



**Boosting  
human  
capabilities**

Cybersecurity  
Rpa consulting  
Infrastructures & Cloud  
Digital Solutions

[avalora.com](https://avalora.com)

Madrid  
Stgo  
Lima



# **IntSights + Active Directory:**

*Automatically Validate and Lock Down Leaked  
Credentials with AD Integration*





# Meet The Team



**Juan Carlos Marín**

SE Manager para América Latina



**Manuela Jaramillo**

Comercial para América Latina



# Agenda

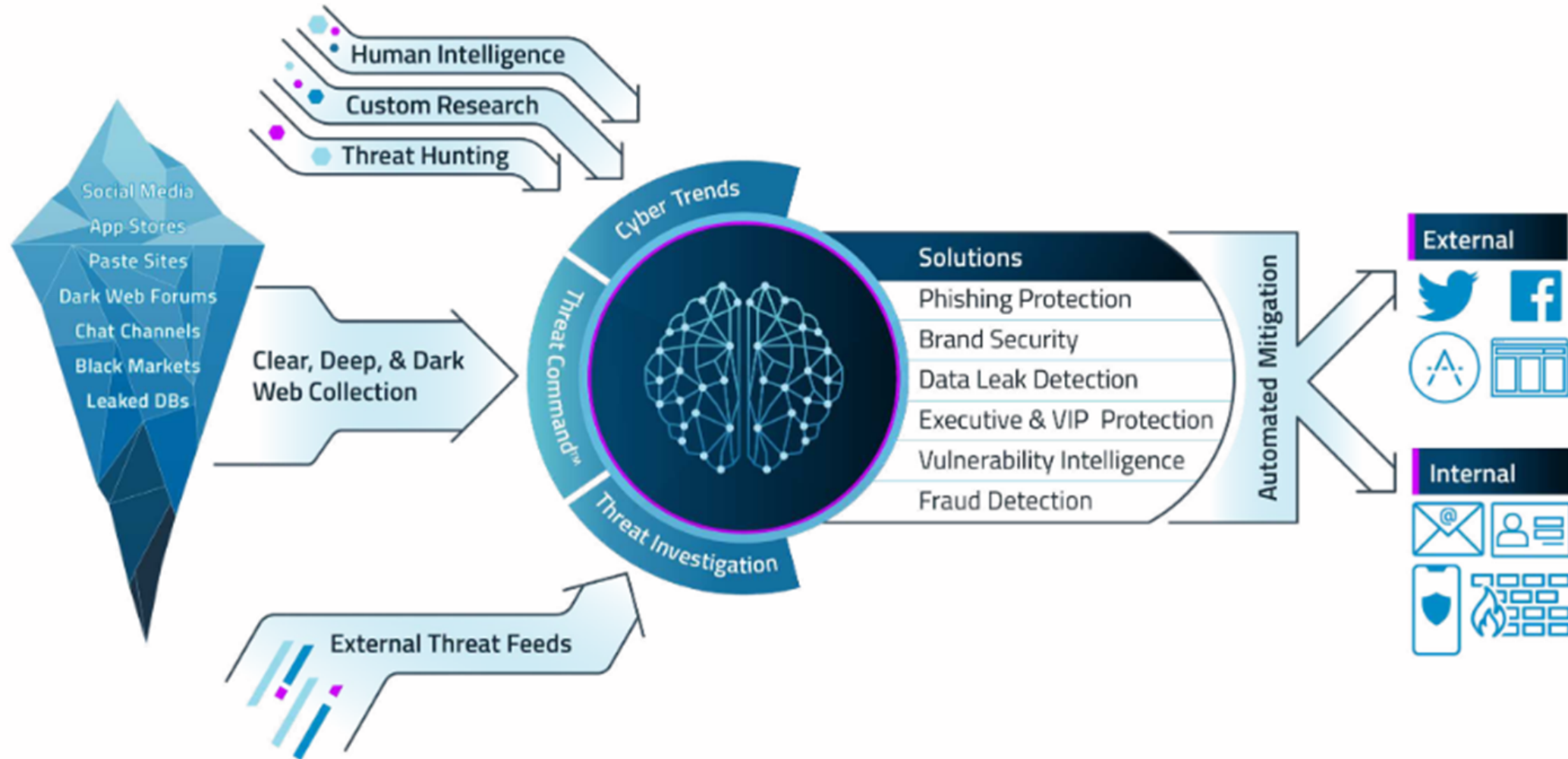
- IntSights Overview
- IntSights Active Directory Integration
  - Overview and Benefits
- Customer Use Case
- Q&A



