The Complete Guide to Cybersecurity Program KPIs

Onyxia

Table of Contents

An Introduction from Lucas Moody, SVP & CISO at Alteryx

All CISOs need to determine how to effectively manage their security programs. There are countless ways to solve this challenge. However, to standardize and create a path where the most crucial elements are measured consistently as the security business evolves, it's essential to find the right metrics and to track them consistently over time.

The difference between a reactive cybersecurity program and a proactive one lies in how well your organization measures and analyzes its performance. CISOs know that a robust strategy is more than just a collection of tools—it's about creating measurable, data-driven outcomes that enhance your security posture while saving time and resources.

Key Performance Indicators (KPIs) tailored for cybersecurity, or as Onyxia refers to them, Cyber Performance Indicators (CPIs), are instrumental in achieving this. They provide critical visibility into the effectiveness of your security program, enabling security leaders to identify trends, detect weaknesses, and drive informed decisions. Understanding and leveraging the right CPIs ensures your organization not only stays ahead of evolving threats but also communicates value to stakeholders efficiently.

This guide from Onyxia, which includes a sampling of metrics from their full CPI library, explores how optimizing your security strategy with the right CPIs can fortify your defenses and streamline executive reporting for maximum impact.

Detection & Response

Effectively managing and monitoring Detection & Response in cybersecurity is critical as it enables organizations to identify and address security incidents quickly, minimizing damage and potential breaches. Prolonged response times increase the risk of malicious actors gaining a foothold, causing significant damage and complicating remediation efforts.

Mean Time To Resolve Incidents tracks the daily average time it takes to close/resolve incidents or alerts within a specified day.

Knowing the time your organization takes to respond to incidents can help give an overall picture of your organization's security situation. A prolonged response time increases the risk of a malicious actor establishing a foothold in the organization's network, potentially leading to a longer and more complex remediation process and significant damage to the organization.

Additionally, a high mean time to close incidents can be an indicator of:

- Inefficiencies in the incident response process
- Deficiencies in the training or staffing of SOC teams
- An unusually high influx of incidents temporarily overwhelming the SOC/Incident Response Teams

Addressing issues related to mean-time resolution can lead to more efficient incident responses, better-trained staff, and a proactive approach to handling increased incident volumes, ultimately bolstering your organization's cybersecurity defenses.

Incident False Positive Rate tracks the percentage of incidents closed/resolved as False Positives within a specified day.

When the number of false positive incidents is high, it indicates the security team spends more time closing false alarms than addressing real threats, significantly reducing the team's effectiveness.

Additionally, high rates of false positive incidents can imply:

- High false positive rate of detection product or logic.
- Inability to define/customize precise detection logic within a detection product.

Resolving a high number of false positive incidents is crucial to ensure that the security team focuses on real threats instead of spending excessive time on erroneous alerts. By reducing these false alarms, the team can efficiently prioritize and address genuine security risks, enhancing their overall effectiveness.

Vulnerability Management

Vulnerability management enables organizations to proactively identify and address weaknesses in their systems and applications before attackers can exploit them. Organizations can reduce their attack surface by effectively managing vulnerabilities and minimizing the risk of data breaches and other security incidents.

