MSSP TRANSITION:

PRACTICAL LESSONS LEARNED AND KEY TAKEAWAYS

Jan Freudenreich

Laura Flaquer

WHY ARE WE HERE?

Show our process

Share lessons learned

Enable professional exchange

MSSP transitions are never "plug & play" - it deeply involves people, processes, and technology

JAN FREUDENREICH

IT SECURITY LEAD

BASLER KANTONALBANK

LAURA FLAQUER

SOC MANAGER

BASLER KANTONALBANK

WHY THIS TRANSITION?

We had the need to change our provider and increase our maturity in a short time frame

MATURITY

Quick maturity increase

SCALABILITY

Scale with future demands

FLEXIBILITY

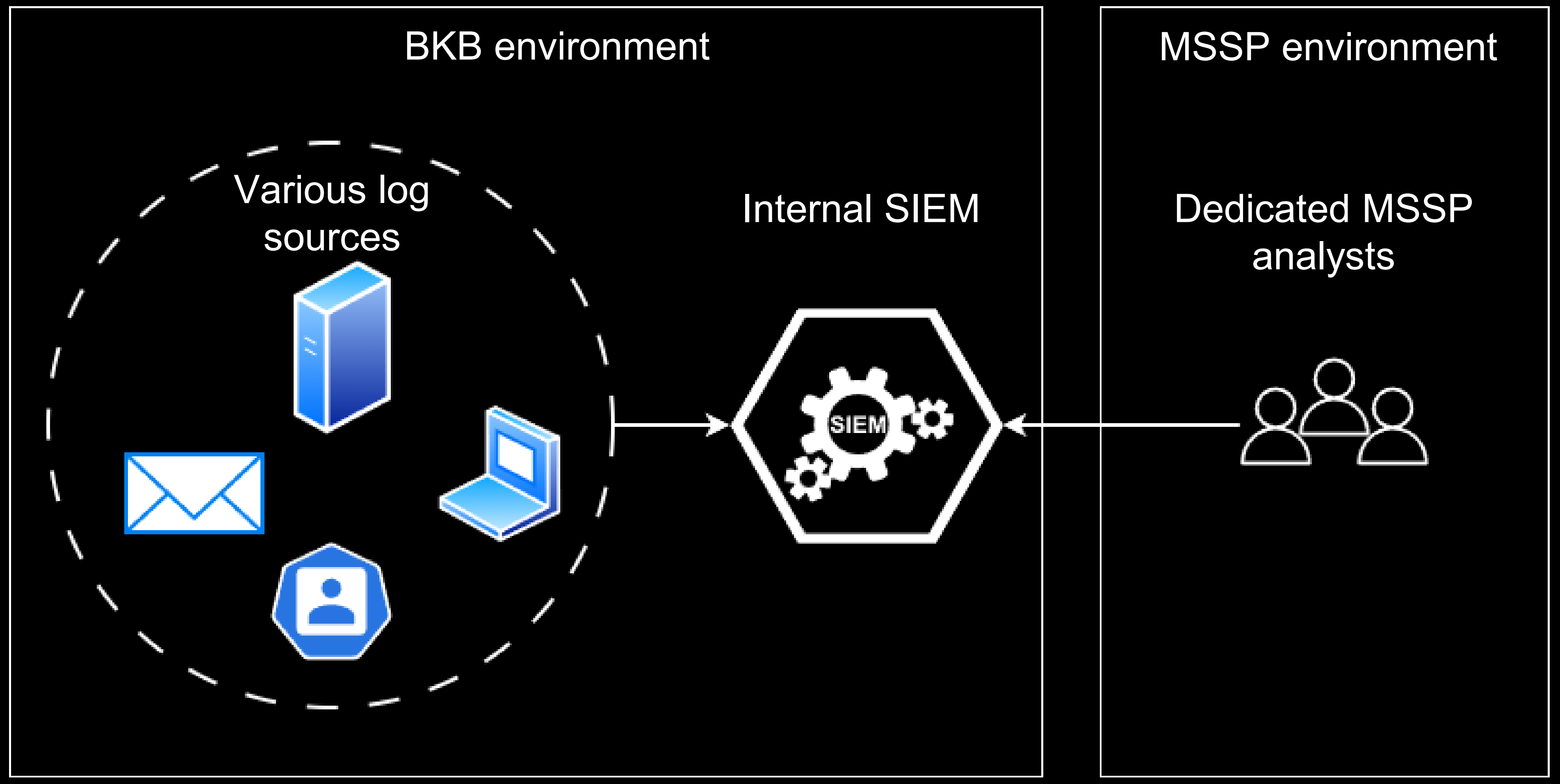
Independence from tools

RESSOURCES

Reduced internal effort

FROM OLD TO NEW SETUP

- Local MSSP
- Maintenance of own SIEM solution
- Limited scalability and process standardisation