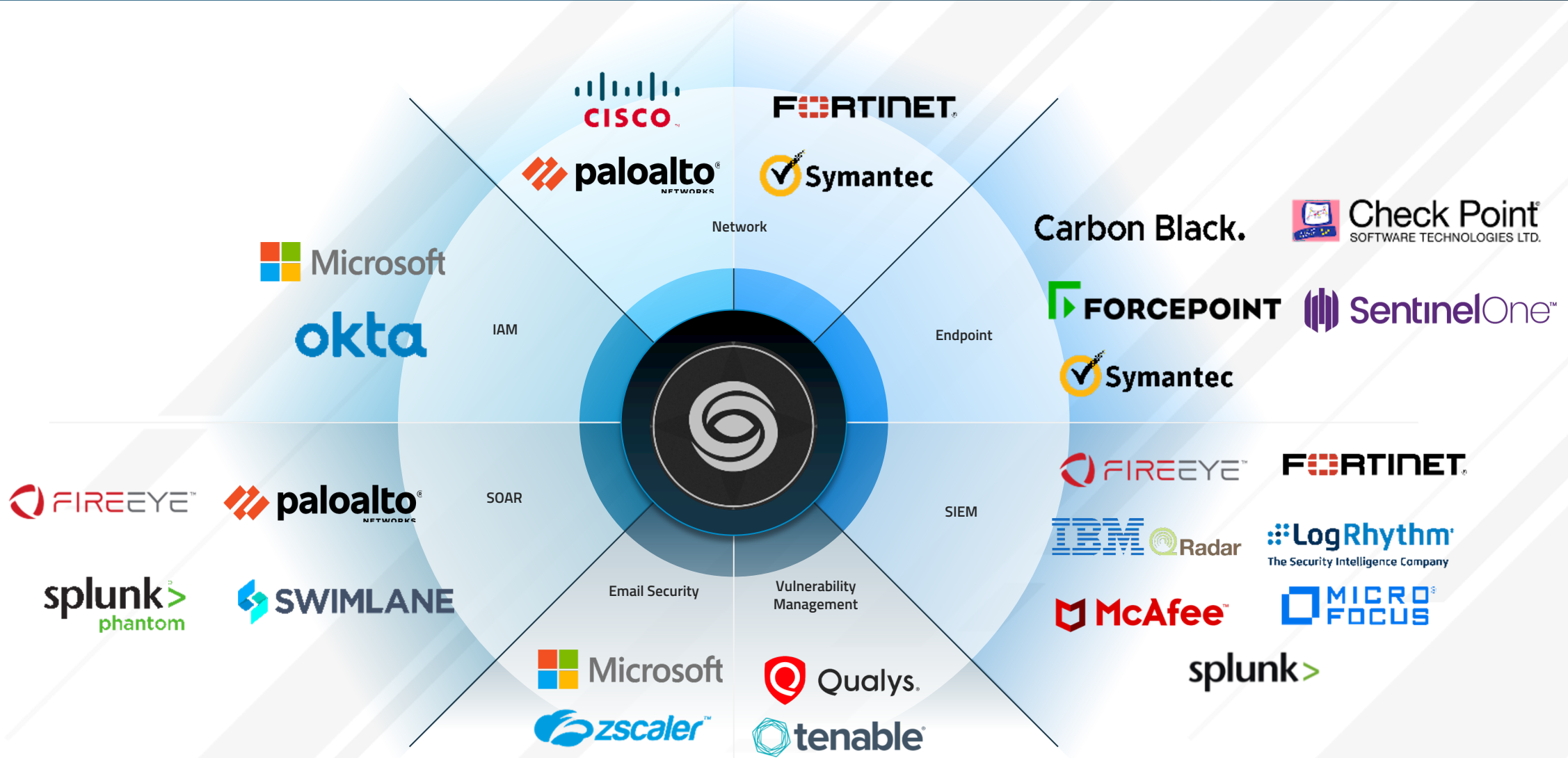


# IntSights Overview

# The IntSights Advantage



# Plug & Play Into Your Existing Infrastructure





# Challenges and the IntSights Solution

- Credential leakage is one of the most popular and successful attack methods used by cyber-criminals to exploit users and breach enterprise organizations due to the commonality of employees re-using passwords from Microsoft Office accounts and their personal online services.
- IntSights discovers leaked credentials from continuous surface, deep and dark web scanning of forums, chat rooms, GitHub, paste sites, leaked databases and more.
- IntSights provides automated notifications security teams about potential credential leakage with instructions for immediate password change and other remediation actions

Username	Email	Password
dan	dan	5:secure. whitepages.com:9F840EA6E04 B22541
anna_	anna_	secur e.whitepages.com:DEF6EC192 37202C11
stacy	stacy	:secur e.whitepages.com:DED686393 7FD1DE41
stacy	stacy	:www. whitepages.com:0645FE59D8C 00A264
tom	tom	:secur e.whitepages.com:EDD913E5B A52F9621
robert	robert	secur e.whitepages.com:2CD2BEAD C6368D281
robert	robert	:www. whitepages.com:6DAECE7DA 5802884
sue	sue	secur e.whitepages.com:8EF60451C 7A816201
yaneke	yanek	:secure. whitepages.com:371F12B58A6 83C981



## 171% Increase in Compromised Employee Credentials

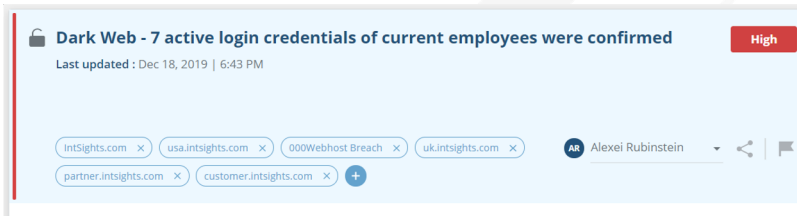




# IntSights Active Directory Integration

# How It Works

## Real-Time Credential Leakage Alerting



## Contextual Actionable Intelligence

1 The leak exposed 8 users, total. 4 users were active, of which 3 had a valid password in the Active Directory.

Description

Dark Web - Login credentials of 8 employees were leaked from 000Webhost, after verification in Active Directory it was found that 7 login credentials are of active accounts and 3 of them have been confirmed as active users with valid passwords.

Recommendations:

It is recommended to update the active directory integration policy to automatically disable active accounts with valid passwords. It is also recommended to advise all the employees not to use their corporate emails or passwords in third party services.

Ask an analyst

Email	Email Status	Password	Password Status	AD Domain
jimp@intsights.com	Active	ullah12	Active	intsights.com
benda@intsights.com	Active	kabul.one	Active	intsights.com
david@intsights.com	Active	j10839	Active	intsights.com
alexai@intsights.com	Active	metallica123	Inactive	usa.intsights.com
mark@intsights.com	Active	sammy321	Inactive	usa.intsights.com
briani@intsights.com	Active	iloveintsights	Inactive	uk.intsights.com
brendac@intsights.com	Active	redcorvette	Inactive	partner.intsights.com
pault@intsights.com	Inactive	04051992qaz	Unknown	customer.intsights.com



## Active Directory Automated Remediation

- Confirm that employee is indeed active on the environment
- If yes, initiate password verification
- If password is verified for active account, proactively block user and alert system administrator
- Lock account or force password change upon next login



