NVIDIA CORPORATION

Submitted by Group 1

1. **Aditi Ashok Kurutala**
2. **Pragya Mittal**
3. **Yu-An Tsai**
4. **James Volante**

Basic Profile

Name: NVIDIA Corporation
Headquarters Location: 2788 San Tomas Express Way, Santa Clara, CA 95051
Number of Employees: ~26,000 employees[1]
Annual Revenue: US $60.922 Billion[2]
Annual Profit: US $26.0 Billion[2]
Business Line(s): +1 (800) 797-6530
Website: https://www.nvidia.com/en-us/
Ticker Symbol: NVIDIA Corp, NASDAQ: NVDA

NVIDIA is a multinational corporation primarily designing and selling GPUs and has a stake in various industries like AI, gaming, autonomous vehicles, and robotics industry. As a leading company in its sector and being one of the top-performing stocks in the market, NVIDIA is a valuable target for cyber attacks. Its market dominance in the GPU market makes it a lucrative target for extortion or ransomware attacks. Disrupting NVIDIA's supply chain could destabilize relations between Taiwan and China. Access to the company's intellectual property, particularly its advanced GPU technology, could provide competitors with a market advantage. Exploiting hardware vulnerabilities in NVIDIA's chips could compromise software running on these devices, leading to data breaches or other security incidents. Additionally, NVIDIA's possession of user data, including credit card information, makes it a target for data theft and financial fraud.

Regarding the quality of our intelligence, on the admiralty code, we will give it a B. A lot of personal accounts that we found (specifically for the list of employees) come from LinkedIn. Many of the accounts could not have been updated, and these employees could have left the company. However, we found that a lot of our sources come directly from NVIDIA themselves, which only boosts our confidence in how actionable this intel is. As for our best intelligence, the technology vulnerabilities are the most useful for an attack. We scoured their job listings, it is evident that these technologies are used in their systems. We also referenced reputed websites to find known vulnerabilities in NVIDIA products and looked at heuristic data of instances of NVIDIA assets being compromised to further bolster our confidence in the quality of the intelligence gathered in this report.

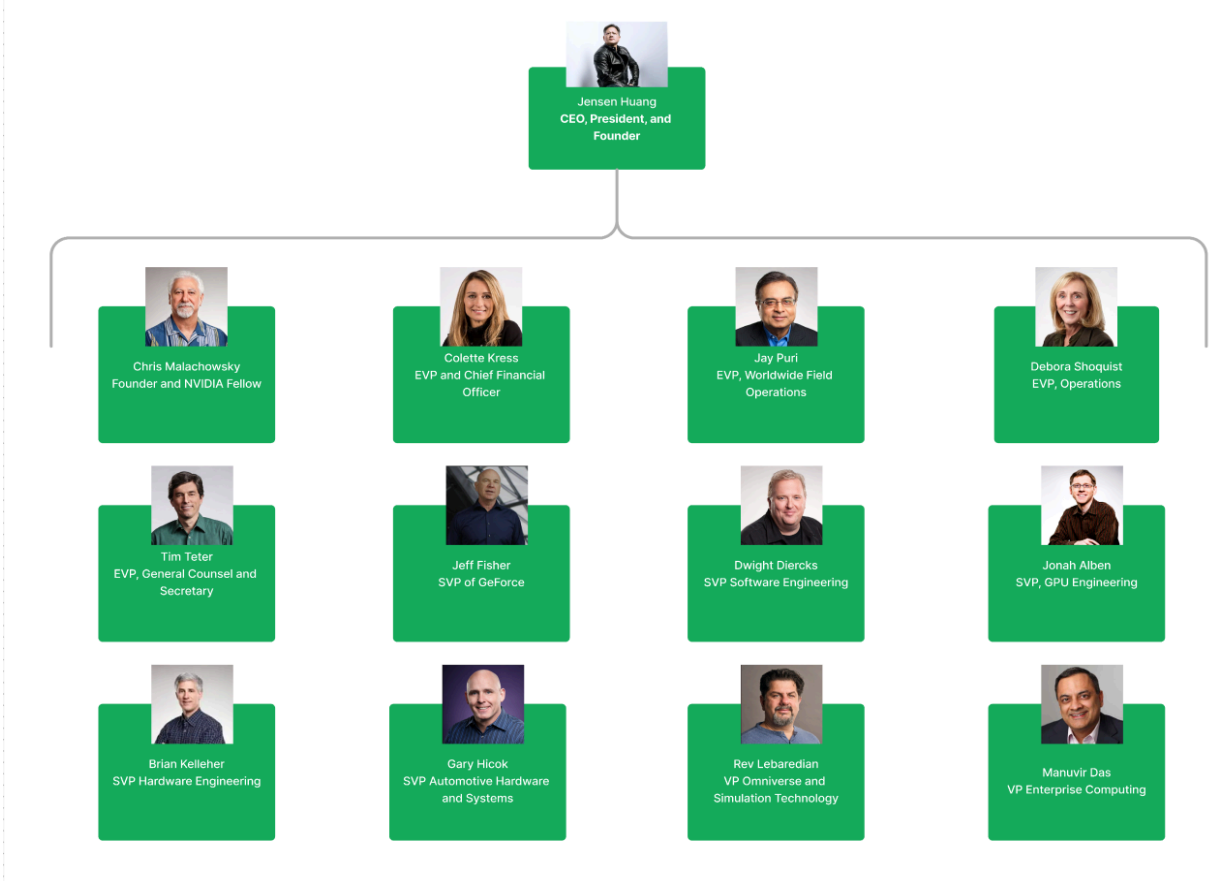
1 https://www.statista.com/statistics/1369574/nvidia-number-of-employees/

