

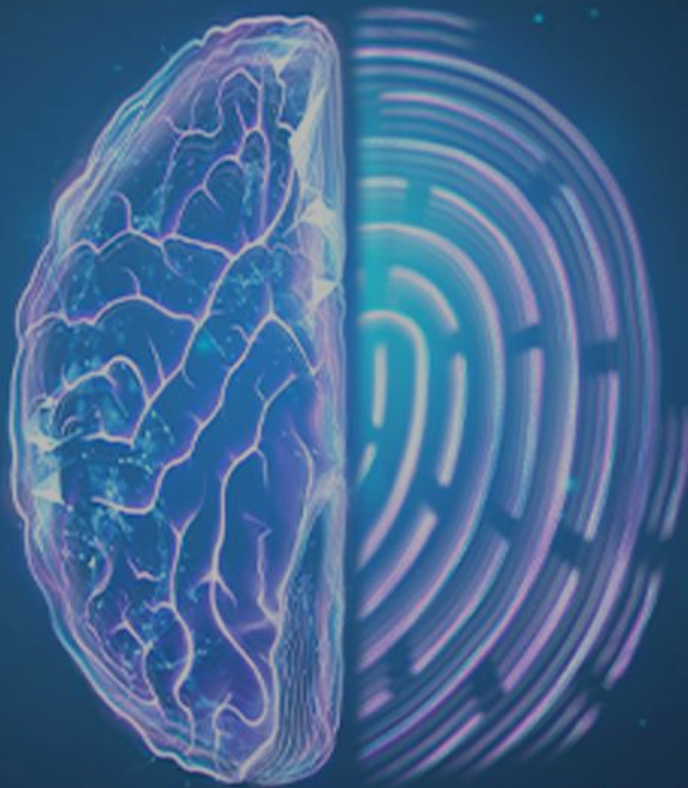
# en GØ ge

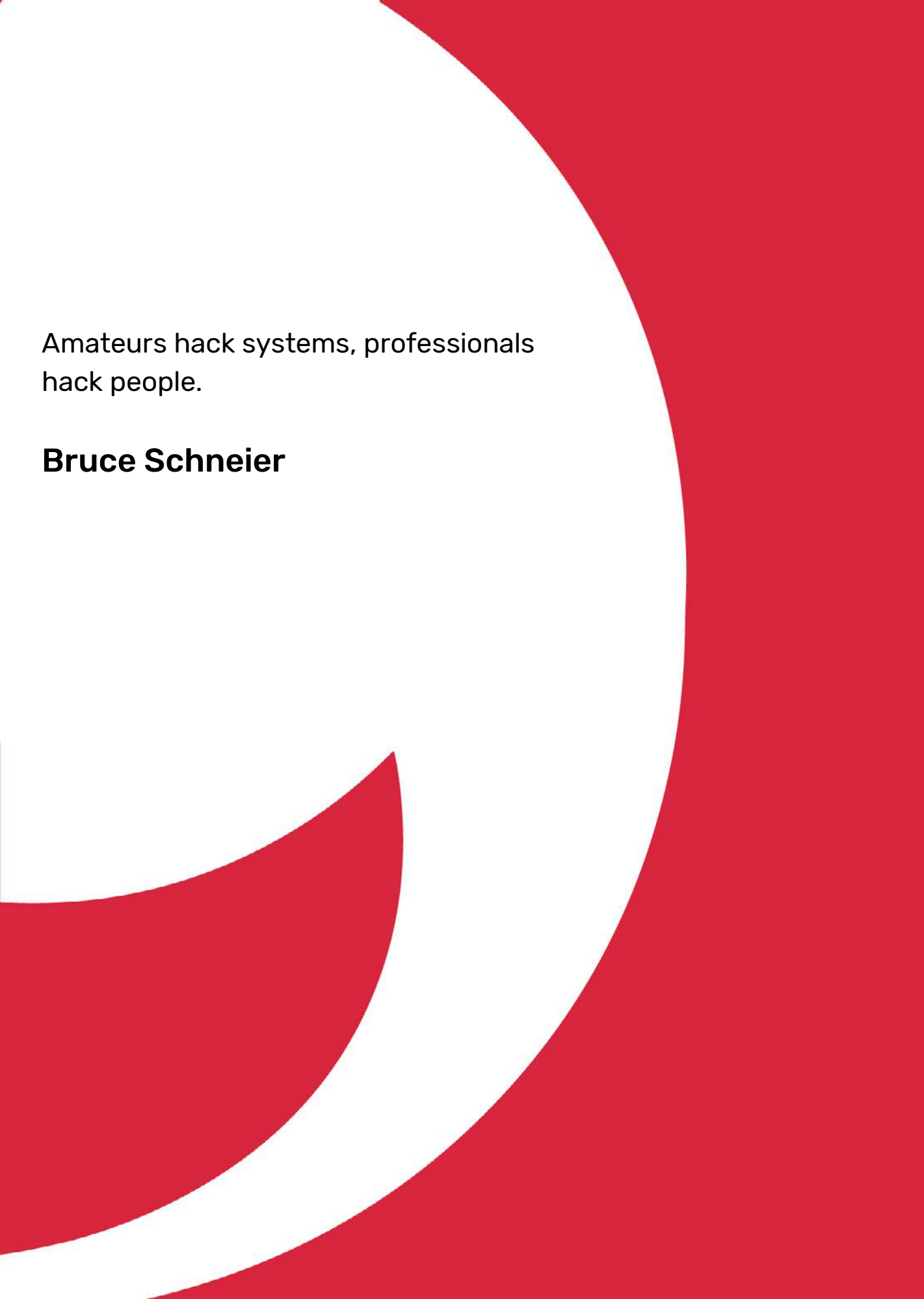
Cybersecurity Special Edition

October 2022

*"Security is always excessive until it's  
not enough."*

**Robbie Sinclair**



The background consists of a solid red field. A large white curved shape, resembling a thick arc or a partial circle, is positioned on the left side, extending from the top towards the bottom. A smaller, similar white curved shape is located below the larger one, also on the left side. The text is placed within the white area.

Amateurs hack systems, professionals  
hack people.

**Bruce Schneier**

# Table of Contents

## 09

### **Cybersecurity as a Service (CaaS) – a Cognitive GS Lab | GAVS Model**

Cybersecurity is essential to most businesses. We bring you an overview of the CaaS model of GS Lab | GAVS.

## 16

### **3D: DANE-DNSSEC-DNS**

**Aravindh S** writes about the technology that can secure DNS. – *“Beside, Security fails with Opportunistic Encryption which leads to unauthorized and compromised certificates, Man-in-the-Middle attacker may downgrade session to non-TLS at the time of email communications.”*

## 14

### **Role of Adaptive Authentication in Access Management for Cybersecurity**

**Sundaramoorthy S** writes about the latest technology in Access Management that offers better security than the current MFA. – *“A basic authentication with user id and password is enough to unlock the system when it is a standalone system, but when systems are connected to network which holds business critical data, the system needs multiple layers of security to ensure the systems are safe.”*

## 18

### **Malware Analysis Benefits Incident Response**

**Vishnu Raj** throws light on why malware analysis is one distinct area of security that has become increasingly beneficial to the process. – *“It helps responders understand the extent of a malware-based incident and identify additional hosts or systems that could be affected.”*

Cyber-attacks have come a long way - from being motivated by financial interests, to being used for political interests (e.g., cyberwarfare), most recently. The world has witnessed a dramatic increase in the number of cybersecurity breaches in the past couple of years, enabled partially by the number and variety that are connected. A vulnerability in even one device can enable hackers to get access to all the others that are connected to it. The increased adoption of cloud and IoT devices also add to the complexity.