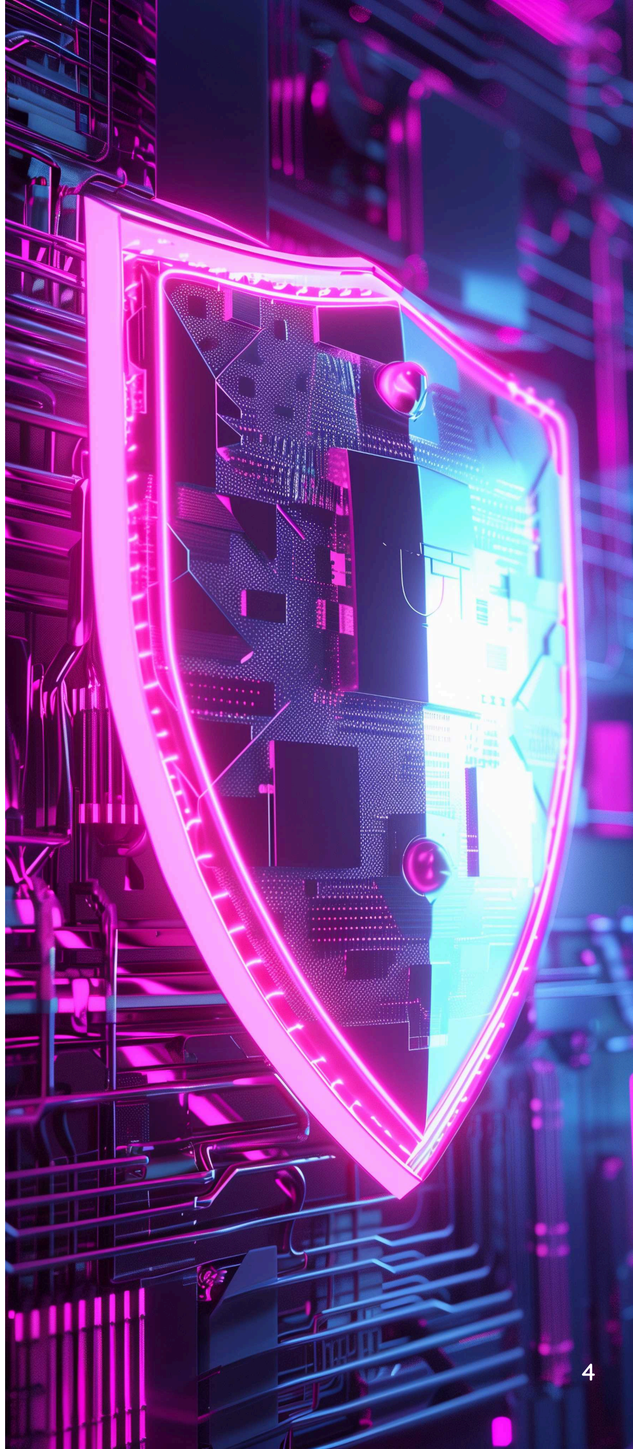
Mean Time To Resolve Vulnerabilities tracks the daily average time it takes to close or resolve vulnerabilities within a specific day.

A lengthy response time heightens the risk of vulnerabilities being exploited by malicious actors, potentially leading to network breaches and significant damage to the organization.

Additionally, a high mean time to resolve vulnerabilities might indicate:

- Inefficiency in vulnerability and patch management systems or processes
- Deficiency in the training or staffing of the Vulnerability Management team

Addressing delays in resolving vulnerabilities is vital for enhancing overall security. Swift action minimizes the risk of breaches by malicious actors, safeguarding the organization's network. A high mean time to resolve vulnerabilities could signal system inefficiencies or deficiencies in team training, urging prompt corrective actions to bolster security measures.



