

**Sample file — not real research.** This page demonstrates the Decision File format as generated by UpSight from a recorded interview. “Dana Whitfield,” the payments company, and the vendors named (LogHarbor, Sentrix, Corvid, NightOwl) are illustrative. [See the interactive version — every underlined claim opens a video receipt ↗](#)

DECISION FILE / SECURITY · SAMPLE

# SIEM Replacement: When Selection Criteria Fail to Differentiate

A CISO at a payments company · Interview analyzed 17 Aug 2026 · Illustrative subject

|               |                                                                                                          |
|---------------|----------------------------------------------------------------------------------------------------------|
| WHO           | A CISO at a payments company                                                                             |
| THE DECISION  | Deciding on a SIEM replacement.                                                                          |
| AT STAKE      | Budget constraints made defending a 28% increase to the CFO untenable.                                   |
| THEY CHOSE    | Dana chose NightOwl mainly for its 3am support despite lacking features.                                 |
| WHAT HAPPENED | Migration cost \$110k and took six months instead of two due to unforeseen complications.                |
| CORE LESSON   | Ensure all critical factors are properly weighted to avoid them becoming de facto decision points later. |

Eight diagrams below. In the live version, every underlined claim opens the buyer’s own words.

[See the receipts, interactively ↗](#)

✓ Everyone passed — decided nothing    — Knocked someone out    ★ This decided it    ✓ Chosen

## WHAT WE SAID VS. WHAT HAPPENED

**They weighted support at 10%, but the 3am named engineer decided the winner; higher-weighted items either passed for everyone or just knocked one vendor out.**

| WHAT WE SAID WE’D JUDGE ON                    | WEIGHT | WHAT ACTUALLY HAPPENED                                                                    |
|-----------------------------------------------|--------|-------------------------------------------------------------------------------------------|
| ✓ <b>Threat detection coverage</b>            | 30%    | All four could detect everything we cared about — it didn’t separate anyone.              |
| — <b>Integrations with our existing stack</b> | 20%    | Sentrix had 9 of 12; the card switch was “on the roadmap.” The others had all 12 day one. |

| WHAT WE SAID WE'D JUDGE ON                | WEIGHT          | WHAT ACTUALLY HAPPENED                                                                                                          |
|-------------------------------------------|-----------------|---------------------------------------------------------------------------------------------------------------------------------|
| — Query performance at our volume         | 15%             | Corvid slowed badly on 90-day lookback searches; the others handled our volume fine.                                            |
| — Price                                   | 25%             | Price knocked out exactly one vendor — the incumbent. The other three landed within about \$30k of each other over three years. |
| ★ Support                                 | 10%             | We bought the 3am phone call — a named engineer in contract. That decided it.                                                   |
| — Will the analysts actually use it daily | not on the list | Our SOC stopped opening Sentrix two weeks into the trial — the UI didn't fit queue-clearing work.                               |

SOURCE: Dana Whitfield (CISO) and team — interview transcript.

▼ Read what Dana said (7 quotes)

"We did it properly, or so we thought. April, we wrote a scorecard before we talked to a single vendor."

"All four could detect everything we cared about."

"We needed twelve connections... LogHarbor, Corvid and NightOwl had all twelve... Sentrix had nine of twelve. The card switch connector was 'on the roadmap.'"

"Corvid slowed badly on 90-day lookback searches... LogHarbor, Sentrix, NightOwl all handled our volume without complaint."

"Price knocked out exactly one vendor — LogHarbor. The other three landed within about 30 thousand of each other on a three-year view."

"The honest truth is we bought the 3am phone call."

"Sentrix, the analyst darling, our SOC guys just stopped opening it two weeks into the trial."

[Hear these in the interactive report ↗](#)

## FEATURE COMPARISON

**Only NightOwl offered a named 3am engineer at the budgeted tier; that single line decided it.**

✓ Yes    ⦿ Partly    💰 Only if we pay more    — No    ★ Yes — and this is what decided it

CAN IT DO THIS?      LOGHARBOR (INCUMBENT)      SENTRIX      CORVID      NIGHTOWL

**A named engineer we can call at 3am**



CAN IT DO THIS?

LOGHARBOR (INCUMBENT)

SENTRIX

CORVID

NIGHTOWL

Has all 12 integrations we  
need (incl. card switch)



90-day lookback query  
performance during incidents



SOURCE: Dana Whitfield (CISO) and team — interview transcript.

▼ Read what Dana said (3 quotes)

"When this breaks at 3am during an incident, who picks up the phone?"

"LogHarbor, Corvid and NightOwl had all twelve, day one. Sentrrix had nine of twelve."

"Corvid slowed badly on 90-day lookback searches."