2 https://investor.nvidia.com/news/press-release-details/2024/NVIDIA-Announces-Financial-Results-for-Fourth-Quarter-and-Fiscal-2024/

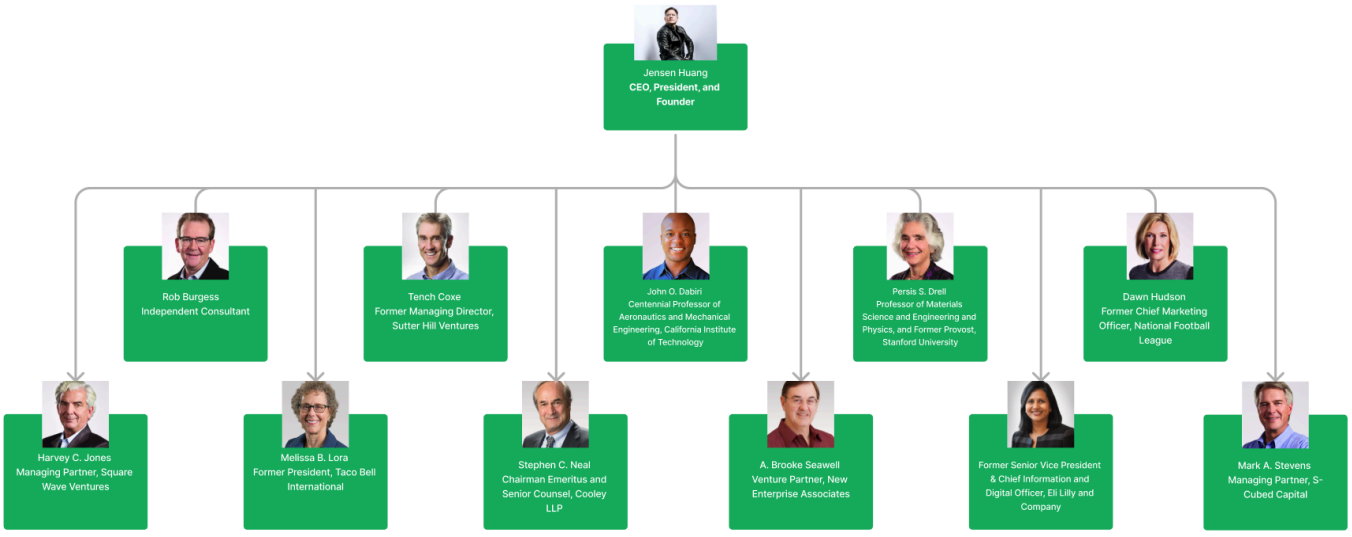
INDEX

COMPANY ORGANIZATION CHART

Top Leadership:



Board of Directors:



NAMES OF STAFF

- Camir Ricketts, Bioinformatics Scientist.
- Ryan McCormick, Senior Software Engineer at NVIDIA.
- David Wright, Vice President & Executive Creative Director.
- Subhan Ali, AI Product Lead for Snowflake.
- Peter C. Blanton, Global Sales Director
- Zubin Ghyara, Senior Director of Supply Chain Operations
- Eva Wasielewski, Senior Director, APAC Corporate Marketing and Enterprise Marketing
- Patty Delafuente, Data Scientist
- John St John, Principal Drug Discovery AI Applied Scientist
- Ameya Mahabalshwarker, Deep Learning Scientist
- Nicholai Tukanov, Software Engineer
- Kevin Wang, Software Engineer
- Sahana Murthy, Senior VLSI CAD Developer
- Deana O'Meara, Manager, Nvidia Product Security Incident Response Team

SOCIAL MEDIA INFORMATION

Camir Ricketts

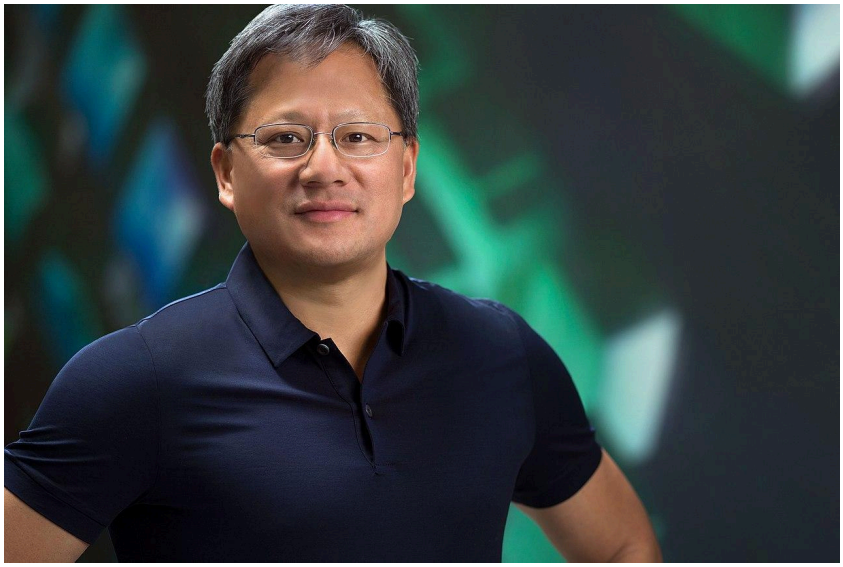
While conducting our intel on NVIDIA, we discovered Camir. Camir has a pretty big public presence compared to some of the other people we tried to investigate. After doing a little searching, we were able to find an active Instagram account, LinkedIn account, and X(Formerly Twitter) account.

