Signal Sciences
Now part of fastly

Brute Force Attack Protection

White Paper

Brute force attacks are a common threat against web applications and may result in compromising user accounts, which lead to unauthorized access to user data and transactions. Signal Sciences enables DevOps and security teams to detect and defend against brute force attacks with Power Rules.

Brute Force Attacks

Brute Force Attacks are repeated request attempts to guess valid credentials or input parameters in order to obtain unauthorized access to the application functionality or data. Brute force attacks come in many different shapes and sizes:

- Username and password guessing against an application's authentication
- Enumeration of user profiles
- Enumeration of web server directories

Brute Force Attack Detection

By inspecting specific attributes in HTTP requests and responses, Signal Sciences can enable early detection of brute force attacks against your application. Using time-series dashboards within the Signal Sciences Console, brute forcing activity can be tracked and observed on a graph showing exactly when the volume of such activity. A spike in this activity is an indicator of an attack and is clearly detected on the graph. Automated detection of brute force attacks is achieved with threshold-based alerting, which is implemented easily and quickly with Power Rules.

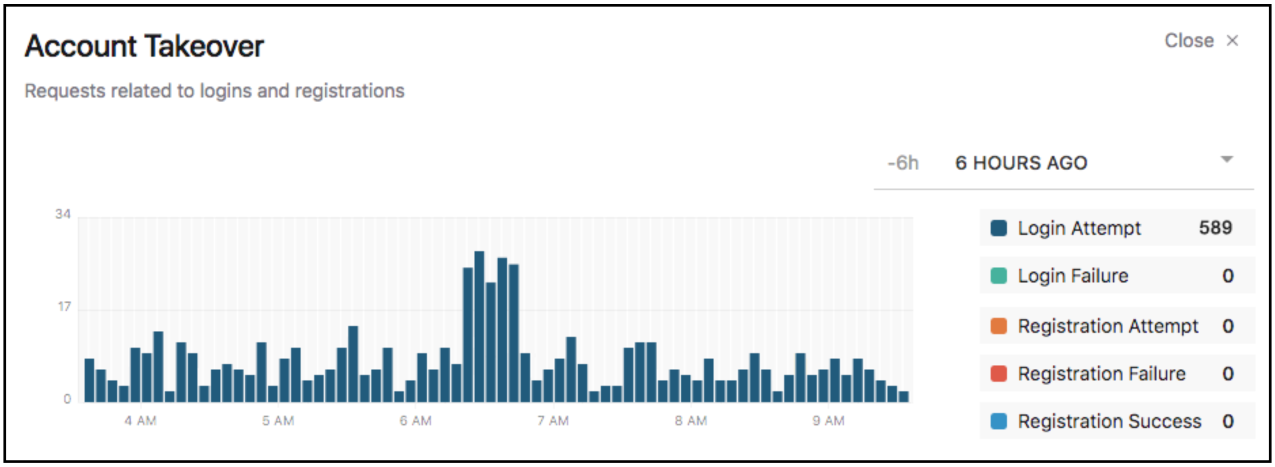
Brute Force Attack Protection

Detecting brute force attacks is the first step to protecting your application in real time. The next step is to automate the blocking of requests associated with the attack. In the same Power Rule used to detect the brute force attack, blocking is implemented to drop failed login requests from IP addresses that previously reached the threshold specified in the Power Rule.

Authentication Brute Force Attacks

Attacks against authentication is one of the most common types of brute force attacks. There are numerous resources on the Internet—like password lists and password file dumps from breaches of major sites—that allow attackers to target authentication systems on web applications. In addition, there are various tools and scripts available to automate the attack. The leading indicator of a brute force attack is a spike in failed authentication attempts which can be observed visually as a graph. In the Account Takeover graph below, we quickly spot a change occurring at about 6:30 a.m. in the volume of attempted logins that indicates the beginning of a brute force attack.