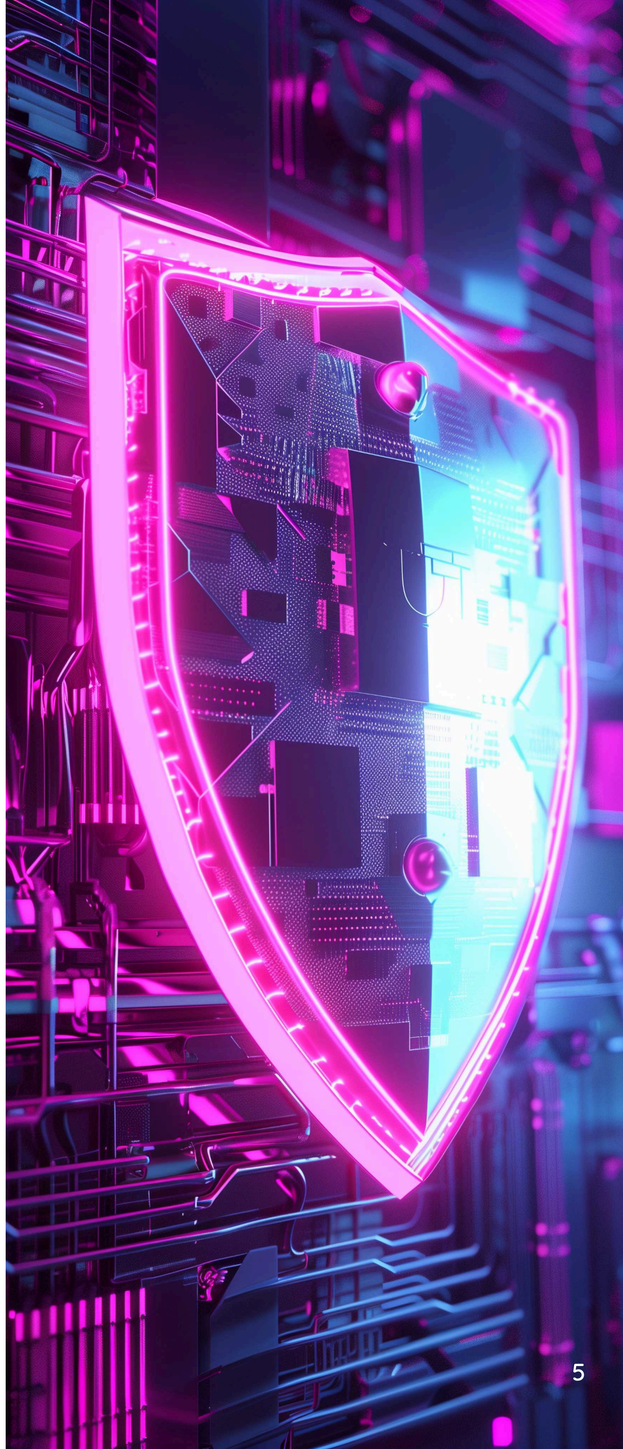
Percent of Open Vulnerabilities with Exploits tracks the percentage of unresolved vulnerabilities with publicly known exploits.

A high percentage of vulnerabilities with known/public exploits significantly increases organizational exposure and risk. This could lead to a network breach, causing substantial damage to the organization.

Additionally, a high percentage of open vulnerabilities with exploits can be an indicator of:

- Inefficiencies in vulnerability and patch management systems or processes.
- Staffing or training deficiencies within the Vulnerability Management team.
- Challenges in prioritizing vulnerabilities for patching.

Addressing a high percentage of vulnerabilities with known exploits is crucial. It helps reduce exposure and prevents network breaches, safeguarding the organization from substantial damage. Moreover, it reveals system inefficiencies, staff training gaps, and challenges in prioritizing patches, allowing for targeted improvements to strengthen overall security.



Training & Awareness

Training & Awareness programs equip employees with the knowledge and skills to identify and respond to potential threats, such as phishing attacks or social engineering. By educating staff on security best practices, promoting a culture of security awareness, and monitoring KPIs related to these efforts, organizations can significantly reduce their risk of successful cyberattacks.

Phishing Simulation Reporting Rate tracks the percentage of users who submitted malicious email reports during simulated phishing email training during a specified month.

Users who are consistently reporting simulated phishing emails are most likely up to date on their security awareness training and capable of identifying potential threats to the organization.

A high phishing report rate can indicate a well-trained employee base that:

- Knows how to identify potential risks to the organization
- Are engaged enough to report the suspicious email so that malicious senders can be blacklisted by the security team

Phishing Simulation Data Surrender Rate tracks the percent of users who submitted data during simulated phishing email training during a specified month.

Users who are consistently reporting simulated phishing emails are most likely up to date on their security awareness training and capable of identifying potential threats to the organization.

