



3 Ways to Prove AI ROI

How MSSPs Get Budget Approved for AI SOC Automation

From Alert Noise to Profitable Scale

This guide shows how to prove AI ROI to leadership —
with numbers they cannot ignore.

Inside, you'll find:

1 The three ROI drivers that leadership teams care about when evaluating AI investments, with examples from European and US-based SOCs:

- ◆ Immediate cost and time savings on false escalations
- ◆ Analyst capacity unlocked
- ◆ Additional alert capacity with the same team

2 How to address common objections you'll hear from the leadership that has seen too many tech projects fail

Among the MSSPs adopting AI SOC Automation:

 Orange
Cyberdefense

Atos

ECI

 **i-TRACING**
CYBERSECURITY

nomios

Almond

 **PERFORMANTA**

#1

Savings on False Escalations

False escalations account for up to 90% of investigations across MSSPs. Let's calculate how much analyst time and cost you save when false escalations no longer require human investigation.

This metric answers:

“How much analyst time and cost can we save on alerts that no longer require human investigation?”

What You Need to Calculate

- ◆ Total yearly alert volume
- ◆ Average investigation time
- ◆ Average false escalation rate
- ◆ Hourly investigation cost

How to Calculate It

#1

Calculate the average hourly investigation cost

Yearly employer cost per SOC analyst
÷ number of working hours per year

#2

Calculate the hours spent on false investigations

(Total yearly alert volume × False escalation rate × Average investigation time)
÷ 60

