

Human Managed

The **Intelligence Decision Action**
(IDEA) Platform

human > managed_

We are **human > managed**

Our data platform empowers businesses to make smarter and faster decisions for cyber, digital, and risk outcomes.



ISO/IEC 27001:2022 certified and SOC 2 Type I compliant



We were founded in **Singapore** in 2018

with 35 engineers, analysts, and operators across the **Philippines, Singapore, India, and Hong Kong**

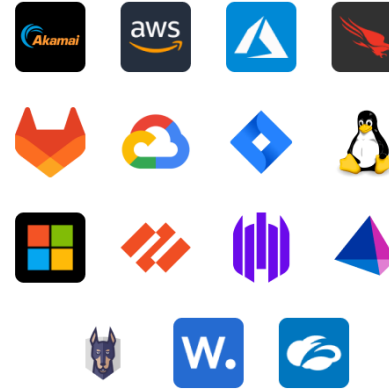


and 24/7 SOC's in **Singapore** and the **Philippines**



History & Operations

Our platform is data-agnostic, cloud-native, and integrates with the world's leading technology providers.



Strategic Partners

We are proud to serve businesses in the essential services sectors:

- finance**
cyber threat and digital fraud platform for one of ASEAN's largest banks
- government**
distributed cybersecurity architecture and threat management
- education**
cyber skills and lab development

Customers

Here are some of our most subscribed use cases to control threats, scale opportunities, and manage risks.

<p>control threats</p> <p>anomaly Detection and resolution of abnormal behaviors in your environments.</p>	<p>control threats</p> <p>denial of service (dos) Detection and resolution of traffic patterns that affect your service quality or availability.</p>	<p>control threats</p> <p>phishing Detection and resolution of attempts to impersonate your internet-facing services.</p>	<p>control threats</p> <p>cloud security posture management (cspm) Detection and resolution of config violations on your cloud resources and services.</p>	<p>control threats</p> <p>application security (appsec) Detection and resolution of weaknesses in your code, package, and applications.</p>	<p>control threats</p> <p>vulnerability Detection and resolution of vulnerabilities in your assets.</p>
<p>manage risk</p> <p>asset management Continuous discovery and profiling of your business assets.</p>	<p>manage risk</p> <p>compliance Discovery and resolution of non-compliance in your assets.</p>	<p>control threats</p> <p>network security posture management (nspm) Detection and resolution of config and rule violations on your network devices and firewalls.</p>	<p>control threats</p> <p>endpoint detection and response (edr) Detection and resolution of malware, compromises, and ransomware in your endpoints.</p>	<p>control threats</p> <p>attack surface management (asm) Discover and resolve your attack vectors.</p>	<p>manage risk</p> <p>fraud Detect and resolve fraud patterns targeting your services.</p>

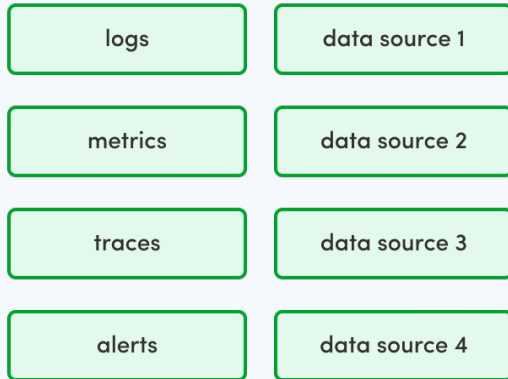
Use Cases

Human Managed's

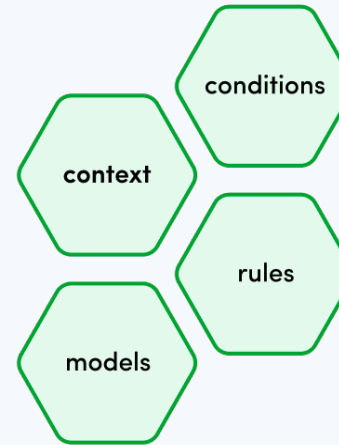
Intelligence Decision Action (I.D.E.A.) Platform

takes data and generates contextualized intel for decisions

1. **Collect, process, and store**
data from any source.



2. Apply **conditions, rules & models** for use cases.



3. Deliver **intelligence, decisions & actions.**



4. **Operationalize** intel
and improve models.



