Engineer

Hændelseshåndtering

⏏ koordineret indsats under en hændelse

Hvad det er

Hændelseshåndtering er arbejdet med at lede en indsats under en driftsforstyrrelse eller en alvorlig trussel mod et system. En hændelse er det, der giver anledning til indsatsen. Håndteringen begynder, når nogen opdager og erklærer hændelsen, og fortsætter med koordinering, afhjælpning og overdragelse af det, der er tilbage. Udvikling, drift og support kan alle have en rolle. Nogle hændelser kræver også en person med myndighed til at træffe sikkerhedsmæssige eller juridiske beslutninger.

NIST beskriver registrering, håndtering og genopretning som dele af arbejdet med sikkerhedshændelser. Forberedelse og løbende forbedring understøtter alle tre. Det er en ramme for cybersikkerhed. Idéen om at fordele opgaver og holde styr på beslutninger er også nyttig, når en udgivelse går galt. Et muligt læk kan kræve, at holdet sikrer dokumentationen og beskytter berørte personer, selv om websiden virker. Ved et almindeligt driftstop er det måske vigtigere at få brugerne igennem en vej, der allerede virker.

Googles beskrivelse af hændelseshåndtering fordeler koordineringen på en indsatsleder, en ansvarlig for de operative ændringer og en ansvarlig for kommunikationen. Én person kan varetage flere funktioner i starten. Når flere deltager, kan navnene føjes til den fælles log. Det gør det muligt at finde den, der træffer beslutninger om driften, og giver supporten et fast sted at hente oplysninger. Fordelingen bør svare til holdets størrelse og situationen.

Brug begrebet i en beslutning

Brug »Hvad er hændelseshåndtering?« i en konkret beslutning. Vi kan knytte begrebet til det system, I bygger eller køber. Overvågning og alarmer, der siger til, mens fejlen stadig er lille, og tallene, der viser, hvor tit den bliver ved med at være det.

Se vores ydelser Kontakt os →

Undersøg antagelserne bag ordet

Brug forklaringen og det tilknyttede arbejde til at formulere spørgsmål til jeres projekt. Vi kan undersøge antagelserne sammen, før et værktøj vælges. Har bygget det første observerbarhedsdashboard — virksomhedens første overblik over sine egne systemer

Har bygget det første observerbarhedsdashboard Kontakt os →

Hvorfor det betyder noget

I de første minutter kommer forskellige oplysninger i forskelligt tempo. En måling kan vise flere betalingsfejl, mens det tager længere tid at afgøre, hvilke kunder og betalingsmåder der er ramt. Support kan få det første brugbare billede. En fælles tidslinje kan fastholde begge observationer, hvor de kommer fra, og hvor sikkert de kan fortolkes. Det gør det lettere for andre at undersøge hændelsen uden at antage, at den første forklaring er rigtig.

Indsatsen giver også kontrol med ændringer under pres. En tilbagerulning og en ændring af indstillingerne kan hver især være fornuftige og give problemer, hvis de gennemføres sammen. Den, der koordinerer, har brug for at vide, hvad andre vil ændre, hvornår det kan måles, og hvordan man kan gå tilbage. Samtidig skal den relevante specialist have plads til at foreslå en løsning.

Genopretning og fejlfinding kan tage forskellig tid. En alternativ vej kan få en tjeneste til at fungere igen, før årsagen er kendt. Holdet kan fastlægge genopretningen ved konkrete observationer, for eksempel at nye ordrer går igennem, og at tidligere ordrer bliver afstemt. Den efterfølgende evaluering ser på årsager, indsatsens forløb og forbedringer. Den står stærkere, når holdet har bevaret beslutninger, testresultater og usikkerhed fra selve indsatsen.

Sådan ser det ud i praksis

Forestil dig en bestillingstjeneste, der trækker betalingen, men af og til ikke udsteder en billet. Support ser de første henvendelser, og en udvikler bekræfter, at forespørgsler er begyndt at fejle. Den første ansvarlige erklærer en hændelse og registrerer, hvornår symptomerne blev opdaget. Holdet aftaler en kort beskrivelse af den kendte virkning og udpeger en person, der har styr på ændringerne. Support får et kontaktpunkt og et tidspunkt for næste besked.