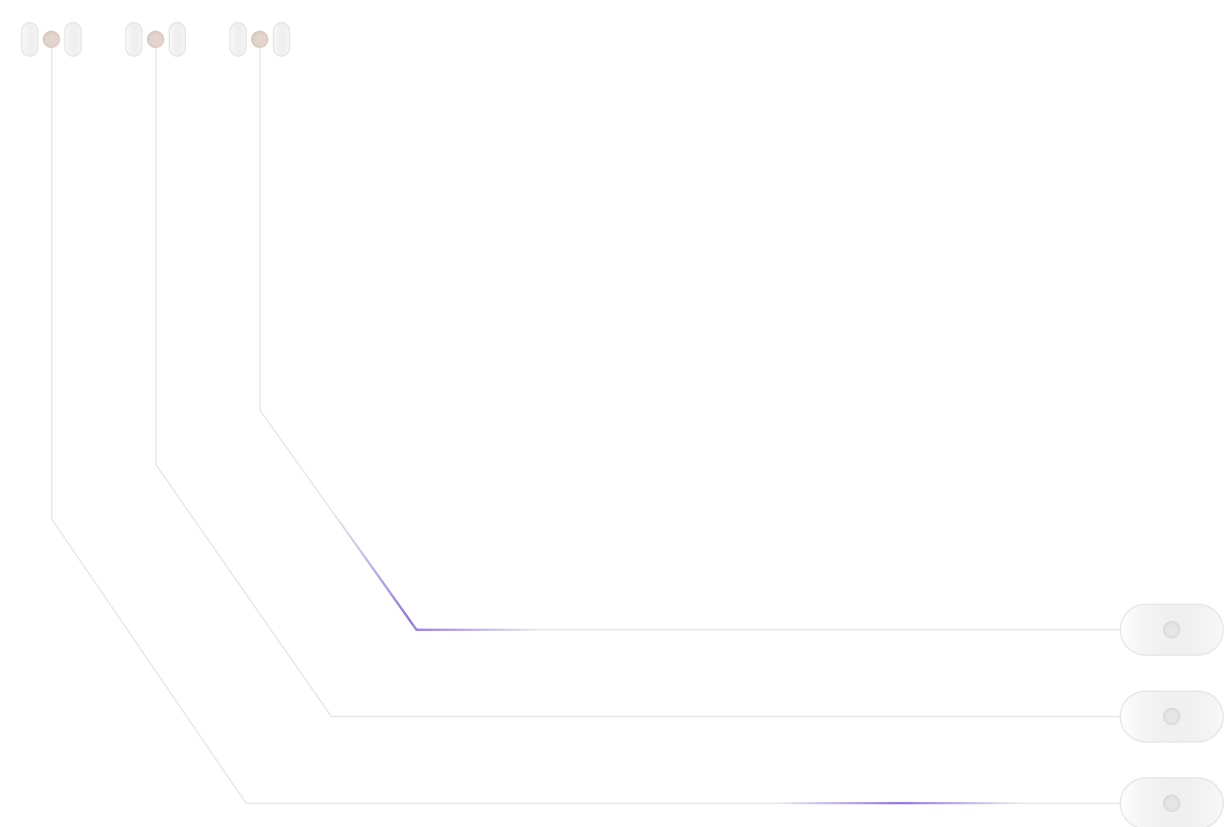
#3

Calculate the total cost of false investigations

Hours spent on false investigations × Average hourly investigation cost

Voilà, you can now see how much time and cost you can save after implementing an AI SOC platform:

- ◆ Confirmed false positives can be auto-closed
- ◆ SOC analysts have up to 6x fewer tickets to investigate



30,000

Yearly alert volume

25%

Expected yearly
alert growth

70%

Average false
escalation rate

40 min

Average
investigation time
per ticket



Scenario: Europe-based SOC

Let's take a SOC based in Germany:

Calculation:

#1

The average hourly investigation cost

€72,000 average employer cost

÷ 1,560 working hours

= €46,15

#2

Hours spent on false investigations

(30,000 × 70% × 40 min)

÷ 60

= 14,000 hours per year

#3

Total cost of false investigations

14,000

× €46,15

= €646,154 per year

Qevlar AI helps SOC teams focus on real threats instead of investigating false positives

See it in action →

Metrics	Now	With Qevlar AI	Results
Alerts needing humans, yearly	30,000	9,000 the rest are auto-closed as false escalations	21,000 fewer alerts requiring manual investigation
Time spent on false escalation, min	40	0	14,000 hours saved on false escalations per year
Minimum time saved with Qevlar AI 14,000 hrs/year			
Cost savings with Qevlar AI €646,154			
Fewer manual alerts 21,000			

A SOC with 30,000 yearly alerts and an average investigation cost of €46.15 per ticket can save €646,154 annually.

#2

Expanding SOC Capacity to Support Growth

As your customer base grows and you expand the services you offer, your SOC capacity must scale as well. Let's calculate how many FTEs you would need to support this business growth and how much additional capacity could be freed for new services.