Through our combing of his social media, we found out Camir has 1 younger sister, 2 younger brothers, and 1 older brother. However, as of right now, he is an uncle with his older brother having a son. Regarding his marital status, recent Instagram photos have shown his ring finger to be missing a ring, which was also common in older photos of himself.

His favorite sports team is the Lakers, with his favorite player being Lebron James who is on that same team. He also enjoys watching college football, specifically his alma mater team the University of Georgia. Currently lives in New York City, and one of his favorite places to go is Distilled NYC to hang out with his friends and colleagues from his alma mater.
One of his favorite places to travel is Paris, France, with a variety of pictures of his time there.

He also enjoys volunteering, he helped develop an app called AllClear that allows users to find nearby COVID-19 sites, and he helps in food drives as well. All information was found via his public social media accounts.

Jensen Huang



Jensen Huang is the current CEO of NVIDIA, which means he is one of the most well-documented personnel in the company. Unlike Camir, the only publicly facing account we were able to find is his LinkedIn. However, due to him being the face of the company, we were able to find quite a bit of information about him via articles written about him, and interviews he has done.

Jensen is currently married with 2 children, Madison Huang and Spencer Huang. He met his wife, Lori Mills, during his tenure at Oregon State University. One of his relatives is actually the current CEO of AMD.

One of Jensen's interests is collecting biker jackets. These leather jackets are usually top-of-the-line premium jackets, with him sporting a Tom Ford leather jacket at a recent talk. He also has an affinity for table tennis, cycling, and baseball. He has even done the first pitch for a game before.

Some of his favorite foods include Dan Zai noodles, Braised pork on rice, beef noodles, Taiwanese bubble tea, and Vietnamese street food which includes snails, beef noodle soup, and egg coffee. Some of his favorite restaurants are the Ningxia Night Market, Flower Restaurant, Raohe Night Market, Fu-Ba-Wang Pigs' Knuckles Restaurant, and Li Yuan Soup Dumpling House.

Some of his most recent vacation spots include Vietnam-Hanoi, China-Shenzhen, Shanghai, and Beijing.

TECHNOLOGIES USED IN THE COMPANY

We collect information on the technologies by looking through open positions at NVIDIA on the official website and LinkedIn.

The following are the possible technologies used in NVIDIA:

- SAP ECC, SAP S/4HANA: The ERP system NVIDIA uses is SAP, either SAP ECC or SAP S/4HANA, and might be in the middle of transitioning.
- HANA DB: HANA DB is standard with SAP S/4HANA.
- Linux/Unix OS: It is not clearly stated which Linux/Unix OS that NVIDIA uses and what for. Red Hat Enterprise Linux (RHEL) could be one that NVIDIA uses and is a standard combination with SAP S/4HANA.
- Cloud services: Azure, AWS, GCP. NVIDIA provides services based on research on the three cloud services and could also be using Azure for Active Directory.
- Windows OS: Active Directory requires Windows OS to work.
- Intel Vtune: NVIDIA uses this tool to analyze performance for Linux and Windows.
- CUDA: It is a product of NVIDIA, and NVIDIA may use it within its IT infrastructure to provide services to its clients.
- Several programming languages and tools are used within NVIDIA: C, C++, Python, Perl, Tensorflow, Pytorch, and Jupyter Notebook.

The following are types of tools NVIDIA uses, but we are not certain what it uses:

- One or more of these Software Asset Management tools: Flexera, Service Now, Productiv, Zylo
- One or more of these Schedulers: SLURM, LSF, UGE
- One or more of these Automation tools: Ansible, Puppet
- Must be using one or more of these code version control and deployment tools: GitHub, GitLab, Perforce, Jenkins, Docker, Kubernetes

TECHNOLOGY VULNERABILITIES

In the following section, we list recent, higher exploitable CVEs that have a higher chance of being related to NVIDIA for technologies that we are more certain that NVIDIA uses. Our main sources of vulnerabilities are the CVE library and the NIST Vulnerability Database.

SAP S/4HANA:
Recent vulnerabilities are related to authorization.

CVE-2024-37172
SAP S/4HANA Finance (Advanced Payment Management) does not perform the necessary authorization check for an authenticated user, resulting in the escalation of privileges. As a result, it has a low impact on confidentiality and availability but there is no impact on the integrity.

