Okta ThreatInsight

Automated detection and prevention against identity attacks

okta

*See Okta ThreatInsight disclaimer included at the end of this whitepaper

Introduction

As identity related attacks have increased in recent years, organizations are continuously evaluating how to optimize the security policies in their environment. In this whitepaper, we cover Okta ThreatInsight, a baseline security feature of the Okta Identity Cloud which helps organizations secure their organization against large scale identity attacks. We start by identifying common identity attacks organizations face today, then introduce ThreatInsight as a method of mitigating account takeover and account lockout, and end with the technical details on how ThreatInsight works.

Today's challenges in securing logins

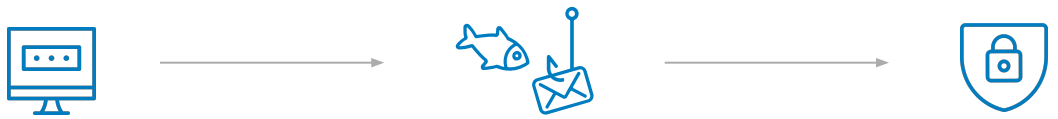
Identity attacks continue to be a common pain point for organizations. This should not come as a surprise, as broken authentication sits at #2 in the OWASP Top 10 Web Application Security Risks as well as the API Security Top 10. While attack methods have evolved through the decades, threat actors continue to use basic identity attacks to takeover accounts.

Password threats are a common form of identity attacks. These attacks are successful for a variety of reasons. First, passwords are easy to compromise - users tend to reuse the same password, use easy-to-guess passwords, and write passwords down. And, many organizations do not enforce multi-factor authentication or do not build multi-factor authentication into their apps. Additionally, in an effort to focus on app functionality, many app developers do not focus on building secure auth practices.

To set the context for this whitepaper, let's first break down the common identity attacks organizations are susceptible to -

Phishing

A threat actor targets either a large group (broad-based phishing) or specific individuals (spear-phishing). The threat actor will usually compromise a legitimate website or create a fake domain. From there, they craft a message that encourages receivers to follow a link to that site. Once a receiver clicks on the link, they are either requested to input their credentials into the site, or the site will download malware that gathers credentials stored on the device or browser memory. The attacker then uses these credentials to steal sensitive data from the individual or their employer.



Hacker acquires emails and designs generic call to action

Hacker distributes phishing message and waits to see who enters credentials

Hacker uses stolen credentials to access sensitive data

Password Spray

A threat actor identifies valid usernames against various online services. From there, the threat actor attempts common passwords against the usernames, aiming for multiple successful logins across various accounts and online services.

Hacker gathers a list of commonly-used passwords

Hacker tries the same common password across multiple accounts

Once a login is successful, hacker harvests the sensitive data

Credential Stuffing

A threat actor acquires credentials from a breach/password dump site (targeted attack on specific uses). The threat actor then (usually) uses automated tools to test credentials across different sites. Once a successful login occurs, the threat actor can execute the next stage of attack.