# Real-Time Credential Leakage Detection & Alerting

## Continuously monitor and detect early signs of leaked credentials including:

- Paste sites
- Dark web and hacking forums
- File sharing websites
- Code repositories

## In the last 6 months alone, IntSights discovered more than 2,000 leaks

- The leaks contain 10,000+ leaked user accounts



# Policies & Automated Remediation

- **Automated Alerting (on every detected leak)**
- **Real-Time Validation**
  - Validate user existence in your AD on-prem and cloud.
  - Once user is validated, perform a password check to validate if the leak matches an active user with valid credentials.
- **Proactive Remediation**
  - Automatically disable user login.
  - Require password change upon next user login.





# Data Leakage Policy Example

Data Leakage Rules List


Rule name		Matched alerts	
Inactive Account		114	
<div><div>Threat profile</div><div>Type: Credentials Leakage</div><div>Severity: High Medium Low</div></div>	<div><div>Internal remediation</div><div>Leaked accounts</div></div>	<div><div>External remediation</div></div>	<div><div>Action</div><div></div><div></div></div>
Active User \ Valid Password		0	
<div><div>Threat profile</div><div>Type: Credentials Leakage</div><div>Severity: High Medium Low</div></div>	<div><div>Internal remediation</div><div>Leaked accounts Leaked passwords</div></div>	<div><div>External remediation</div></div>	<div><div>Action</div><div></div><div></div></div>
Active User \ Invalid Password		60	
<div><div>Threat profile</div><div>Type: Credentials Leakage</div><div>Severity: High Medium Low</div></div>	<div><div>Internal remediation</div><div>Leaked accounts Leaked passwords</div></div>	<div><div>External remediation</div></div>	<div><div>Action</div><div></div><div></div></div>

</








# Context-Rich Actionable Intelligence


- Real-time contextual alerts
- Organization-specific credential leakage alerts

 **Dark Web - 19 login credentials including encrypted passwords of employees were leaked** Medium

Last updated : Feb 26, 2020 | 12:01 AM

ActiveUserInvalidPassword  

unassigned   

 The leak exposed 19 users, total. 8 users were active, of which 0 had a valid password in the Active Directory. Download CSV

**Description**

Dark Web - Login credentials of 19 employees were leaked from Avvo (Full leak). The leak includes usernames and passwords that are most likely encrypted. They might be used to infiltrate the company's systems.

Username	Email	Password	Role
john.doe@avvo.com	john.doe@avvo.com	1234567890	Admin
jane.smith@avvo.com	jane.smith@avvo.com	9876543210	Admin
john.doe@avvo.com	john.doe@avvo.com	1234567890	Admin
jane.smith@avvo.com	jane.smith@avvo.com	9876543210	Admin
john.doe@avvo.com	john.doe@avvo.com	1234567890	Admin
jane.smith@avvo.com	jane.smith@avvo.com	9876543210	Admin
john.doe@avvo.com	john.doe@avvo.com	1234567890	Admin
jane.smith@avvo.com	jane.smith@avvo.com	9876543210	Admin
john.doe@avvo.com	john.doe@avvo.com	1234567890	Admin
jane.smith@avvo.com	jane.smith@avvo.com	9876543210	Admin
john.doe@avvo.com	john.doe@avvo.com	1234567890	Admin
jane.smith@avvo.com	jane.smith@avvo.com	9876543210	Admin
john.doe@avvo.com	john.doe@avvo.com	1234567890	Admin
jane.smith@avvo.com	jane.smith@avvo.com	9876543210	Admin
john.doe@avvo.com	john.doe@avvo.com	1234567890	Admin
jane.smith@avvo.com	jane.smith@avvo.com	9876543210	Admin
john.doe@avvo.com	john.doe@avvo.com	1234567890	Admin
jane.smith@avvo.com	jane.smith@avvo.com	9876543210	Admin
john.doe@avvo.com	john.doe@avvo.com	1234567890	Admin
jane.smith@avvo.com	jane.smith@avvo.com	9876543210	Admin

**Recommendations**

- It is recommended to change the passwords of the affected accounts.
- It is also recommended to advise all the employees not to use their corporate emails in third party services.