[Hear these in the interactive report ↗](#)

#### DECISION TIMELINE

**Nine months of trials and comparisons ended with one question — "who picks up at 3am?" — and then migration ran four months long.**

MARCH



**Renewal quote jumps 28%**

Pricing model changed; at our volume it was untenable, so we went to market.

MAY–DECEMBER  
9 months



**Head-to-head evaluation and trials**

Two full head-to-head trials; ~60 hours of team time.

MID-  
EVALUATION  
6 weeks



**Seriously considered building it**

Modeled an open-source stack but killed it due to staffing reality.

JANUARY  
one meeting



**The 3am question decides it**

One meeting — only NightOwl had a named 3am engineer at our tier.

POST-  
DECISION  
6 months (4  
months late)



**Migration ran long**

Took six months instead of two; four months late.

MAY



## Go-live on NightOwl

Live in May instead of January.

● What started it / how it ended   ● The tipping point   ● A stretch of time

SOURCE: Dana Whitfield (CISO) and team — interview transcript.

### ▼ Read what Dana said (5 quotes)

"The renewal quote... was 28 percent higher than the year before."

"Nine months. Two full head-to-head trials..."

"We did, seriously, for about six weeks in the middle of the evaluation."

"When this breaks at 3am during an incident, who picks up the phone?"

"It cost about 110, and it took six months — we went live in May instead of January."

[Hear these in the interactive report ↗](#)

### WHO DROPPED OUT, AND WHY

**The incumbent fell on price; Sentrrix fell on real-world use; Corvid fell on support at budget; NightOwl won for the 3am named engineer.**

|   |                                  |                                 |                                                                                                                                                                    |
|---|----------------------------------|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| — | <b>LogHarbor<br/>(incumbent)</b> | <b>Too expensive</b>            | 28% renewal hike and pricing model change made it untenable; price knocked out exactly one vendor — the incumbent.                                                 |
| — | <b>Sentrrix</b>                  | <b>Nobody used it</b>           | Analysts stopped opening it two weeks into the trial; UI fit threat hunting, not queue clearing. Also missing the card switch connector and no named 3am engineer. |
| — | <b>Corvid</b>                    | <b>Above budget for support</b> | A named 3am engineer required Enterprise Plus (+\$95k/yr); also slowed on 90-day lookbacks.                                                                        |
| ✓ | <b>NightOwl</b>                  | <b>Chosen</b>                   | Included a named on-call engineer at our tier — we bought the 3am phone call.                                                                                      |

SOURCE: Dana Whitfield (CISO) and team — interview transcript.

### ▼ Read what Dana said (4 quotes)

"Price knocked out exactly one vendor — LogHarbor."

"Our SOC guys just stopped opening it two weeks into the trial."

“Corvid — yes, but only on the Enterprise Plus tier, which was 95 thousand a year above what we'd budgeted.”

“The honest truth is we bought the 3am phone call.”

[Hear these in the interactive report ↗](#)

WHAT THE MONEY ACTUALLY BUYS

**Versus the cheapest finalist, they paid about \$75k more over three years — ~\$40k effectively for the 3am phone call and ~\$35k from a migration overrun.**

| WHAT WE'RE PAYING TO SOLVE                                                 | SENTRIX          | CORVID           | NIGHTOWL (CHOSEN)     |
|----------------------------------------------------------------------------|------------------|------------------|-----------------------|
| <b>A named engineer we can call at 3am</b><br><i>This line decided it.</i> | not offered      | +\$95,000/yr     | <b>included</b>       |
| <b>Migration overrun</b><br>Ran 4 months long                              | n/a              | n/a              | +\$35,000 (over plan) |
| <b>Three-year total</b>                                                    | <b>\$735,000</b> | <b>\$765,000</b> | <b>\$810,000</b>      |

SOURCE: Dana Whitfield (CISO) and team — interview transcript.

▼ Read what Dana said (3 quotes)

“Versus the cheapest finalist we paid about 75 thousand more over three years. 40 of that was the 3am phone call... The other 35 was the migration overrun...”

“Sentrix came to roughly 735 total over three years, Corvid 765, NightOwl 810.”

“Corvid — yes, but only on the Enterprise Plus tier, which was 95 thousand a year above what we'd budgeted. NightOwl — yes, included.”