Visulaizing Brute Force Attacks



Account Takeover

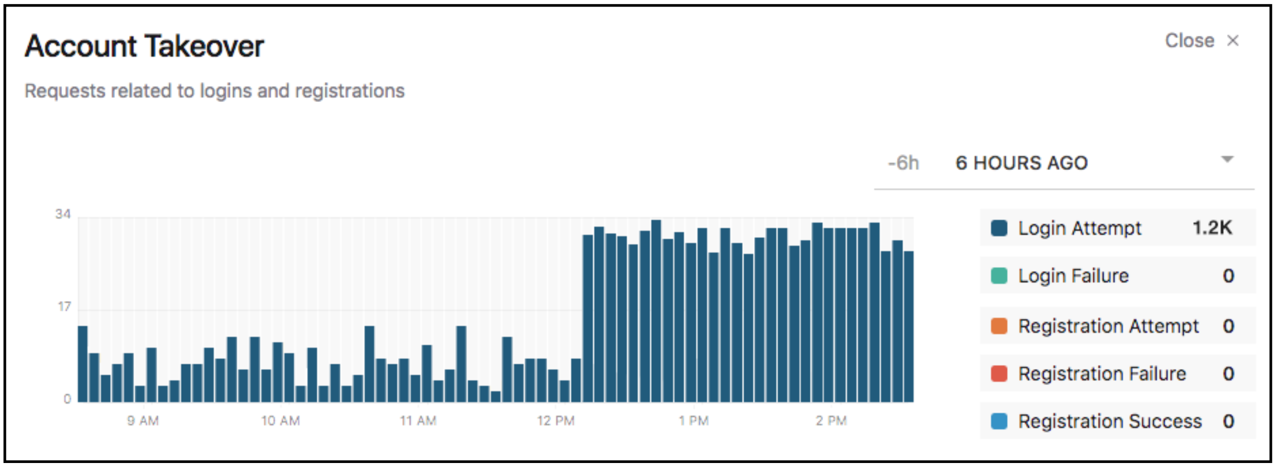
Requests related to logins and registrations

Close ×

-6h 6 HOURS AGO

🟦 Login Attempt	589
🟩 Login Failure	0
🟧 Registration Attempt	0
🟥 Registration Failure	0
🟦 Registration Success	0

As another example, the graph below illustrates an attack persisting over a period of time from about 12:30 p.m. onwards.



Account Takeover

Requests related to logins and registrations

Close ×

-6h 6 HOURS AGO

🟦 Login Attempt	1.2K
🟩 Login Failure	0
🟧 Registration Attempt	0
🟥 Registration Failure	0
🟦 Registration Success	0

The above is just one example of monitoring capabilities available from Signal Sciences. Additional activity such as login failure, registration attempt, and registration failure can be monitored with no additional configuration.