CVE-2024-34691
Manage Incoming Payment Files (F1680) of SAP S/4HANA does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. As a result, it has a high impact on integrity and no impact on the confidentiality and availability of the system.

CVE-2024-30217
Cash Management in SAP S/4 HANA does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. By exploiting this vulnerability, an attacker can approve or reject a bank account application affecting the integrity of the application. Confidentiality and Availability are not impacted.

CVE-2024-30216
Cash Management in SAP S/4 HANA does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. By exploiting this vulnerability, an attacker can add notes in the review request with a 'completed' status affecting the integrity of the application. Confidentiality and Availability are not impacted.

RHEL:
CVE-2024-6387
A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition that can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set period.

CVE-2024-6238

pgAdmin <= 8.8 has an installation Directory permission issue. Because of this issue, attackers can gain unauthorized access to the installation directory on the Debian or RHEL 8 platforms.

SAP ECC:

CVE-2024-22132

SAP IDES ECC systems contain code that permits the execution of arbitrary program code of the user's choice. An attacker can therefore control the behavior of the system by executing malicious code which can potentially escalate privileges with low impact on confidentiality, integrity, and availability of the system.

Azure:

CVE-2024-37897

SFTPGo is a full-featured and highly configurable SFTP, HTTP/S, FTP/S, and WebDAV server - S3, Google Cloud Storage, Azure Blob. SFTPGo WebAdmin and WebClient support password reset. This feature is disabled in the default configuration. In SFTPGo versions before v2.6.1, if the feature is enabled, even users with access restrictions (e.g. expired) can reset their password and log in.

CVE-2024-27099

The uAMQP is a C library for AMQP 1.0 communication to Azure Cloud Services. When processing an incorrect `AMQP_VALUE` failed state, may cause a double free problem. This may cause an RCE.

Windows OS:

CVE-2024-7980

Insufficient data validation in Installer in Google Chrome on Windows before 128.0.6613.84 allowed a local attacker to perform privilege escalation via a crafted symbolic link. (Chromium security severity: Medium)

CVE-2024-7358

A vulnerability was found in Point B Ltd Getscreen Agent 2.19.6 on Windows. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file getscreen.msi of the component Installation. The manipulation leads to the creation of temporary files with insecure permissions. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The identifier VDB-273337 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but was not able to provide a technical response in time.

CVE-2024-39600 *Also relates to SAP

Under certain conditions, the memory of SAP GUI for Windows contains the password used to log on to an SAP system, which might allow an attacker to get hold of the password and impersonate the affected user. As a result, it has a high impact on the confidentiality but there is no impact on the integrity and availability.

CVE-2024-4030
On Windows a directory returned by tempfile.mkdtemp() would not always have permissions set to restrict reading and writing to the temporary directory by other users, instead usually inheriting the correct permissions from the default location. Alternate configurations or users without a profile directory may not have the intended permissions.This issue was caused by Python not supporting Unix permissions on Windows.

Azure, AWS, GCP:
CVE-2023-37262
CC: Tweaked is a mod for Minecraft that adds programmable computers, turtles, and more to the game. Before versions 1.20.1-1.106.0, 1.19.4-1.106.0, 1.19.2-1.101.3, 1.18.2-1.101.3, and 1.16.5-1.101.3, if the cc-tweaked plugin is running on a Minecraft server hosted on a popular cloud hosting providers, like AWS, GCP, and Azure, those metadata services API endpoints are not forbidden (aka "blacklisted") by default. As such, any player can gain access to sensitive information exposed via those metadata servers, potentially allowing them to pivot or privilege escalate into the hosting provider.

CVE-2023-37261
OpenComputers is a Minecraft mod that adds programmable computers and robots to the game. This issue affects every version of OpenComputers with the Internet Card feature enabled; that is, OpenComputers 1.2.0 until 1.8.3 in their most common, default configurations. If the OpenComputers mod is installed as part of a Minecraft server hosted on a popular cloud hosting provider, such as AWS, GCP, and Azure, those metadata services' API endpoints are not forbidden (aka "blacklisted") by default. As such, any player can gain access to sensitive information exposed via those metadata servers, potentially allowing them to pivot or privilege escalate into the hosting provider. In addition, IPv6 addresses are not correctly filtered at all, allowing broader access into the local IPv6 network. This can allow a player on a server using an OpenComputers computer to access parts of the private IPv4 address space, as well as the whole IPv6 address space, to retrieve sensitive information. OpenComputers v1.8.3 for Minecraft 1.7.10 and 1.12.2 contains a patch for this issue. Some workarounds are also available. One may disable the Internet Card feature completely. If using OpenComputers 1.3.0 or above, using the allow list (`opencomputers.internet.whitelist` option) will prohibit connections to any IP addresses and/or domains not listed; or one may add entries to the block list (`opencomputers.internet.blacklist` option).

Intel Vtune:

CVE-2024-29015

An uncontrolled search path in some Intel(R) VTune(TM) Profiler software before version 2024.1 may allow an authenticated user to potentially enable escalation of privilege via local access.

CVE-2023-45320

An uncontrolled search path element in some Intel(R) VTune(TM) Profiler software before version 2024.0 may allow an authenticated user to potentially enable escalation of privilege via local access.