Hacker acquires credentials from website breach or password dump site

Hacker uses automated tools to test credentials across different sites

When a successful login occurs, hacker executes next stage of attack

Brute Force Attacks

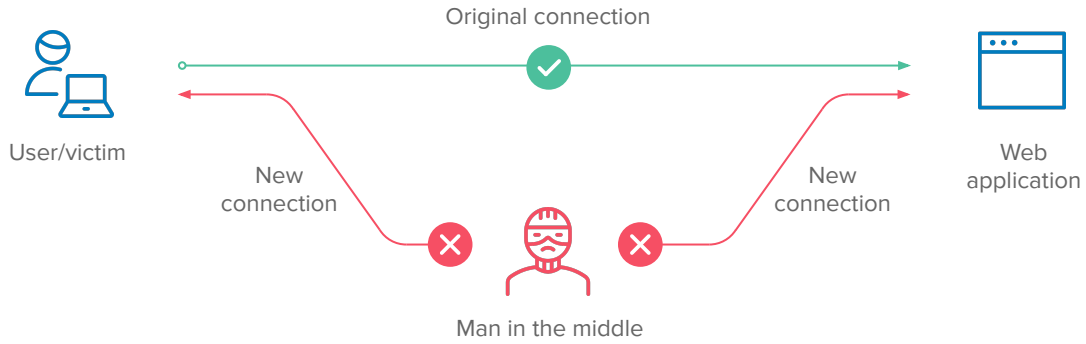
A threat actor uses the trial-and-error method to take over accounts. Brute force attacks are typically slow (and can be ongoing), with the final goal being takeover of a large number of accounts. Brute force attacks typically do not involve a specific strategy, threat actors simply use automation to attempt different password combinations until they find one that works. Brute force attacks can also include dictionary attacks, where a threat actor guesses passwords by entering common words and phrases - in some cases, every word in the dictionary. The hacker validates some of the username and password combinations which are identified by the brute force tool, and uses these credentials to carry out the next phase of attack.

```
[80] [http-get-form] host: 192.168.100.155  login: james password: password
[80] [http-get-form] host: 192.168.100.155  login: john password: p@ssword
[80] [http-get-form] host: 192.168.100.155  login: robert password: 12345
[80] [http-get-form] host: 192.168.100.155  login: david password: 1234567890
[80] [http-get-form] host: 192.168.100.155  login: brian password: 123456
[80] [http-get-form] host: 192.168.100.155  login: steven password: 1234567
[80] [http-get-form] host: 192.168.100.155  login: kevin password: 1q2w3e4r

1 of 1 target successfully completed, 12 valid passwords found
```

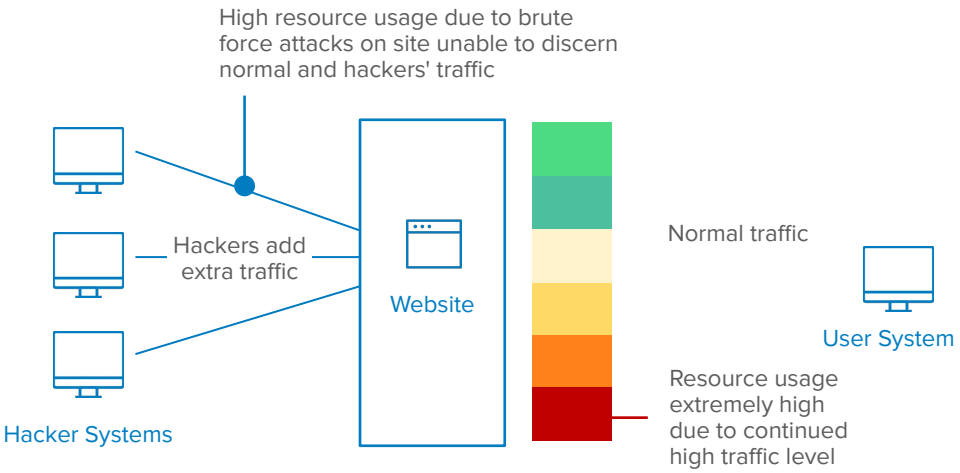
Man-in-the-middle

A highly targeted attack which can result in a full take of credentials and data-in-transit. A threat actor first intercepts a network connection that compromises a user's web session. For skilled attackers, this can be done easily on public wifi connections. Or, take Evilginx for example, an attack framework for setting up phishing pages and capturing all data being transmitted between a user and a legitimate website. If data is encrypted, the threat actor may attempt to decrypt it by tricking the user into installing a malicious certificate. From there, the threat actor will attempt to hijack the user session before initial authentication by stealing credentials, as the threat actor monitors all user inputs. Alternatively, the threat actor may steal a session token after authentication, and is able to authenticate into the account and execute the next state of the attack.



DDoS (Distributed Denial-of-Service)

This type of attack is slightly different from the previously mentioned attacks as the primary goal for the threat actor is to disrupt a web service, while the aforementioned attacks are focused on account takeover. However, the method of attack is very similar (in some cases, the exact same) as a brute force attack. A threat actor uses and/or develops automated tools to generate a large number of guesses with various username and password combinations. Many times, this causes high resource usage on the web application, causing it to become unusable. Automated DDos and brute force attacks continue to rise - in 2019, bad bot traffic comprised 24.1% of all website traffic.



