DATA SHEET

Exploit Intelligence

Accelerate remediation efforts by focusing on exploitable vulnerabilities in your attack surface

BENEFITS

Focus on the most impactful issues on your attack surface - those being actively exploited by attackers in the wild.

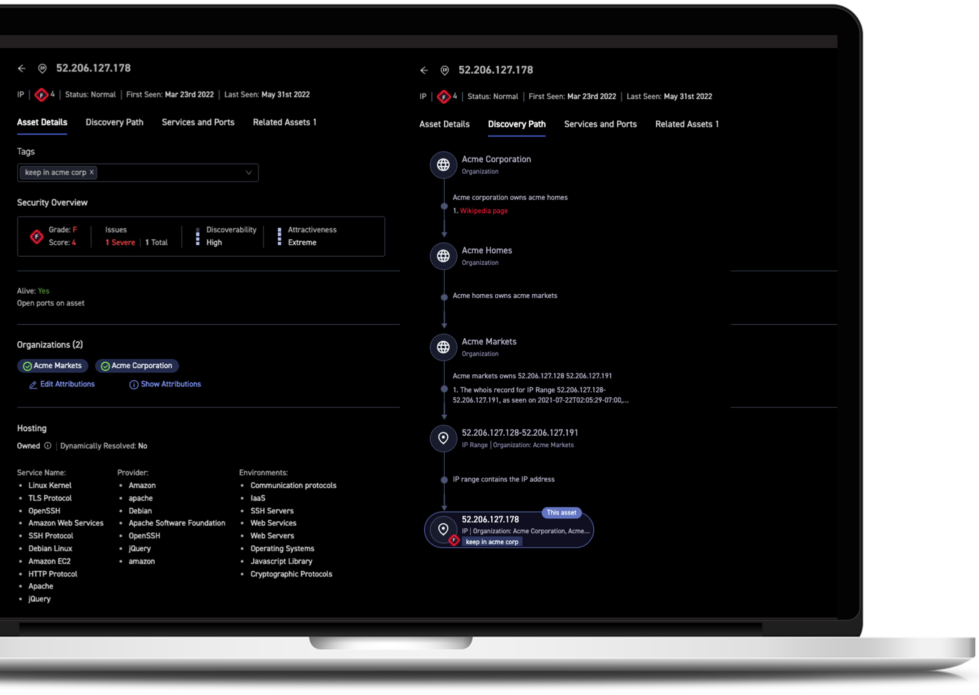
Easily and safely validate whether an issue in your attack surface is exploitable.

Understand what an attacker would do to exploit a weakness or vulnerability and the possible traces (IOCs) of an attack.

Safely simulate an attack while testing your defenses

CyCognito Exploit Intelligence offers an end-to-end solution that prioritizes which risks to remediate immediately—before they are exploited—by proactively discovering external assets, testing vulnerabilities, and providing expert threat- and risk-based insight.

Developed to help security teams focus on the most critical risks first, Exploit Intelligence creates in-platform advisories about threats being exploited in-the-wild and aligns them with assets in the organization's external attack surface. Operations teams can spend their time fixing issues instead of figuring out how to fix issues with our prescriptive and intelligent remediation guidance, supporting evidence and the ability to simulate the remediation in a virtual environment lab.



52.206.127.178

IP | F 4 | Status: Normal | First Seen: Mar 23rd 2022 | Last Seen: May 31st 2022

Asset Details | Discovery Path | Services and Ports | Related Assets 1

Tags

keep in acme corp ×

Security Overview

Grade: F | Score: 4 | Issues: 1 Severe | 1 Total | Discoverability: High | Attractiveness: Extreme

Alive: Yes

Open ports on asset

Organizations (2)

Acme Markets | Acme Corporation

Edit Attributions | Show Attributions

Hosting

Owned | Dynamically Resolved: No

Service Name:
- Linux Kernel
- TLS Protocol
- OpenSSH
- Amazon Web Services
- SSH Protocol
- Debian Linux
- Amazon EC2
- HTTP Protocol
- Apache
- jQuery

Provider:
- Amazon
- apache
- Debian
- Apache Software Foundation
- OpenSSH
- jQuery
- amazon

Environments:
- Communication protocols
- IaaS
- SSH Servers
- Web Services
- Web Servers
- Operating Systems
- Javascript Library
- Cryptographic Protocols

52.206.127.178

IP | F 4 | Status: Normal | First Seen: Mar 23rd 2022 | Last Seen: May 31st 2022

Asset Details | Discovery Path | Services and Ports | Related Assets 1

Acme Corporation
Organization

Acme corporation owns acme homes
1. Wikipedia page

Acme Homes
Organization

Acme homes owns acme markets

Acme Markets
Organization

Acme markets owns 52.206.127.128 52.206.127.191
1. The whois record for IP Range 52.206.127.128-52.206.127.191, as seen on 2021-07-22T02:05:29-07:00,...