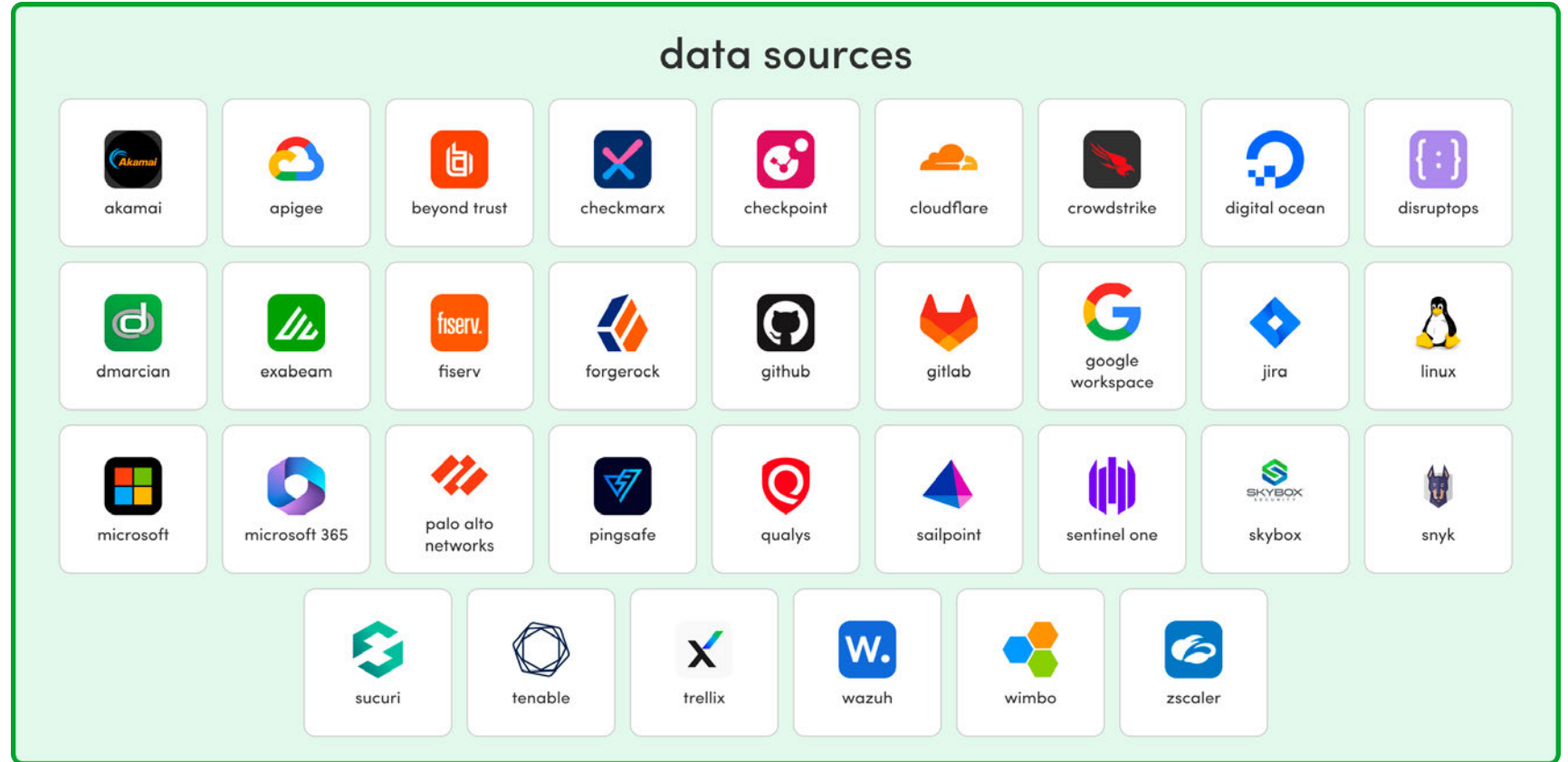
/. Collect, process, and store data from any source.

