



Blumira

**Automated Threat
Detection and Response**

01

Current Challenges in SecOps



Blumira

Current SecOp Challenges



Limited Teams

Companies can't afford SecOps & current teams may have limited security expertise.



Alert Fatigue

With over 10k alerts a day, how can analysts parse, analyze and investigate every alert?



Manual Process

Fine-tuning SIEMs to get actionable data and real security value out of them is slow & manual

Complex Security Tools

Log Ingestion

Log Parsing

Threat Intelligence

Detection Rules

Alerting

Validate

Prioritize

Investigate

Respond

Report



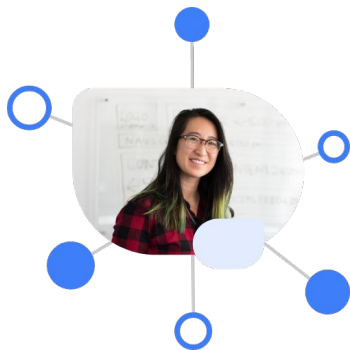
02

How Blumira Works



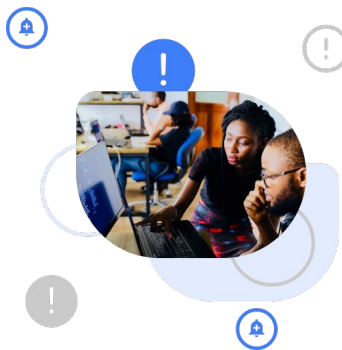
Blumira

Blumira Enables IT/Security Teams



Deploy in Hours

Cloud-delivered, small teams can deploy



Eliminate Noise

Prioritizes real security threats & risks



Take Action

Automated response with security playbooks

→ How Blumira Does It

Automated Security Operations

- Log ingestion & parsing
- Correlated threat intelligence
- Defined detection rules
- Alerting & prioritization
- Honeypot detections

