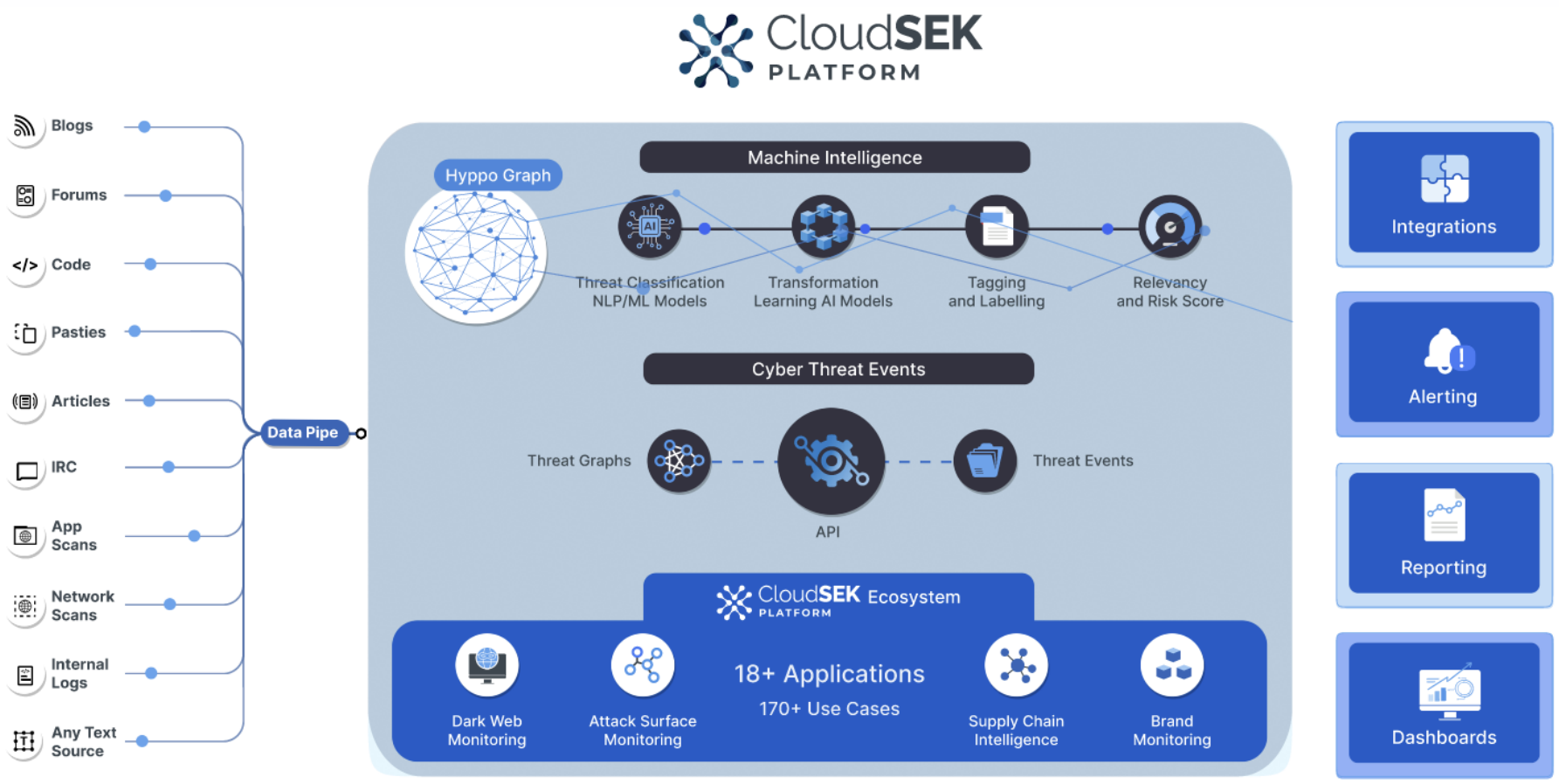
We Predict Cyber Threats



Monitor **Analyse** **Predict**

Schedule a Demo of our platform today:

By Monitoring the vast amount of data available on cyber threats, both open source and proprietary, CloudSEK uses machine intelligence to analyse patterns and trends that can be used to **predict future cyber threats.**