logs

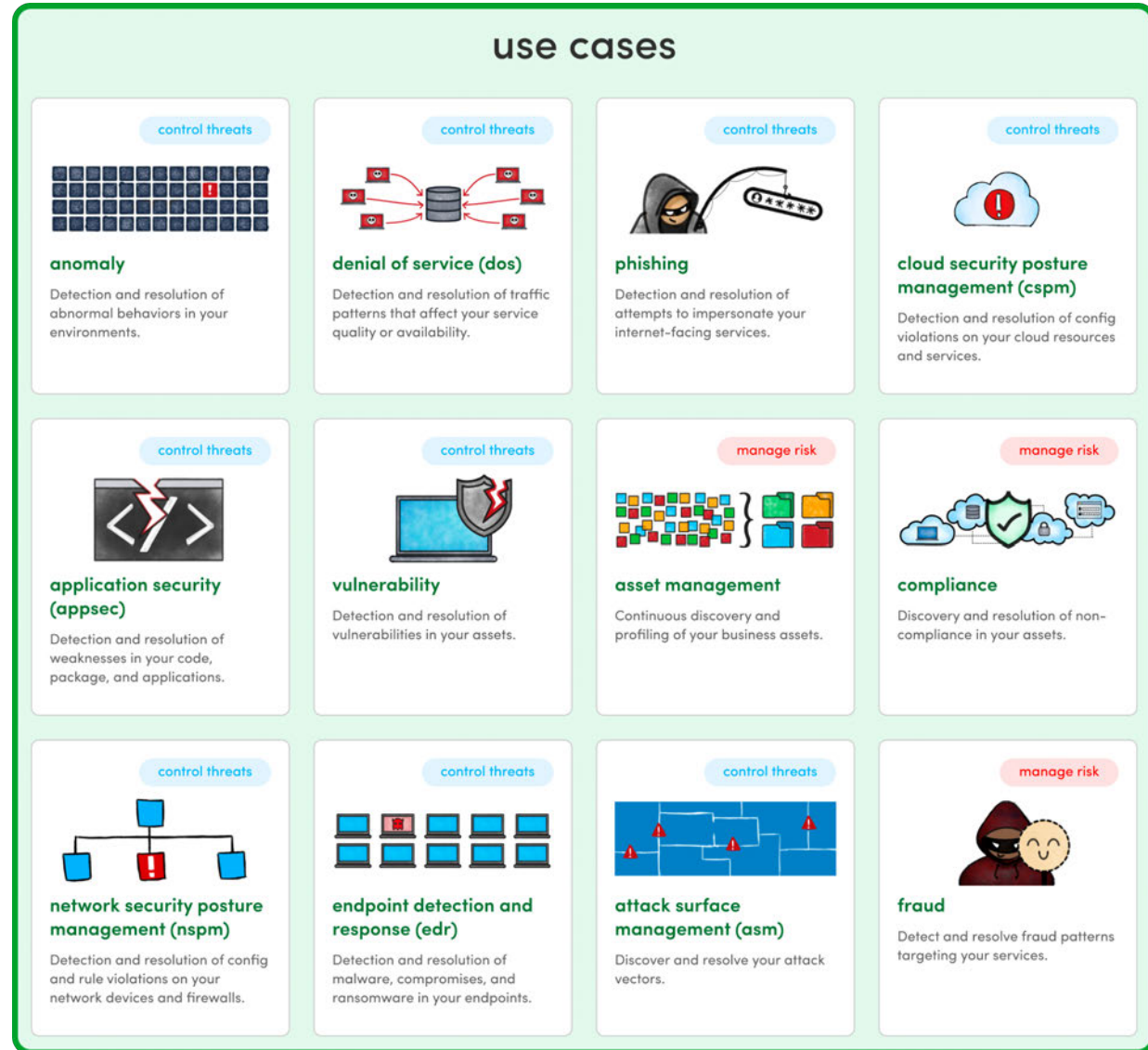
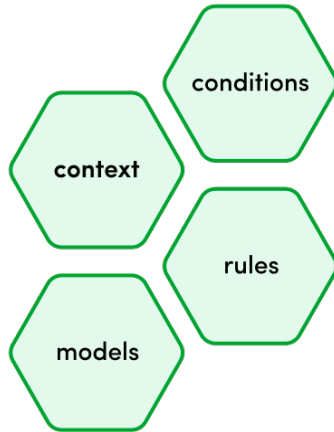
metrics

traces

alerts



2. Apply **conditions, rules & models** for use cases.



3. Deliver intelligence, decisions & actions.



home > usecases > cspm

DASHBOARD **IDEA**

IDE.A. for Cloud Security Posture Management

Last scan: 08 August 2023, 02:49 (UTC+08:00)

Summarized Intel
Violations by severity

Recommended Decision
Violations to prioritize

Recommended Action
Rules to revise

1,124

30
violations from 4 critical severity checks

4
configurations affecting 8 assets

659 Results

Check Name	Severity	Asset Affected	Variety	Cloud Provider	Account ID	Environment	Region
Ensure no security groups allow ingress from 0.0.0.0/0 to remote server ad...	★★★★	table text	AWS::EC2::SecurityGroup	AWS	table text	testing	ap-southeast-1
Ensure AWS Security Hub is enabled	★★★★	table text	AWS::EC2::SecurityGroup	AWS	table text	testing	ap-southeast-2
Ensure AWS Security Hub is enabled	★★★★	table text	Custom::AWS::Region	AWS	table text	testing	us-east-2
Ensure AWS Security Hub is enabled	★★★★	table text	Custom::AWS::Region	AWS	table text	testing	us-west-1
Ensure that IAM Access analyzer is enabled for all regions	★★★★	table text	Custom::AWS::Region	AWS	table text	testing	us-west-2
table text	★★★★	table text	table text	Azure	table text	table text	table text
table text	★★★★	table text	table text	WS	table text	table text	table text
table text	★★★★	table text	table text	WS	table text	table text	table text
table text	★★★★	table text	table text	WS	table text	table text	table text
table text	★★★★	table text	table text	zune	table text	table text	table text
table text	★★★★	table text	table text	WS	table text	table text	table text

detect

Friday, April 12th

alert-notification APP 08:00 PM

12 Assets Discovered

New Asset Discovered | 2024-03-10T23:07:44.085051

updated assets (12)

- name: ip-10-... type: Server first seen: 2024-03-10T04:15:17Z
- name: ip-10-... type: Server first seen: 2024-03-10T04:15:17Z
- name: ip-10-... type: Server first seen: 2024-03-10T04:15:17Z
- name: ip-10-... type: Server first seen: 2024-03-10T04:15:17Z
- name: ip-10-... type: Server first seen: 2024-03-10T04:15:17Z
- name: ip-10-... type: Server first seen: 2024-03-10T04:15:17Z

Remediation Steps [DOWNLOAD STEPS](#)

Perform the following to determine if VPC Flow logs is enabled: From Console:

1. Sign into the management console
2. Select Services then VPC
3. In the left navigation pane, select Your VPCs
4. Select a VPC
5. In the right pane, select the Flow Logs tab
6. If no Flow Log exists, click Create Flow Log
7. For Filter, select Reject
8. Enter in a Role and Destination Log Group
9. Click Create Log Flow
10. Click on CloudWatch Logs Group