Concerns related to identity attacks

The concerns that enterprises have today as a result of the aforementioned identity attacks are typically -

Account takeover

The primary goal of these identity attacks is for the threat actor to steal some form of data or personal information/ assets - whether it is confidential business information, bank account details, credit card info etc, when a threat actor is able to take over an account, they have full access to execute the next stage(s) of the attack. The aforementioned identity attacks continue to be successful because users use the same password on multiple applications (both corporate and personal), many users are not able to identify phishing emails, and, ultimately, the numbers are in the threat actor's favor as many users choose to set common passwords on their account. Furthermore, multi-factor authentication, a critical security measure, is not always enabled by default. In fact, a survey conducted by Ponemon tells us that 67% of respondents do not use any form of two-factor authentication on their personal accounts. And, the same study tells us that 55% of employees do not use multi-factor authentication at work.

Account lockout

End user experience has always been critical for customer and consumer use cases, and more recently, the demand for consumer-like experiences when accessing corporate apps has made end user experience important for the workforce as well. Some attacks targeting passwords cause account lockout when multiple incorrect username and password combinations are attempted - specifically DDoS and brute force attacks, and, in some cases, password spray attacks. Many times, consumer applications automatically lock users out of their account for a set number of minutes/hours after a large number of failed login attempts. Enterprise-ready authentication providers also provide soft lockout settings which will lock a user out of their account for a specified period of time after a number of failed login attempts, as defined by the administrator. While these protections aim to prevent threat actors from taking over an account, in most cases the legitimate user is also locked out, which impacts end user experience.

67%

of respondents do not use any form of two-factor authentication on their personal accounts

55%

of employees do not use multi-factor authentication at work

Organizations can employ a variety of security measures to help protect against these common password attacks. In this document, we focus on a baseline security feature in the Okta Identity Cloud, Okta ThreatInsight, which specifically helps to prevent account takeover and account lockout due to large identity attacks targeting passwords.

Introducing Okta ThreatInsight

A feature powered by the Okta Insights platform service, ThreatInsight is Okta's approach to protect organizations against large scale identity attacks, especially attacks which target passwords. With ThreatInsight, customers can take advantage of the global network intelligence driven by Okta's network effect.

Okta ThreatInsight is a component of Okta's risk engine and security intelligence, in which login patterns are analyzed to then enable secure access decisions. When Okta identifies large-scale identity attacks such as DDoS and password spray across all customers, those IPs are added to the ThreatInsight database. Organizations can then choose to block access from those IP addresses. Okta ThreatInsight allows you to secure your business before you're the victim of an identity attack.

How Okta ThreatInsight fits into the sequence of authentication policies

Authentication policies in Okta can generally be categorized into the following steps -

1

Edge/Infrastructure (global router level for all customers)

Okta's security detection and response team monitors for and takes action against threats and suspicious activity across its ecosystem of thousands of customers and partners. Along with a range of security controls across encryption, tenant data security, network segregation and security and more, known malicious IPs are placed in a blocklist at the edge layer, blocking access from these IPs to any Okta tenant. More detail on the many security precautions built into Okta are explained in the whitepaper here.