A high data surrender rate can indicate an untrained employee base that:

- Is more likely to follow links found in malicious emails and surrender credentials to attackers
- Unknowingly creates a pathway for malicious actors to gain access to organization assets

Cloud Security

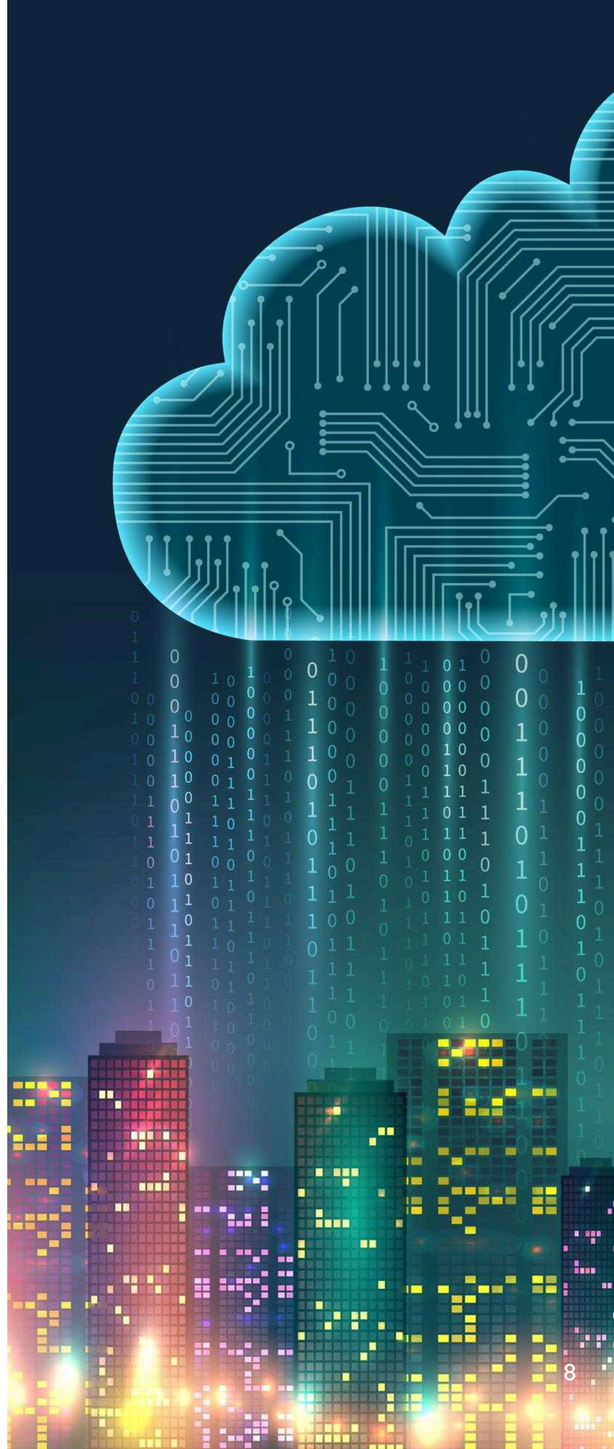
Cloud security efforts protect an organization's data and applications in the cloud environment. Given the increasing reliance on cloud computing, robust cloud security, and management of cloud security metrics, is critical for maintaining data confidentiality, integrity, and availability, ensuring business continuity, and safeguarding sensitive information.

Number of Externally Exposed Cloud Resources tracks the daily number of cloud resources that are exposed to access from the internet.

A high number of externally exposed cloud resources increases the risk of unauthorized access, data breaches, and cyberattacks, making the organization more vulnerable to exploitation.

A high count of externally exposed resources can indicate:

- Misconfigured security controls or lack of proper network segmentation.
- Increased attack surface, making systems more susceptible to threats.
- A need for stricter access controls and firewall policies.
- Potential compliance violations due to unintended public exposure.
- Insufficient monitoring or governance over cloud resource deployments.

