DATA SHEET

Blumira

Threat Detection
& Response

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, alerting you to high priority threats across your entire environment and giving you the guidance to respond quickly.

Cloud Infrastructure

- Common misconfigurations
- Modified security groups
- Attempts to connect with C2 (attacker-controlled) servers
- Credential exfiltration

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, Powershell Empire, Bloodhound, Sharphound and more
- Unknown or blocklisted applications
- Compromised processes running on devices within your network

Discover Attacks at Any Stage

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

While the final stage we detect is **Impact**, our objective is to surface real findings in the below stages to empower your IT team to act quickly and respond - containing the threat before it results in damaging impact to your company.

Here's a summary of some of Blumira's top detections mapped to the threat actor tactics identified by the MITRE ATT&CK framework:

Reconnaissance

Gathering info to use in future attacks

- Internal Port Scanning and Recon
- Enumeration through AS-REP Roasting
- Enumeration through Kerberoasting
- SYSVOL enumeration
- Unusual Java Discovery Commands
- Honeypot Access
- Domain Enumeration Anomalies

Initial Access

Trying to get into your network

- High number of MFA requests
- Web authentication anomalies
- Repeat Failed Logons
- RDP, FTP, SSH, SMB, etc Connections from Public IP
- Phishing Attempts
- Remote Access Tools (RATs)

Execution

Running malicious code

- Attacker tool execution through Powershell
- Command and Scripting Interpreter - Script Running in Memory
- Signed Binary Proxy Execution
- Suspicious Parent Processes
- Suspicious Macros and Attachments

Persistence

Maintain a foothold

- Abnormal Cron Jobs
- Admin Level Account Addition
- New Services
- New Scheduled Tasks
- Web shell interactions
- Suspicious Java in Startup locations
- Registry Run Scripts
- Create or Modify System Processes

Privilege Escalation

Gain higher-level permissions

- New IAM role assumed by new resource
- Sudo Exploit Attempts
- Disabling UAC
- Memory Dumping
- Pass-the-Hash
- Process Injection - Compromised Process
- Malicious In-Memory Behavior
- User added to privileged group

Defense Evasion

Avoid being detected

- Changes in Audit Policy Logging
- Bash/Zsh History Manipulation
- Reverse Proxy Process Creation
- Real-Time protections disabled
- Disabled Firewalls, Windows Event Logging, Command History Logging
- Domain Policy Modification

Credential Access

Stealing account names and passwords

- User Authentication MFA Bypass
- Brute-Force - Anomalous Access Attempts
- Successful console login by non-MFA user
- Attacker Tools - Mimikatz
- AWS IAM Credential Exfiltration
- Unsecured Credentials
- Application Password Creation

Discovery

Figure out your environment

- Bloodhound File Write
- Findstr Password discovery
- Injected Explorer Discovery
- Net Recon Commands
- Null Session activity
- Registry Permission Weakness
- Account Discovery
- Network Share Discovery
- File and Directory Discovery

Lateral Movement

Moving through your network

- Registry Lateral Movement
- WinRM Remove Code Execution
- Linux Reverse Shell
- Honeytoken Activity
- RDP one to many
- Remote Schedule task creation
- Compromised EC2 Traffic
- Lateral Tool Transfer
- NTLM Authentication Tampering

Command & Control

Communicate with compromised systems

- EC2 C2 Activity
- Attack tool C2 reports
- Remote Access Tools (RATs)
- DNS Anomalies
- External Proxy Detection
- Keyhole VNC Activity
- RDP over Reverse Tunnel
- DNS Tunneling
- Malicious Webshell Connections

Exfiltration

Trying to steal data

- Exfiltration Over C2 Channel, Physical Medium, Other Network Medium
- ARP Poisoning
- External Document Shares
- Azcopy and Rclone Execution
- Multiple Outbound Suspicious Connections
- Tor Tunnel Traffic
- Compressed Data for Exfiltration

Impact

Disrupt or destroy systems and data

- Clearing of Event Logs
- Admin Changes
- Unsafe File Permissions
- Mass Deletion of Objects
- .PST file export
- Key Vault Tampering
- 100% CPU
- Failing Hard Drive
- Backup Errors
- Cryptomining Traffic Blocked

Blumira

DATA SHEET

Pre-Tuned to Reduce Noise = Less Alerts

Blumira takes a radically different approach to defensive security to focus on what's critical and urgent, and less on sending you tons of noisy alerts. This results in better security outcomes for your organization.

Our incident detection engineering team strives to:

- **Creating actionable intelligence** and automating level 1 SOC duties into the alert analysis and workflows
- **Test every detection rule** in lab environments, tuning it for noisy false positives before rolling it out to our platform to reduce alert fatigue
- **Consolidating all correlated logs** and evidence under open findings, instead of opening multiple findings to significantly reduce alert volume and give additional context for repeat alerts
- **Prioritize every finding automatically** by different threat levels to make sure Priority 1 Threat alerts get the attention they deserve

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:

- Developing and maintaining data parsers
- Gathering and subscribing to threat intelligence feeds
- Writing, testing, tuning and updating detections weekly
- Creating new third-party integrations
- Helping create security reports
- Custom detection rule development
- Onboarding assistance with sensor setup
- Log flow troubleshooting
- Expert security advice when you need it the most

Meet compliance controls, save time on security tasks, focus on real threats and protect against a breach faster than ever with Blumira.

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

BLUMIRA'S FREE SIEM

Sign up free (no credit card required) to get:

- 3 cloud integrations, deploy in minutes
- Cloud SIEM with detection & response
- Automated detection rules applied
- Playbooks on how to respond to threats
- Security reports to see risk trends

SIGN UP FREE

blumira.com/free