Ask an analyst Close alert



# Customer Use Case Introduction

**Leveraging IntSights, Ulta was able to achieve demonstrable enhancements in system manageability, ease of use, direct impact on ROI, and bottom-line efficacy including:**

- Real-time visibility and control of potential leaked credentials
- Ability to lock down users (require immediate PW change)
- Dramatic time and cost savings, and a measurable impact on bottom line





# Customer Use Case

# First Things First



The first rule of any technology used in a business is that automation applied to an efficient operation will magnify the efficiency.

The second is that automation applied to an inefficient operation will magnify the inefficiency...

Bill Gates





# The Good, The Bad, and The Ugly...

## — The Good...

- High productivity through efficiency and proper alerting
- Takes pressure off “alert fatigue” and backlog
- **Automation + Good Process = Efficiency**

## — The Bad...

- You may miss large breaches if these are not reviewed each week
  - Monitor these events in the dashboard
- Increase in tickets and calls to your Service Desk or End User Services
- **Automation + Lack of Process = No Efficiency**

## — The Ugly...

- Typically not from misuse, but rather neglect
- Ignoring potential due to lack of knowledge of the platform
  - Challenge your account managers to help you
- Not knowing when to “pull the plug”
  - Failure is ok



# Ultra Use Case – Implementation

**INTEGRATIONS**

**On-Premises** Cloud

Devices 2

Search

Microsoft Active Directory

**Microsoft Active Directory**  
Microsoft Active Directory

☒ Password policy validation

IntSights will first validate if the leaked password satisfies the domain password policy. If it does not, it will not be checked against the Active Directory password of the affected user, thus reducing the number of passwords to be checked.

**Login attempts rate limit**

Less than 10 logins per minute might cause leaked account validation longer to complete in the case of many leaked accounts.

30 logins per minute

Save



# Ultra Use Case – Implementation

The screenshot displays the 'POLICY' configuration page in the Ultra interface. On the left sidebar, the 'Data Leakage' policy is selected and highlighted with an orange box. An orange arrow points from this policy to the main content area. The main content area shows a 'Data Leakage Rules List' with three rules. Each rule entry includes a 'Rule name', 'Matched alerts' count (highlighted with a pink box), 'Threat profile', 'Internal remediation', 'External remediation', and 'Action' options. A pink arrow points from the '48' matched alerts for the first rule to the '10' matched alerts for the second rule, with the text 'Audit These' next to it.

**POLICY**

Global

- All Threat Types 0
- Threat Command
  - Phishing 3
  - Data Leakage 3**
  - Brand Security 2
  - Attack Indication 2
  - Exploitable Data 0
- IOC Management
  - IOC 3

**Data Leakage Rules List**

Rule name	Matched alerts	Threat profile	Internal remediation	External remediation	Action
AD - Active User Account - NO	48	Type: Credentials Leakage Severity: High, Medium, Low	Leaked accounts		Envelope, Tag
AD - Active User Account - YES	10	Type: Credentials Leakage Severity: High, Low, Medium	Leaked accounts, Leaked passwords		Envelope, Warning
AD - Active User Account - YES, Password is Valid - YES	0	Type: Credentials Leakage Severity: High, Medium, Low	Leaked accounts, Leaked passwords		Envelope

**Audit These**

**AVALORA**

# Ultra Use Case – Focus on Efficiency and Speed

**POLICY**

Global

- All Threat Types 0
- Threat Command
- Phishing 3
- Data Leakage 3**
- Brand Security 2
- Attack Indication 2
- Exploitable Data 0

IOC Management

- IOC 3

**Data Leakage Rules List**

Rule name	Matched alerts
AD - Active User Account - NO	48
AD - Active User Account - YES	10
AD - Active User Account - YES, Password Valid - YES	0