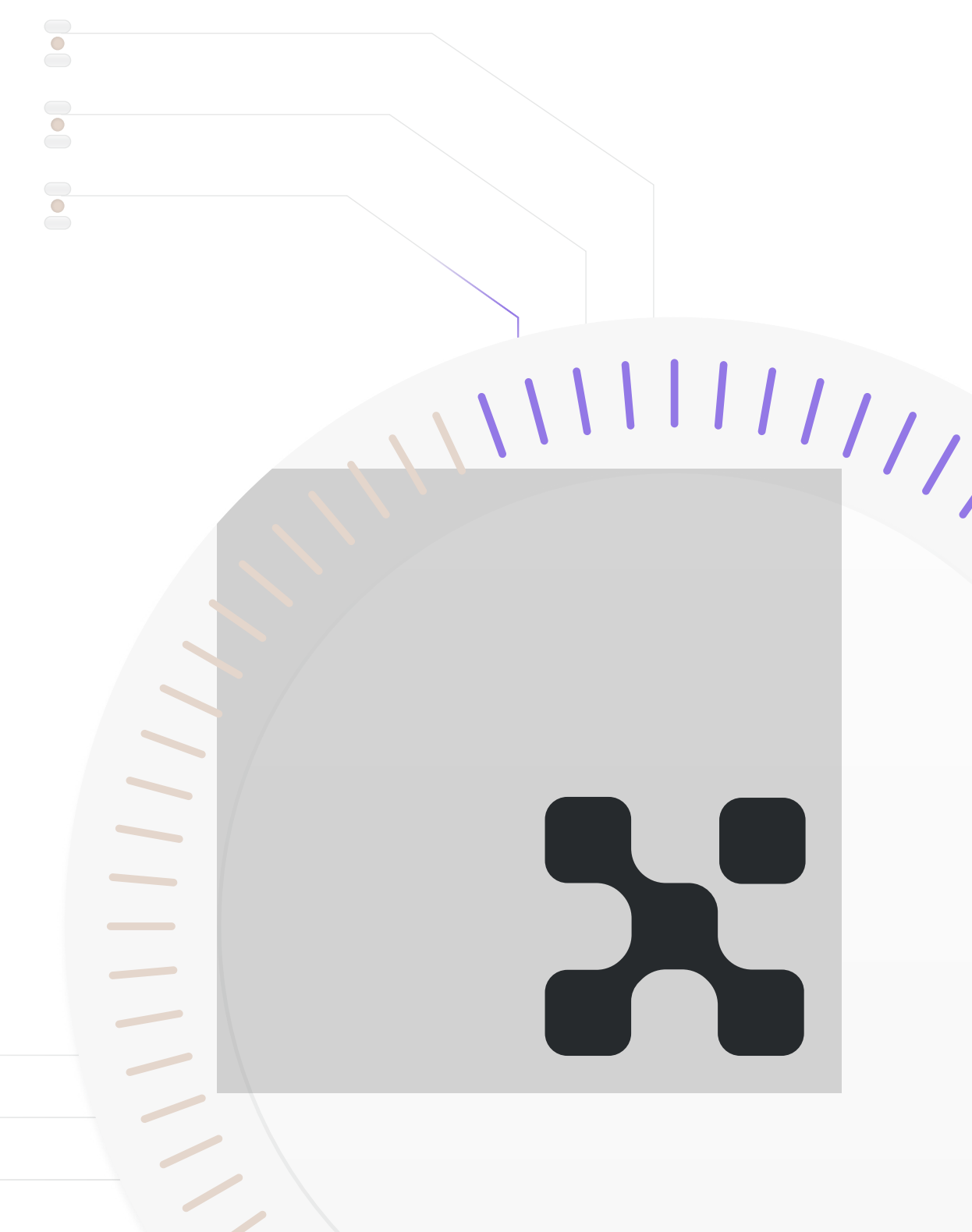


This metric answers:

“How many SOC analysts do we actually need to support business growth, and how much additional capacity can AI automation free up?”

What You Need to Calculate

- ◆ Current yearly alert volume
- ◆ Expected yearly alert growth (to reflect business growth)
- ◆ Number of SOC analysts investigating alerts on a daily basis
- ◆ Average false escalation rate