CVE-2022-41982

An uncontrolled search path element in the Intel(R) VTune(TM) Profiler software before version 2023.0 may allow an authenticated user to potentially enable escalation of privilege via local access.

CUDA:

CVE-2024-0111 *This vulnerability has been documented since 2023 and has not yet been resolved.

NVIDIA CUDA Toolkit contains a vulnerability in the command 'cuobjdump' where a user may cause a crash or produce incorrect output by passing a malformed ELF file. A successful exploit of this vulnerability may lead to a limited denial of service or data tampering.

Other vulnerabilities to take into account:

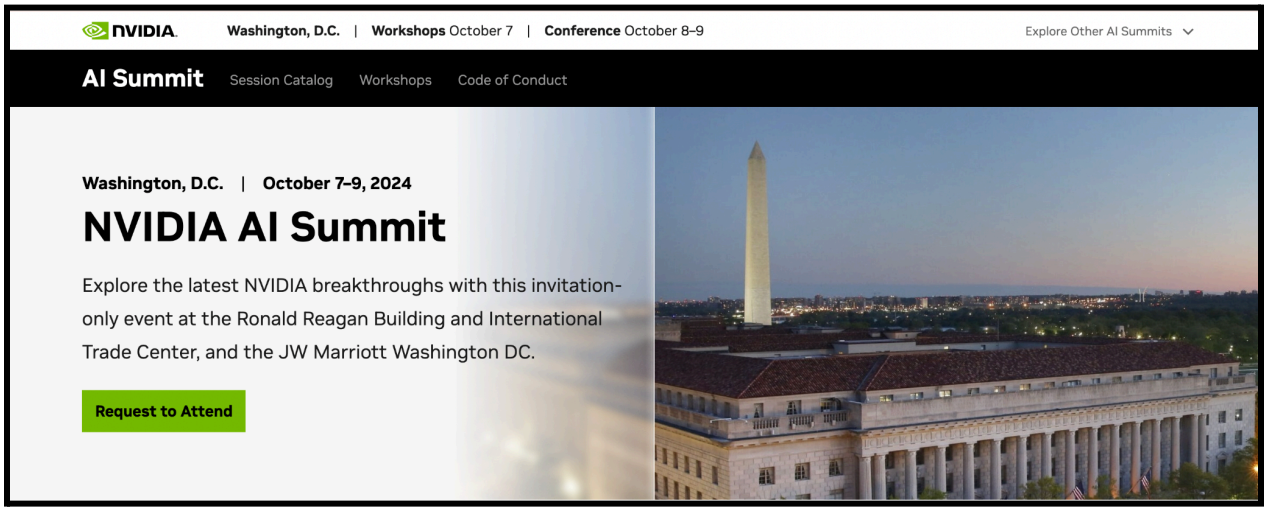
Since NVIDIA could be using its products to provide services to clients, vulnerabilities related to NVIDIA's products could also be exploited. NVIDIA itself discloses any known vulnerability within its products, and another website listed NVIDIA's product vulnerability trends throughout the years.

PLACES TO MEET THE EMPLOYEES

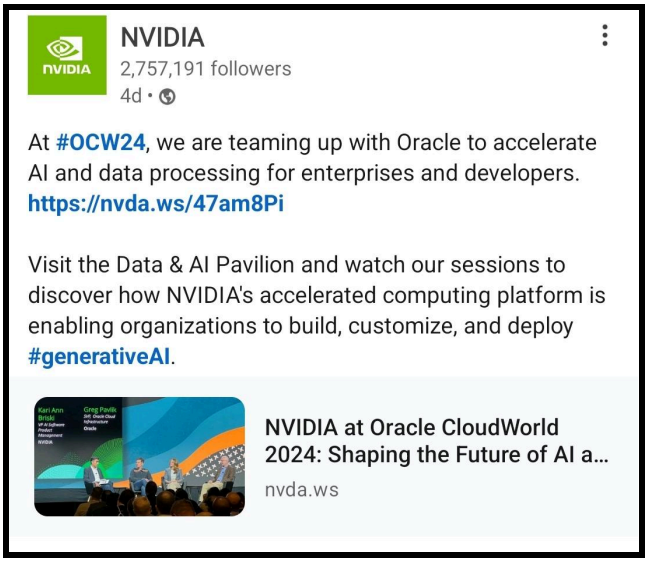
There are various places and occasions where one can meet NVIDIA employees. Some of them are annual events, while others depend on the lifestyle of the individual employees. Places visited by the employees can also be traced by following their social media and other public data repositories. Few of them have been listed here.