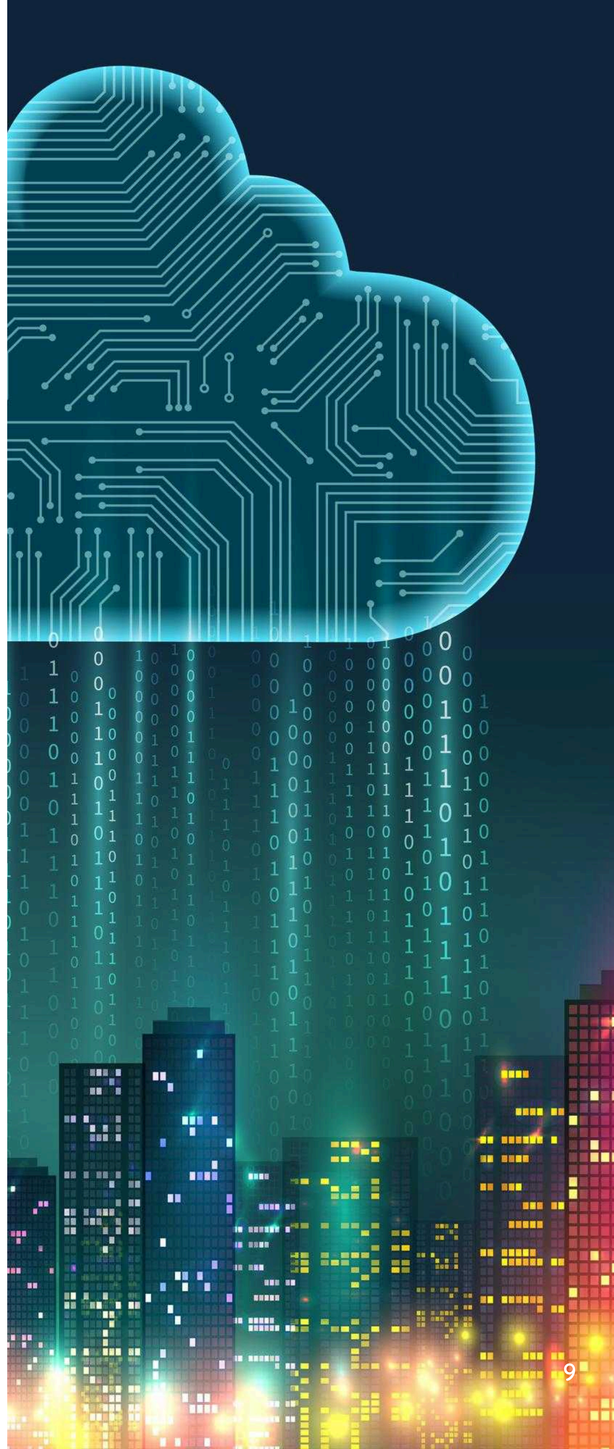


Number of Daily Open Cloud Alerts tracks the number of daily cloud alerts. Alerts can indicate misconfigurations, compliance failures, and suspicious activity.

A high number of cloud resources is indicative of widespread security non-compliance, greatly increasing the risk that a malicious actor will establish a foothold in the organization's network.

A high number of daily cloud alerts can indicate:

- An ineffective set of onboarding policies and procedures for onboarding new cloud assets.
- A deficiency in the training or staffing of the security team to update policies from the “Lessons Learned” phase of the alert triage phase which would otherwise help prevent repeats of the same type of alert from repeating.
- An unusually high influx of compliance or configuration settings which are temporarily overwhelming the security teams.



Identity & Access Management

Identity and Access Management (IAM) controls user access to an organization's critical systems and data. By implementing strong IAM practices and continually assessing IAM-related KPIs, organizations can ensure that only authorized users have appropriate access, minimizing the risk of unauthorized access, data breaches, and other security incidents.

Percent of Inactive Privileged Users tracks the percentage of privileged user accounts that have been inactive over the threshold.

A high percentage of inactive privileged user accounts could be indicative of unsecured off-boarding processes; this greatly increases the attack surface of an organization providing an opportunity for malicious actors to establish a foothold in the organization’s network leading to data breaches and potentially total business disruption. The risk posed by this issue is greatly increased due to the accounts having elevated privileges.