How to Calculate It



#1

Current alert capacity per FTE

Current yearly alert volume
÷ Number of SOC analysts investigating alerts

#2

Forecasted alert volumes for the next 1-3 years

Current yearly alert volume
× Anticipated yearly alert growth

#3

FTEs needed

Forecasted alert volumes per year
÷ Current alert capacity per FTE

#4

Volume of false escalations per year

Forecasted alert volume per year
× Average false escalation rate

#5

Residual manual investigations

Forecasted alert volume
– Volume of false escalations per year

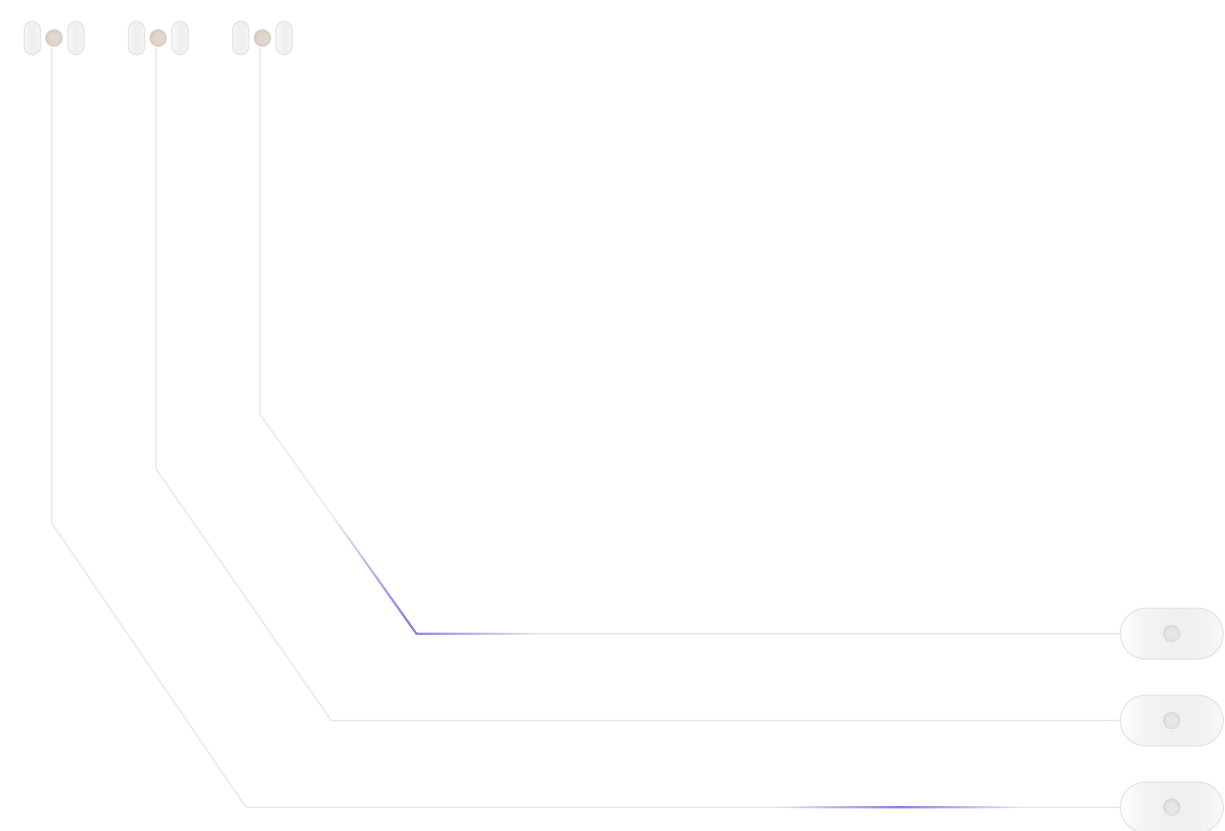
#6

Equivalent FTE capacity freed

Number of SOC analysts investigating alerts
– (Residual manual investigations ÷ Current alert capacity per FTE)

Voilà, you can clearly see how many FTEs would be required to support alert growth without changing your operating model, and how much analyst capacity can be freed by using AI SOC platforms to automate investigations.

This freed capacity can translate into additional capacity for onboarding new customers and delivering premium services.



45,000

Current yearly
alert volume

25%

Expected yearly
alert growth

12

Number of SOC
analysts investigating
alerts on a daily basis

80%

Average false
escalation rate



Scenario: US-based SOC

Let's take an example of a SOC
based in the USA with:

Calculation:

#1 Current alert capacity per FTE
45,000
÷ 12 =
3,750 alerts/analyst

#2 Forecasted alert volumes for the next 1-3 years
2026: 45,000 * 1,25 = 56,250
2027: 56,250 * 1,25 = 70,313
2028: 70,313 * 1,25 = 87,891

#3 FTEs needed
2026: 56,250 ÷ 3,750 = 15 analysts
2027: 70,313 ÷ 3,750 = 19 analysts
2028: 87,891 ÷ 3,750 = 24 analysts

#4 Volume of false escalations per year
2026: 56,250 * 0,8 = 45,000 alerts
2027: 70,313 * 0,8 = 56,250 alerts
2028: 87,891 * 0,8 = 70,313 alerts

