Security KPI & Metrics Analysis

Ten Operational Security Metrics Applied to Real-World Incidents

A practical analysis of ten cybersecurity KPIs and how each can be used to measure security performance against real incidents.

CIS CONTROLS | Security Metrics | MTTD / MTTR | Vulnerability Management | Access Control | Vendor Risk | Logging | Penetration Testing

AT A GLANCE

Scope	Ten KPIs: five security-operations measures, five extending into asset visibility, logging, allowlisting, configuration and penetration-testing coverage
Method	For each KPI: definition and real-world use, a 2026 incident from public reporting, and how the metric would have measured or improved the response
Cases	Hugging Face · Stryker · ServiceNow · Klue · LastPass · Fortinet · Klaviyo · 2026 open-source supply-chain compromises
Sources	Fortinet, Atlassian and Bitsight KPI glossaries; CIS Controls Assessment Specification

Sean Richard

sean@autom8ionlab.com · linkedin.com/in/a8l-sean-richard · +1.352.818.9694

Portfolio edition based on original Full Sail University coursework. Substantive project content is preserved; classroom-only submission headers were removed.

PROJECT SCOPE

Ten indicators, ten incidents

This analysis examines ten cybersecurity key performance indicators. The first five focus on common security-operations measures, while the remaining five extend measurement into asset visibility, logging, allowlisting, configuration, and penetration-testing coverage.

#	KPI	APPLIED TO
01	Mean Time to Detect (MTTD)	Hugging Face breach (July 2026)
02	Mean Time to Resolve (MTTR)	Stryker network disruption (March 2026)
03	Patching Cadence	ServiceNow data-exposure bug (June 2026)
04	Access Management	Klue legacy-credential breach (June 2026)
05	Average Vendor Security Rating	LastPass exposure via Klue (June 2026)
06	Software Inventory Tool Coverage	Fortinet firewall campaign (June 2026)
07	Audit Log Coverage	Hugging Face breach (July 2026)
08	Application Allowlisting Installation Coverage	2026 open-source supply-chain compromises
09	Standard Configuration Coverage	Klaviyo sign-up form misconfiguration (August 2026)
10	Unauthenticated Penetration Testing Coverage	ServiceNow data-exposure bug (June 2026)

KPI 01

Mean Time to Detect (MTTD)

Source: https://www.fortinet.com/resources/cyberglossary/secops-metrics

EXPLANATION AND REAL-WORLD USE

Mean Time to Detect measures the average amount of time between the beginning of a security incident and the point when the security team detects it. Organizations calculate it from incident start and detection timestamps and review the result by severity, business unit, or detection source. In a real security operations center, a falling MTTD indicates that monitoring, alerting, and analyst workflows are identifying threats faster. A rising MTTD can reveal gaps in logging, detection rules, staffing, or visibility that allow attackers to remain active longer.

CASE STUDY

Hugging Face confirms breach affected internal datasets and credentials, urges users to take action

TechCrunch, July 20, 2026

https://techcrunch.com/2026/07/20/hugging-face-confirms-breach-affected-internal-datasets-and-credentials-urges-users-to-take-action/

HOW THE KPI APPLIES

Hugging Face reported that its anomaly detection identified malicious activity after attackers exploited a vulnerability, escalated permissions, and accessed internal systems. The company also used server logs to analyze the attack. MTTD could be used to measure the exact elapsed time between the attacker's first malicious action and the first confirmed detection. Tracking that value across future incidents would show whether new detection rules, logging improvements, and automated analysis are actually reducing attacker dwell time.

KPI 02

Mean Time to Resolve (MTTR)

Source: https://www.atlassian.com/incident-management/kpis/common-metrics

EXPLANATION AND REAL-WORLD USE

Mean Time to Resolve measures the average time required to fully resolve an unplanned incident, including detection, diagnosis, repair, restoration, and work performed to reduce the chance of recurrence. It is calculated by adding the total resolution time for incidents during a defined period and dividing by the number of incidents. In real operations, MTTR helps leaders evaluate incident response efficiency, compare performance against service goals, and identify whether delays occur in diagnosis, repair, coordination, or recovery.

CASE STUDY

Stryker Network Disruption — Customer Updates

Stryker, March 2026

https://www.stryker.com/us/en/about/news/2026/a-message-to-our-customers-03-2026.html

HOW THE KPI APPLIES

Stryker disclosed a cyberattack that caused a global network disruption beginning March 11, 2026. The company activated its incident response plan, contained the incident, worked with outside experts, and progressively restored systems supporting customers, ordering, shipping, and manufacturing. MTTR could measure the full resolution time for each affected business service instead of treating recovery as one single event. Comparing those results would identify which systems were restored efficiently and which recovery processes need improvement before another major incident.

KPI 03

Patching Cadence

Source: https://www.bitsight.com/glossary/cybersecurity-kpi-dashboard

EXPLANATION AND REAL-WORLD USE

Patching Cadence measures how quickly an organization deploys security patches after they become available or after a vulnerability is identified as high risk. A useful implementation can track average days to patch as well as the percentage of critical patches completed within the organization's required service level. In a real environment, security and IT teams use the trend to identify systems or departments that repeatedly fall behind, prioritize exposed assets, and determine whether vulnerability management resources are keeping pace with risk.