A high percentage of inactive privileged user accounts can indicate:

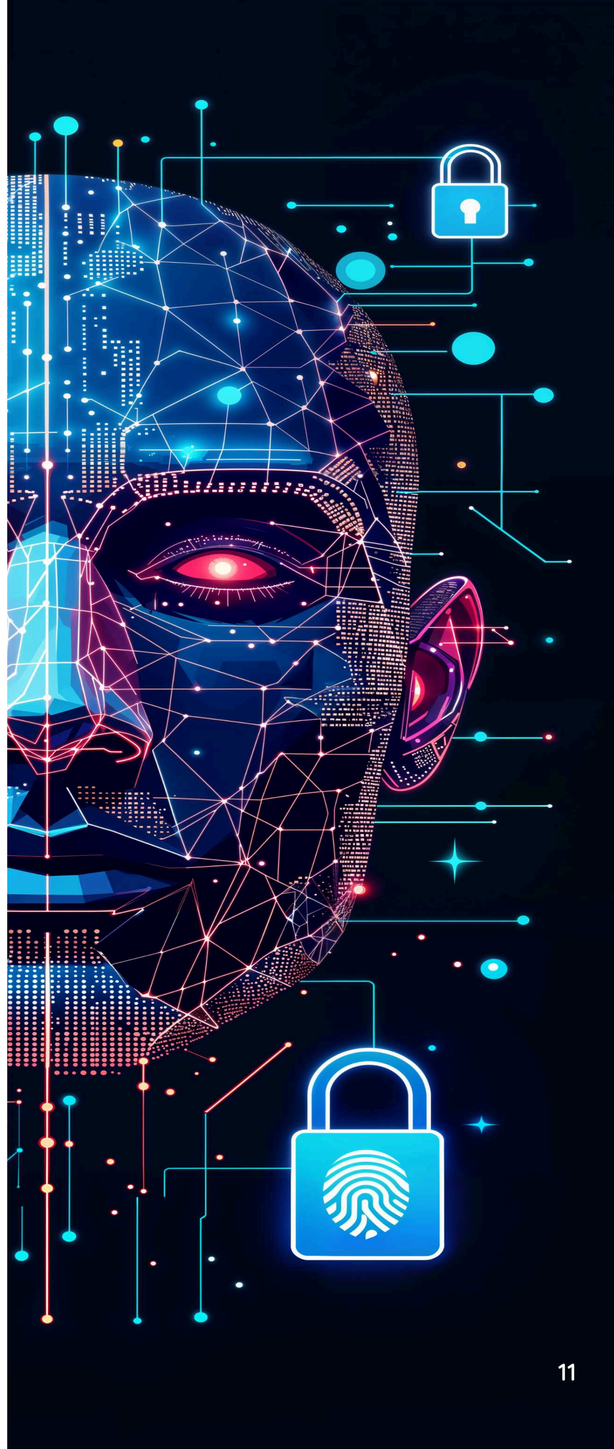
- A need to redefine and enforce proper off-boarding protocols.
- A deficiency in the training or staffing of the security team to remediate IAM misconfigurations.
- A need to enforce least privileges

Percent of Users Without MFA Enabled tracks the percentage of all user accounts that do not have MFA.

A high percentage of user accounts that do not have multi-factor authentication puts the organization at high risk as those accounts are much more vulnerable to takeover by malicious actors, which can potentially lead to data breaches and total business disruption.

A high percentage of users without MFA can indicate:

- IAM security best practices are not being followed.
- A deficiency in user training to ensure their accounts are secure.
- A high risk of account takeover.



Device Management

Device management helps ensure that devices are properly configured, updated, and compliant with security policies. Effective device management enables organizations to reduce their vulnerability to cyberattacks, protect sensitive data, and maintain the overall security of their network.

Percent of Devices Without Cloud Backup tracks the percentage of devices without cloud backup across various platforms.

This metric is significant because a high percentage of devices without cloud backup significantly increases the risk of data loss due to hardware failure, ransomware attacks, or other unforeseen events. This lack of redundancy compromises business continuity, potentially leading to critical operational disruptions and financial losses.