BKB environment

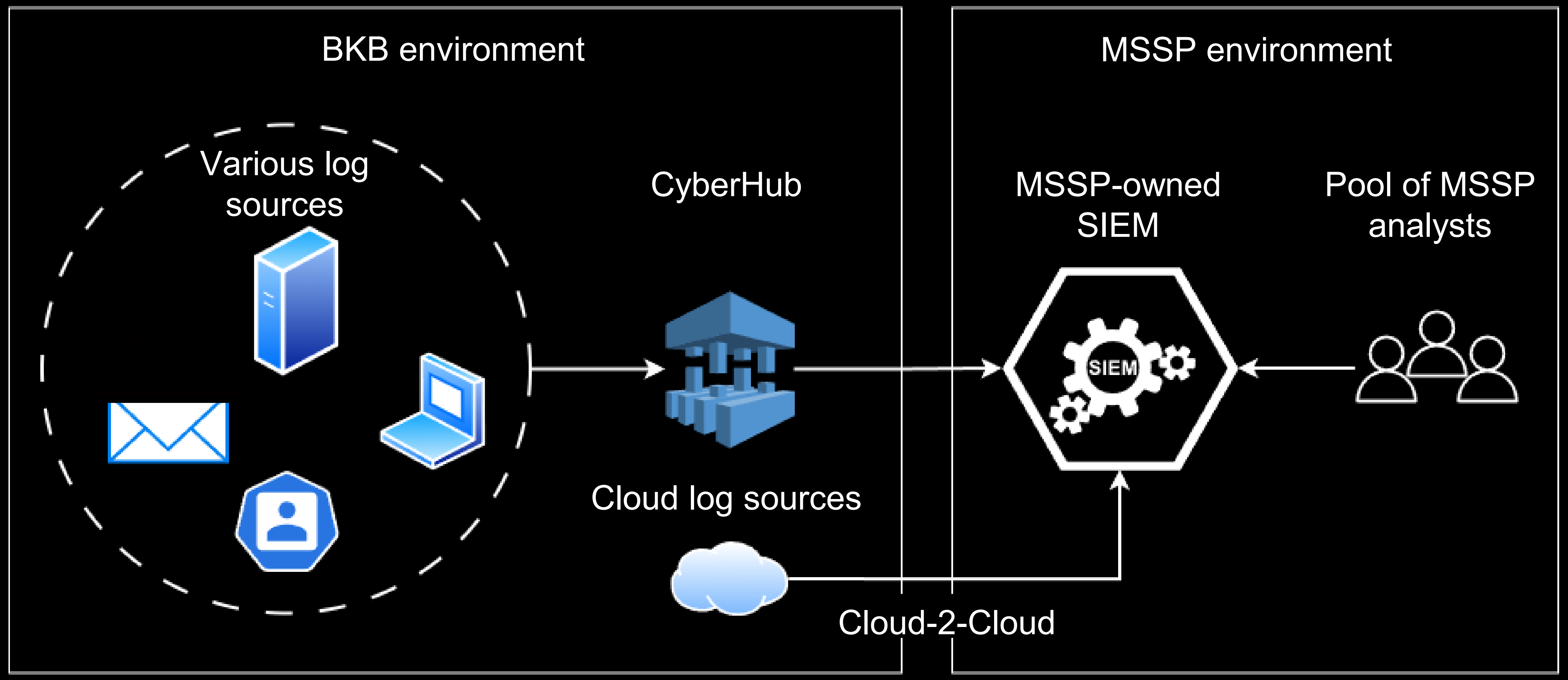
Various log sources

Internal SIEM

MSSP environment

Dedicated MSSP analysts

- International MSSP
- MSSP-owned and managed SIEM
- Ability to leverage use cases and IoCs centrally defined for all clients of the MSSP
- High degree of standardisation



BKB environment

Various log sources

CyberHub

Cloud log sources

Cloud-2-Cloud

MSSP environment

MSSP-owned SIEM

Pool of MSSP analysts

WHAT WAS OUR TIMELINE?

PREPARATION
Extensive planning
TRANSITION
Like for Like
DUAL OPERATIONS
Fallback in case of issues
CONTINOUS IMPROVEMENT
Coverage increase and process optmisation
Maturity
Stress
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct

PEOPLE JOURNEY

Key points to consider during your people journey:

- Stakeholder involvement
- Trust building
- Workshops
- Multiple rounds of communication
- Don't make it personal

WINS

- Getting everything on the table
- Removable of barriers

STRUGGLES

- Cultural shift

PRACTICAL TIPS FOR SUCCESS

- ✓ Plan enough time
- ✓ Listen to input and communicate transparently
- ✓ Don't expect things to change overnight
- ✓ Don't make it personal

PROCESS JOURNEY

Key points to consider during your process journey:

- Governance model establishment
- Service Level Agreements (SLAs) definition
- Escalation processes formalisation
- Authority clarification
- Incident response playbooks development

WINS

- Clear escalation paths
- Defined powers of the MSSP
- Standardised services & playbooks

STRUGGLES

- Access model
- MSSP-analysts playbooks

PRACTICAL TIPS FOR SUCCESS

- ✓ Empower the MSSP (in/out working hours)
- ✓ Define access requirements to empower the MSSP
- ✓ Create lived-by incident response playbooks
- ✓ Establish clear metrics to track success

TECHNOLOGY JOURNEY

Key points to consider during your technology journey:

- Architecture redesign
- SIEM replacement
- Log forwarding configuration
- Technical integrations
- Compliance enforcement
- Alert fine-tuning

WINS

- Centralised log forwarding
- Leverage of global MSSP engineering

STRUGGLES

- Initial engineering efforts
- Technical integrations timeline

PRACTICAL TIPS FOR SUCCESS

- ✓ Define priorities: Budget? Strategy? Flexibility? Transition timeline?
- ✓ Define technical requirements early
- ✓ Account for compliance considerations
- ✓ Test, tune, and communicate throughout the process

KEY TAKEAWAYS

If done correctly, the benefits are worth the effort

COMPLEXITY

MSSP transitions are not a plain vendor swap

JOINT EFFORT

People, process, technology must move together

EXPECT BUMPS

Success = preparation + communication