Driften gennemgår nogle af de berørte bestillinger og finder en nylig ændring, der kan forklare tidspunktet. Indsatslederen beder holdet undersøge, om gennemførte betalinger stadig er synlige efter en tilbagerulning. Én person

gennemfører ændringen, mens en anden følger betalinger og billetter. Support gemmer bestillingsnumre til opfølgning og fortæller kunderne, hvad de kan gøre med en ubekræftet bestilling. Beskeden kan ændres, når holdet ved mere.

Holdet vurderer virkningen ud fra hele forløb, hvor betalingen knyttes til den rigtige billet. Det følger også listen over bestillinger, der mangler at blive afstemt. Registrér, hvornår tjenesten igen kunne bruges, og hvem der gennemgår de bestillinger, der stadig ikke er afklaret. Når driften kan overtage det aktuelle ansvar, får undersøgelsen af årsagen sin egen ansvarlige og en dato.

Engineers sag om voksende hukommelsesforbrug i en macOS-app dokumenterer særskilte målinger og det efterfølgende arbejde med at begrænse mængden af gemte hændelser. Den viser, hvorfor målingernes rækkevidde har betydning ved opfølgning. Eksemplet med billetter er tænkt til at vise, hvordan selve indsatsen kan organiseres.

Når næste vagt overtager, læser holdet tidslinjen igennem sammen. Den, der træder af, nævner den seneste bekræftede observation, den ændring, der stadig kan være i gang, og tidspunktet for næste besked til kunderne. Så kan afløseren fortsætte arbejdet uden at gennemlæse hele chatten, mens en handling allerede er ved at blive gennemført.

Hvor det går galt

Holdet venter på sikkerhed, før det erklærer en hændelse. En sandsynlig virkning kan undersøges med en navngiven ansvarlig og en aftalt opdatering. Holdet kan afblæse indsatsen, hvis de næste oplysninger viser, at situationen er mindre alvorlig.

Alle ændrer systemet på én gang. Skriv planlagte og udførte handlinger i en kort fælles log. Se, hvad ændringen gjorde, før en anden sættes i gang, når det er muligt. Adskil opgaver, der faktisk kan udføres sideløbende.

Kunderne hører gæt. Beskriv, hvad de kan opleve, hvad de trygt kan gøre og hvornår de får nyt. Fortæl, hvilke fakta der stadig undersøges, og forklar årsagen, når den kan underbygges.

Det uafsluttede arbejde forsvinder, når driften vender tilbage. Giv afstemning, kundekontakt og midlertidige beskyttelsestiltag en ansvarlig. Før opgaverne ind i det system, holdet bruger, når hændelseskanalen lukker.

Læs mere

- NIST SP 800-61 Rev. 3 — håndtering af sikkerhedshændelser, forberedelse og forbedring.
- Googles vejledning om at lede hændelser — roller, kommunikation og fælles log.
- Hændelseshåndtering i Googles SRE-håndbog — erfaringer og eksempler fra konkrete indsatser.

Ordliste

Vælg ud fra jeres faktiske vilkår

Medbring udrulningsforløbet, driftsrisiciene og dem, der har vagten. Vi kan afgrænse en ændring med kontroller, en vej tilbage og tydeligt ansvar.

Se, hvad det koster Kontakt os →

Gør begreberne praktiske

Spørg, hvordan »Hvad er hændelseshåndtering?« gælder i jeres organisation. Et konkret eksempel fra jeres nuværende system er nok til at begynde samtalen.

Se vores ydelser

welcome@engineer.company +45 50 10 61 84 København, Danmark

Tag denne side med dig

Visitkort

Lavet med kærlighed af **D.**

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Copyright © 2025 – nu · Engineer ApS · Alle rettigheder forbeholdes.

Udskrevet fra https://engineer.company/da/glossary/incident-response/