SECURITY BLUE TEAM

SOC LEADERS

TRAINING PLAYBOOK

OVERVIEW

Training Effectiveness

This guide is here to help you make training in your SOC more effective. It shows you how to cut wasted spend, strengthen your team, and get measurable results when budgets are tight and threats are evolving.

You are balancing headcount, shift cover, and incident load every week. Training is one of the levers you can pull that directly reduces risk, closes skills gaps, and protects your budget.

Scale of the Challenge

- Organisations reporting high levels of security skills shortage faced average total breach costs of **$5.22M,** compared with **$3.65M** for those with low or no shortage. IBM Cost of a Data Breach Report 2025, Figure 42
- Human error accounts for **26% breaches,** so risk sits inside the SOC as well as outside. IBM Cost of a Data Breach Report 2025, Figure 11
- The global workforce gap stands at **4.8M** unfilled roles, **up 19%** year on year. ISC2 Cybersecurity Workforce Study 2024

Training Priorities

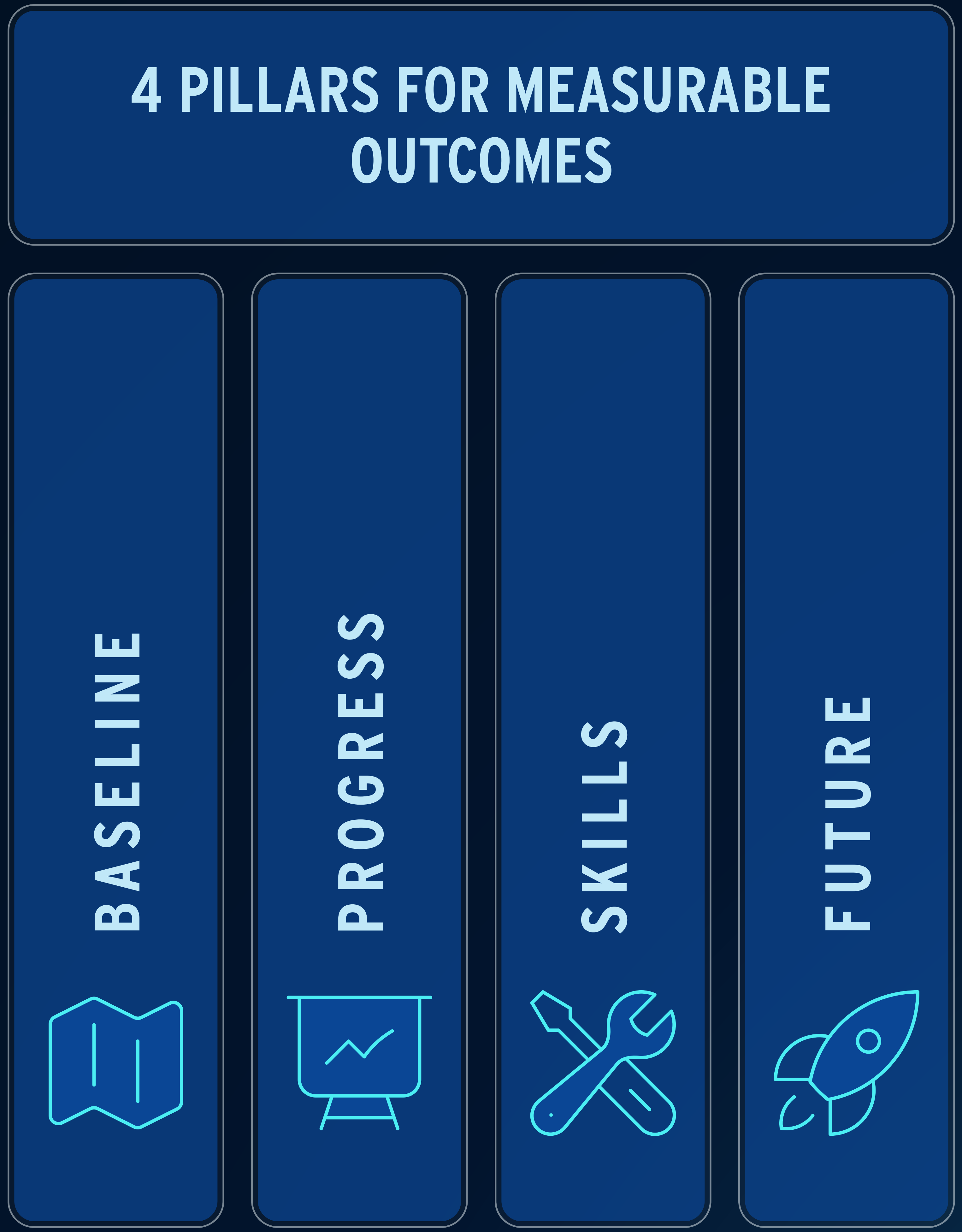
The IBM report also identifies employee training as a top cost mitigating factor, lowering breach costs by an average of $192,000 per incident. IBM Cost of a Data Breach Report 2025, Figure 39

