TR CYBERSECURITY ALLIANCE

Top 10 Best Practices for Cybersecurity Asset Management

INTRODUCTION

The first step in cybersecurity is asset management. In all regulations, knowing your assets is a fundamental requirement. However, after the discovery phase, deficiencies are often observed in areas such as classification, monitoring, risk analysis, and lifecycle management. For this reason, TR Cybersecurity Alliance dedicated its seventh workshop to cybersecurity asset management.

In this study, we addressed essential topics such as asset discovery, risk-based lifecycle management, configuration management, and service continuity. As a result, a common set of best practices was compiled and presented below.

1. Automatically Discover All Assets

Every entity carrying cyber risk is an asset. User accounts, servers, computers, software, APIs, SSL certificates, cloud services, and IoT devices should all be considered within this scope. Form the foundation of your cybersecurity strategy by first creating a corporate-level Asset Classification Table. Automatically detect and classify active and passive assets using your discovery systems.

2. Keep Your Asset Inventory Centralized and Continuously Updated

Maintain a centralized inventory of all assets through a CMDB system to ensure visibility of risk scores and enable prompt action. Avoid manual inventory updates — instead, integrate APIs, perform automated scans, and use DHCP or telemetry data for real-time updates.

3. Classify Assets by Criticality

Evaluate each asset based on its impact and risk potential. Classify them using objective and measurable criteria. These classifications are essential for prioritizing your risk assessments and remediation processes.

4. Produce a Risk Score for Each Asset

Assign a risk score to each asset based on its vulnerabilities and exposure. Use these scores to guide vulnerability management, access control, and patch management processes.

5. Continuously Monitor Vulnerabilities and Misconfigurations

Perform automated scans to detect vulnerabilities and configuration errors. Regularly check SSL certificates, open ports, default passwords, and other system configurations to maintain a secure environment.

6. Standardize Security Configurations Across Assets

Create standard security configuration profiles for all asset types within your organization. Ensure newly added systems or applications comply with these standards. Refer to CIS Benchmarks, NIST Hardening Guides, and vendor security recommendations.

7. Monitor Access and Authorizations

Manage access permissions according to Zero Trust principles. Secure administrative access with multi-factor authentication (MFA), Just-In-Time (JIT) provisioning, and Privileged Access Management (PAM) solutions.

8. Promptly Remove Decommissioned Assets from the Inventory

Apply automated deletion and deactivation policies for assets leaving the network or system. Ensure data belonging to these assets is securely deleted or archived.

9. Measure, Monitor, and Report Processes

On a monthly or quarterly basis, measure and report metrics such as:

- Number of active assets
- Percentage of unidentified assets
- Percentage of critical assets
- Unauthorized access attempts or asset exposure rates

10. Make Asset Management Part of Organizational Culture

Asset management is not only an IT responsibility — it's a shared responsibility across the organization. Promote a unified culture among information security, operations, and management teams.

Increase awareness of the value and risks associated with every asset. Adopt the principles of the ISO/IEC 19770 IT Asset Management standard to manage costs, licenses, configurations, changes, and security comprehensively.

CONCLUSION

To build a strong cybersecurity defense, organizations must have full visibility into their assets and manage them centrally and securely. The 10 practices outlined in this study aim to help organizations bring visibility to hidden assets, analyze risks, and standardize security configurations.

At TR Cybersecurity Alliance, we believe that building resilience requires not only technological tools but also corporate awareness, disciplined processes, and strong collaboration. Turning asset management into an organizational culture is key to sustainable cyber resilience. With our future guides, we aim to strengthen this awareness even further.

Contributors

Ahmet Özkan

Ali Dinçkan

Ali Tursun

Asım Yıldız

Caner Dağlı

Fatih Özen

Fuat Kılıç

Hakan Uluğ

Kadir Çakıcı

Kayıhan Altınöz

Mehtap Kılıç

Murat Çağlar

Onur Mutlu İmamoğlu

Ömer Çuhadaroğlu

Serkan Akcan

Yasin Durgaç