Mail us at **info@cloudsek.com** or visit **https://cloudsek.com**

Book an online Product Demo

Gain access to a free trial and Detailed POC on the CloudSEK Platform

CloudSEK

We Predict Cyber Threats

Initial Attack Vector Protection Platform

Founded in **2015**

200+ *CloudSters*

3 Offices
HQ: ***Singapore,***
Offices:
Bangalore,India
London, UK

200+ *Clients Globally*

4 *Products*

We secure some of the Fortune 500 and Unicorns

... And we are backed by eminent investors

Accelerated by

NVIDIA INCEPTION PROGRAM

NETAPP EXCELLERATOR

CloudSEK is a **Customer First** Company

We are a **Gartner Peer Insights Customer First Vendor** for Security Threat Intelligence Products and services. We have been featured in several Gartner market guides and are a **qualified AWS partner**. We are the **Highest Rated Security Threat Intelligence company** on Gartner Peer Insights from the Asia Pacific region.

NETAPP EXCELLERATOR BEST GROWTH STRATEGY 2019

ISO 27001

ISO 22301

DSCI Excellence Awards Security Product Company of the Year 2020

aws PARTNER

NASSCOM Emerge 50 Awards 2020

Gartner Peer Insights Customer First

Highest Rated Security Threat Intelligence Vendor in Asia Pacific

Gartner Rated 4.6+ peerinsights™

About CloudSEK

CloudSEK is a contextual AI company that predicts Cyber Threats.

At CloudSEK, we combine the power of Cyber Intelligence, Brand Monitoring, Attack Surface Monitoring, Infrastructure Monitoring and Supply Chain Intelligence to give context to our customers' digital risks.

CloudSEK

www.cloudsek.com
info@cloudsek.com

CloudSEK
www.cloudsek.com

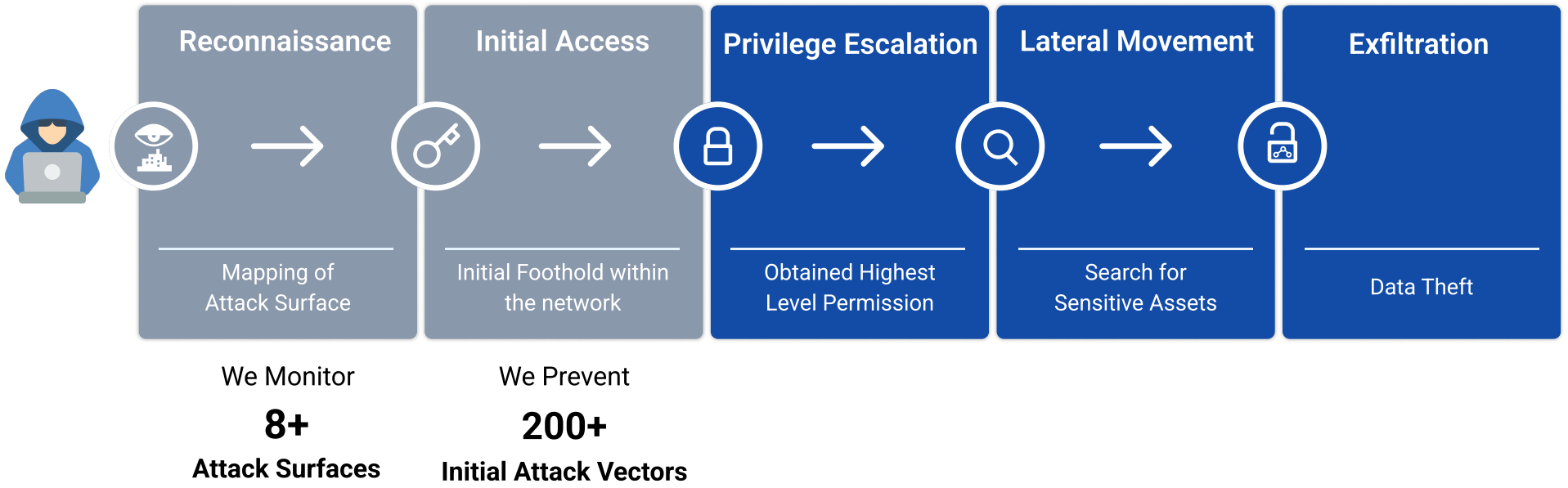
We Predict
Cyber Threats

What does CloudSEK do?

CloudSEK is a contextual AI company that predicts cyber threats.

Predicting cyber threats and preventing future attacks before they even occur may sound like something out of a science fiction novel. However, it is not. Similar to how predicting the rain and the weather is done through mathematical modelling, predicting cyber threats is a very scientific concept too. By using the vast amount of data available on cyber threats - both open source and proprietary - CloudSEK uses machine intelligence to identify patterns and trends that can be used to predict future cyber threats. As opposed to Reactive Indicators of Compromise (IOCs) that the industry follows, **CloudSEK follows Indicators of Attacks (IOAs)**. These can be used to proactively identify vulnerabilities, anticipate attacks, and develop strategies to prevent them before they occur.