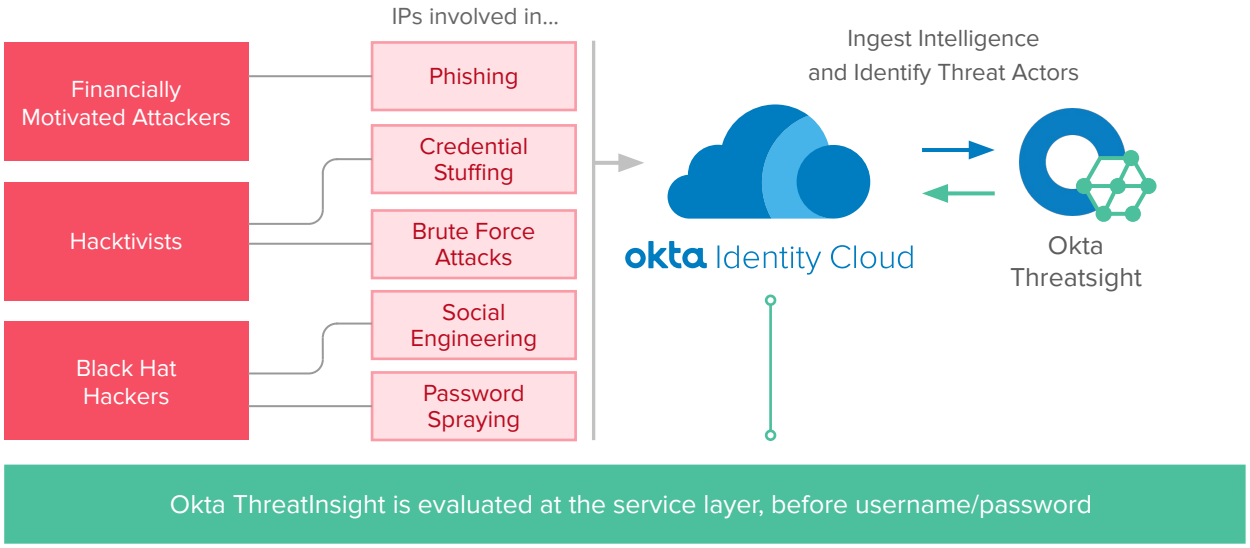
2

Okta ThreatInsight

For every known malicious IP blocked at the edge layer, Okta sees many more suspicious events coming from IP addresses that cannot be confirmed malicious with 100% certainty. There could be a legitimate use case for multiple failed logins depending on the scenario, such as when a hotel hosts a large conference. In these scenarios, it isn't unreasonable to have dozens, hundreds or even thousands of login failures across multiple accounts in multiple Okta orgs, all of which appear to come from the same source (i.e. the hotel's network). Blocking those IP addresses could actually block legitimate authentication attempts, which would ultimately be just as bad as falling victim to a DDoS attack.

This is where Okta ThreatInsight comes into play; suspicious IP addresses are defined as IPs involved in identity attacks across Okta's full customer base. This means that even if a suspicious IP address has not attempted to access your org, if Okta has seen it involved in an identity attack on another customer, it will automatically be added to the ThreatInsight database. Access from that IP will then be blocked on any Okta org which has set ThreatInsight to run in block mode. Alternatively, administrators can choose to just log access from IPs identified by ThreatInsight and review data in Okta's Syslog. .

In case of false positives, administrators can identify certain IPs to be exempt from the Okta ThreatInsight check. Suspicious IP addresses are identified based on logins across Okta's customer base. Okta ThreatInsight is evaluated on a rolling window, and suspicious IP addresses which stop exhibiting suspicious activity by the next evaluation will be removed from the ThreatInsight database. Okta ThreatInsight is evaluated before any other policy checks, including evaluation of username.



3

Pre-Authentication

Geolocation and other network based policies defined at the org level are evaluated prior to evaluating a user's password. This helps avoid account lockout for legitimate users.