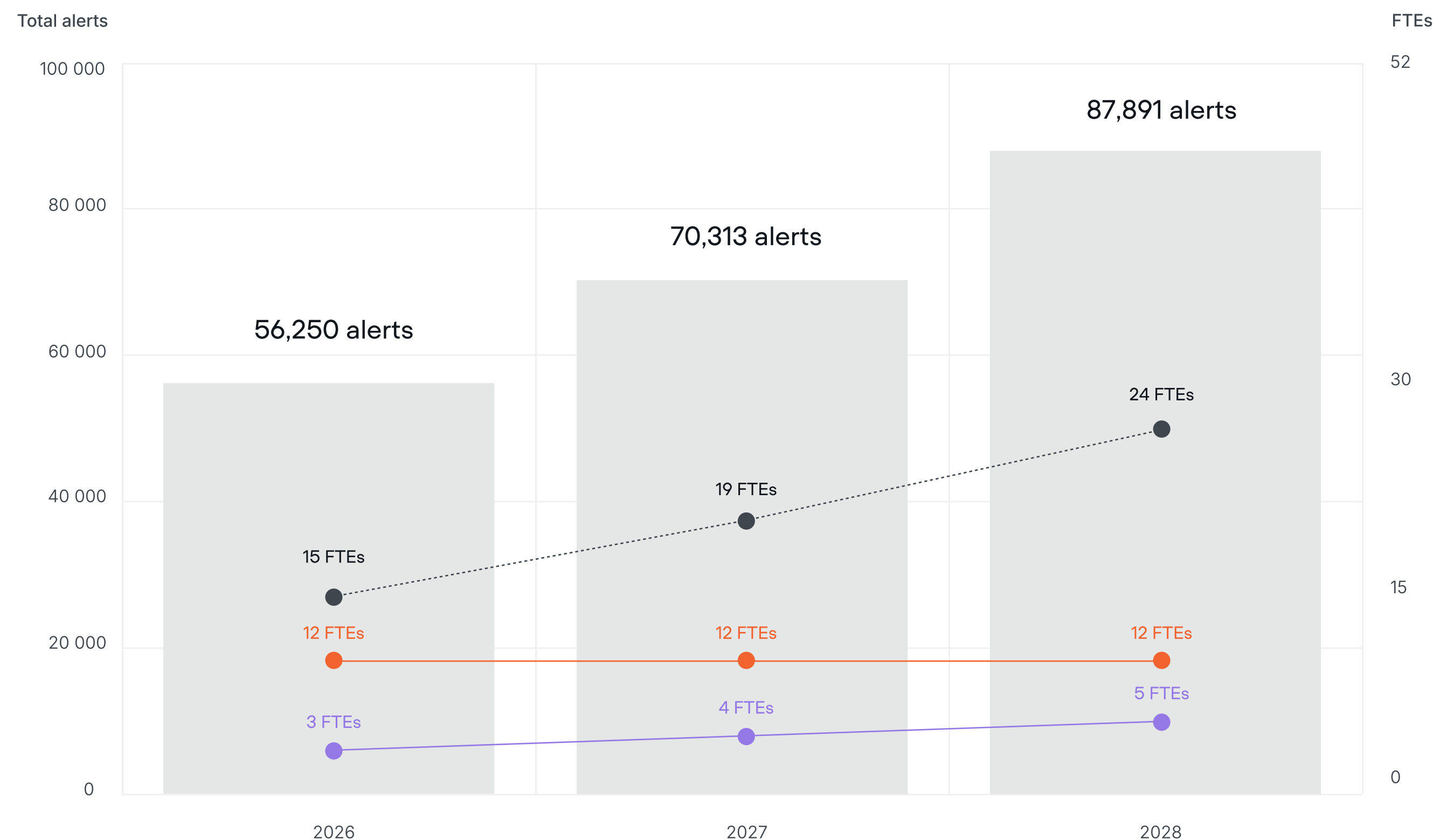
These are the number of tickets that can be automatically investigated by an AI SOC Platform and closed, meaning almost no human involvement is required.

#5 Residual manual investigations
2026: 56,250 - 45,000 = 11,250 alerts
2027: 70,313 - 56,250 = 14,063 alerts
2028: 87,891 - 70,313 = 17,578 alerts

These are the number of tickets that still require human oversight, such as mitigation, additional data validation, or response actions.

AI SOC platforms like Qevlar AI support this stage as well: alerts arrive pre-enriched and fully investigated with relevant logs, telemetry, and threat intelligence, so analysts can act without starting from scratch.

#6 Equivalent FTE capacity freed
2026: 12 - 11,250 ÷ 3,750 = 9
2027: 12 - 14,063 ÷ 3,750 = 8
2028: 12 - 17,578 ÷ 3,750 = 7



- Current FTEs
- Required FTEs (without Qevlar AI)
- Required FTEs (with Qevlar AI)

☐

☐

☐

Cost savings from avoided additional hiring

Year	Extra FTEs Required	Extra Salary Budget Required
2026	3	\$378k
2027	7	\$882k
2028	12	\$1,512k

See your AI SOC ROI in minutes

Plug in your alert volumes, analyst costs, and growth projections to see the real financial impact on your SOC.