Automated Detection & Response

- Built-in SOAR
- Automate SecOps workflow
- Enable IT w/ response playbooks

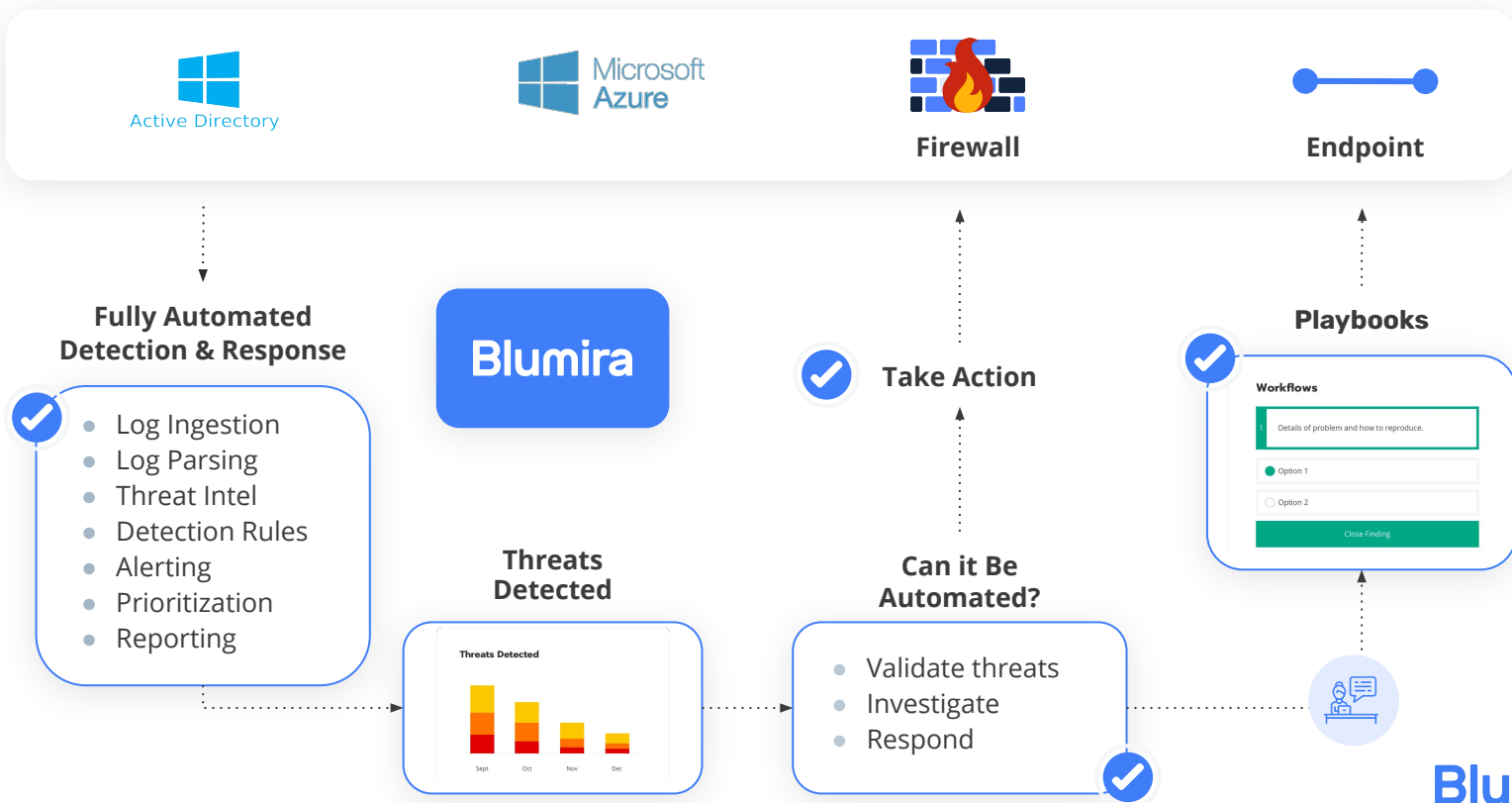
Cloud SIEM

- Deploys in hours
- 100+ pre-built integrations
- Scalable SaaS platform
- Automated reporting

Product / Security Expertise

- Hands-on deployment
- Consult on identified threats
- In-product interaction
- Access to expertise

End-to-End Threat Detection



→ Threats Detected by Blumira

Ransomware

Reconnaissance Scanning

Privilege Escalation

New Admin Accounts

Data Exfiltration

Malicious Executables

Malware Applications

Misconfiguration

RDP / SMB Exposure

Privileged Access

Access Attempts

Password Spraying

Brute-Force Attacks

Geo-Impossible Login

Multiple Failed Logins

Account Lockouts

Hacker Tool: Credential Theft

Exploits

Bluekeep

Cobalt Strike

Note: Blumira detects much more! These are only a few key examples.