52.206.127.128-52.206.127.191
IP Range | Organization: Acme Markets

IP range contains the IP address

This asset
52.206.127.178
IP | Organization: Acme Corporation, Acme...
F keep in acme corp

Exploit Intelligence in Action

The CyCognito platform's Exploit Intelligence capability gives teams all they need to swiftly respond to emerging threats in days, rather than weeks.

01. Time is of the essence

Adversaries consistently scan target networks for critical and high vulnerabilities within days of the vulnerability's public disclosure (source:joint advisory by NSA,CISA,FBI)

02. Be efficient

Leverage curated threat intelligence to show how vulnerabilities are being actively exploited by attackers in the wild and how those threats map to vulnerabilities in your attack surface.

03. Quickly Assess Impact

A detailed summary graph paints a clear picture of assets at risk and shows what subset of assets remain vulnerable and what subset are protected.

04. Know who to approach to remedy

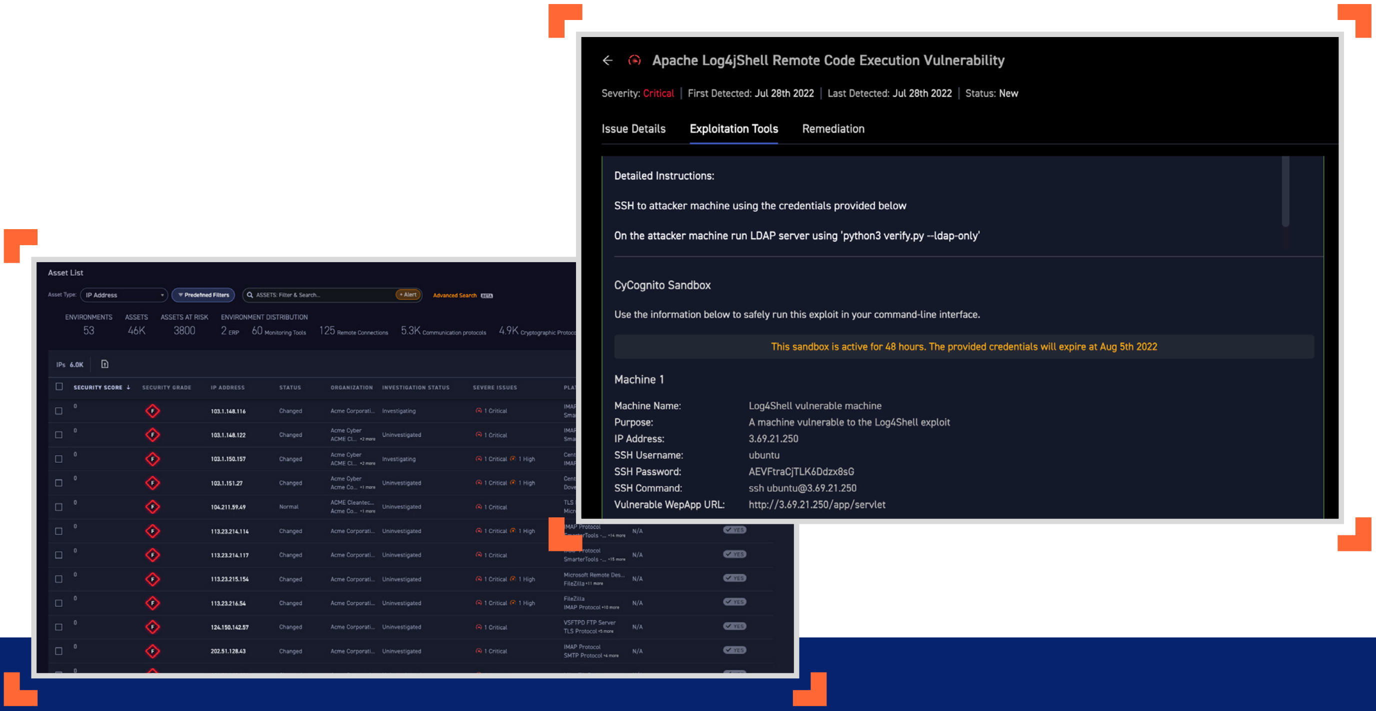
Receive evidence that identifies the organization responsible for remediating the vulnerability assets