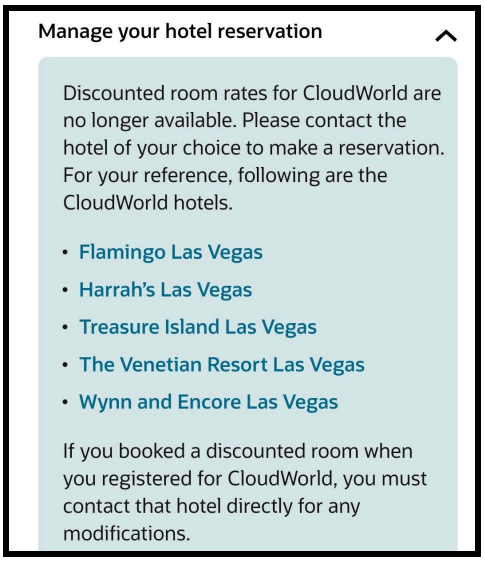
Conferences & Events

- SIGGRAPH: SIGGRAPH stands for "Special Interest Group on Computer Graphics and Interactive Techniques". NVIDIA is one of the most prominent organizations attending this conference each year. In 2024, many employees, including the CEO were in attendance.
- AI Summit Washington, D.C.: At AI Summit Washington, D.C., NVIDIA will be conducting hands-on workshop training and conference sessions. These events provide opportunities to network with their employees and possibly have more intimate conversations.



- Oracle Cloud World: Employees of NVIDIA will be present at Oracle Cloud World 2024. The site also lists some hotels for the attendees and speakers to stay.





- Utah Cloud and AI/ ML Summit: An AI/ML and Cloud Summit in the last week of September 2024, where the Head of ML in NVIDIA will be present. Most likely his team and other representatives will be present to coordinate the event.
- Emmy Awards: CEO Jensen Huang will receive the Charles F. Jenkins Lifetime Achievement Award during the 76th Engineering, Science & Technology Emmy Awards.

Some more niche and private events and conferences are listed below, which NVIDIA employees usually attend:

- Wells Fargo TMT Summit: Terranea Resort in Rancho Palos Verdes, California
- GPU Festival: ExCel London, Royal Victoria Dock, 1 Western Gateway London
- BofA Securities 2024 Global Technology Conference: The Westin St. Francis Hotel, San Francisco, CA
- Morgan Stanley Technology, Media & Telecom Conference: The Palace Hotel in San Francisco, CA

Restaurants/Bars/Cafes Near Offices

Below listed are some of the restaurants that are around NVIDIA offices, that we speculate that the employees might visit during their breaks and outside office hours.

Headquarters

- **Restaurants:**
  - Puesto Santa Clara
  - Chennai Tiffins Indian Restaurant
- **Bars:**
  - Metro City Restaurant & Bar
  - Fibbar MaGees
  - Quarter Note Bar & Grill
- **Cafes:**
  - Coffee & More Cafe
  - Bagel Street Cafe

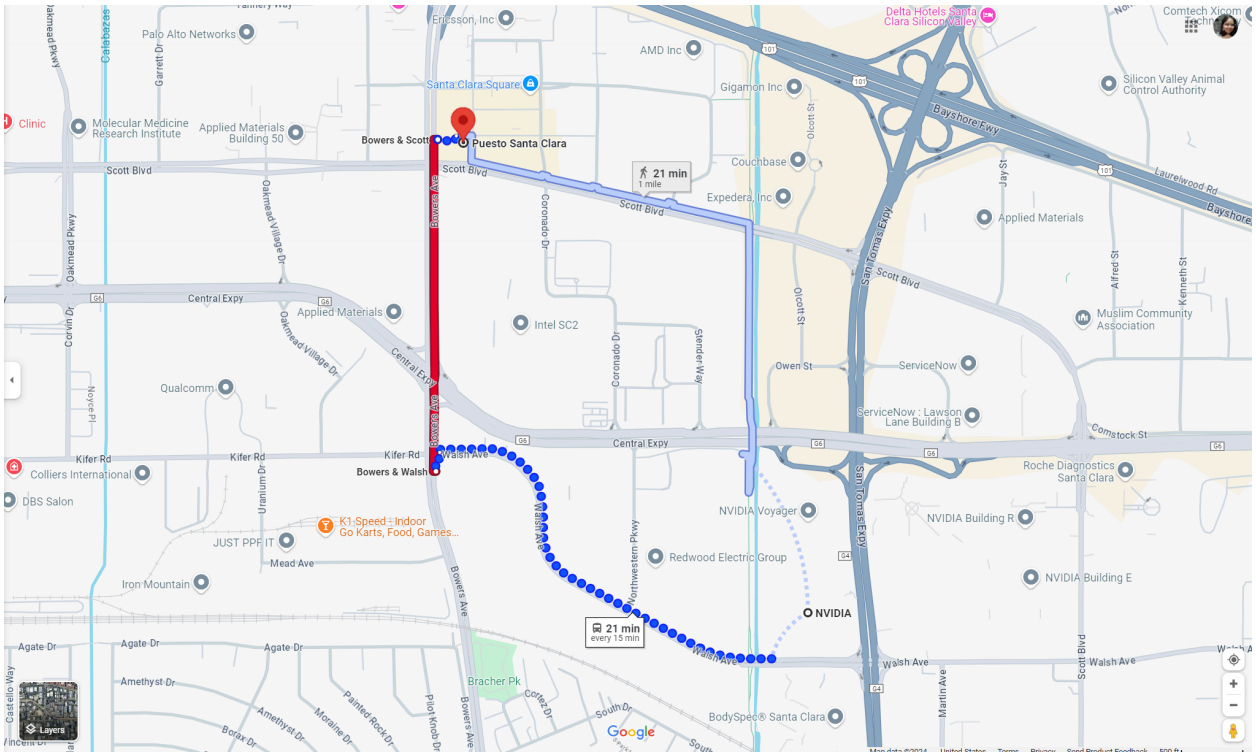


Figure: Location of Puest Santa Clara from NVIDIA headquarters

Tokyo Office

- **Restaurants:**
  - Tsutsui
  - Lawry’s The Prime Rib Akasaka
  - Akasaka Ogino
  - Kyoto Hyoki Akasakaten
  - Kien
- **Bars**:
  - Satin
  - Dracula
- **Cafes**:
  - BunCoffee Akasaka
  - Key's Cafe