How does CloudSEK predict and prevent cyber threats?



We Monitor
8+
Attack Surfaces

We Prevent
200+
Initial Attack Vectors

CloudSEK stops the Kill Chain by predicting and preventing Initial Access Vectors

A cyber attack occurs in 5 steps. Firstly, attackers do a *reconnaissance* of their intended target to scope out vulnerabilities, misconfigurations etc. Then, attackers use the identified vulnerability to *gain initial access* to the target's network using an **Initial Attack Vector (IAV)**. Thereafter, attackers *escalate their privileges*, *search for sensitive assets* and *exfiltrate data*.

Hence, it's absolutely necessary that the attackers are stopped before they can gain initial access within the network.

CloudSEK stops the kill chain attackers follow even before they can gain an initial foothold within the network. We do this by mapping customers' attack surfaces and all IAVs commonly used by threat actors. Killing the IAV would prevent a cyber threat from happening.

At CloudSEK, we combine the power of Cyber Intelligence, Brand Monitoring, Attack Surface Monitoring, Infrastructure Monitoring and Supply Chain Intelligence to give visibility and context to our customer's IAVs.

Request a free demo by visiting our website at cloudsek.com/request-a-demo or mail us at info@cloudsek.com

CloudSEK
www.cloudsek.com

We Predict
Cyber Threats

Indicators of Attack (IOA): The Future of Cyber Threat Intelligence

Cyber Threat Intelligence (CTI) - The fundamental objective of CTI is to understand an attacker's target, motives and behavior so that the organization can be better prepared for cyber threats. CTI provides organizations with intelligence support to tactical, operational and strategic cyber security needs. Automated CTI consumption comes in the form of IOCs (Indicator of Compromise). An IOC is the evidence on a computer that indicates that the security of the network has been breached. It also provides valuable information about the tools, techniques, and tactics used in the attack. However, a drawback of IOCs is that they are reactive and after the attack has occured. Also, they are effective only against known attacks.

Indicators of Attack (IOAs) are, hence, the future of Cyber Threat Intelligence. IOAs are signatures of malicious activity that can be used to detect, diagnose, and respond to a cyber attack. It is a piece of evidence that suggests that an attack is underway or has been attempted. IOAs can be found in many different places, but they all have one thing in common: they provide clues that can be used to detect, diagnose, and respond to attacks.

IOAs are future forward and are not reliant on specific details of the attack. This is why IOAs take center stage in our endeavour to prevent and predict cyber attacks. By monitoring IOAs, we are able to adopt a proactive approach and prevent cyber attacks before they are even under way.

How are **Indicators of Attack (IOAs)** and **Indicators of Compromise (IOCs)** different?

Indicators of Compromise (IOC)

IOCs Provide Information about:

- Malicious Files and Malware hashes.
- Malicious Domains & hashes.

Reactive

v/s

Indicators of Attack (IOA)