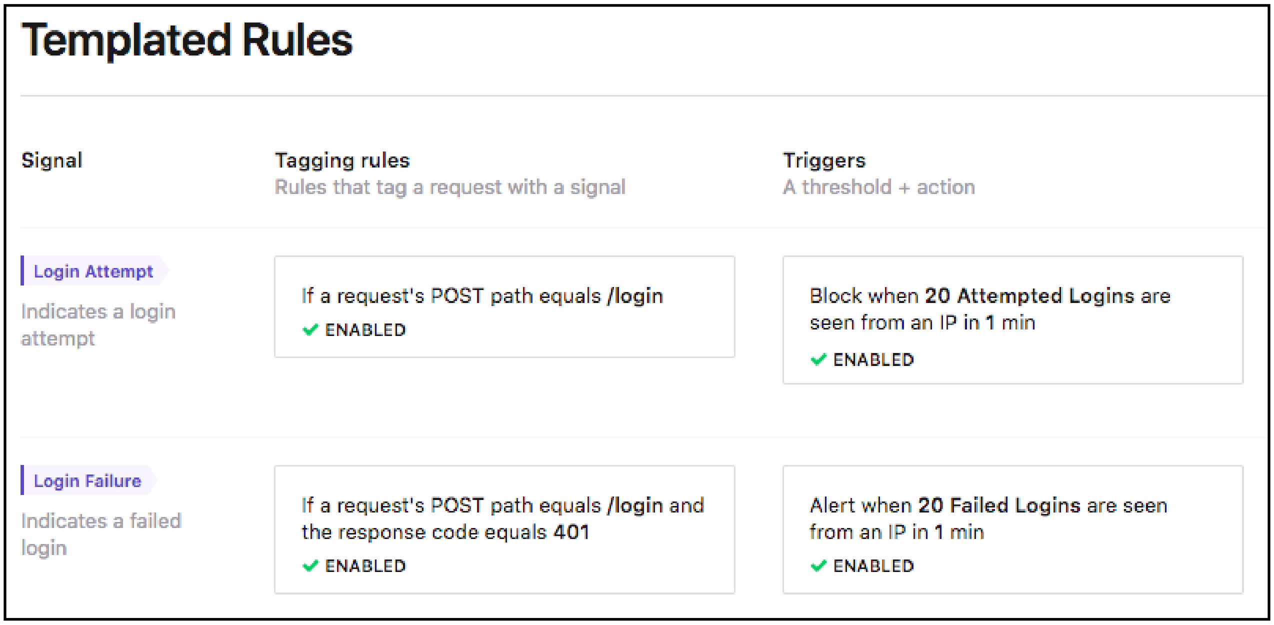
Detection and Protection with Power Rules

While monitoring provides security teams visibility that builds situational awareness, Signal Sciences empowers organizations to automatically stop brute force attacks involving registrations and logins. We also provide customers the means to deploy virtual patches to known vulnerabilities so IT, DevOps, or security teams can respond and update impacted systems.

With Power Rules, values specific to an organization's web application and business rules are used to define thresholds within the Signal Sciences Console. These rules can quickly detect and automatically block brute force attacks.

Below are examples of two templated Power Rules for the "Login Attempt" and "Login Failure" signals. The "**Login Attempt**" signal has a rule defined that monitors login attempts using the `POST` method and the directory path equals /`login`. A trigger based on reaching a threshold of 20 attempted logins from a single IP address within one minute is also enabled for this rule. If the threshold values are met for this rule's trigger, subsequent login attempts are automatically blocked.

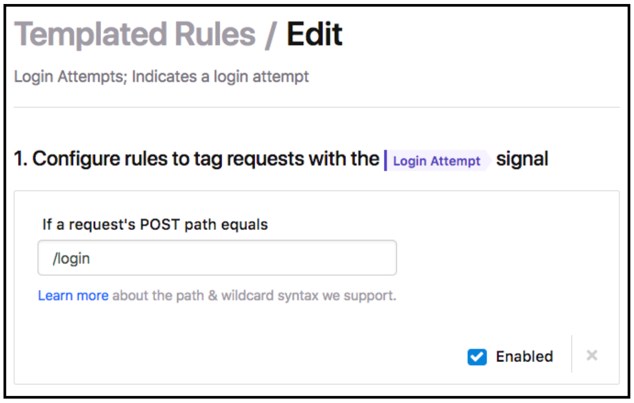
In the "**Login Failure**" rule, the DevOps team has enabled automated alerts on subsequent login attempts from an IP address after 20 failed logins.



