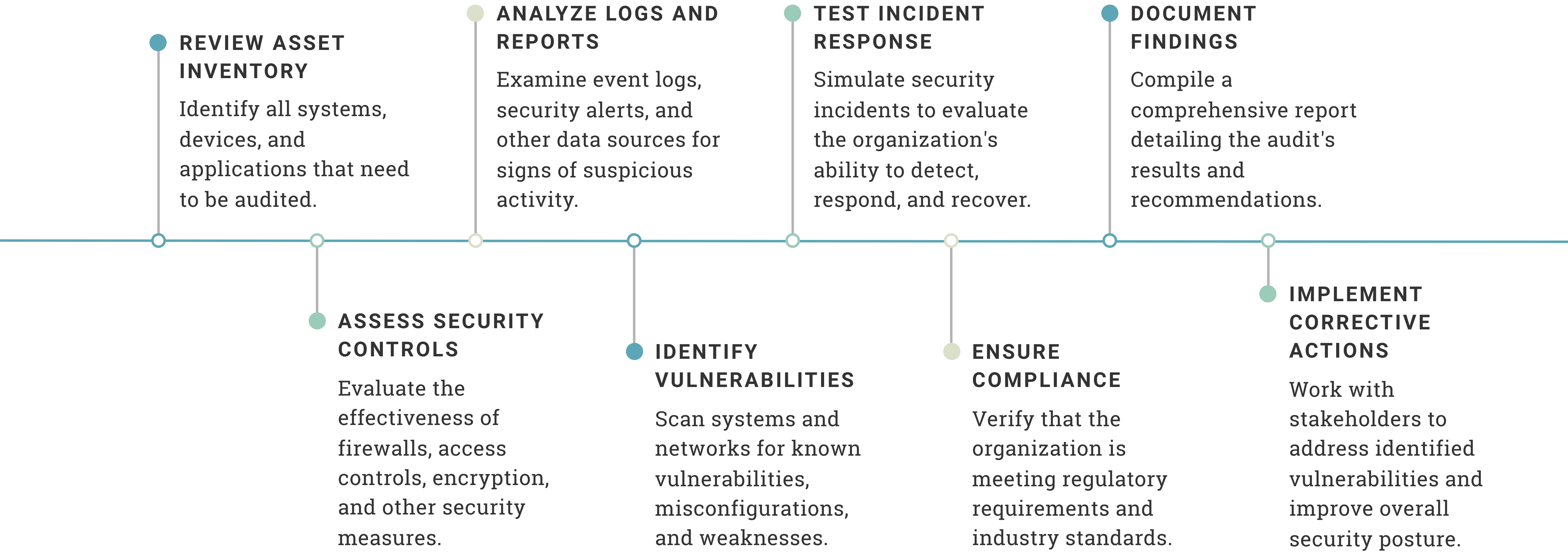
COMMON MFA METHODS

Some common MFA methods include SMS or email-based one-time codes, authenticator apps, biometric factors like fingerprints or facial recognition, and hardware security keys.

IMPLEMENTING MFA

Businesses and organizations can implement MFA across various systems and applications to enhance their overall security posture and protect against data breaches and cyber attacks.

Cybersecurity Audits



REVIEW ASSET INVENTORY

Identify all systems, devices, and applications that need to be audited.

ASSESS SECURITY CONTROLS

Evaluate the effectiveness of firewalls, access controls, encryption, and other security measures.

ANALYZE LOGS AND REPORTS

Examine event logs, security alerts, and other data sources for signs of suspicious activity.

IDENTIFY VULNERABILITIES

Scan systems and networks for known vulnerabilities, misconfigurations, and weaknesses.

TEST INCIDENT RESPONSE

Simulate security incidents to evaluate the organization's ability to detect, respond, and recover.

ENSURE COMPLIANCE

Verify that the organization is meeting regulatory requirements and industry standards.

