Blumira

BLUMIRA MANAGED

MANAGED DETECTION & RESPONSE

Responsibility Matrix

Defines what your Blumira Managed support team executes, advises, or owns at each phase of incident response — and what remains with you and your IR partner.

Blumira executes on only these response surfaces: Microsoft 365 · Microsoft Entra ID (tenant-integrated) · On-premises endpoints with the Blumira Agent deployed. All other surfaces are limited to Blumira Recommends or IR Partner actions.

Actor & Action Definitions

The table below outlines who each of the actors are within the Blumira Managed service, and which actions each actor takes as part of each phase or function within the service.

TYPE	SYMBOL	MEANING
ACTOR	Blumira Security Analyst	A Blumira Security Analyst who supports Blumira Managed customers according to their defined responsibilities and service-level agreement.
	Customer	An enrolled, active Blumira customer who entered into the Blumira Managed service agreement.
	IR Partner	Incident Response firm or partner required — outside of Blumira Managed scope.
ACTION	EXECUTE	Someone directly executes an action (such as when an analyst follows the pre-approved playbook or has explicit customer consent).
	EXECUTE WITH APPROVAL	Analyst executes after obtaining approval, or after making a best attempt to obtain approval. Note: a Blumira Security Analyst attempts to confirm with either of the two required customer contacts before they will act without approval.
	APPROVAL	Someone provides approval to take action.
	OBSERVE	Monitoring only, with no action taken.
	RECOMMEND	A Blumira Security Analyst advises the customer on what to do without taking any action.

TYPE	SYMBOL	MEANING
	— N/A	Not applicable — the actor is not involved with or responsible for the stated activity.

Phase 1 — Detection & Monitoring

ACTIVITY	SECURITY ANALYST	CUSTOMER	IR PARTNER	NOTES
24/7 monitoring of High & Critical cases	EXECUTE	—	—	*Continuous eyes-on-glass via Kindling; SLA starts on case creation*
Monitoring of Low & Medium severity cases	—	EXECUTE	—	*Managed does not respond to Low/Medium*
Log collection, forwarding, and sensor maintenance	RECOMMEND	EXECUTE	—	*Customer must maintain integrations and agent coverage*
Threat detection rule tuning	EXECUTE	RECOMMEND	—	*Blumira owns detection engineering*
Proactive threat hunting	EXECUTE *(best-effort)*	—	—	*Analysts perform during non-queue time; best effort, not SLA-bound*
Third-party EDR alert monitoring	OBSERVE & RECOMMEND	EXECUTE	—	*Blumira can observe but cannot act in non-integrated EDR*

Phase 2 — Triage & Investigation

ACTIVITY	SECURITY ANALYST	CUSTOMER	IR PARTNER	NOTES
Case triage (High/Critical)	EXECUTE & RECOMMEND	EXECUTE *if blockers are identified (previous agreement, misconfiguration, lack of connection)*	—	*60-minute SLA from case creation to documented analyst action*
Initial investigation & timeline reconstruction	EXECUTE	—	—	*Via Kindling case workflow and evidence bundles*
Customer notification of active incident	EXECUTE	—	—	*Primary and secondary contacts required*
Root cause determination	EXECUTE & RECOMMEND	EXECUTE	—	*Blumira leads; customer provides environment context*
Deep forensic / DFIR investigation	RECOMMEND	—	EXECUTE	*Requires contracted IR firm; Blumira provides case handoff package*
Legal hold or chain-of-custody evidence	—	EXECUTE	EXECUTE	*Outside Blumira scope*

Phase 3 — Containment

ACTIVITY	SECURITY ANALYST	CUSTOMER	IR PARTNER	NOTES
M365 / Entra ID — Disable compromised user account	EXECUTE	—	—	*Pre-approved playbook*
M365 / Entra ID — Revoke active sessions / tokens	EXECUTE	—	—	*Pre-approved playbook*
M365 / Entra ID — Block sign-in	EXECUTE	—	—	*Pre-approved playbook*
M365 / Entra ID — Reset MFA / conditional access changes	RECOMMEND	EXECUTE	—	*Analyst recommends*
M365 / Entra ID — Quarantine mailbox / block mail rules	RECOMMEND	EXECUTE	—	*Analyst recommends*
On-prem host isolation (Blumira Agent)	EXECUTE WITH APPROVAL	APPROVAL	—	*Analyst confirms host is not critical infra (DC, etc.) before acting*
On-prem process termination (Blumira Agent)	EXECUTE WITH APPROVAL	APPROVAL	—	*Confirmation required; documented in case record*
Network segmentation / VLAN changes	RECOMMEND	EXECUTE	—	*Customer executes; Blumira advises on scope*
Firewall rule changes (block C2 / IOC)	RECOMMEND	EXECUTE	—	*Blumira provides IOCs; customer implements*
DNS sinkholing	RECOMMEND	EXECUTE	—	—
EDR-based host isolation (non-Blumira EDR)	RECOMMEND	EXECUTE	—	*Blumira cannot act in third-party EDR surfaces*
OT / ICS / SCADA isolation	RECOMMEND	EXECUTE	—	*High-risk; Blumira will not act without specialized IR guidance*