Cloud Security Posture Management

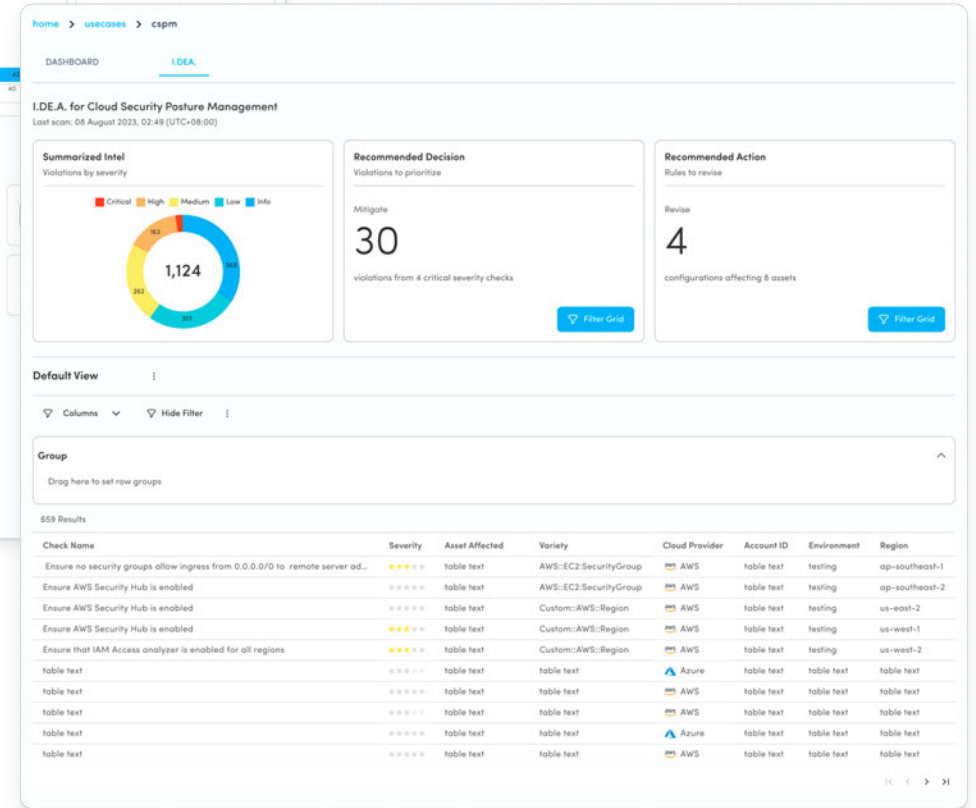
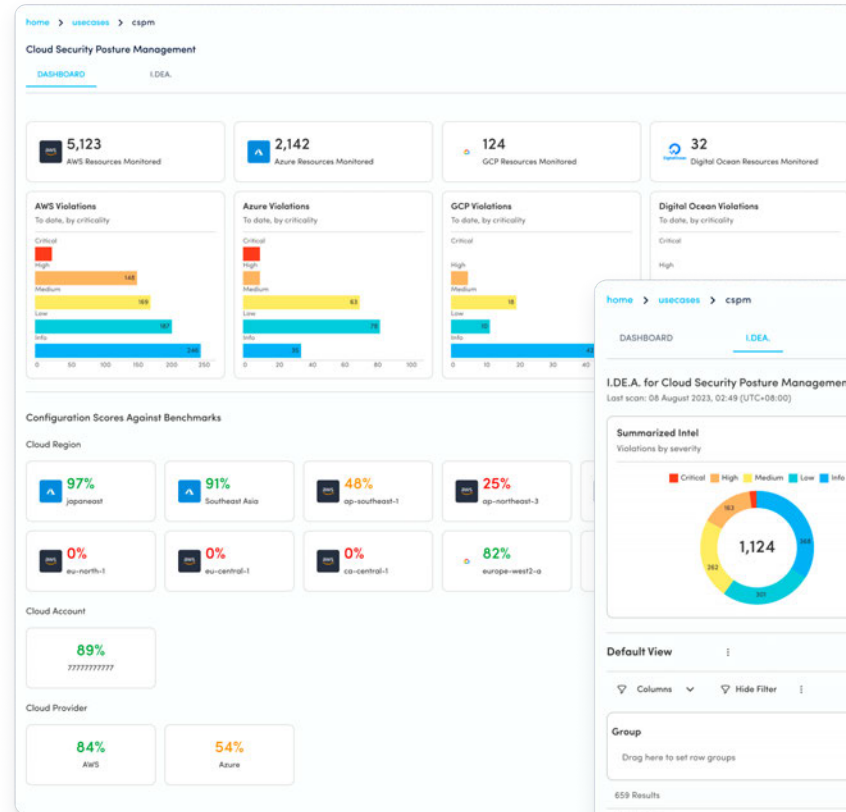
Detect violations and weaknesses in your cloud assets and get prioritized recommendations to resolve them.