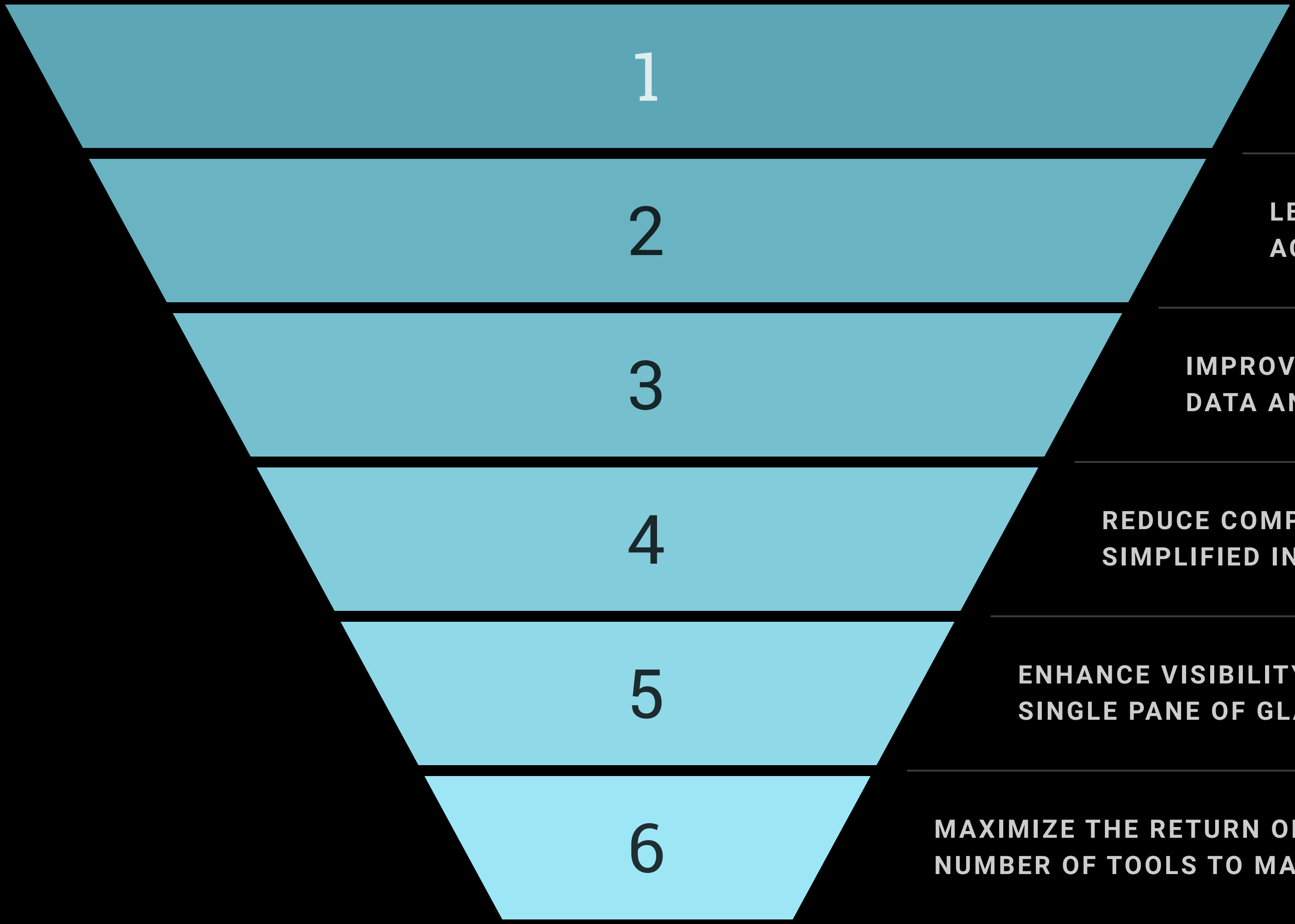
DOCUMENT FINDINGS

Compile a comprehensive report detailing the audit's results and recommendations.

IMPLEMENT CORRECTIVE ACTIONS

Work with stakeholders to address identified vulnerabilities and improve overall security posture.

Simplify Technology Infrastructure



1. CONSOLIDATE SECURITY TOOLS AND SERVICES INTO A COMPREHENSIVE SOLUTION
2. LEVERAGE A UNIFIED PLATFORM TO MANAGE SECURITY ACROSS YOUR ENTIRE ENVIRONMENT
3. IMPROVE INCIDENT RESPONSE TIMES BY CENTRALIZING SECURITY DATA AND WORKFLOWS
4. REDUCE COMPLEXITY AND IMPROVE OPERATIONAL EFFICIENCY WITH A SIMPLIFIED INFRASTRUCTURE
5. ENHANCE VISIBILITY AND CONTROL OVER YOUR SECURITY POSTURE WITH A SINGLE PANE OF GLASS
6. MAXIMIZE THE RETURN ON YOUR SECURITY INVESTMENTS BY MINIMIZING THE NUMBER OF TOOLS TO MANAGE