A high percentage of devices without cloud backup can indicate:

- Insufficient implementation or enforcement of backup policies across the organization
- A lack of employee training on the importance of data redundancy and backup best practices
- Gaps in IT infrastructure, such as insufficient storage capacity or inadequate cloud backup solutions
- Increased exposure to risks such as prolonged recovery times in the event of a cybersecurity incident or hardware failure

Percent of Non-Compliant Managed Devices tracks the percentage of managed devices that fail compliance checks against the organization's policies.

A high percentage of Non-Compliant Devices could be indicative of either compliance policies that are misconfigured and thus unachievable, or a large number of devices not onboarded properly. Depending on the strictness of compliance policies, this could indicate that the company has a rather large attack surface as non-compliant devices should indicate devices that pose a risk of being exploited.

A high percentage of Non-Compliant Devices can indicate:

- An ineffective set of policies and procedures for onboarding new devices.
- A deficiency in the training or staffing of remediating compliance issues.

Application Security

Effective Application security helps protect software applications from threats such as unauthorized access and data breaches. Implementing the proper security measures during design, development, and deployment phases can help organizations minimize the risk of vulnerabilities being exploited by malicious actors.

Mean Time to Fix AppSec Vulnerabilities tracks the daily average time it takes to close or fix AppSec vulnerabilities within a specific day.

A lengthy response time heightens the risk of AppSec vulnerabilities being exploited by malicious actors, potentially leading to network breaches and significant damage to the organization.

A high mean time to fix AppSec vulnerabilities might indicate:

- Inefficiency in vulnerability and patch management systems or processes.
- Deficiency in the training or staffing of the Vulnerability Management team.

Addressing delays in resolving vulnerabilities is vital for enhancing overall security. Swift action minimizes the risk of breaches by malicious actors, safeguarding the organization's network. A high mean time to fix AppSec vulnerabilities could signal system inefficiencies or deficiencies in team training, urging prompt corrective actions to bolster security measures.

Percent of Overdue AppSec Vulnerabilities tracks the percentage of AppSec vulnerabilities in Open Status that surpass their Time to Fix threshold, out of all Open vulnerabilities within a given day.

A high rate of overdue AppSec vulnerabilities increases organizational exposure and the risk of exploitation by malicious actors, potentially leading to network breaches and significant damage to the organization.

A high rate of overdue AppSec vulnerabilities can be an indicator of:

- Inefficiencies in vulnerability and patch management systems or processes.
- Deficiencies in the training or staffing of the Vulnerability Management team.

Addressing high rates of overdue AppSec vulnerabilities is crucial to reducing organizational risk and preventing potential network breaches. Resolving these issues enhances immediate security and promotes more efficient operational practices, bolstering your organization’s resilience against cyber threats.

The Importance of Benchmarking

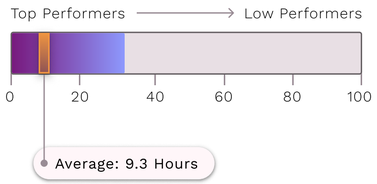
Benchmarking is crucial for assessing and enhancing program performance. By comparing your program's historical data, you can track its progress over time. Furthermore, benchmarking against industry standards provides achievable goals and reveals your organization's competitive standing. This valuable insight informs strategic decisions to optimize performance and achieve superior results.

Industry benchmarking allows you to gauge your organization's position relative to competitors, while external benchmarking against high-performing industries encourages exceeding expectations and fosters continuous improvement.

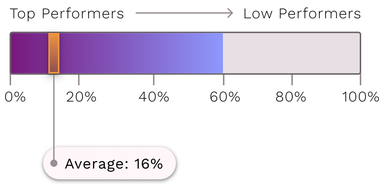
Below are some relevant benchmarks provided in our previous Key Metrics to Defend Against Threats and Regulations, Reporting, and Risk Management CISO research reports. The Onyxia platform includes a full suite of benchmarks per domain and CPI, as well as comparisons against several key industries.