Key intel:

config violation

rule violation

cloud compliance





Network Security Posture Management

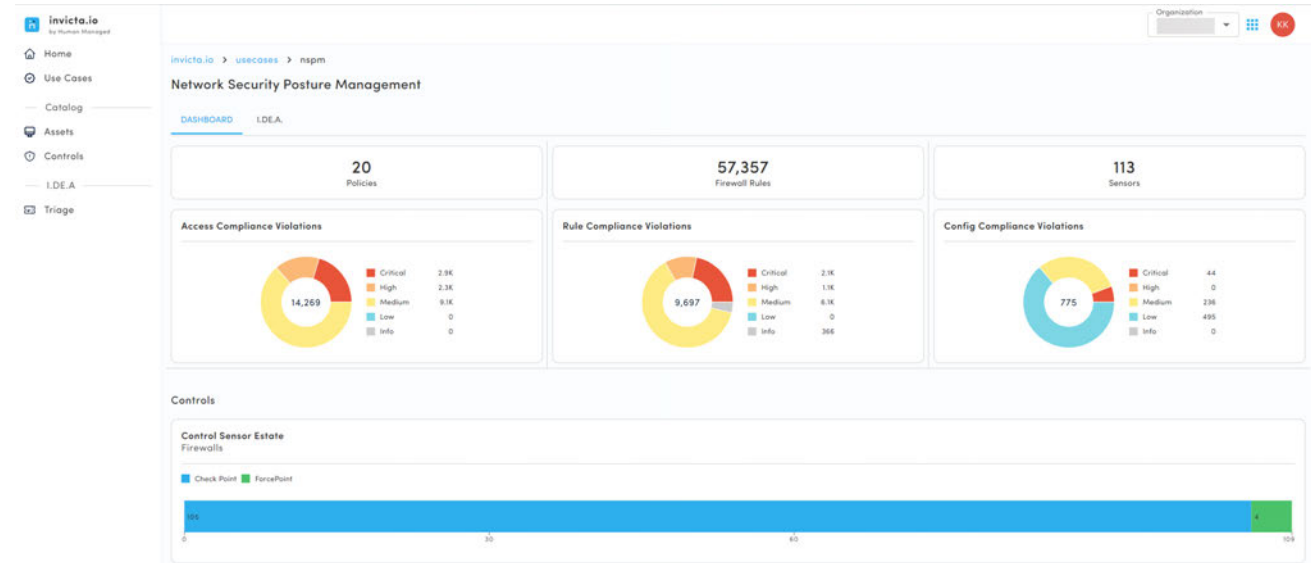
Detect violations and weaknesses in your network assets and get prioritized recommendations to resolve them.

Key intel:

access compliance

rule compliance

config compliance



Check Name	Check Description	Violation Sever...	Policy	Rule ID	Violating Ports
Block Windows NetBIOS	this group of services should not be allowed between network zones of different security levels, as these services are known to have a large number of vulnerability occurrences.	-----	_Main_Policy_Network	39	(TCP) 123 (TCP) 69 (UDP) 123 (UDP) 79 (TCP) 9050 (TCP) 4450 (TCP) 515 (TCP) 445 (UDP) 137-138 (UDP) 137 (TCP) 135 (TCP) 445 (TCP) 135 (UDP) 139 (TCP)
Block RPC and NFS	RPC and NFS services between External zone and Internal zone should be blocked. According to NIST publication 800-41, RPC and NFS services should not be allowed between network zones of different security levels, as these services are known to have a large number of vulnerability occurrences.	-----	_Main_Policy_Network	39	2049 (TCP) 4045 (TCP) 2049 (UDP) 4045 (UDP) 111 (TCP) 111 (UDP)
Block ICMP Echoing Messages	ICMP echoing messages between External zone and Internal zone should be blocked. According to NIST publication 800-41, ICMP echoing messages (e.g. Echo Request) should not be allowed between network zones of different security levels. ICMP echoing messages can be used as part of a network reconnaissance, which is the basis for cyber attacks.	-----	_Main_Policy_Network	39	12 (ICMP) 8 (ICMP) 4 (ICMP)
Block X-Windows	X-Windows services between External zone and Internal zone should be blocked. According to NIST publication 800-41, the X-Windows service should not be allowed between network zones of different security levels. X-Windows service enables remote administration, and should be allowed from trusted sources only.	-----	_Main_Policy_Network	39	6000-6255 (TCP)
Block VPN Access	VPN access between Internal zone and External zone should be blocked. Violation of this rule could expose rouge or unauthorized outbound VPN access.	-----			
Block Login Services	Login services between External zone and Internal zone should be blocked. According to NIST publication 800-41, login	-----			