Templated Rules

Signal	Tagging rules Rules that tag a request with a signal	Triggers A threshold + action
Login Attempt Indicates a login attempt	If a request's POST path equals **/login** ✓ ENABLED	Block when **20 Attempted Logins** are seen from an IP in **1** min ✓ ENABLED
Login Failure Indicates a failed login	If a request's POST path equals **/login** and the response code equals **401** ✓ ENABLED	Alert when **20 Failed Logins** are seen from an IP in **1** min ✓ ENABLED

Enabling Threshold Blocking



Templated Rules / Edit

Login Attempts; Indicates a login attempt

1. Configure rules to tag requests with the Login Attempt signal

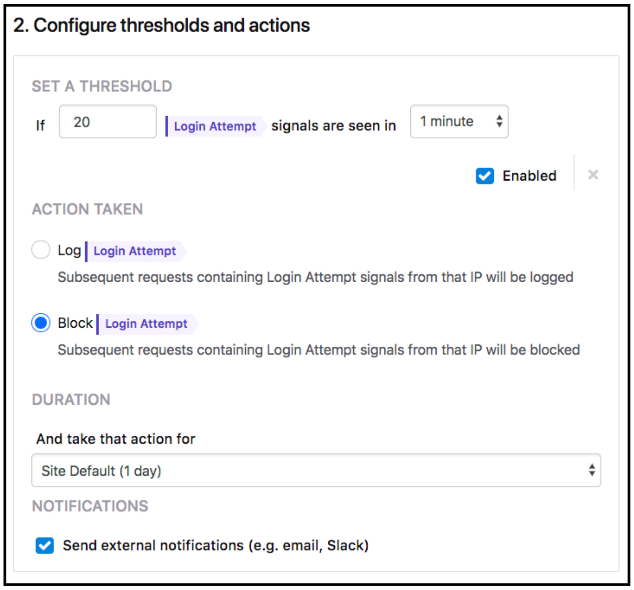
If a request's POST path equals

/login

Learn more about the path & wildcard syntax we support.

☑ Enabled ×

Setting up the templated Power Rule and defining the thresholds to trigger an alert and automatic blocking can be done in minutes. The below screens show how a SOC manager can easily set up the above "Login Attempts" rules. In step one, they set the POST path to monitor to `/login`.



2. Configure thresholds and actions

SET A THRESHOLD

If 20 Login Attempt signals are seen in 1 minute

☑ Enabled ×

ACTION TAKEN

○ Log Login Attempt
Subsequent requests containing Login Attempt signals from that IP will be logged

● Block Login Attempt
Subsequent requests containing Login Attempt signals from that IP will be blocked

DURATION

And take that action for

Site Default (1 day)

NOTIFICATIONS

☑ Send external notifications (e.g. email, Slack)

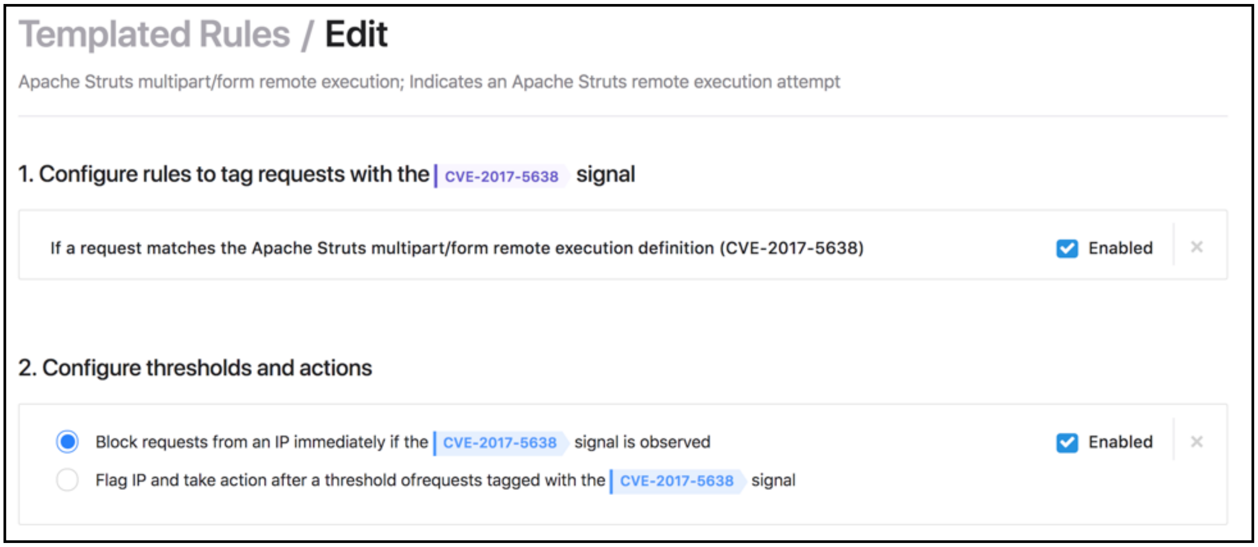
In step two, the SOC manager defines the thresholds and actions if those thresholds are met. In this specific Power Rule, they enter the number of login attempts within a specific timeframe that would trigger the desired action. If there are 20 login attempts within one minute, subsequent login requests from the same IP address will be blocked automatically for one day. The blocking duration can be set for a time period from 10 minutes to 24 hours (one day is the default).