Training can often be fragmented with one off sessions and tick box training, that doesn't help analysts when they are working a live incident.

This guide has been designed to show you how other SOC leaders are cutting wasted spend on training and getting measurable outcomes by focusing on four pillars.

1. **Establishing a baseline** so every analyst meets a minimum defensive standard
2. **Building progression** to retain talent and close the mid-level gap
3. **Keeping skills sharp** to retain talent and close the mid-level gap
4. **Preparing for the future** by developing the skills to defend against emerging threats, including AI driven attacks and ransomware

By structuring training around these four pillar, you can build a team that is **resilient, confident,** and **ready for what comes next.**



4 PILLARS FOR MEASURABLE OUTCOMES

BASELINE

PROGRESS

SKILLS

FUTURE

1 ESTABLISH A BASELINE

SET A MINIMUM DEFENSIVE STANDARD FOR EVERY ANALYST BEFORE THEY WORK LIVE TICKETS

Why it Matters

The human element is involved in roughly 60% of breaches. A clear baseline reduces avoidable mistakes and speeds. 2025 Data Breach Investigations Report – Verizon

What Good Looks Like

- Short, practical baselines to reflect tools and data, not a generic syllabus
- One pass or fail assessment with artefacts from your environment
- A visible register that shows who is cleared for which tasks
- A refresh after ninety days to catch analyst drift
- Runbooks and ticket examples linked to baseline skills

Do This

- Define 3-5 baseline outcomes you expect from analysts. Keep them practical
- Build one hands-on check using your own logs, alerts, and an incident scenario
- Set pass criteria and a named approver. No production access until sign-off
- Add a ninety-day refresher with a short drill taken from a real ticket
- Publish the register of baseline-cleared analysts for shift leads to use

Measure It

- Time to first independent ticket closed for new analysts
- Rework and escalation accuracy in the first ninety days
- Mean time to identify when a baseline-cleared analyst is first responder
- Percentage of analysts with current baseline sign off
- Number of high severity incidents with avoidable human error in the root cause

1 ESTABLISH A BASELINE

SET A MINIMUM DEFENSIVE STANDARD FOR EVERY ANALYST BEFORE THEY WORK LIVE TICKETS

Checklist:

- □ Five most common incidents captured with expected steps and evidence
- □ One page baseline rubric with pass criteria
- □ Named approver and a dated sign off log
- □ A ninety-day refresher drill pulled from a real case
- □ Links from the rubric to the exact runbooks in your wiki

Example

Many leaders use the BTL1 certification as the benchmark, so every analyst meets a consistent defensive standard before joining the rota. Pair it with a short, in-house check that uses your tooling and runbooks, so it maps to daily work.

2 BUILD PROGRESSION

GIVE ANALYSTS A CLEAR PATH FROM BASELINE TO MID-LEVEL TO RETAIN AND RAISE CAPABILITY

Why it Matters

Only 72% of cybersecurity roles are currently filled worldwide. Growing talent from within reduces hiring pressure and closes gaps faster. BCG 2024 Cybersecurity Workforce Report

What Good Looks Like

- published skills framework with clear outcomes for levels 1-3
- Competency based progression with evidence, not time served
- Mentoring on live work plus targeted practice to build depth
- Protected time for progression labs that do not clash with shifts
- Quarterly review points with fair criteria and simple documentation

Do This

- Define level two competencies for your SOC and share them with the team
- Pair newer analysts with seniors on real tickets and rotate ownership weekly
- Create small evidences per analyst using ticket write ups and lab results
- Schedule one progression lab per month linked to those competencies
- Hold a quarterly progression board with clear decisions and next steps

Measure It

- Retention at six and twelve months for new analysts
- Percentage achieving level two within six and twelve months
- Reduction in escalations that need senior intervention
- Internal fill rate for level two roles
- Analyst sentiment on progression clarity from a short pulse survey