2.11 Radius or TACACS+ server

Ensure Radius or TACACS+ server is configured

Resource Checked

DEVICE NAME	IP
CHECK OUTCOME	VIOLATION CREATED
CATEGORY	PROVIDER
DEVICE STATUS	MANAGER NAME



Attack Surface Management

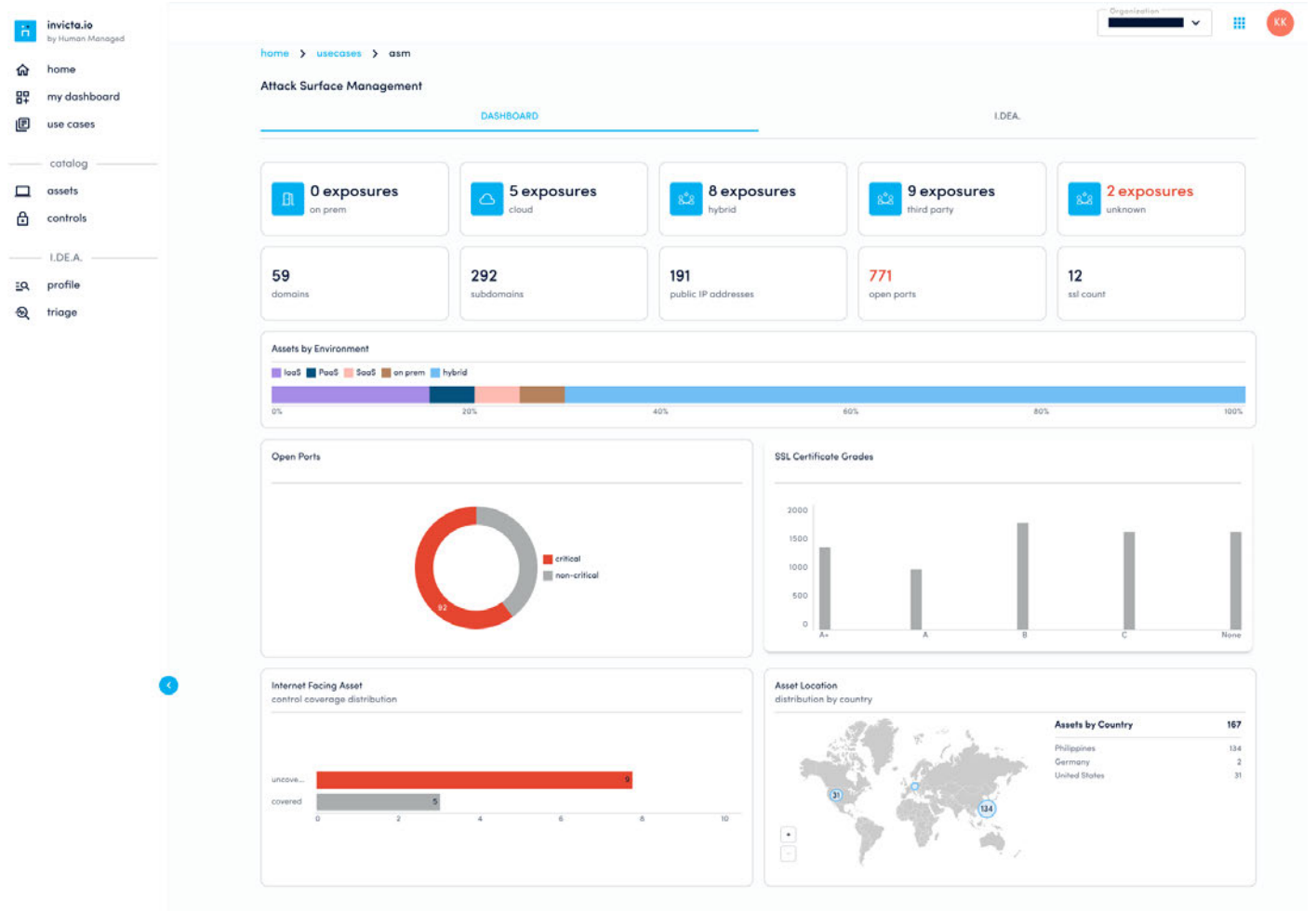
Detect exposures and threat in your assets and get prioritized recommendations to resolve them.

Key intel:

internet facing asset

exposure

active asset





Vulnerability Management

Detect vulnerabilities affecting your assets and get prioritized recommendations to resolve them.

Key intel:

vulnerability

CPE, CVE, CVSS, CWE

asset version



Vulnerability Management

DASHBOARD I.D.E.A.

I.D.E.A. for Vulnerability Management

Summarized Intel
Vulnerabilities by CVSS severity

Unknown	21.5K
Medium	1.7K
High	767
Critical	335
Low	239

Recommended Decision
Vulnerabilities to prioritize

Fix
106
assets with critical CVE severities.

Recommended Action
Assets to Update

Execute recommendation:
Refer to Cisco advisory [cisco-sa-20170317-cmp](https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170317-cmp) (https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170317-cmp) for updates and patch information. Workaround: There are no workarounds that address this vulnerability. Recommended Settings- Disabling the Telnet protocol as an allowed protocol for incoming connections would eliminate the exploit vector. Disabling Telnet and using SSH is recommended by Cisco. Customers unable or unwilling to disable the Telnet protocol can reduce the attack surface by implementing infrastructure access control lists (ACLs). Patch: Following are links for downloading patches to fix the vulnerabilities: <http://software.cisco.com/download/navigator.html?mdfid=281458049> to address critical CVEs with most assets affected.