Figure: Photo of Tsutsui which is located near the NVIDIA Tokyo office

Bengaluru Office

- **Restaurants:**
  - Punjabi Chulha
  - North Indian Bhukkads - NIB
  - Neo Kitchen By Hilton
- **Bars:**
  - One for the Road
  - Nagavara SOCIAL
- **Cafes**:
  - De Cafe Max
  - The Mint Cafe

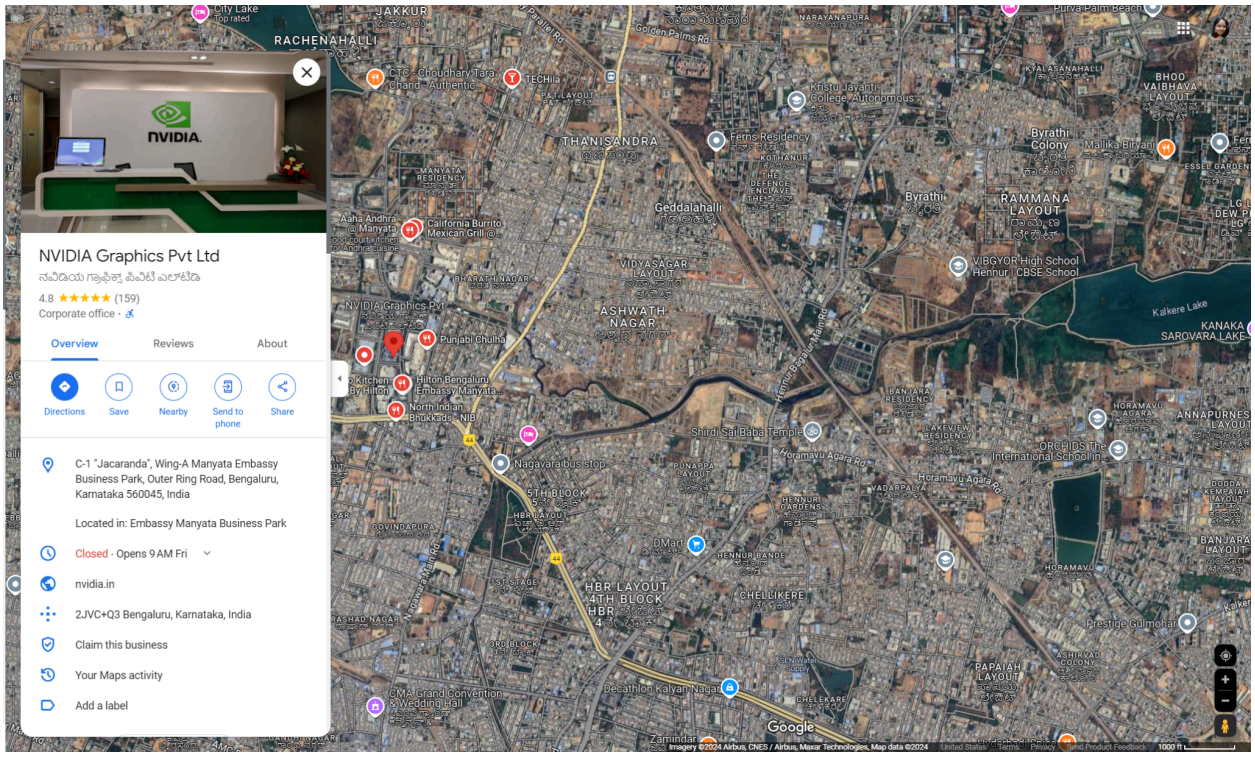


Figure: Map of restaurants near the NVIDIA Bengaluru office

London Office

- Restaurants:
    - Luna Rossa Italian Restaurant
    - Indigo at One Aldwych Restaurant
- Bars:
    - Banyan Bar & Kitchen
    - The Atrium Bar
- Cafe:
    - Costa Coffee
    - The Jazz Cafe