Run the ROI calculation →

With 25% yearly alert growth, a SOC would need to double its team within three years. With Qevlar AI, the same SOC team can free up 65% of its current capacity and offer more services to more clients.

#3

Extra Alert Capacity With the Same Team

From the previous step, you've seen how much analyst capacity AI SOC automation can free up. The next question is simple: what can you actually do with that extra capacity? In practice, it means more investigations, more clients, and more revenue — with the same team.

This metric answers:

“With the same team size, how many additional alerts (and clients) could we absorb before hiring?”

What You Need to Calculate

- ◆ Current yearly alert volume
- ◆ Expected yearly alert growth (to reflect business growth)
- ◆ Average false escalation rate
- ◆ Number of SOC analysts investigating alerts on a daily basis

How to Calculate It

#1

Reuse steps 1–6 from the previous section

"Expanding SOC Capacity to Support Growth."

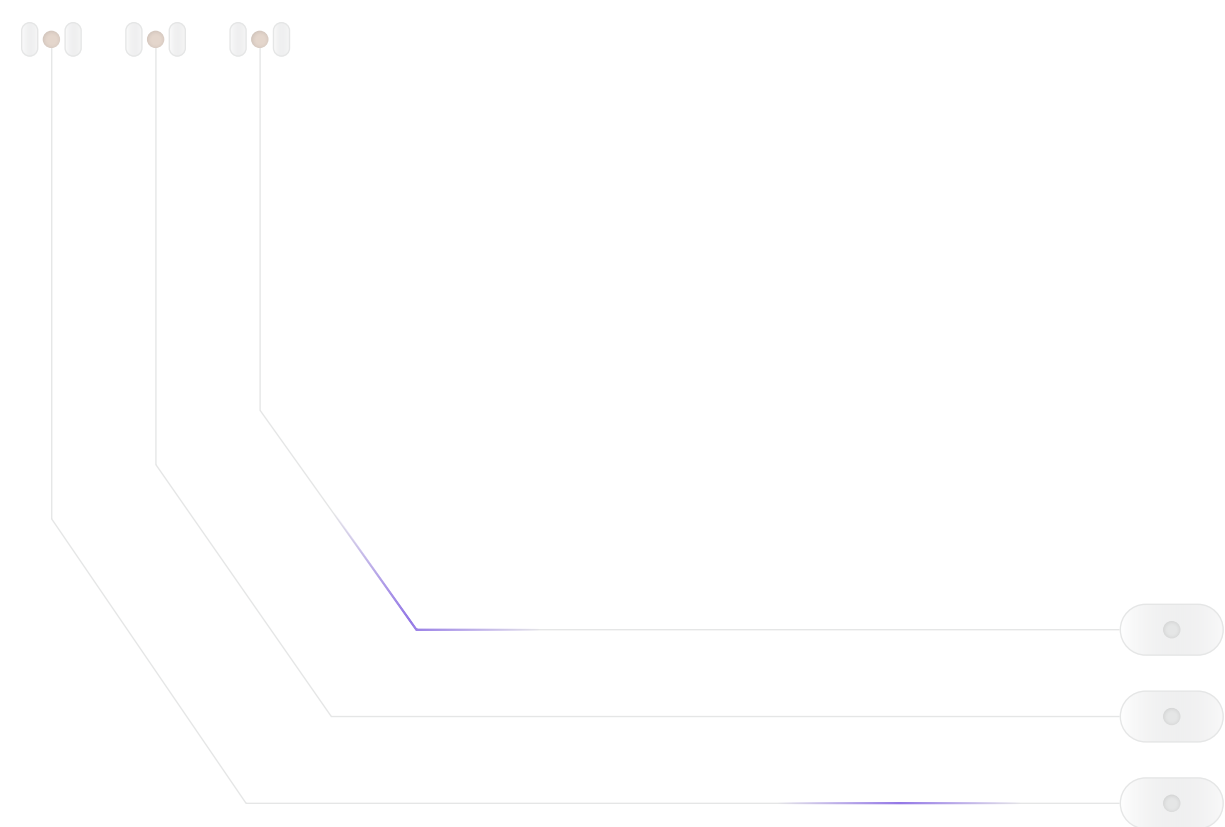
#2

Calculate the extra alert capacity

Current yearly alert volume – Residual manual investigations per year

The idea is simple: your current team can already handle today's alert volume.

