Blumira

Incident Detection Engineering (IDE)

With our SIEM + XDR platform and expert teams combined, ***you get 24/7 coverage*** *-- there's no need to hire full-time analysts to manage your security.*

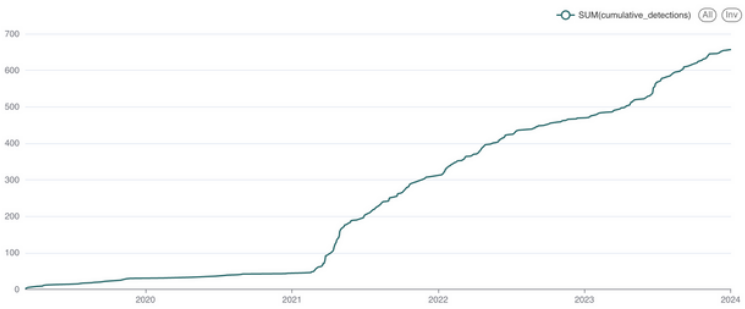
MANAGED DETECTION RULES

The incident detection team manage the detection rules that power Blumira's platform to identify indicators of compromise early & often for our customers:

- Threat hunting & releasing new detections every week
- Actionable findings are sent within minutes (or less) of initial detection for the fastest response times
- Proactive outreach to customers about malicious activity seen in their environment

FOCUS ON CRITICAL VULNERABILITIES & EXPLOITS

The IDE team prioritizes detection work scheduled for highest customer value first; they do so by calculating threat risk, and focusing on company and product priority. Critical security vulnerabilities and exploits are always at the top of their list for effort and impact.



The IDE team continues to add valuable detection rules to the platform every week to make sure our customers are protected against the latest exploits.

BLUMIRA'S RESPONSE TO EMERGING THREATS

Blumira responds rapdily to emerging security threats. The IDE team helps customers and the community by:

- Sharing educational information about threats and their remediation/mitigation on our blog
- Sending customers security advisories about threats
- Creating detections that help to surface potential threats in Blumira customer environments
- Providing public commentary about threats through blog posts and/or media interviews