4

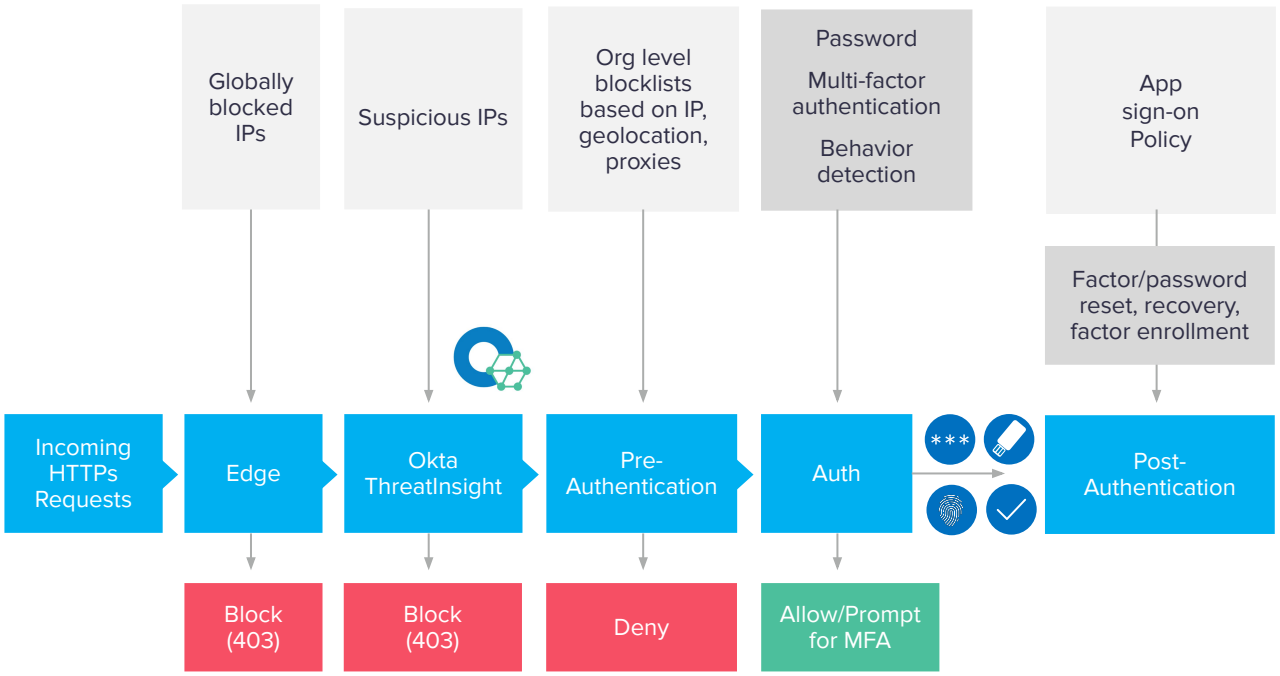
Authentication

This includes password verification, prompting the user for multi-factor authentication (if enabled), and validation of the factor.

5

Post-Authentication

This includes app-specific policies such as Device Trust.



Why is Okta ThreatInsight an important security measure?

Earlier in the whitepaper, we outlined customer concerns around account takeover and account lockout. Okta ThreatInsight helps organizations protect against these concerns.

Prevent account takeover

When ThreatInsight is enabled in block mode, any access attempt to Okta from a suspicious IP will be blocked. This means IP addresses involved in known brute force attacks, password spray etc. will be automatically blocked from accessing Okta, regardless of the username initiating the login. Automatically blocking suspicious IPs that have caused login failures across the Okta network means reduced likelihood of a threat actor taking over a user's account in an org with ThreatInsight enabled in block mode.

> **Sample use case:**
>
> A consumer ticketing app sees an increase in threat actors compromising user accounts to purchase tickets for large concerts and sporting events. Upon further investigation, it looks like a common set of 20-50 rotating IP addresses are causing failed logins amongst the user base. By enabling ThreatInsight, the ticketing app can reduce account takeover attempts, and also use Syslog to track these IPs.

Prevent account lockouts

This is critical in preserving end user experience. Because ThreatInsight only blocks access to Okta from IPs identified as suspicious, legitimate users will still be able to log into their account. When ThreatInsight is blocking suspicious IP addresses, login attempts from suspicious IPs do not count towards a user's login attempts. This means that legitimate users accessing Okta from a known device will still be able to access their account.

> **Sample use case:**
>
> A large manufacturing organization which employs 50,000+ employees is in the process of modernizing their applications, but still has thousands of users accessing Office 365 via legacy email clients that do not support modern auth or multi-factor authentication. Therefore, the organization cannot completely turn off access from the Office 365 legacy endpoint. Because of these security deficiencies, attackers attempt to take over user accounts through the Office 365 legacy app, which in turn locks out hundreds of users each day - even if they are not logging into Office 365 legacy apps. This becomes overwhelming for IT as helpdesk tickets are never-ending. By enabling ThreatInsight, the organization is able to drastically reduce the number of users being locked out due to the Office 365 legacy endpoint.

Okta ThreatInsight - Tech Details

What specific attack types does ThreatInsight capture?

Okta ThreatInsight captures the following categories of identity attacks -

- Password Spray
- Brute Force

How does Okta ThreatInsight define a suspicious IP address?

The section below provides an examples of how Okta defines thresholds for suspicious IP addresses (specific threshold numbers have been obfuscated):

Brute force detection

In the last X hours, Okta identifies a Y% failure rate for all logins originated from an IP address/set of IP addresses*

**IP address must cause at least Z # of failed logins*

Password spray detection

Sequence of events

- In the last X hours, if Okta identifies an IP address using the same password with at least Y # of different usernames, where all login attempts failed, a password spray event is logged

  In this scenario, all failed logins attempts with the same IP address + password combination after the first Z # of logins automatically generates a password spray event

- Then, If X% of all login attempts from the IP are marked with a password spray event → mark as suspicious and add to Okta ThreatInsight database

How frequently does Okta ThreatInsight check for suspicious IP Addresses?

