Blumira

Blumira's Threat Detection

Comprehensive Security Coverage

Blumira's platform leverages threat intelligence, threat hunting at scale and behavioral analytics to detect real attack patterns that can lead to ransomware or a breach, alerting you to high priority threats across your entire environment with guidance for faster response.

Cloud Infrastructure

- Common misconfigurations
- Modified security groups
- Malware indicating a compromised cloud instance
- Attempts to connect with C2 (attacker-controlled) servers

Identity & Access

- Attempts to log in to your systems
- Geo-impossible logins
- Fraudulent login attempts that could indicate the theft of usernames and passwords

Email & Document

- Anomalous access attempts
- External document sharing
- Email forwarding
- New inbox rules created by attackers to evade detection by deleting sent emails or incoming messages

Endpoint Security

- Malware running on devices
- Attacker tools like Mimikatz, Cobalt Strike, Adfind and more
- Unknown or blocklisted applications
- Compromised processes running on devices within your network

Operational

- Messages Have Been Delayed
- User Requested to Release a Quarantined Message
- Malware Auto Purge Failed Due to User Configuration
- User Restricted From Sending Email
- Potential Issue With Log Flow
- Tenant Allow/Block List Entry is About to Expire
- New Inbound Receive Connector
- System Failover Event
- Admin Group Change
- New Firmware Available
- Secret Created in Secret Manager
- Exchange Domain Added
- Application Password Deletion
- New Firmware Available

Uncover Attacks Earlier & Faster

Threat actors use a wide variety of techniques to learn about your systems, gain initial access, maintain persistence inside of your environment, and execute malware.

Blumira notifies you with findings at every stage of attack to empower your IT team to respond faster - stopping threats before they result in damage to your company. Get a summary of Blumira's top detections mapped to threat actor tactics in the MITRE ATT&CK framework:

Reconnaissance

Gathering info to use in future attacks

- Active Scanning - Public to Private Recon in Individual Connections
- Gathering Victim Host, Identity, Network and Org Info
- Phishing for Info
- Searching Open Technical Databases, Open Domains, Victim-Owned Websites
- Advanced IP Scanner
- Honeypot Actively Scanned
- SoftPerfect Network Scanner
- SYSVOL Enumeration of Saved Credentials

Initial Access

Trying to get into your network

- Drive-By Compromise
- Authentication by Known Attack Tool
- SQL Injection Attempt
- Cross-Site Scripting
- EC2 Misconfiguration
- External Remote Services
- Hardware Additions
- RDP Connection from Public IP
- Phishing Attempts
- Supply Chain Compromise
- Credential Dump from Registry (also Privilege Escalation & Credential Access)
- Potentially Malicious ISO file (LNK)

Execution

Running malicious code

- Ransomware Activity
- Attacker Tools/Malware - Cobalt Strike
- Command and Scripting Interpreter - Script Running in Memory
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication
- Malware Detection
- Unblocked Malicious Website
- Vulnerability Exploit Attempt

User Execution

- User Clicked Questionable Link

Persistence

Maintain a foothold

- SSH, FTP, SMB Connection from Public IP
- Admin Level Account Addition
- Compromise Client Software Binary
- Create Account
- Create or Modify System Processes
- Hijack Execution Flow
- Pre-OS Boot
- Traffic Signaling
- Custom Admin Role Created

Privilege Escalation

Gain higher-level permissions

- Process Injection - Compromised Process
- Malicious In-Memory Behavior
- Admin Account Addition or Changes
- Access Token Manipulation
- Boot or Logon Autostart Execution
- Domain Policy Modification
- Elevation of Admin Privileges

Defense Evasion

Avoid being detected

- Changes in Audit Policy Logging
- Disabled Cloud Logs
- Disabled Firewalls, Windows Event Logging, Command History Logging
- Deobsfucate/Decode Files or Info
- Exploitation for Defense Evasion
- Indicator Removal on Host
- Decimal Character Encoded Command

Credential Access

Stealing account names and passwords

- Brute-Force - Anomalous Access Attempts
- User Login Failures
- OS Credential Dumping
- Attacker Tools - Mimikatz
- AWS IAM Credential Exfiltration
- Man-in-the-Middle
- Network Sniffing
- Steal Web Session Cookie
- Two-Factor Authentication
- Unsecured Credentials
- Activity From Infrequent Country
- Unusual ISP for an OAuth App
- Authentication Outside of U.S.

Discovery

Figure out your environment

- Attacker Tools - Adfind
- Account Discovery
- Application Window Discovery
- Cloud Infrastructure Discovery
- Network Share Discovery
- File and Directory Discovery
- Domain Trust, Remote System, System Info and System Owner/User Discovery
- Network Service Scanning
- Non-Browser Public IP Lookup
- Advanced Port Scanner
- Null Session Activity - Large Amount of Total Authentications

Lateral Movement

Moving through your network

- Exploitation of Remote Services
- Internal Spearphishing
- Remote Service Session Hijacking
- Lateral Tool Transfer
- Remote Services
- Replication Through Removal Media
- Software Deployment Tools
- Taint Shared Content
- NTLM Authentication Tampering
- SSH Connection From Public IP (also under Persistence)
- RDP One to Many: Greater than 5
- PsExec Service Execution

Command & Control

Communicate with compromised systems

- Application Layer Protocol
- Encrypted Channel
- Ingress Tool Transfer
- Remote Access Software
- Data Encoding
- Data Obfuscation
- Non-Standard Port
- Protocol Tunneling
- Traffic Signaling
- Web Service
- Proxy Avoidance
- Keyhole VNC Activity
- Remote Access Tool: Atera

Exfiltration

Trying to steal data

- Exfiltration Over Alternative Protocol
- Exfiltration Over Web Service
- Exfiltration to Cloud Storage
- Exfiltration to Code Repository
- Exfiltration Over C2 Channel, Physical Medium, Other Network Medium
- Transfer Data to Cloud Account
- File Shared With Personal Email Addresses

Impact

Disrupt or destroy systems and data

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation
- Defacement
- Disk Wipe
- Endpoint Denial of Service
- Network Denial of Service
- Firmware Corruption
- Inhibit System Recovery
- Resource Hijacking
- System Shutdown/Reboot
- 100+ File Deletions in 15 Minutes

Blumira

Managed Detections by Blumira

The incident detection team manages 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

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 on an ongoing basis to make sure our customers are protected against the latest exploits.

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

Blumira responds rapidly 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

We do the heavy lifting for you to make it as easy as possible for your IT team to manage on a daily basis, taking care of:

- Creating data parsers & third-party integrations
- Gathering and subscribing to threat intelligence feeds
- Writing, testing, tuning and updating detections weekly
- Custom detection rule development
- Onboarding assistance with sensor setup
- Log flow troubleshooting

EASY

Reduce reliance on humans to complete manual security tasks to save time and refocus efforts

EFFECTIVE

Accelerate breach prevention and ransomware protection with security automation

EFFICIENT

All-in-one open platform simplifies workflows with hybrid coverage, satisfying more compliance controls

> ***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*

DEMO XDR TODAY

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

Contact us to see a demo of Blumira's SIEM + XDR platform.

blumira.com/demo