IDE AREAS OF FOCUS

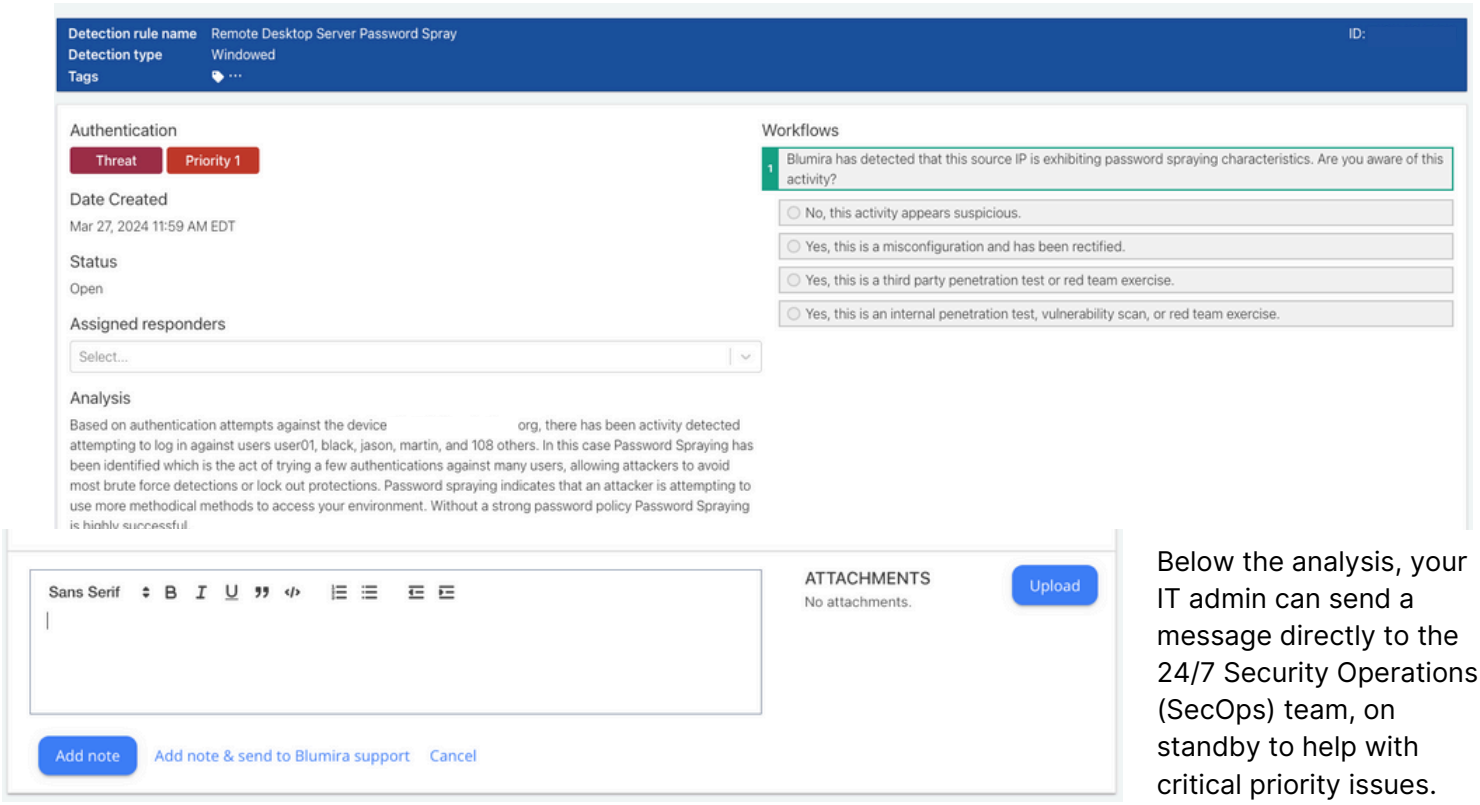
- **Research:** Threat research to identify detection opportunities related to emerging threat disclosures; new tech to enhance current analysis & workflows
- **Incident Detection:** Building on existing integrations with live lab testing & exploitation, customer log testing, query creation, workflow and IR creation, zero-day detections, and more.
- **Product Focus:** Net-new detections for new integrations or product features; developing detections and documentation
- **Customer Focus:** Creating custom detections for customers, assisting in incident response activities during a customer incident, and tuning detections to reduce false positives.

Blumira

WE PROACTIVELY REACH OUT TO CUSTOMERS WHEN OUR PLATFORM IDENTIFIES A MALICIOUS FINDING THAT'S CRITICAL TO STOP AN ATTACK EARLY.

An example finding in the Blumira platform, seen below includes the work of our IDE team:

- Detection rule name & type
- Type of event (threat) and priority level (priority 1)
- Detection analysis to explain what happened
- Workflow to guide you through response steps (playbook)



Below the analysis, your IT admin can send a message directly to the 24/7 Security Operations (SecOps) team, on standby to help with critical priority issues.

HOW RULES ARE ADDED TO BLUMIRA'S PLATFORM:

IDEATION ---→ **PRIORITIZATION** ---→ **RESEARCH** ---→ **RULE CREATION**

---→ **TUNING** ---→ **TESTING** ---→ **WORKFLOWS / ANALYSIS** ---→ **RELEASE**

The biggest value is that you have people configuring the alerts to catch potential threats. If we had to configure our own alerts, we wouldn't. ***Having your research team and threat hunters behind the scenes building the rules to trigger those findings is extremely valuable.***
-- Monte Sonksen, IT Manager, City of Bettendorf

TRY XDR TODAY

Blumira makes security easy and effective for SMBs, helping them detect and respond to cybersecurity threats faster to stop breaches and ransomware.

Sign up for a free 30-day trial to experience Blumira's SIEM + XDR platform.

Visit blumira.com/free