Blumira

BLUMIRA MANAGED

MANAGED DETECTION & RESPONSE

Escalation Paths & Response Catalog

How your Blumira Managed support team escalates, communicates, and responds — step by step.

Escalation Path

Every High and Critical case follows this path from detection to closure. The Response SLA is measured from detection (Step 1) to documented analyst action — including a preliminary investigative message to the customer (Step 2) — targeted at 30 minutes.

STEP	WHO	ACTION	TIMING / SLA
1 **Detection**	**Blumira Platform**	Alert fires; the Kindling case is created automatically. High and Critical cases trigger an analyst page.	Immediate / automated **Response SLA starts here**
2 **Analyst Pickup**	**Blumira Security Analyst**	Analyst acknowledges the page, picks up the case in Kindling, and sends a preliminary investigative message to the customer — not an auto-response message.	Within 30 minutes
3 **Initial Triage**	**Blumira Security Analyst**	Analyst reviews alert context, correlated events, and customer environment notes (critical host exclusions, known activity). Confirms severity and determines whether the threat is active and imminent.	Ongoing within case

STEP	WHO	ACTION	TIMING / SLA
4a **Pre-Approved Action**	Blumira Security Analyst	If the threat is confirmed and the appropriate pre-approved playbook applies (e.g., disable compromised account, revoke sessions, quarantine mailbox), the analyst executes immediately. Action and rationale documented in the case record.	As soon as confirmed
4b **Approval-Gated Action**	Blumira Security Analyst + Customer	If the required action falls under EA (e.g., host isolation, MFA reset, OAuth removal), the analyst contacts the customer's primary emergency contact for verbal or written approval before executing. If the primary is unreachable, the analyst attempts the secondary contact. If neither responds within 10 minutes (the response window we state to the customer), the analyst documents the attempt and acts in the customer's best interest to contain the threat.	10-minute approval window
5 **Customer Notification**	Blumira Security Analyst	Analyst sends a case update: what was observed, what was executed, and what the customer must do next. Notification goes to the primary contact (and secondary if paged). This satisfies the SLA documentation requirement.	Post-action
6 **Ongoing Monitoring**	Blumira Security Analyst	Analyst maintains a heightened watch on the affected account/host for signs of reinfection or lateral movement. Additional actions are taken as needed under the same approval framework.	Post-action, duration per case

STEP	WHO	ACTION	TIMING / SLA
7 **IR Handoff**	Blumira Security Analyst + Customer	If the incident requires DFIR, malware removal, legal hold, or recovery beyond Blumira's scope, the analyst formally escalates to the customer and recommends engaging their IR partner. Blumira provides a documented case handoff package (timeline, evidence, actions taken, IOCs).	As soon as scope is exceeded
8 **Case Closure**	Blumira Security Analyst	Case closed in Kindling when the threat is contained within Blumira's scope, or when IR handoff is confirmed. Post-incident summary issued to the customer.	After threat contained or handed off

⚠ **If neither emergency contact responds within 10 minutes:** The analyst documents all contact attempts in the case record, notes the action that would have been taken and why, and acts in the customer's best security interest to contain the threat. All actions are fully documented. Repeated failure to respond may result in removal from the service.

Response Catalog

Every specific action a Blumira Security Analyst may execute — the trigger conditions and the approval level required. Actions not listed here require IR partner engagement or customer execution.

APPROVAL LEVEL KEY

LEVEL	MEANING
PRE-APPROVED	Analyst executes immediately when trigger conditions are met. No customer confirmation required per signed authorization.
APPROVAL-GATED (EA)	Analyst contacts an emergency contact and obtains explicit verbal or written consent before executing. Consent documented in the case record.
ADVISE ONLY	Blumira provides a recommendation; the customer executes. Available to both tiers.

MICROSOFT 365 / ENTRA ID ACTIONS

ACTION	TRIGGER CONDITIONS	APPROVAL	WHAT BLUMIRA DOES	WHAT CUSTOMER MUST DO AFTER
Disable user account	Confirmed account compromise: impossible travel, credential stuffing success, attacker-controlled session, MFA fatigue attack succeeded.	PRE-APPROVED	Disables the account in Entra ID, preventing further sign-in. Documents account name, timestamp, and rationale in the case record.	Verify with the user that compromise is confirmed; re-enable the account and force a password reset when safe to do so.
Revoke all active sessions / tokens	Confirmed or highly suspected active attacker session; token-theft indicators; anomalous sign-in from an attacker IP actively in progress.	PRE-APPROVED	Revokes all refresh tokens for the affected user, terminating active sessions across all connected apps. Documents the action in the case record.	User must re-authenticate on all devices; monitor for re-compromise.
Block sign-in	Active sign-in attempts from a confirmed malicious IP or credential spray in progress; account not yet fully compromised but the attack is active.	PRE-APPROVED	Sets the sign-in blocked flag on the account in Entra ID. Documents the action and associated alert in the case record.	Unblock the account after password reset and MFA re-enrollment; confirm no persistence mechanisms remain.