IOAs Provide Information about

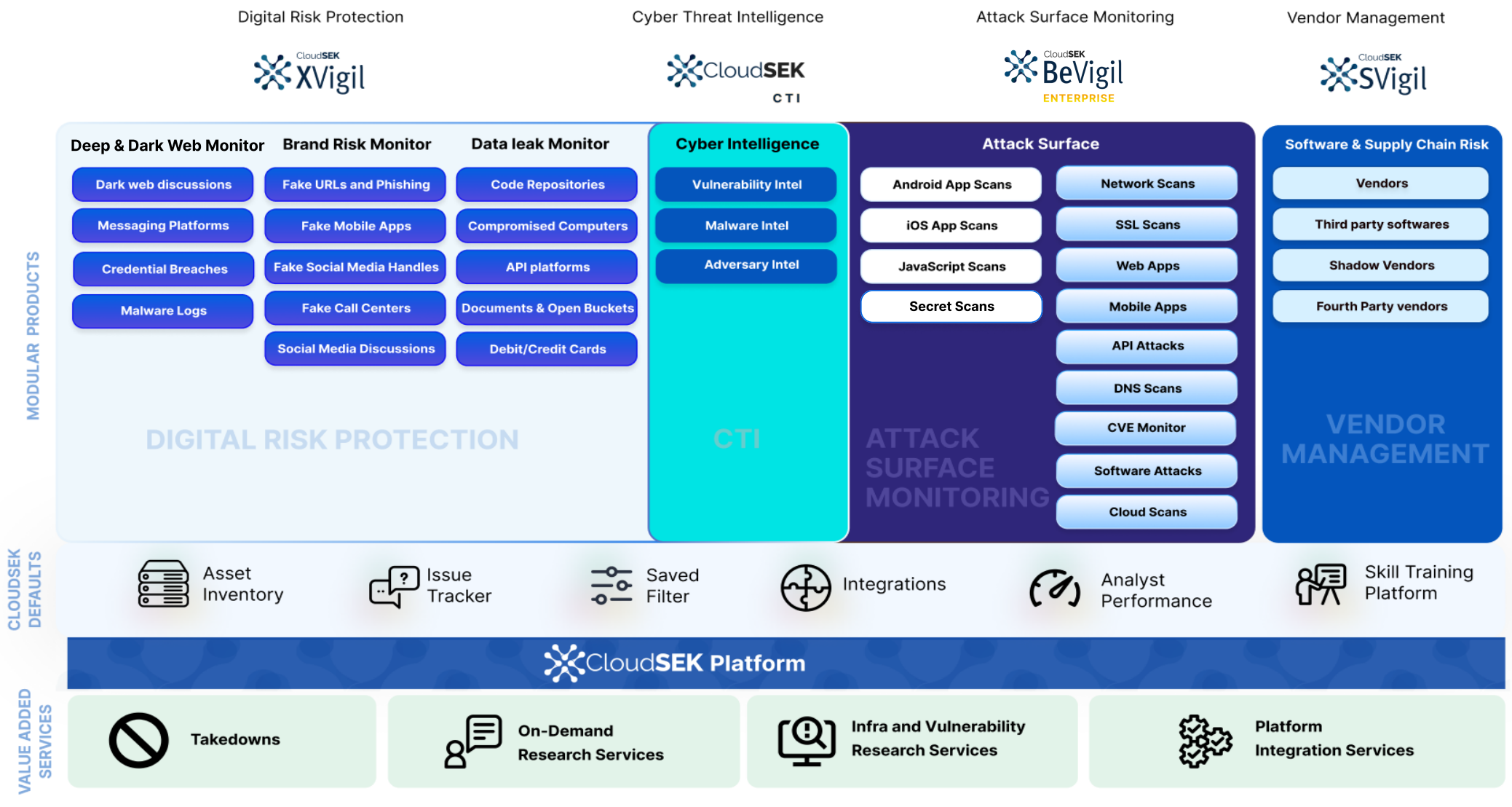
- Compromised API Keys & Tokens used for IAV
- Exposed Vulnerable Software service used for IAV
- Vulnerable web Application used for IAV
- Vulnerable third party code used for IAV
- Compromised passwords available on darkweb
- Discussion on Darkweb about an Attack

Proactive

CloudSEK
www.cloudsek.com

We **Predict**
Cyber Threats

Product Overview



Our IAV-centric Use Cases

Cyber Threat Intelligence

- Adversary Intelligence
- Vulnerability Intelligence
- Malware Intelligence
- Ransomware Intelligence
- Time-sensitive Research Bytes

Dark & Deep Web Monitor

- Telegram, Discord, IRC Conversation Monitoring
- YouTube Hacking Tutorials
- Credit/Debit Card Leaks
- Underground Discussions & Marketplaces

Phishing & Brand Monitor

- Fake Social Media Brand Profiles
- Fake or Rogue Mobile Applications
- Fake or Impersonated Domains
- Fake Web Pages
- Fake Customer Service / Support Nos.

Data Leak Monitor

- Source Code Leaks
- Server Credential Leaks
- Board Member Credential Leaks
- 3rd Party Data Leaks
- API key leaks

Infrastructure Monitor

- Network Scanner
- Web Application Scanner
- Cloud Asset Scanner
- Mobile Application Scanner
- Continuous Attack Surface identification
- Outdated SSL softwares

Software & Supply Chain Monitor

- Vendor Information Security Risk
- Insecure Libraries
- Vulnerable Plugins
- Misconfigurations on cloud services