[Hear these in the interactive report ↗](#)

WHAT WE SKIPPED

**Skipping reference calls is what bit them — a few calls would have surfaced the 4-month migration overrun risk.**

|                                                       |                                   |                                                                            |
|-------------------------------------------------------|-----------------------------------|----------------------------------------------------------------------------|
| — <b>Formal RFP</b>                                   | <b>Skipped</b>                    | Cost nothing — we went straight to vendors on procurement’s approved list. |
| — <b>Second trial round across all business units</b> | <b>Cut to 2 weeks in one unit</b> | No specific damage called out; renewal deadline was breathing on us.       |

|   |                 |              |                                                                             |
|---|-----------------|--------------|-----------------------------------------------------------------------------|
| ✓ | Security review | Kept in full | Avoided issues there — nobody was willing to shorten it, and I’m glad.      |
| ★ | Reference calls | Skipped      | Three phone calls would have saved a four-month migration overrun surprise. |

SOURCE: Dana Whitfield (CISO) and team — interview transcript.

▼ Read what Dana said (2 quotes)

- “Our normal process has a formal RFP — we skipped it... The one that actually cost us: reference calls.”
- “It cost about 110, and it took six months — we went live in May instead of January.”

[Hear these in the interactive report ↗](#)

STAKEHOLDER MAP

The CFO set the constraint, the SOC decided more than the scorecard did, and nobody blocked — the decisive vote came from analysts who simply stopped opening a product.

|   |                                                                                                   |           |         |
|---|---------------------------------------------------------------------------------------------------|-----------|---------|
| D | <b>Dana Whitfield, CISO</b><br>Owned the evaluation — “we bought the 3am phone call.”             | Decision  | Champ   |
| C | <b>The CFO</b><br>Set the constraint — defending a 28% increase was untenable.                    | Sponsor   | Skeptic |
| S | <b>SOC analysts &amp; leads</b><br>Ran both trial rounds; walked away from Sentrrix two weeks in. | Influence |         |
| P | <b>Procurement</b><br>The approved-vendor list stood in for the skipped RFP.                      | Influence |         |
| ? | <b>Blocker</b><br>None surfaced — the security review was kept in full, unopposed.                | Gap       |         |

SOURCE: Dana Whitfield (CISO) and team — interview transcript.

▼ Read what Dana said (3 quotes)

- “Sentrrix, the analyst darling, our SOC guys just stopped opening it two weeks into the trial.”
- “We went straight to vendors on procurement's approved list.”
- “The honest truth is we bought the 3am phone call.”

[Hear these in the interactive report ↗](#)

## THE CFO VIEW — WHAT THE PREMIUM BUYS BACK

**The 3am line cost ~\$25k a year. The only other vendor offering it priced the same line at \$95k a year — against the real alternative, NightOwl's premium pays back in under a year.**

| THE PATH                                                                                 | 3-YEAR COST      | THE 3AM LINE             |
|------------------------------------------------------------------------------------------|------------------|--------------------------|
| <b>Sentrix — the cheapest finalist</b><br>The baseline every premium is measured against | \$735,000        | not offered at any price |
| <b>Corvid + Enterprise Plus</b><br>The only other way to buy a named 3am engineer        | \$1,050,000      | +\$95,000/yr             |
| <b>NightOwl — chosen</b><br>Including the \$35k migration overrun                        | \$810,000        | <b>included</b>          |
| <b>Premium over cheapest — vs. saving against the real alternative</b>                   | <b>+\$75,000</b> | <b>-\$240,000</b>        |

SOURCE: Dana Whitfield (CISO) and team — interview transcript.

### ▼ Read what Dana said (3 quotes)

"Versus the cheapest finalist we paid about 75 thousand more over three years. 40 of that was the 3am phone call... The other 35 was the migration overrun..."

"Corvid — yes, but only on the Enterprise Plus tier, which was 95 thousand a year above what we'd budgeted. NightOwl — yes, included."

"Sentrix came to roughly 735 total over three years, Corvid 765, NightOwl 810."

[Hear these in the interactive report ↗](#)

## How they decided

Ran a nine-month evaluation including trials and created a scorecard.

CONSULTED SOC leads · Security team

SKIPPED Skipped reference calls and a full RFP process.

## What they'd do differently

Score migration effort as a criterion and conduct reference calls before deciding.

## Unknowns — what one case can't tell you

This case does not indicate whether NightOwl will continue to meet needs long-term.

**“Ensure all critical factors are properly weighted to avoid them becoming de facto decision points later.”**

— Dana Whitfield, CISO (illustrative subject)

**METHODOLOGY** In the interactive version, underlined claims open the interview moment behind them — a video receipt, timestamped to the words above. [Try it in the interactive report ↗](#)

**SAMPLE DISCLOSURE** Generated by UpSight to demonstrate what a Decision File looks like end-to-end — brief, six diagrams, evidence, narrative — from a seed interview transcript. Not one of the real files in the published series; real files use real subjects and subject-approved quotes.

[Download PDF](#) 