ON-PREMISES ACTIONS VIA BLUMIRA AGENT

ACTION	TRIGGER CONDITIONS	APPROVAL	WHAT BLUMIRA DOES	WHAT CUSTOMER MUST DO AFTER
Host isolation / network quarantine	Confirmed active malware execution, ransomware precursor behavior, lateral movement from host, active C2 beacon detected on endpoint.	APPROVAL-GATED	With confirmation that the host is not on the critical exclusion list (DCs, production servers, PLCs): isolates the host from the network via the Blumira agent. The host retains its management channel to Blumira. Documents host name, IP, isolation timestamp, and rationale.	Engage IR partner for malware removal and forensic imaging; do not reconnect the host until cleared; update the critical host exclusion list if relevant.
Terminate malicious process	Active malicious process identified (confirmed by hash, behavior, or analyst review): ransomware encryption process, credential dumper, reverse shell.	APPROVAL-GATED	Terminates the identified process via the Blumira agent. Documents process name, PID, parent process, and termination timestamp. Does not delete files.	Engage IR for persistence removal; assume the host is still compromised — do not trust it until imaged or rebuilt.
Disable user account	Confirmed account compromise: impossible travel, credential stuffing success, attacker-controlled session observed, MFA fatigue attack succeeded.	PRE-APPROVED	Disables the account on the domain controller, preventing further sign-in. Documents account name, timestamp, and rationale in the case record.	Verify with the user that compromise is confirmed; re-enable the account and force a password reset when safe to do so.

Agent action limits: Blumira analysts will never use agent access to delete files, modify the registry, or perform any action not listed in this catalog. If a threat requires those steps, it is an IR handoff.

ADVISE ONLY ACTIONS

Blumira investigates and provides specific, actionable recommendations — the customer or their IR partner executes.

RECOMMENDATION TYPE	WHAT BLUMIRA PROVIDES	WHO EXECUTES
Credential reset (beyond Entra block)	Identifies affected accounts; recommends reset scope and sequence; provides IOCs for password spray or spray tooling.	Customer
Firewall / network block (C2 IP, malicious domain)	Provides specific IOCs (IPs, domains, hashes) with confidence level and source; recommends block scope.	Customer
DNS sink-holing	Provides malicious domain list and recommended sinkhole targets.	Customer
EDR-based host isolation (non-Blumira EDR)	Identifies affected host, confirms isolation is appropriate, provides rationale and recommended scope.	Customer (via their EDR console)
Network segmentation / VLAN change	Recommends which segment to isolate and why; provides supporting evidence from the case.	Customer network team
Vulnerability patching	Identifies exploited or at-risk CVEs observed in the incident; prioritizes by exploitability and blast radius.	Customer
Malware / persistence removal	Documents observed persistence mechanisms (scheduled tasks, registry keys, startup entries, services); provides removal guidance.	Customer or IR partner
Security policy hardening	Post-incident: documents configuration gaps that enabled or amplified the threat; provides specific recommended changes.	Customer
IR partner engagement	Provides a documented case handoff package: full timeline, evidence bundle, actions taken, IOCs, and recommended next steps.	Customer (engages IR); IR partner (executes)

IR Handoff Triggers

Blumira will formally recommend IR engagement and prepare a handoff package in any of the following scenarios:

- Active ransomware encryption confirmed
- Confirmed data exfiltration requiring forensic scoping
- Incident requires legal hold, chain-of-custody, or regulatory notification
- Attacker dwell time exceeds 30 days and full scope is unknown
- Malware removal or host rebuild required
- Incident involves OT/ICS/SCADA systems
- Scope of compromise spans infrastructure Blumira cannot observe (cloud workloads, third-party EDR-only endpoints)
- Customer requests DFIR services

> **IR partner recommendation:** All Blumira Managed customers are recommended to have a named IR firm with a current retainer on file before enrollment.