Okta ThreatInsight is evaluated on a rolling window. Each time Okta receives new login data about an IP address, Okta will check for login behavior during this rolling window to place the IP in the ThreatInsight database, or remove the IP from the ThreatInsight database.

What is the difference between Log Mode vs Block Mode?

- **Log mode**
  Okta's syslog captures suspicious IP addresses attempting to access an Okta org, but no action is taken when a suspicious IP attempts to access the org. Administrators can view these login attempts in Syslog.
- **Block mode**
  Access from any suspicious IP is automatically blocked (unless the IP has been added to the list of exempt IPs.

Which Okta endpoints does ThreatInsight secure?

- **Modern Auth**

```
/api/v1/authn
```

- **O365**

```
/app/office365/{key}/sso/wsfed/active
```

```
/app/office365/{key}/sso/wsfed/passive
```

Getting Started - Recommendations

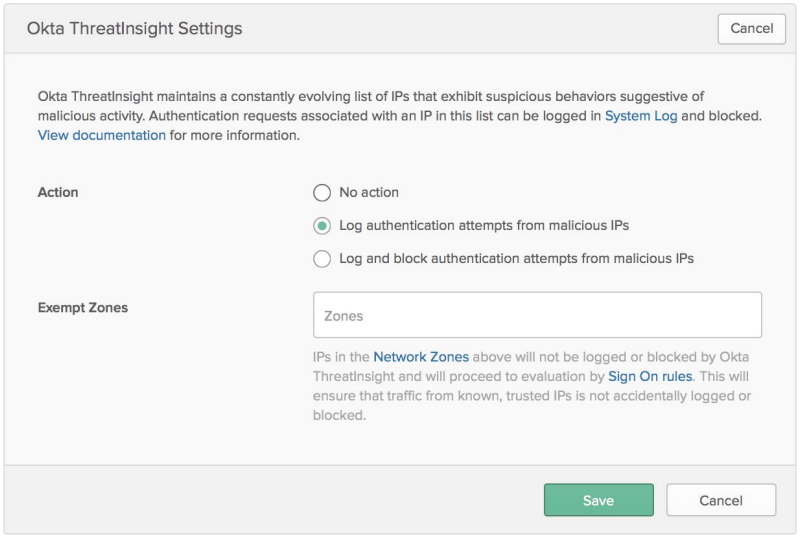
Okta ThreatInsight is available for all Okta customers. Recommendations on enabling the feature are included below.

Enabling ThreatInsight in Log or Block mode

Follow these steps to setup ThreatInsight:

1. Under Security - General, there is a section for Okta ThreatInsight Settings with the following choices:

Action name	Description
No action	Okta ThreatInsight will not check for any suspicious IPs.
Log authentication attempts from malicious IPs	Only log suspicious IPs in Syslog, but do not block access from these IPs
Log and block authentication attempts from malicious IPs	Log and block access from suspicious IPs



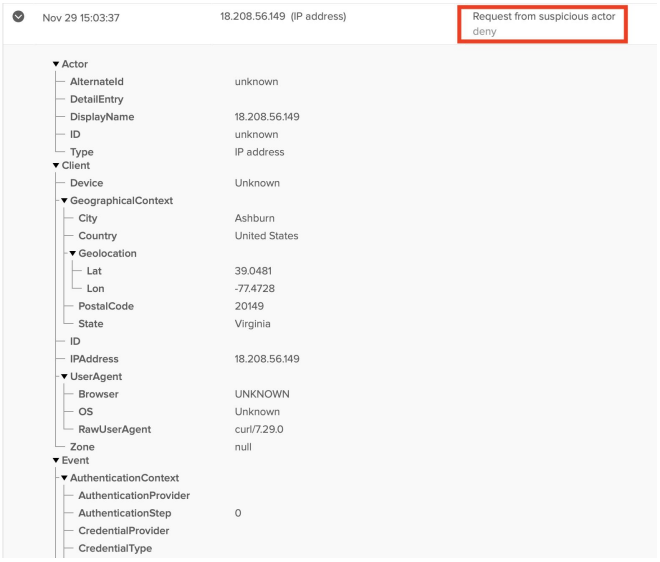
This is the only setup required for administrators.