05. Verify and Act With Confidence

Safely simulate the remediation with guidance in your CyCognito virtual lab before alerting the right Security Operations, Risk and IT teams.

06. Remediate and Repeat

Integrations provide remediation guidance and validation steps with SIEM/SOAR and ticketing tools, allowing for quicker MTTR. Once the issue has been remediated, CyCognito will validate that the vulnerability has been resolved.



Apache Log4jShell Remote Code Execution Vulnerability

Severity: Critical | First Detected: Jul 28th 2022 | Last Detected: Jul 28th 2022 | Status: New

Detailed Instructions:

SSH to attacker machine using the credentials provided below

On the attacker machine run LDAP server using 'python3 verify.py –ldap-only'

CyCognito Sandbox

Use the information below to safely run this exploit in your command-line interface.

This sandbox is active for 48 hours. The provided credentials will expire at Aug 5th 2022

Machine 1

Machine Name: Log4Shell vulnerable machine
Purpose: A machine vulnerable to the Log4Shell exploit
IP Address: 3.69.21.250
SSH Username: ubuntu
SSH Password: AEVFtraCjTLK6Ddzx8sG
SSH Command: ssh ubuntu@3.69.21.250
Vulnerable WepApp URL: http://3.69.21.250/app/servlet

Asset List

ENVIRONMENTS	ASSETS	ASSETS AT RISK	ENVIRONMENT DISTRIBUTION				
53	46K	3800	2 ERP	60 Monitoring Tools	125 Remote Connections	5.3K Communication protocols	4.9K Cryptographic Protoco

IPs 6.0K

☐	SECURITY SCORE ↓	SECURITY GRADE	IP ADDRESS	STATUS	ORGANIZATION	INVESTIGATION STATUS	SEVERE ISSUES	PLA		
☐	0	F	103.1.148.116	Changed	Acme Corporati...	Investigating	1 Critical	IMA Sma		
☐	0	F	103.1.148.122	Changed	Acme Cyber ACME Cl... +2 more	Uninvestigated	1 Critical	IMA Sma		
☐	0	F	103.1.150.157	Changed	Acme Cyber ACME Cl... +2 more	Investigating	1 Critical 1 High	Cent IMA		
☐	0	F	103.1.151.27	Changed	Acme Cyber Acme Co... +1 more	Uninvestigated	1 Critical 1 High	Cent Dove		
☐	0	F	104.211.59.49	Normal	ACME Cleantec... Acme Co... +1 more	Uninvestigated	1 Critical	TLS Micr		
☐	0	F	113.23.214.114	Changed	Acme Corporati...	Uninvestigated	1 Critical 1 High	IMAP Protocol SmarterTools -... +14 more	N/A	✓ YES
☐	0	F	113.23.214.117	Changed	Acme Corporati...	Uninvestigated	1 Critical	Protocol SmarterTools -... +15 more	N/A	✓ YES
☐	0	F	113.23.215.154	Changed	Acme Corporati...	Uninvestigated	1 Critical 1 High	Microsoft Remote Des... FileZilla +11 more	N/A	✓ YES
☐	0	F	113.23.216.54	Changed	Acme Corporati...	Uninvestigated	1 Critical 1 High	FileZilla IMAP Protocol +10 more	N/A	✓ YES
☐	0	F	124.150.142.57	Changed	Acme Corporati...	Uninvestigated	1 Critical	VSFTPD FTP Server TLS Protocol +5 more	N/A	✓ YES
☐	0	F	202.51.128.43	Changed	Acme Corporati...	Uninvestigated	1 Critical	IMAP Protocol SMTP Protocol +4 more	N/A	✓ YES

To learn how the CyCognito platform uniquely helps you identify and prioritize the paths of least resistance into your IT ecosystem, so that you can eliminate them, visit **cycognito.com**.

CYCOGNITO