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
- 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

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:

Blumira

DATA SHEET

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

Initial Access

Trying to get into your network

- Drive-By Compromise
- SQL Injection Attempt
- Cross-Site Scripting
- EC2 Misconfiguration
- External Remote Services
- Hardware Additions
- RDP Connection from Public IP
- Phishing Attempts
- Supply Chain Compromise

Execution

Running malicious code

- Attacker Tools/Malware - Cobalt Strike
- Command and Scripting Interpreter - Script Running in Memory
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication

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

Privilege Escalation

Gain higher-level permissions

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

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

Blumira

DATA SHEET

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

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

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

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

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

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

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.

AUTOMATE TASKS FOR YOU

We do all the heavy lifting for your team to save them time, including parsing, creating native third-party integrations, and testing and tuning detection rules to reduce noisy alerts.

FASTER TIME TO SECURITY

Our unique approach to detections notifies you of threats other security tools may miss, sending you real-time alerts in under a minute of initial detection to help you respond to threats faster than ever.

EASILY MEET COMPLIANCE

With a year of data retention and deployment that takes minutes to hours, we help you meet cyber insurance and compliance easily and quickly with the team you have today.

BLUMIRA FREE EDITION

Protect your Microsoft 365 environment in minutes! Sign up free (no credit card required) to get:

- 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