03

Setting Up Blumira

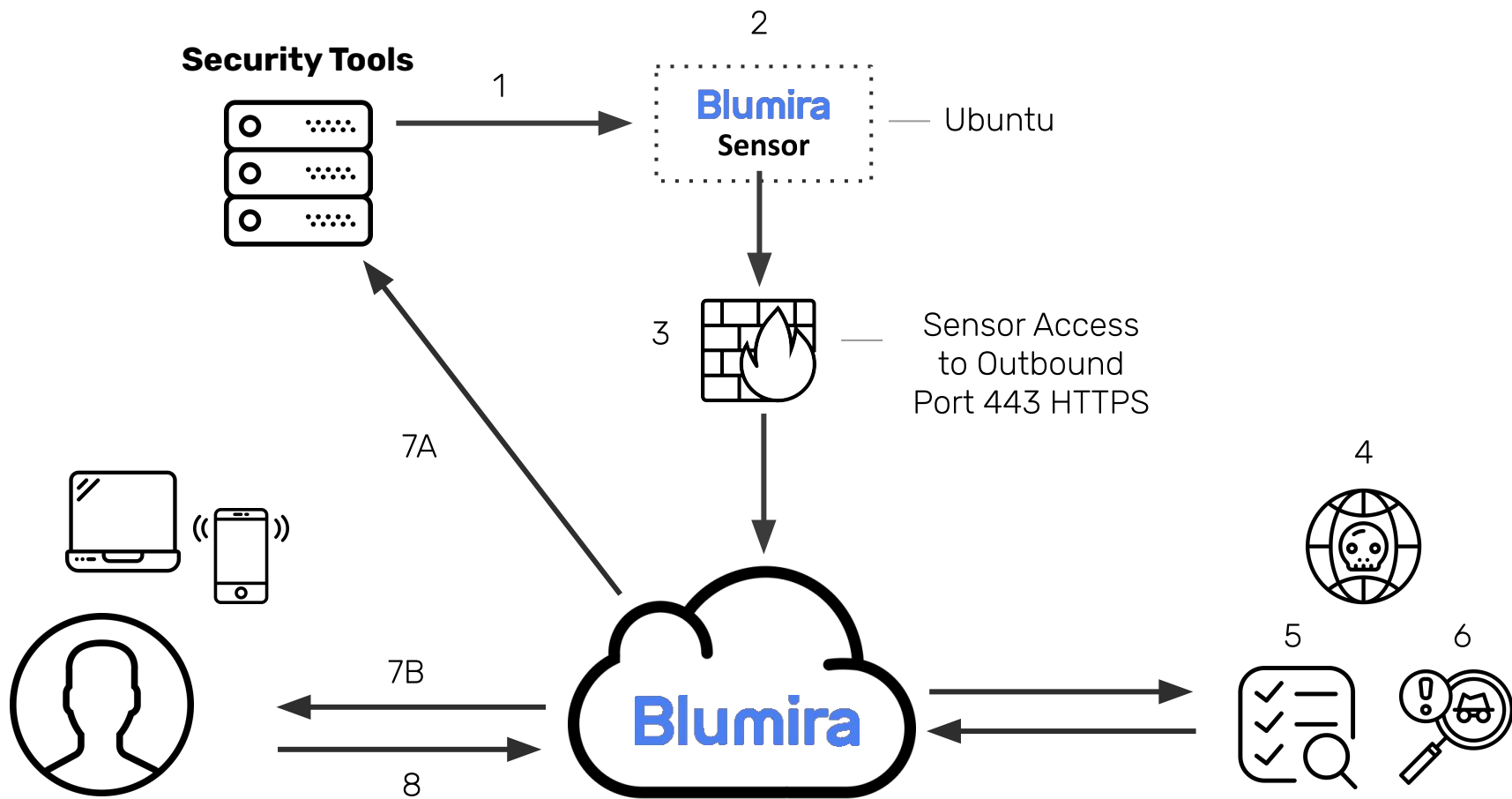


Blumira

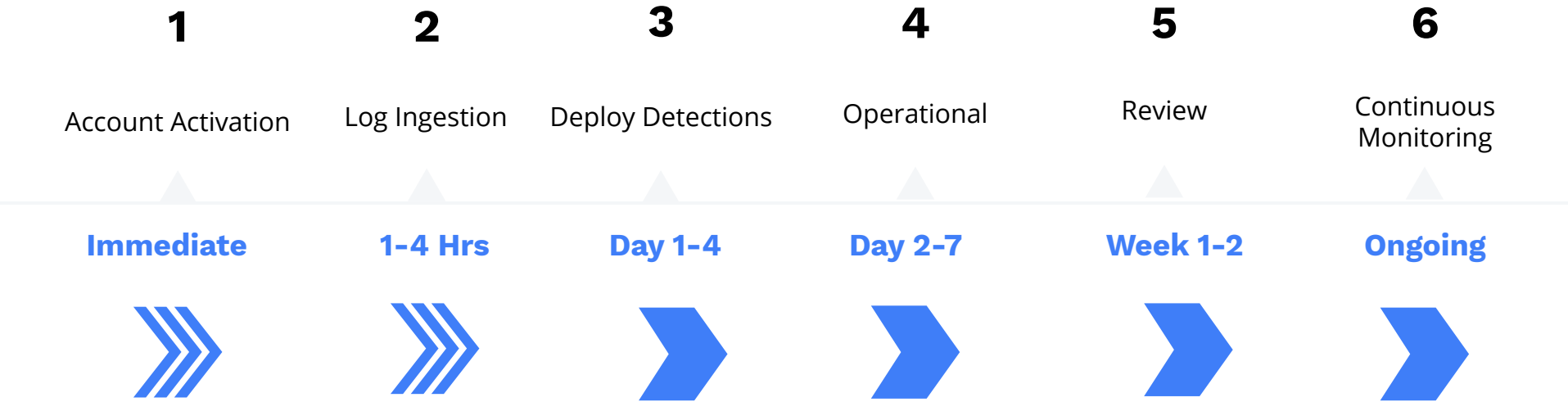
Blumira Integrates With Any Service

Firewall	      
Endpoint	      
Identity	     
Productivity	    
Hosts	   

Blumira



Blumira Deployment Timeline



Blumira G2 Awards



Thank You

The background image shows a woman with curly hair and glasses, wearing a patterned top, sitting at a desk and smiling broadly while looking at a laptop. Another person is partially visible in the background, also smiling. The entire image is overlaid with a solid blue color.

Blumira