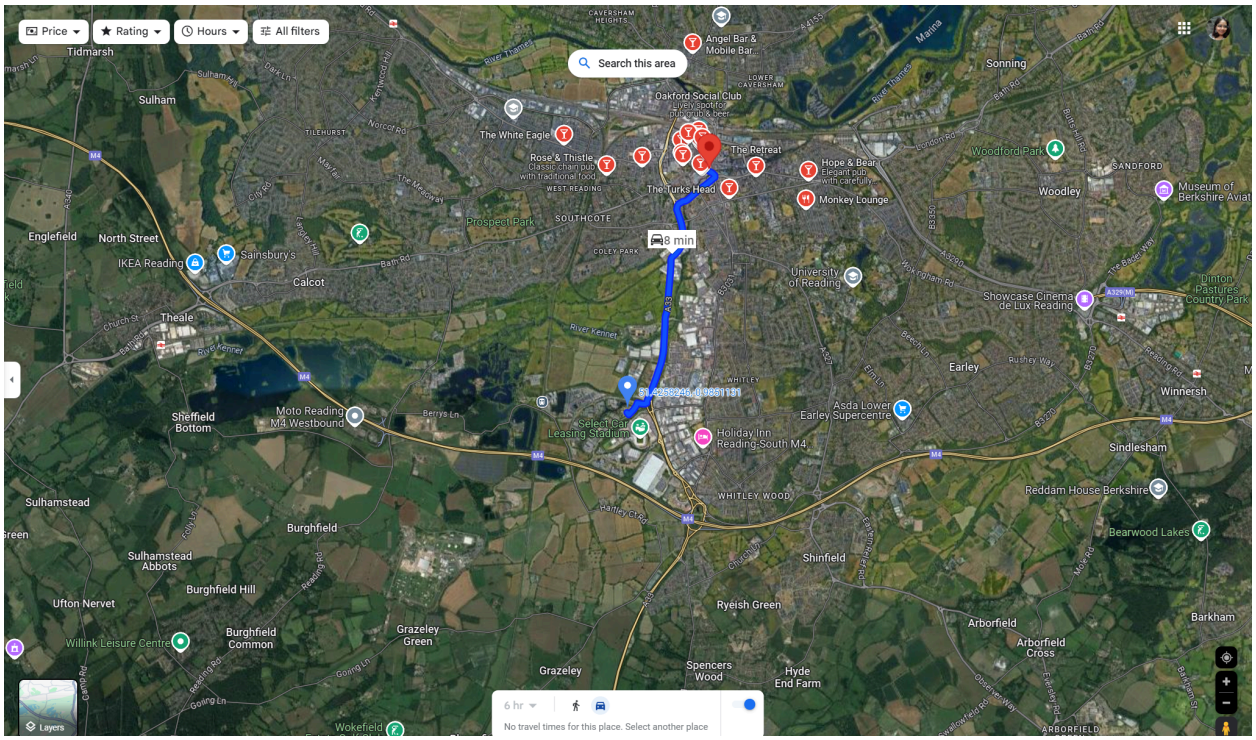
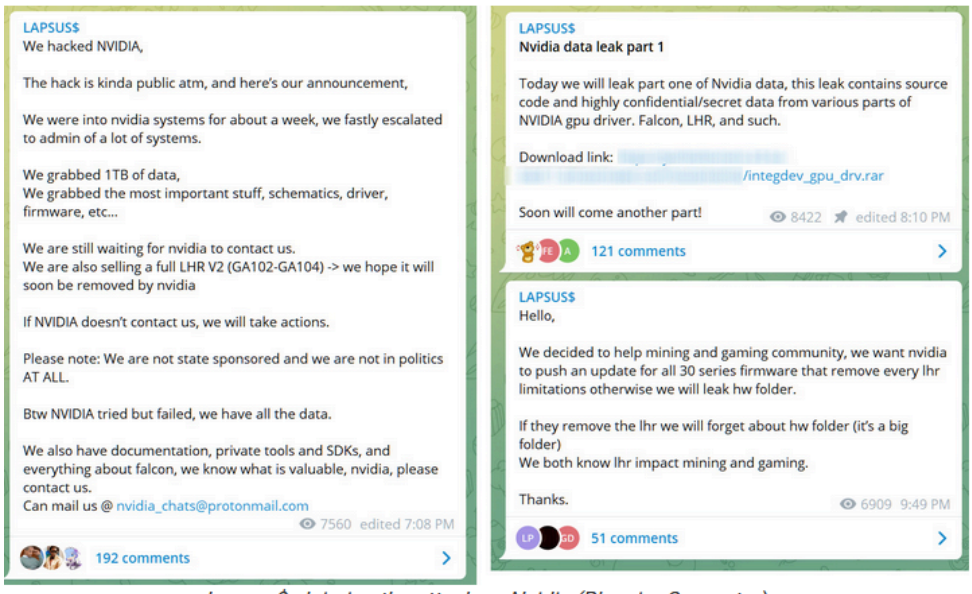


Figure: Map of bars near NVIDIA London office

ADDITIONAL INTEL

Data Breach

In 2022, NVIDIA was targeted by Lapsu$. During the breach, they were able to extract 1 terabyte of data from their servers. 20 gigabytes of that data included hashes of employee passwords.



Lapsus$ claiming the attack on Nvidia (BleepingComputer)

"However, we are aware that the threat actor took employee credentials and some NVIDIA proprietary information from our systems and has begun leaking it online. Our team is working to analyze that information", Nvidia told BleepingComputer.

Antitrust Lawsuit

On August 5th, 2024, the Department of Justice announced that they are investigating complaints that Nvidia is cornering the market and pressuring its customers to unfairly return business.

"Nvidia is the world's chip gatekeeper," the groups wrote, arguing the company had "bullied its way into a prominent investment position" by leveraging scarce supply alongside tactics like blocking customers from doing business with competitors. "Such a company deserves the most aggressive scrutiny that the Department of Justice can bring to bear."