ACTIVITY	SECURITY ANALYST	CUSTOMER	IR PARTNER	NOTES
Cloud infrastructure isolation (AWS/GCP/Azure non-M365)	RECOMMEND	EXECUTE	—	*Outside current response surface*
Unauthorized app / OAuth grant removal (M365)	RECOMMEND	EXECUTE	—	*Analyst recommends*

Phase 4 — Eradication

ACTIVITY	SECURITY ANALYST	CUSTOMER	IR PARTNER	NOTES
Compromised credential reset guidance	RECOMMEND	EXECUTE	—	*Blumira recommends; customer executes resets beyond Entra block*
Malware / implant removal	RECOMMEND	EXECUTE	EXECUTE	*Blumira will not delete files or manipulate disk content*
Persistence mechanism removal (registry, scheduled tasks, etc.)	RECOMMEND	EXECUTE	EXECUTE	*Documented recommendation provided in case record*
Re-imaging / OS rebuild	RECOMMEND	EXECUTE	EXECUTE	*Outside Blumira scope*
Vulnerability patching	RECOMMEND	EXECUTE	—	*Blumira identifies; customer remediates within agreed SLA*

Phase 5 — Recovery

ACTIVITY	SECURITY ANALYST	CUSTOMER	IR PARTNER	NOTES
System and service restoration	RECOMMEND	EXECUTE	EXECUTE	*Fully outside Blumira scope*
Data recovery / backup restoration	RECOMMEND	EXECUTE	EXECUTE	*Fully outside Blumira scope*
Business continuity / DR plan activation	RECOMMEND	EXECUTE	—	*Customer owns BCP/DRP*
Post-containment monitoring (watch for reinfection)	EXECUTE	—	—	*Blumira maintains heightened monitoring post-incident*
Security configuration hardening recommendations	RECOMMEND	EXECUTE	—	*Delivered as documented findings in case record*
Threat Surface Assessment re-evaluation	EXECUTE	EXECUTE *(implements & remediates)*	—	*Blumira initiates; customer commits to remediation timeline*

Phase 6 — Post-Incident & Ongoing

ACTIVITY	SECURITY ANALYST	CUSTOMER	IR PARTNER	NOTES
Incident case documentation	EXECUTE	—	—	*Full case record in Kindling*
Post-incident summary to customer	EXECUTE	—	—	*"What we did vs. what you must do" format*
Lessons learned / detection improvement	EXECUTE	RECOMMEND	—	*Blumira tunes detections; customer reviews recommendations*
Executive / board briefing	RECOMMEND	EXECUTE	—	*Blumira can provide supporting data; customer owns delivery*
Regulatory / breach notification (HIPAA, PCI, etc.)	—	EXECUTE	EXECUTE	*Outside Blumira scope; Blumira provides timeline data to support*
Law enforcement coordination	—	EXECUTE	EXECUTE	*Customer decision; Blumira provides evidence package on request*
Emergency contact confirmation	EXECUTE *(quarterly)*	EXECUTE	—	*Minimum 2 contacts; re-confirmed on a regular cadence*

Hard Boundaries — What Blumira Will Never Do

The following are strictly out of scope regardless of customer request:

- Delete files or wipe disk/memory content
- Make architectural or long-term configuration changes to your environment
- Act on ambiguous or non-imminent threats without customer consent
- Perform routine IT administration or maintenance
- Respond to Low or Medium severity cases under the Managed SLA
- Operate within unsupported third-party EDR shells, OT/ICS, or cloud infrastructure outside M365/Entra
- Execute response actions on hosts not covered by the Blumira Agent, M365 integration, or other supported Blumira integration

Customer Prerequisites — Enrollment Gates

Before Blumira can commit to any action, the following must be in place:

1. Complete the Blumira Managed onboarding checklist (SA-confirmed coverage).
2. Have an active contract with a named IR firm (contact info on file, current retainer) — or explicitly accept the risk of not having one, as Blumira will not be performing IR and only what is listed as part of this responsibility matrix.
3. Identify a minimum of two emergency contacts with expected response availability.
4. Document any hosts that require a call before isolation (domain controllers, PLCs, critical servers).
5. Accept that persistent unresolved risks surfaced by Blumira are subject to a remediation SLA — repeated after-hours pages for a known unpatched issue are not within scope.