**Matched alerts: 10**

Last Day Last Week Last Month

Title	Source URL	Date
1 login credentials including clear text password o...	https://anonfile.com/Zfh1...	<a href="#">Go to alert</a>
VIP - 1 login credentials including encrypted passw...		<a href="#">Go to alert</a>
Dark Web - 15 login credentials including encrypte...		<a href="#">Go to alert</a>
VIP - 1 login credentials including encrypted passw...		<a href="#">Go to alert</a>
Dark Web - 1 login credentials including encrypted...		<a href="#">Go to alert</a>
Dark Web - 12 login credentials including encrypte...		<a href="#">Go to alert</a>
Dark Web - 4 login credentials including encrypted...		<a href="#">Go to alert</a>
Dark Web - 45 login credentials including encrypte...		<a href="#">Go to alert</a>
Dark Web - 4 login credentials including encrypted...		<a href="#">Go to alert</a>
1 login credentials including clear text password o...		<a href="#">Go to alert</a>

< 1 >



# Ultra Use Case – Real-World Example

**Dark Web - 2 login credentials including clear text passwords of employees were leaked**

Last updated : Nov 11, 2019 | 10:29 AM

Source date : Jun 30, 2018 | 7:00 PM

Low

The leak exposed 2 users, total. 1 user was active, of which 0 had a valid password in the Active Directory.

Download CSV

**Description**

Dark Web - Login **credentials** of 2 employees were leaked from **Shein**. They might be used to infiltrate the company's systems.

Username	Email	Password	Raw

**Recommendations**

- It is recommended to change the passwords of the affected accounts.
- It is also recommended to advise all the employees not to use their corporate emails in third party services.





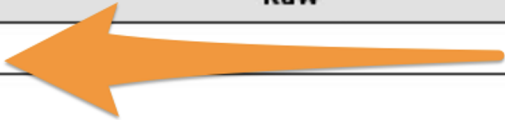
# Ultra Use Case – Real-World Example

! The leak exposed 2 users, total. 1 user was active, of which 0 had a valid password in the Active Directory. [Download CSV](#)

### Description

Dark Web - Login credentials of 2 employees were leaked from Shein. They might be used to access internal systems.

Username	Email	Password	Raw
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]



**Pop Out for Quick Review**

Username	Email	Password	Raw
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

### Recommendations

- It is recommended to change the passwords of the affected accounts.
- It is also recommended to advise all the employees not to use their corporate emails in third party services.



# Ultra Use Case – Real-World Example

ALERTS

9 All 7 High 1 Medium 1 Low

Dark Web - 2 login credentials including clear text passwords of...

10 login credentials including clear text passwords of employees...

Dark Web - 46 login credentials including encrypted passwords of...

Dark Web - 77 login credentials including clear text passwords of...

Dark Web - 39 login credentials including clear text passwords of...

Dark Web - 18 login credentials including clear text passwords of...

Dark Web - 226 login

Dark Web - 2 login credentials including clear text passwords of employees were leaked

Low

Last updated : Source date :

The leak exposed 2 users, total 1

Download CSV

Description

Dark Web - Login credentials of 2 employees were leaked from Shein. They might be used to infiltrate the company's systems.

UsernameEmailPasswordRaw

Recommendations

It is recommended to change the passwords of the affected accounts.

It is also recommended to advise all the employees not to use their corporate emails in third party services.

Ask an analyst

Reopen

In June 2018, online fashion retailer SHEIN suffered a data breach. The company discovered the breach 2 months later in August then disclosed the incident another month after that. A total of 39 million unique email addresses were found in the breach alongside MD5 password hashes.

Hover Over For Quick Access to Breach Data

© 2020 IntSights. Reproduction Prohibited

AVALORA

# Customer-Specific Benefits

- **We leverage IntSights to deliver increased visibility and continuous monitoring for:**
  - Forums, chat rooms, and social media platforms to identify potential credential leaks
- **We consume and proactively address incoming alerts to mitigate credential leakage:**
  - Automatically disable user login
  - Force password reset and enforce password strength





# Q&A



# Thank You

Learn more about how IntSights can help  
you build a better cyber defense.

**[Request a demo](#)**