We cater to **200+ Use Cases / IAVs**

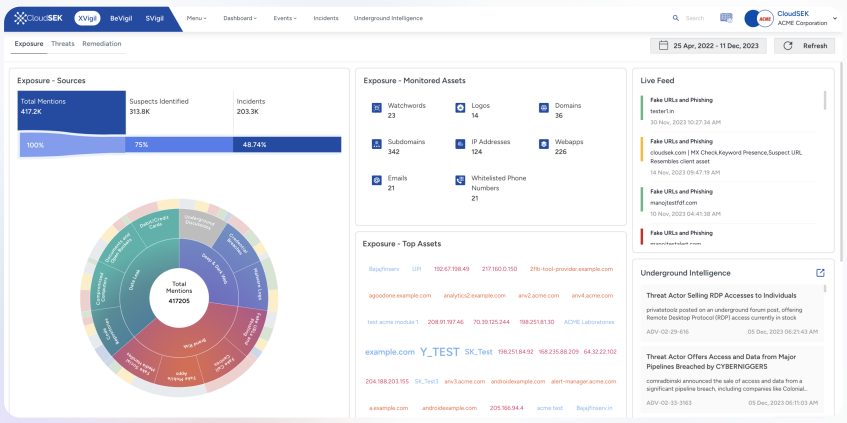
CloudSEK
www.cloudsek.com

Our Products

CloudSEK XVigil

Initial Attack Vector Protection for employees and customers.

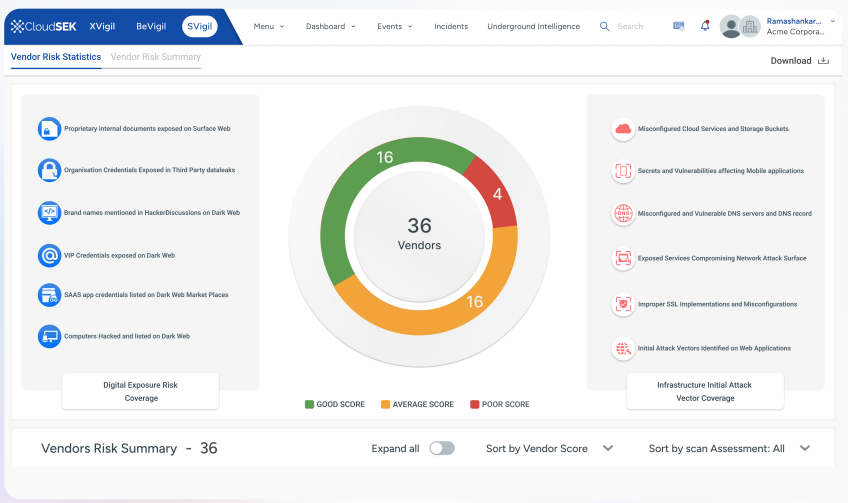
CloudSEK's Contextual AI engine uses Cyber Threat Intelligence and Attack Surface Monitoring to proactively predict and prevent an organisation's Employees and Customers from Phishing, Data Leak, DarkWeb and Brand Threats and Infra threats.



CloudSEK SVigil

Initial Attack Vector Protection for Software and Supply Chain risks.

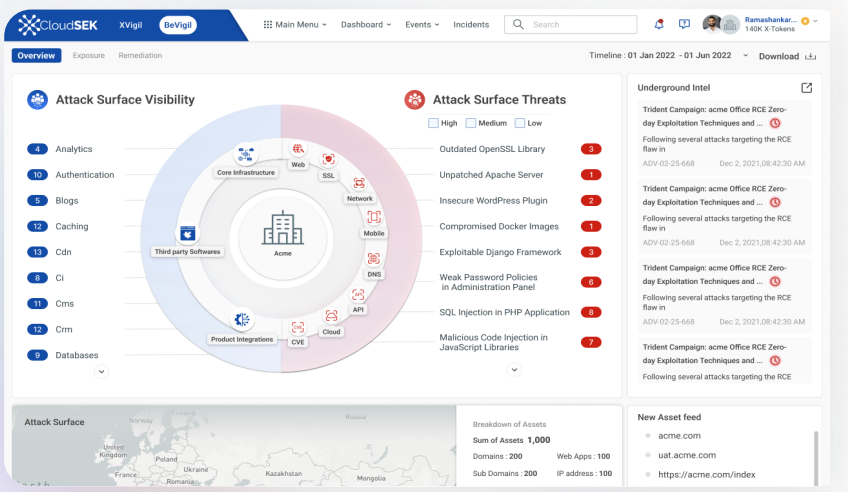
CloudSEK's Contextual AI identifies software supply chain risks by monitoring Vendors, third party Softwares, Shadow vendors and fourth party vendors.