Default View

search

COLUMNS RESET FILTERS

Outcome	Check Name	Check Severity	Device IP	OS	CVE ID	CVE Description	CVE Severity
Failure	PHP Versions Prior to 5.6.12/5.5.28/5.4.44 Multiple Vulnerabilities	High	[Redacted]	-	CVE-2015-8867	The openssl_random_pseudo_bytes function in ext/openssl/openssl.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 incorrectly relies on the deprecated RAND_pseudo_bytes function, which makes it easier for remote attackers to defeat cryptographic protection mechanisms via unspecified vectors.	HIGH
Failure	PHP Versions Prior to 5.6.12/5.5.28/5.4.44 Multiple Vulnerabilities	High	[Redacted]	-	CVE-2015-8867	The openssl_random_pseudo_bytes function in ext/openssl/openssl.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 incorrectly relies on the deprecated RAND_pseudo_bytes function, which makes it easier for remote attackers to defeat cryptographic protection mechanisms via unspecified vectors.	HIGH
Failure	NTP ntpd Multicast Security	Medium	[Redacted]	-	CVE-2016-9310	The control mode (mode 6) functionality in ntpd in NTP before 4.2.8p9 allows remote attackers to set or unset traps via a crafted control mode packet.	MEDIUM
Failure		High	[Redacted]	-	CVE-2017-6462	Buffer overflow in the legacy Datum Programmable Time Server (DPTS) relock driver in NTP before 4.2.8p10 and 4.3.x before 4.3.94 allows local users to have unspecified impact via a crafted /dev/datum device.	HIGH
Failure		Medium	[Redacted]	-	CVE-2016-7427	The broadcast mode replay prevention functionality in ntpd in NTP before 4.2.8p9 allows remote attackers to cause a	MEDIUM

PHP Versions Prior to 5.6.12/5.5.28/5.4.44 Multiple Vulnerabilities

PHP is a general purpose scripting language that is especially suited for web development and can be embedded into HTML. PHP Group released version 5.5.28/5.6.12/5.4.44 of PHP, fixing multiple vulnerabilities. Affected Versions: PHP Versions Prior to 5.5.28/5.6.12/5.4.44

Details

OUTCOME failure TARGET IP [Redacted]

VULNERABILITY CREATED Jul 24, 2024

Vulnerability Details

PHP Versions Prior to 5.6.12/5.5.28/5.4.44 Multiple Vulnerabilities: PHP Versions Prior to 5.6.12/5.5.28/5.4.44 Multiple Vulnerabilities detected on port 7004 over TCP.

Check Impact

The vulnerabilities can be exploited by malicious users to execute arbitrary code in the context of the application, access sensitive information or cause denial of service conditions.

Recommendation

Users are advised to upgrade to the latest version of the software. For more information, please refer to the PHP Web site (<http://www.php.net/>). Patch: Following are links for downloading patches to fix the vulnerabilities: PHP 5.5.28/5.6.12/5.4.44 (php) (<http://www.php.net/>)



Asset Management

Continuously discover and profile your assets to model your unique intelligence and business context.

Key intel:

- asset priority
- asset attribute
- asset relationship



Good Morning, Chiqui

35,118 ^{+1%} Assets This month

5 ^{NA} Connected Data Streams This month

5 ^{+13%} New Assets Discovered This month

Assets: Criticality Distribution
Asset attributes applied

Criticality	Count
Critical	~1,000
High	~1,000
Medium	~10,000
Low	~23,000

Assets: Category Distribution
Asset attributes applied

Category	Count
Device	17,870
User	13,450
Network	3,700
Unknown	~1,000

Assets: Context
Asset attributes applied

Owner Identified	42%
Criticality Assigned	100%

I.D.E.A. for End-of-Life Assets Use Case: End of Life Assets

Summarized Intel
Assets with eol software

Status	Count
Unknown	~400
Supported	~100
End of Support	~88

Recommended Decision
OS software to update

Prioritize assets installed with

4 end-of-life OS [FILTER GRID](#)

Recommended Action
Assets to patch

Patch

33 assets with end-of-life OS

I.D.E.A. for Dormant Assets Use Case: Dormant Assets

Summarized Intel
Aging of dormant assets

Last seen	Count
Last seen 30 days	209
Last seen 60 days	174
Last seen 90 days	154

Recommended Decision
Assets to validate

Validate

209 assets last seen beyond 30 days [FILTER GRID](#)

Recommended Action
Assets to patch

Revoke

154 assets have been inactive for more than 90 days. [FILTER GRID](#)