Detection and Response

Mean Time to Resolve Incidents

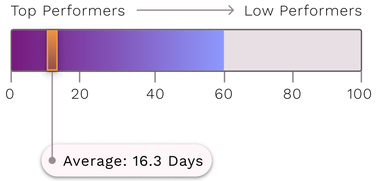


Incident False Positive Rate

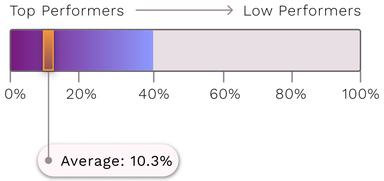


Vulnerability Management

Mean Time to Resolve Vulnerabilities

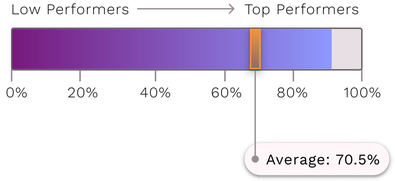


Percent of Overdue Vulnerabilities with Exploits



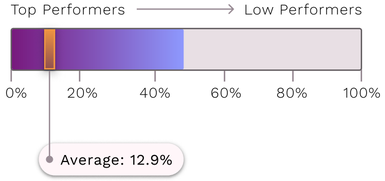
Training and Awareness

Phishing Simulation Reporting Rate

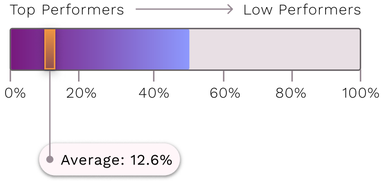


Identity and Access Management

Percent of Inactive Privileged Users

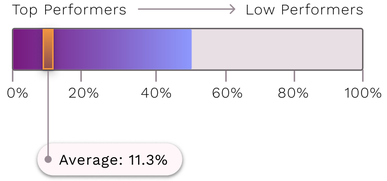


Percent of Users without MFA Enabled



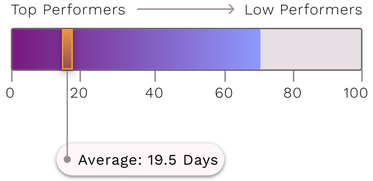
Device Management

Percent of Non-Compliant Managed Devices



Application Security

Mean Time to Fix AppSec Vulnerabilities



How Onyxia Can Help You Take a Data-Driven Approach to Cybersecurity Program Management

Onyxia's Cybersecurity Management Platform is a core solution for CISOs and security leaders to strengthen their high-level security strategy and streamline day-to-day, tactical program management.

Through our Security Data Fabric, we provide all of the KPIs above and more – out of the box. We enable CISOs to standardize performance tracking, accurately benchmark their program, align their data to key compliance frameworks, and automate board reporting. Moreover, with OnyxAI, our Predictive Cybersecurity Management Engine, security leaders receive actionable insights to improve security program performance and optimize program SLAs. They also gain valuable program trend predictions that can help reduce risk and prevent future crises.

With Onyxia, CISOs and security leaders can leverage all the data they have, across many disparate data sources, and more easily connect their critical security strategies to important business outcomes.

Manage Your Program in a Data-Driven Way

Measure the metrics that matter to you most, compare your security program across industry benchmarks, and continuously evaluate previous program performance with a matter of clicks.

Optimize Your Security Stack Efficiency and Coverage

Our Security Stack Map (SSM), makes it easy to identify gaps, overlaps, and redundancies in tool coverage, adhere to compliance frameworks, and make your tech stack as efficient and effective as possible.

Effectively Demonstrate Business Value

Quickly pull customized reports, demonstrate compliance with industry regulations and effortlessly communicate the most important business outcomes.

Harness AI to Reduce Risks and Threat Exposure

Onyxia effectively utilizes artificial intelligence to your advantage. Reduce threat exposure with actionable insights and intelligent program predictions.

About Onyxia

Onyxia Cyber is on a mission to empower Chief Information Security Officers and security leaders with the ability to continually strengthen their security programs and proactively reduce risk exposure. Our intelligent Cybersecurity Management Platform, which delivers powerful predictive insights, provides real-time security assessment and benchmarking, full security stack visibility, and streamlined board reporting. With Onyxia, CISOs gain a simplified way to ensure organizational compliance, improve risk management, and align their security initiatives with business goals.

Book a Demo