DATA SHEET

Blumira
Threat Detection & Response

Top MITRE ATT&CK Techniques

Easily and Quickly Detect Techniques Used in 90% of Attacks

MITRE's Sightings Ecosystem report identified the top techniques used in 90% of attacks from 2019-2021. Most of them abused legitimate system tools, making it difficult for the majority of security tools to detect.

Blumira's behavior-based detections identify these techniques -- helping you respond faster to contain them. Here are some of the top MITRE techniques that Blumira can detect:

Scheduled Task/Job - T1053

Abusing task scheduling to execute malicious code

T1053.002
- At.exe Scheduled Task

T1053.003
- Cron Persistence
- Abnormal Cron Job: Curl-Wget

T1053.005
- New Remote Scheduled Task
- New Local Scheduled Task
- Scheduled Task 7 Day Hunt

Hijack Execution Flow - T1574

Executing malicious payloads by hijacking the way operating systems run programs

T1574.011
- Abnormal Service ImagePath Change
- Service Registry Permissions Weakness
- Abnormal Service ImagePath Change
- Service Registry Permissions Weakness

Command & Scripting Interpreter - T1059.001

Abusing command and script interpreters to execute commands

- Default Execution Flags PoshC2
- Default Execution Flags PowerShell Empire
- Default Execution Flags for Cobalt Strike
- Suspicious Powershell Command
- Invoke-WebRequest - Powershell
- Potentially Malicious PowerShell Command
- PowerShell Malicious Execution Detection: Posh C2
- PowerShell Malicious Execution Detection: Cobalt Strike
- PowerShell Malicious Execution Detection: PowerShell Empire
- Indicator: PowerUp Privilege Escalation Module
- Indicator: PowerShell Empire Module
- PowerShell Fileless Script Execution
- Schedule Task Reading PowerShell from Registry
- Abnormal Download: Potential DiskWiper Precursor
- Potentially Malicious PowerShell Command - Event ID 4104
- Potentially Malicious PowerShell Command - Event ID 4688

Blumira

DATA SHEET

Proxy - T1090

Using proxies to disguise the source of malicious traffic

- Ngrok Proxy Detection
- Cloudflared External Proxy Detection

Masquerading - T1036

Renaming or manipulating location of objects to make them appear legitimate

- DLL Masquerading as an Image

T1036.003
- Renamed PowerShell

Signed Binary/Proxy Execution - T1218

Bypassing process or signature-based defenses by proxying execution of malicious content with signed binaries

T1218.005
- Signed Binary Proxy Execution: Mshta

T1218.007
- Signed Binary Proxy Execution: Msiexec - Execute Remote MSI file

Process Injection - T1055

Injecting code into processes to evade process-based defenses and elevate privileges

- Process Injection
- Suspicious Process Parents dllhost.exe/taskhost.exe
- Cylance Indicator - Suspicious In-Memory Behavior
- Cylance Indicator - Malicious In-Memory Payload
- Suspicious Process Parents services.exe
- Suspicious Process Parent lsass.exe
- Suspicious Process Parent winlogon.exe/wininit.exe
- Suspicious Process Parent svchost
- Process Injection via mavinject.exe
- Suspicious Parent Process Print Spooler

Impair Defenses - T1562

Maliciously modify components to hinder or disable defensive mechanisms

T1562.001
- Unload Sysmon Filter Driver

T1562.008
- AWS CloudTrail: Impair Defenses: Disable GuardDuty

Blumira

DATA SHEET

Remote Services - T1021

Using valid accounts to log in and accept remote connections

T1021.001
- Enable Remote Services: Remote Desktop Protocol in the registry
- RDP One to Many: Greater than 10
- RDP One to Many: Greater than 20
- RDP One to Many: Greater than 5

T1021.006
- Suspected WinRM Remote Code Execution
- Suspected WinRM Remote Code Execution via wsmprovhost.exe

Modify Registry - T1112

Using valid accounts to log in and accept remote connections

- Modify registry to store logon credentials: WDigest

Windows Management Instrumentation - T1047

Abusing WMI to execute malicious commands and payloads

- WMI Process Call Create : Remote Code Exec
- WMI Reconnaissance List Remote Services
- Impacket WMI exec

Ingress Tool Transfer - T1105

Transferring tools or other files from an external system into a compromised environment

- Certutil Download
- Bitsadmin Download
- Rclone Execution via Command Line or PowerShell

Blumira

DATA SHEET

Shine a Light on What Your EDR Misses

Blumira identifies key findings of real attacker patterns, found in 90% of attacks to help you stop an attack in progress.

These top attacker techniques are effective because they're hard to distinguish from legitimate user behavior.

Traditional security tools like endpoint detection and response (EDR) and antivirus often miss these types of attacker techniques, as they rely on signature-based detections.

Blumira's approach incorporates behavior-based detections to identify techniques that use legitimate Windows tools and processes to evade detection by typical security tools.

With Blumira's detection and response platform, you can gain valuable visibility into what your EDR may miss. We provide playbooks to walk you through next steps to quickly respond and contain a threat.

We do the heavy lifting for you to make it as easy as possible for your IT team to manage on a daily basis.

Our engineering and SecOps team takes care of many typically-manual SIEM duties to reduce the burden on your team:

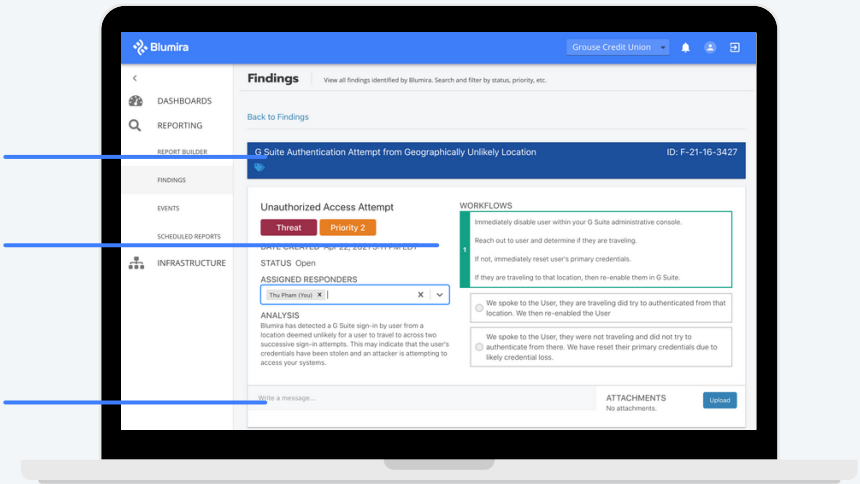
- Developing and maintaining data parsers
- Gathering and subscribing to threat intelligence feeds
- Writing, testing, tuning and updating detections weekly
- Creating new third-party integrations
- Helping create security reports
- Custom detection rule development
- Onboarding assistance with sensor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

Actionable Findings, Automated Response & Access to Experts

Threat Analysis

Playbooks For Response

Direct Message a Security Expert



"We chose Blumira for its simplicity – I needed a solution that would simplify, consolidate and show me what I really need to see."

- Jim Paolicelli, IT Director, Atlantic Constructors

Sign Up Free!
blumira.com/free