Organization Posture Management

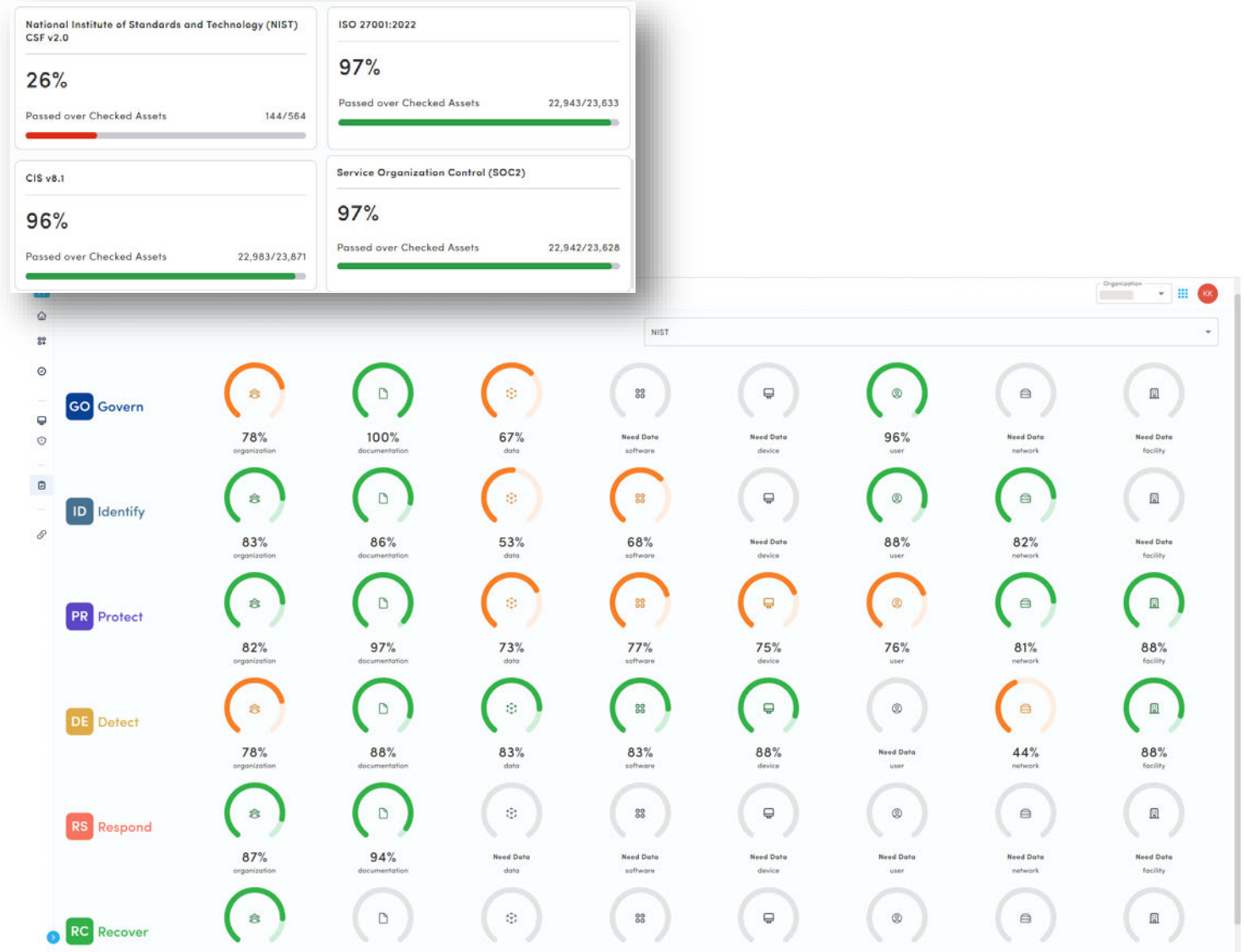
Assess your enterprise level compliance and risk posture to control frameworks, benchmarks, and regulations and make recommendations to resolve non-compliance

Key intel:

compliance posture

control coverage

organizational maturity





Fraud

Detect suspicious or fraudulent behaviors in your services and get prioritized recommendations to resolve them.

Key intel:

fraud tactic

fraud technique

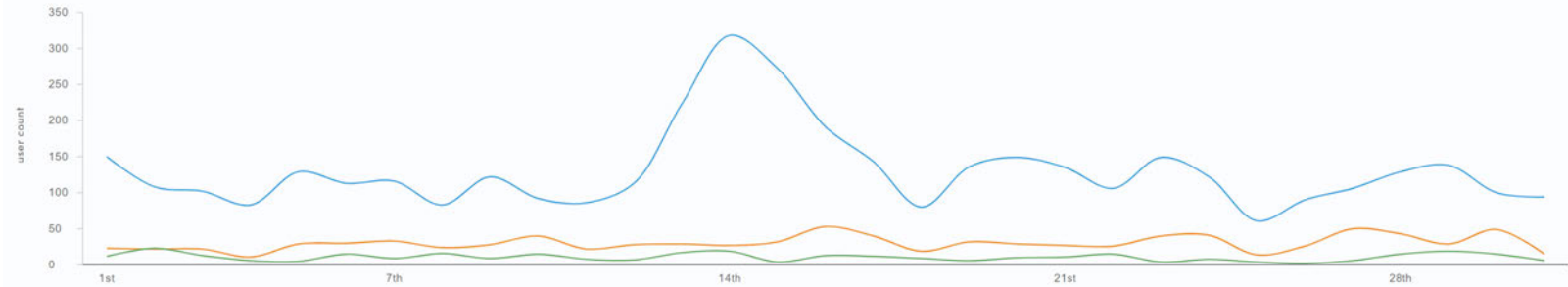
behavior pattern



home > online banking > online banking fraud

DASHBOARD DETECTIONS

December 2022 < > date filter month



Technique Breakdown

technique	count	% change	by detection	view detections
High Money Transfer	333	5.38 %	 received >100k transferred >50k	VIEW DETECTIONS
Identity Obfuscation	4039	31.52 %	 no device & IMEI device w/ multiple IMEIs one IMEI, multiple devices	VIEW DETECTIONS
OTP Cancellation	933	37.81 %	 otp cancellation	VIEW DETECTIONS

subtechniques for Identity Obfuscation:
no device & IMEI : 0
device w/ multiple IMEIs : 4025
one IMEI, multiple devices : 14

machine run, human managed.