CASE STUDY

ServiceNow tells customers a bug left some of their data exposed to the internet

TechCrunch, June 10, 2026

https://techcrunch.com/2026/06/10/servicenow-tells-customers-a-bug-left-some-of-their-data-exposed-to-the-internet/

HOW THE KPI APPLIES

ServiceNow reported that a software bug allowed unauthenticated users to gain greater access to customer-hosted data than intended and that affected customer instances were patched. Patching Cadence could measure the elapsed time from vulnerability validation to deployment of the corrective update across the customer environment. The company could also track the percentage of affected instances patched within a critical-risk deadline. That information would show whether the patching process can consistently reduce exposure quickly when an internet-facing security flaw is discovered.

KPI 04

Access Management

Source: https://www.fortinet.com/resources/cyberglossary/identity-based-attacks

EXPLANATION AND REAL-WORLD USE

Access Management metrics measure whether users, service accounts, vendors, and administrators have only the access required for their responsibilities. Examples include the number of privileged accounts, the percentage of privileged accounts reviewed on schedule, stale accounts, and credentials that remain active after their business purpose ends. In real-world security operations, these metrics support least privilege and account lifecycle management. They also give management a measurable way to identify excessive access before it becomes a path for privilege escalation or unauthorized data access.

CASE STUDY

Klue says hackers stole credential from 2022 that led to customer data breaches

TechCrunch, June 23, 2026

https://techcrunch.com/2026/06/23/klue-says-hackers-stole-credential-from-2022-that-led-to-customer-data-breaches/

HOW THE KPI APPLIES

Klue said attackers used a legacy credential that had originally been provided to a third party for a limited pilot in 2022. The credential remained usable years later and contributed to the 2026 breach. Access Management KPIs could have tracked the age of third-party credentials, the percentage of vendor accounts reviewed on schedule, and the number of credentials with no current business owner. A recurring review metric could have exposed the unnecessary credential long before attackers were able to use it.

KPI 05

Average Vendor Security Rating

Source: https://www.bitsight.com/glossary/cybersecurity-kpi-dashboard

EXPLANATION AND REAL-WORLD USE

Average Vendor Security Rating summarizes the security posture of third-party providers using a consistent quantitative rating and tracks how that average changes over time. Organizations can use the metric to compare vendors, identify deteriorating security posture, and determine which providers require deeper assessment or remediation. In practice, the rating should not replace a full vendor risk assessment, but it provides a useful dashboard indicator that helps security teams prioritize attention across a large vendor population and communicate third-party risk to management.

CASE STUDY

Password manager maker LastPass says hackers stole customer support case data during Klue breach

TechCrunch, June 23, 2026

https://techcrunch.com/2026/06/23/password-manager-maker-lastpass-says-hackers-stole-customer-support-case-data-during-klue-breach/

HOW THE KPI APPLIES

LastPass disclosed that customer information was stolen because hackers compromised its technology partner Klue, even though LastPass said its own infrastructure and password vaults were not affected. This demonstrates why vendor risk must be measured beyond the organization's internal network. An Average Vendor Security Rating could help identify vendors whose external risk posture is worsening and trigger additional review. Combined with contract requirements and access reviews, the metric can help prioritize vendors that have access to sensitive customer or operational data.

KPI 06

Software Inventory Tool Coverage

Source: https://cas.docs.cisecurity.org/en/latest/source/Controls2/

EXPLANATION AND REAL-WORLD USE

Software Inventory Tool Coverage measures the percentage of applicable endpoints that are visible to automated software inventory tools. The metric can be calculated by dividing the number of endpoints covered by inventory tooling by the total number of endpoints capable of running software. In a real environment, a high coverage rate gives security teams confidence that they can identify installed applications and versions across the enterprise. Low coverage creates blind spots where outdated, unauthorized, or vulnerable software may remain unknown and unmanaged.

CASE STUDY

Cybercriminals allegedly hacked tens of thousands of Fortinet firewalls used by major companies all over the world

TechCrunch, June 17, 2026

https://techcrunch.com/2026/06/17/cybercriminals-allegedly-hacked-tens-of-thousands-of-fortinet-firewalls-used-by-major-companies-all-over-the-world/

HOW THE KPI APPLIES

The reported Fortinet campaign targeted large numbers of exposed firewalls and VPN gateways and used known credentials to gain access. Software Inventory Tool Coverage would not stop a credential attack by itself, but complete inventory visibility would help an organization quickly identify every Fortinet device it owns, the software running on those devices, and the responsible system owner. Teams could then target password resets, configuration reviews, monitoring, and other remediation actions without losing time searching for unmanaged or forgotten devices.