2 BUILD PROGRESSION

GIVE ANALYSTS A CLEAR PATH FROM BASELINE TO MID-LEVEL TO RETAIN AND RAISE CAPABILITY

Checklist:

- □ Role profiles with level one, level two, and level three competencies
- □ Named mentors with time set aside for coaching
- □ A simple progression rubric and evidence list
- □ A monthly lab plan mapped to competencies
- □ A calendar invite for the quarterly progression board

Example

You can use the BTL2 certification as a progression milestone, with a mentor sign off, a short evidence pack from real tickets, and a clear date for the next review

3 KEEP SKILLS SHARP

BUILD SHORT REGULAR PRACTICE INTO THE WORKING WEEK TO REDUCE SKILLS FADE

Why it Matters

Employee training is a top cost-mitigating factor and lowers breach costs by about $192,000 per incident. IBM Cost of a Data Breach Report 2025, Figure 39.

What Good Looks Like

- A fixed weekly practice slot that doesn't move
- Micro drills based on recent tickets and common failure points
- Labs for core skills such as phishing analysis, log triage and endpoint checks
- A short write-up of what was learned and what changed in runbooks
- A simple tracker that shows who has completed the last four sessions

Do This

- Set a forty five minute lab practice window each week, protect it in the rota
- Rotate scenarios from real incidents and include one fresh IOC each time
- Use a one-page checklist to score each drill and capture updates to runbooks
- Record completions in a shared tracker for team leads to review
- Share one lesson learned in the next stand-up so changes stick

Measure It

- Phish click and report rates by team across the quarter
- Mean time to identify for tickets handled by recent participants
- Lab completion and pass rates
- Number of runbooks updated after drills
- Analyst confidence pulse score after sessions

3 KEEP SKILLS SHARP

BUILD SHORT REGULAR PRACTICE INTO THE WORKING WEEK TO REDUCE SKILLS FADE

Checklist:

- □ Calendar slots for the next twelve weeks for lab practice
- □ Three ready-to-run scenarios pulled from recent tickets
- □ A one-page drill checklist and pass criteria
- □ A shared tracker for completions and actions
- □ A wiki page for lessons learned and runbook changes

Example

Get teams to use Blue Team Labs Online during quieter periods or during practice windows. They can practice without leaving the floor and then log updates to runbook afterwards.

4 PREPARE FOR THE FUTURE

BUILD DETECTION ENGINEERING AND RANSOMWARE SKILLS TO ADAPT TO EVOLVING THREATS

Why it Matters

IBM reports that attackers' use of AI featured in 16% of breaches, often to scale phishing and deepfakes. Preparing your team for this shift reduces exposure and recovery costs. IBM Cost of a Data Breach Report 2025

What Good Looks Like

- A workflow for proposing, building, testing, deploying, and tuning detections
- Version control and simple CI checks for rules and playbooks
- A small catalogue of high quality, in-house detections with owners and tests
- Monthly hunts that produce at least one new or improved detection
- Feedback loops from incidents straight into new rules and runbooks

Do This

- Publish a one-page detection workflow with roles, gates, and timeboxes
- Store rules in Git and run basic tests on every change before deployment
- Start a monthly hunt hour and require one actionable output each time
- Tag incidents that led to new detections, so learning is traceable
- Review false positives fortnightly and tune or retire noisy rules

Measure It

- Detections authored or materially improved each quarter
- False positive rate and time to tune after deployment
- Mean time to identify for alerts triggered by in-house detections
- Percentage of significant incidents that resulted in a new rule
- Coverage of priority threats mapped to your environment

4 PREPARE FOR THE FUTURE

BUILD DETECTION ENGINEERING AND RANSOMWARE SKILLS TO ADAPT TO EVOLVING THREATS

Checklist:

□ One-page workflow with owners and gates

□ Git repo for detection rules with tests

□ Calendar invite for a monthly hunt hour or lab practice sessions

□ Template for documenting detections and linking to incidents

□ A shortlist of priority threats to target first

Example

Use CJDE for a repeatable detection engineering practice and reinforce with Blue Team Labs Online investigations that mirror real attack paths, as well as Ransomware training to equip analysts to cover cyber extortions.

SECURITY BLUE TEAM

MORE INFORMATION

🌐 www.securityblue.team/corporate-training

✉ corporatesupport@securityblue.team