CloudSEK BeVigil ENTERPRISE

Comprehensive Attack Surface Fingerprinting and Monitoring (ASM)

CloudSEK BeVigil Enterprise comprehensive ASM solution helps organizations detect and control risks associated with external attack surfaces. BeVigil Enterprise monitors 8+ attack surfaces and provides robust protection.



cloudsek.com

CloudSEK
www.cloudsek.com

Our Integrations

Don’t Replace, Integrate!

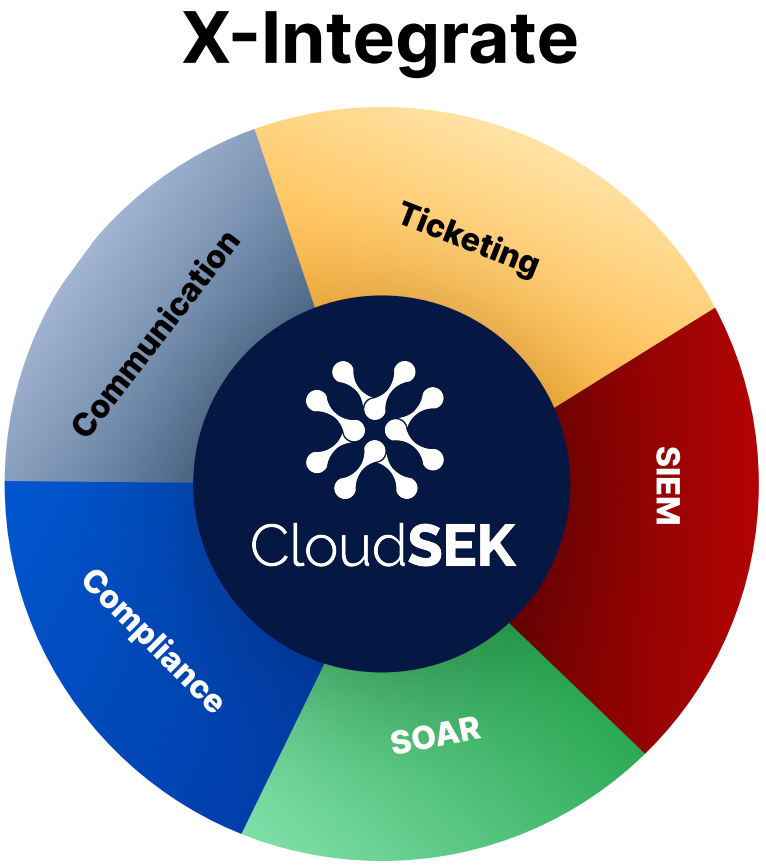
CloudSEK platform integrates seamlessly with the core components of an organization's security operations like SIEM, SOAR, ITSM tools etc. Our Platform is a SaaS-based Digital and Infrastructure Risk Monitoring Platform. This industry-leading AI & ML system collects intelligence data in real-time, across open and closed sources. Our Platform dashboard provides specific, actionable, and timely digital risk warnings that help you mitigate your digital risk footprint. This can help clients assess their security posture in real-time from the perspective of an attacker. Furthermore, **by feeding this IAV based intelligence into your prior security investments, your organization can move from “Reactive” to “Proactive”.**

This can be done by leveraging the seamless API-based integration with third-party security solutions such as:

- SIEMs
- Incident Management Systems
- Ticketing Systems
- Threat Intelligence Platforms
- Communication Tools

The integration with the above mentioned tools will help the organization reap the following benefits:

- Faster, risk-based alert triage
- Focus on strategic decisions
- Reduced dwell time
- Unknown threats revealed



Request a free demo by visiting our website at cloudsek.com/request-a-demo or mail us at info@cloudsek.com

CloudSEK

We Predict Cyber Threats

Monitor. Analyse. Predict.

Secure your Organisation, Today!

Request for a Free Demo of our platform:

Mail us at **info@cloudsek.com** or visit **https://cloudsek.com**

Book a Zero commitment Product Demo

Gain access to a free trial and Detailed POC on CloudSEK Platform

Registered Office: HQ (Singapore)

CloudSEK Research Pte Ltd.
51 Chin Swee Rd. #07-12
Manhattan House., Singapore 16

Regional Office: Bangalore (India)

CloudSEK Information Security Private Limited, 1st Floor, 16/1, Cambridge Rd, Halasuru, Cambridge Layout, Jogupalya, Bengaluru, Karnataka 560008

Regional Office: London (UK)

CloudSEK, 4th floor, Rex House,4, 12 Regent Street, London, SW1Y 4PE - United Kingdom