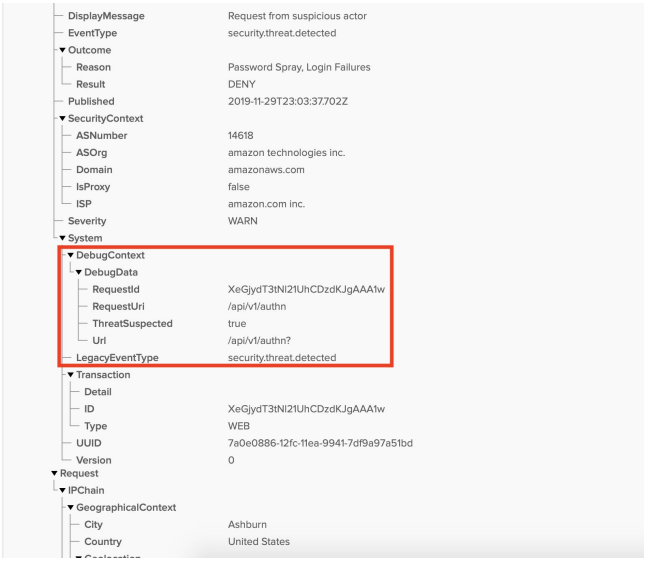
Review access from suspicious IP addresses in Syslog

When ThreatInsight is enabled on an org, requests from suspicious IP addresses will be logged in Syslog. This is true whether ThreatInsight is enabled in log or block mode.

Check for the following events in Syslog

- Request from suspicious actor
- security.threat.detected



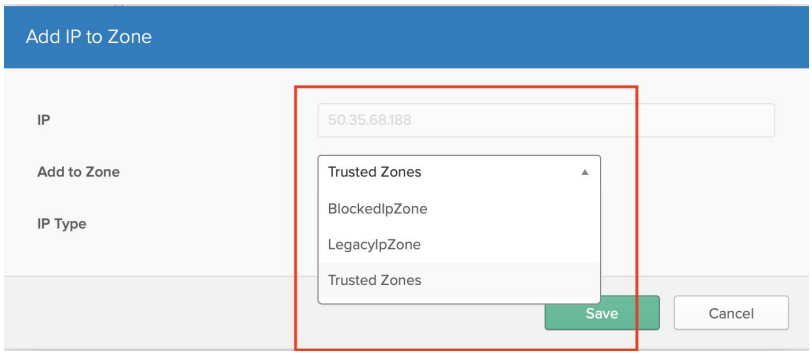


Additional setup guidance

1

Add IP Addresses to exempt zones

In case of false positives, IP Addresses can be added to the ThreatInsight exempt list. IP Addresses can be added to known/trusted network zones directly from Syslog.



2

Export Okta ThreatInsight events to SIEM tools

To export ThreatInsight events to SIEM tools and other security tools which can ingest data from Okta's API, query the following event -

```
security.threat.detected
```

More details on Okta ThreatInsight can be found in the documentation here.

**Okta ThreatInsight is just one tool in the security toolbox. It cannot guarantee 100% malicious IP address detection or 100% threat detection. Okta ThreatInsight covers and blocks certain malicious traffic to the following endpoints – api/v1/authn, app/office365/{key}/sso/wsfed/active, and wsfed/passive. Please note, per our Master Subscription Agreement, endpoints are considered Free Trial Services.*

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud connects and protects employees of many of the world's largest enterprises. It also securely connects enterprises to their partners, suppliers and customers. With deep integrations to over 6,500 applications, the Okta Identity Cloud enables simple and secure access for any user from any device.

Thousands of customers, including 20th Century Fox, Adobe, Dish Networks, Experian, Flex, LinkedIn, and News Corp, trust Okta to help them work faster, boost revenue and stay secure. Okta helps customers fulfill their missions faster by making it safe and easy to use the technologies they need to do their most significant work.

Learn more at: www.okta.com