KPI 07

Audit Log Coverage

Source: https://cas.docs.cisecurity.org/en/latest/source/Controls8/

EXPLANATION AND REAL-WORLD USE

Audit Log Coverage measures the percentage of systems or service providers that are properly configured to collect the logs required by the organization. A security team can define the population of critical applications, cloud services, servers, and providers, then calculate how many are producing usable logs in the required location. In real operations, this KPI identifies monitoring blind spots. High coverage improves investigations and detection because analysts have the events needed to reconstruct activity, while missing or incomplete logs can prevent reliable detection and incident analysis.

CASE STUDY

Hugging Face confirms breach affected internal datasets and credentials, urges users to take action

TechCrunch, July 20, 2026

https://techcrunch.com/2026/07/20/hugging-face-confirms-breach-affected-internal-datasets-and-credentials-urges-users-to-take-action/

HOW THE KPI APPLIES

During the Hugging Face incident, the company said its anomaly detection identified the attack and that an AI model was used to analyze server logs containing records of the malicious activity. Audit Log Coverage could measure whether every critical workload, sandbox, identity service, and data platform is producing the required telemetry. If coverage is less than the target, the missing systems become known investigation gaps. Maintaining high log coverage would support faster detection, stronger forensic analysis, and more reliable lessons learned after an attack.

KPI 08

Application Allowlisting Installation Coverage

Source: https://cas.docs.cisecurity.org/en/latest/source/Controls2/

EXPLANATION AND REAL-WORLD USE

Application Allowlisting Installation Coverage measures the percentage of enterprise assets capable of supporting allowlisting that actually have an allowlisting control installed. Organizations can also track whether the control is properly configured. In real-world use, allowlisting limits execution to approved software, scripts, or libraries and reduces opportunities for unauthorized code to run. The KPI helps management determine whether the control is consistently deployed across the environment instead of assuming that a policy or tool purchase provides protection everywhere.

CASE STUDY

Hacked, leaked, and held for ransom: The worst breaches of 2026 so far

TechCrunch, July 7, 2026

https://techcrunch.com/2026/07/07/the-worst-hacks-and-breaches-of-2026-so-far/

HOW THE KPI APPLIES

TechCrunch reported that several open-source projects and security tools were compromised in 2026 and that backdoored software was used to steal passwords, credentials, and tokens from downstream users. Application Allowlisting Coverage could reduce some endpoint exposure by ensuring that only approved software and scripts are permitted to execute. The metric would show whether allowlisting is actually installed across eligible systems. It would not eliminate trusted software supply-chain risk, so it should be combined with software integrity checks, monitoring, and vendor controls.

KPI 09

Standard Configuration Coverage

Source: https://cas.docs.cisecurity.org/en/latest/source/Controls4/

EXPLANATION AND REAL-WORLD USE

Standard Configuration Coverage measures the percentage of authorized software or systems that have documented and maintained secure configuration standards. The organization first defines approved security settings, then measures how much of the environment is covered by those standards and, where possible, whether deployed configurations conform to them. In real operations, the KPI helps prevent security from depending on individual administrator choices. It also gives teams a measurable way to reduce configuration drift, identify unsupported systems, and prioritize areas where no secure baseline exists.

CASE STUDY

Signed up for Klaviyo? Dozens of advertisers may have seen your password

TechCrunch, August 10, 2026

https://techcrunch.com/2026/08/10/signed-up-for-klaviyo-dozens-of-advertisers-may-have-seen-your-password/

HOW THE KPI APPLIES

Security research found that Klaviyo's sign-up form had been misconfigured in a way that could send customer sign-up information, including passwords, to third-party advertising and technology trackers. Standard Configuration Coverage could require every customer-facing form and tracking integration to follow an approved configuration baseline that prohibits credential fields from being transmitted to analytics services. Measuring coverage would identify applications without that baseline, while automated configuration testing could verify that security requirements remain in place after website or tracking changes.

KPI 10

Unauthenticated Penetration Testing Coverage

Source: https://cas.docs.cisecurity.org/en/latest/source/Controls16/

EXPLANATION AND REAL-WORLD USE

Unauthenticated Penetration Testing Coverage measures the percentage of applications that have undergone unauthenticated penetration testing according to the organization's established testing process. The metric focuses on what an external attacker can reach without valid credentials and is especially useful for internet-facing applications. In real-world security programs, the KPI helps ensure that testing is not limited to a few high-profile systems. A low percentage reveals applications that may contain exposed access-control, authentication, input-validation, or configuration weaknesses that have never been tested from an attacker perspective.

CASE STUDY

ServiceNow tells customers a bug left some of their data exposed to the internet

TechCrunch, June 10, 2026

https://techcrunch.com/2026/06/10/servicenow-tells-customers-a-bug-left-some-of-their-data-exposed-to-the-internet/

HOW THE KPI APPLIES

The ServiceNow issue allowed unauthenticated users to obtain greater access to hosted customer data than intended, and the activity was associated with security researchers testing for vulnerabilities. Unauthenticated Penetration Testing Coverage could help organizations find similar problems before they are discovered externally. A company could set a target that all critical internet-facing applications receive unauthenticated testing on a defined schedule and track the percentage completed. Findings would still need separate remediation metrics, but coverage confirms that the external attack surface is being tested consistently.