When an AI SOC platform removes most of the false-positive workload, the remaining alert volumes show how much real investigation capacity is left — and how many additional alerts your team could handle.



45,000

Current yearly
alert volume

25%

Expected yearly
alert growth

12

Number of SOC
analysts investigating
alerts on a daily basis

80%

Average false
escalation rate



Scenario: US-based SOC

Let's continue the calculation using the
SOC from the previous section:

Calculation:



#1 From the previous calculations, we know the residual manual investigations:

2026: 11,250 alerts
2027: 14,063 alerts
2028: 17,578 alerts

#2 We can now calculate the extra alert capacity per year

2026: 45,000 – 11,250 = 33,750 alerts
2027: 45,000 - 14,063 = 30,937 alerts
2028: 45,000 - 17,578 = 27,422 alerts

With an AI SOC platform, the same team can not only handle 25% higher alert volumes but also create additional capacity to support more clients and deliver more services.



Year	Total alerts	Alerts handled by Quevlar AI	Residual manual investigations	Extra alert capacity
2026	56,250	45,000	11,250	33,750
2027	70,313	56,250	14,063	30,937
2028	87,891	70,313	17,578	27,422

The same team could handle up to 90,000 (56,250+33,750) alerts this year before needing to hire.

Calculate your AI SOC ROI in minutes

Enter your alert volumes, costs, and growth forecast to uncover cost savings and capacity gains.

Run the calculation →

Addressing the Objections You'll Hear



Objection 1

"Our analysts won't trust AI"

Your Response:

This concern is valid. Analysts won't use tools they don't trust, and they shouldn't. The question is whether the system earns that trust through consistent, transparent performance.

Platforms like Qevlar AI work differently. Thanks to the graph orchestrator, they investigate alerts the same way an analyst would by following the evidence, correlating across data sources, and documenting every step.

What this looks like in practice:

- ◆ Analysts see the full investigation trail for every decision the AI makes
- ◆ They can review auto-closed alerts anytime to verify the reasoning
- ◆ The AI doesn't "guess". It follows structured investigation paths with clear evidence at each step
- ◆ Quality remains consistent regardless of alert volume or time of day

Instead of spending 80% of their time on false positives and routine alerts, your analysts focus exclusively on complex threats that require human expertise.

Objection 2

"It'll take too long to deploy"

Your Response:

The deployment timeline is fundamentally different with modern AI platforms. Qevlar AI's fastest implementation took 10 minutes.

Here's why:

- ◆ Qevlar AI connects to your existing security stack via APIs
- ◆ It works with whatever tools you're already using: SIEM, EDR, XDR, SOAR, NDR, Email Security platforms.

Addressing the Objections You'll Hear



Objection 3

"We'll lose quality and miss real threats"

Your Response:

When your analysts are drowning in 50-100 alerts per day, they're making quick judgments about what looks important and what can wait. And sometimes, real threats get buried under the noise of false positives.

What changes with AI:

- ◆ 100% of alerts get enriched and investigated consistently — no matter the alert volume, type, time of day, or day of the week. No missed investigation steps
- ◆ Every verdict is backed up by evidence and facts.

What MSSPs report after deployment:



"We can now detect threats more quickly and accurately, while focusing our analysts' expertise on the most complex and critical incidents."

Objection 4

"The ROI calculations are always inflated"

Your Response:

We can calculate the ROI ourselves, with our own numbers.

Use:

- ◆ Your actual alert volumes
- ◆ Your real costs
- ◆ Your growth forecasts

See exactly how much more your current SOC can do.

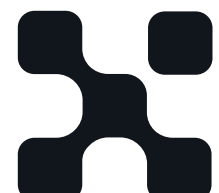
[Calculate your AI ROI →](#)



Surface real
signals from
the noise

Book a demo →

 Follow us on [LinkedIn](#)

 **Qevlar AI**

Trusted by:

 **Cyberdefense**

Atos

sodexo^{*}

FORTUNE
GLOBAL
500

ECI⁺

MediaMarkt

 **I-TRACING**
CYBERSECURITY

stoik

 **GlobalConnect**

nomios

Almond

 **PERFORMANTA**