A notification has also been enabled for this rule. When the threshold is met, an alert will be sent via Slack, email or other notification means, keep the DevOps, operations and infrastructure staff aware and engaged in the security of the applications they develop and oversee.

With Signal Sciences integrations, alerts are distributed in an effective and timely manner. Signal Sciences integration and collaborations include PagerDuty, Slack, HipChat, Microsoft Teams, Pivotal Tracker, Jira, and VictorOps.

Virtual Patching

Power Rules also provide the ability to apply virtual patching to immediately block or log requests matching specific vulnerabilities. In the below example, requests will be blocked if they seek to leverage the Apache Struts vulnerability that leads to remote code execution. The vulnerability-to-exploit cycle can occur in hours, so organizations need a proactive means to block these attacks, while providing the necessary to update impacted systems. This is exactly what Signal Sciences provides through our virtual patching feature which stops vulnerabilities in their tracks, providing DevOps and security teams time to respond.



Templated Rules / Edit

Apache Struts multipart/form remote execution; Indicates an Apache Struts remote execution attempt

1. Configure rules to tag requests with the CVE-2017-5638 signal

If a request matches the Apache Struts multipart/form remote execution definition (CVE-2017-5638) ☑ Enabled

2. Configure thresholds and actions

● Block requests from an IP immediately if the CVE-2017-5638 signal is observed ☑ Enabled

○ Flag IP and take action after a threshold ofrequests tagged with the CVE-2017-5638 signal

Note: Signal Sciences is an extensible platform and provides additional options for managing and automating blocking via an API. For example, the API can be leveraged to integrate with other control systems or sensors on your network to manage IP whitelists and blacklists.

Enumeration & Directory Brute Force Attacks

Enumeration Attacks

An enumeration attack is a form of brute force attack that is typically automated with tooling and targets application parameters. Enumerable application parameters will typically be identifiers like usernames, account numbers, or object reference IDs. The objective of enumeration attacks is to either identify resources (e.g. a user account) for further targeted attacks or to discover unprotected resources in the application.

Directory Brute Forcing

A directory brute force attack, also typically automated, will use predefined lists of directory and file names to determine if they exist on the target web server. These lists consist of directory and file names that are associated with applications or data files. The objective of directory brute forcing attacks is to discover unprotected resources on the web server.

As with authentication brute force attacks, by applying the Signal Sciences approach to detection and protection, enumeration and directory brute forcing attacks can be mitigated. Using Signal Sciences Power Rules and alerts provides early detection of repeated attempts to discover unprotected resources. Coupling early detection with automated blocking enables real-time protection against brute force attacks.

With early detection in place and automated blocking enabled, Signal Sciences will notify operational and security teams while defending the application.

Signal Sciences Power Rules and alerts enable early detection of brute force attacks. With early detection in place and automated blocking enabled, Signal Sciences will notify operational and security teams while defending the application. Having the ability to detect brute force attacks is critical to defending your web applications in real time.

Signal Sciences

Now part of fastly

Please visit www.signalsciences.com to learn more about our platform.