CIS Controls visar vad som bör göras. Hur vet ni vad som faktiskt är gjort?

CIS Controls ger organisationer en prioriterad struktur för cybersäkerhetsarbetet. IG1 samlar den grundläggande cyberhygienen. IG2 bygger vidare med fler säkerhetsåtgärder för organisationer med större komplexitet och risk.

CIS Controls v8.1, IG1 och IG2 Oktober 2026 4 min läsning

Ramverket beskriver vad som bör finnas på plats. Det säger inte hur väl åtgärderna faktiskt är genomförda i den egna IT-miljön. Det är där mätningen börjar.

01 / Från krav till faktiskt tillstånd

Ta en teknisk åtgärd som multifaktorautentisering, kryptering eller klientskydd. Det kan finnas ett beslut om hur den ska användas och en konfiguration som ser korrekt ut. Ändå kan användare, enheter eller delar av miljön sakna det avsedda skyddet.

Tre saker behöver därför hållas isär:

Beslutat	Konfigurerat och tilldelat	Observerat
Vad organisationen har bestämt ska gälla.	Hur funktionen har satts upp och var den ska tillämpas.	Vad tekniska data faktiskt visar för den miljö som mäts.

En korrekt konfiguration är inte i sig bevis för att hela den avsedda populationen omfattas.

02 / Vad går faktiskt att verifiera?

Många av säkerhetsåtgärderna i CIS Controls går att kontrollera med tekniska data från organisationens befintliga system. Andra kan bara verifieras delvis, medan exempelvis rutiner, ansvar och utbildning kräver andra former av uppföljning.

Skillnaden är viktig. Att kunna verifiera en del av en säkerhetsåtgärd betyder inte att hela åtgärden är genomförd. Ett tillförlitligt mätresultat måste visa både vad som har kunnat kontrolleras och var underlaget inte räcker till.

CIS Controls ger strukturen för vilka säkerhetsåtgärder som är viktiga. Den tekniska mätningen visar hur läget faktiskt ser ut i organisationens IT-miljö.

03 / Ett exempel: MFA

Beslutat: alla användare ska använda multifaktorautentisering. Konfigurerat: det finns en policy som kräver det. Observerat, i en exempelmätning: 3 667 av 5 092 användare (72 %) loggade in med MFA. Policyn kan vara korrekt och ändå inte nå hela populationen. Det är skillnaden mellan konfiguration och observerat tillstånd, och det är den som mätningen gör synlig.

EXEMPELMÄTNING / MFA

Beslutat Alla användare ska använda MFA

Konfigurerat Policy som kräver MFA finns

Observerat 3 667 av 5 092 användare 72 %

Illustrativt exempel, inte kunddata.

04 / En mätning är mest värdefull när den går att jämföra med nästa

Ett resultat får större betydelse när det kan följas över tid. Då räcker det inte att spara en procentsiffra. Man behöver veta:

vad som mättes,

vilken population som omfattades,

vilka datakällor som användes,

hur resultatet beräknades.

Om antalet enheter i underlaget ändras mellan två mätningar måste det gå att förstå vad förändringen betyder. Annars kan ett bättre resultat bero på ett förändrat underlag i stället för ett förbättrat säkerhetsläge.

05 / Från ramverk till arbetsunderlag

För IT ligger värdet inte i ytterligare en tolkning av CIS Controls. Det ligger i att se var det tekniska läget avviker, vilka objekt det gäller och vilket underlag bedömningen bygger på, och i att kunna använda det i de verktyg och processer som redan finns.

Iviron bygger på den principen. Iviron använder säkerhetsdata från organisationens befintliga system och fastställer ett datumstämplat, låst tekniskt säkerhetsläge. Relevanta mätresultat relateras till etablerade ramverk som CIS Controls. Mätningen sker read-only. Iviron ändrar inget i miljön, och åtgärderna görs i organisationens egna system.

Principen Mät. Åtgärda. Verifiera.

Nästa mätning använder samma metod och visar vad som faktiskt förändrats och vad som återstår. Samma fakta presenteras på den detaljnivå ledningen behöver.

Verifierat betyder här att mätresultatet är reproducerbart och spårbart till definierad källa, population, omfattning och mätprincip. Det är inte en revision eller certifiering, och Iviron är inte ett CIS-certifieringsverktyg.

Källor och vidare läsning

CIS Critical Security Controls v8.1 www.cisecurity.org

CIS Controls Implementation Groups www.cisecurity.org

CIS Controls Assessment Specification www.cisecurity.org

CIS Controls Assessment Specification, dokumentation cas.docs.cisecurity.org