Advances in technology have enabled cybersecurity teams defend themselves better against such attacks. Cybersecurity strategies are not reactive any longer. Organizations now invest in resources to build comprehensive strategies to prevent and minimize the loss from cyber-attacks.

A concept that has been gaining ground is 'Zero Trust'. It is a broad concept, but basically means that no part of a company's IT systems should assume that any other part—human or software—is who or what it claims to be. All systems are assumed to be compromised already.

The zero-trust architecture keeps validating the identity at every stage of a digital interaction. It also includes giving the 'least-privilege access' to the users.

However, humans remain the weakest link. Knowingly or unknowingly, people have made some of the major cyber breaches possible. Also, as consumers, we should be aware and must make informed decisions about using secure apps/software/devices and not giving away our personal data.

We are celebrating Cybersecurity Awareness month at GS Lab | GAVS entire October. We have curated an interesting line up of articles in this edition.

The members of the Cybersecurity team have written, '**Cybersecurity as a Service (CaaS) – a Cognitive GS Lab | GAVS Model**'.

**Aravindh S** has written, '**3D: DANE-DNSSEC-DNS**'.

**Sundaramoorthy S** has written, '**Role of Adaptive Authentication in Access Management for Cybersecurity**'.

**Vishnu Raj** has written, '**Malware Analysis Benefits Incident Response**'.

### Happy Reading!

I would like to thank Gayatri Rairkar who's the Marketer for the Cybersecurity vertical at GS Lab | GAVS for her efforts in making this edition possible.

# Editor's Note

SOUMIKA DAS



"Cybersecurity matters!!

As cybersecurity is becoming important for all the organizations, it is also becoming challenging to make everyone aware of these challenges. Organizations and people are becoming a target especially after pandemic.

Working in this field helps me stay informed about the ongoing and emerging threats, to raise the cyber awareness. I believe this as an opportunity to acquire more and more knowledge and experience." -**Gayatri Rairkar**

# Leader Speak



*“Security is of paramount importance always and more so in today’s times where everything is in hybrid models. Technology is advancing well and so is human intelligence. As a key service provider and partner, it is paramount that we protect ourselves and our customers and help customers prevent any fraudulent issues and potential vulnerabilities. With the advent of AI/ML we can move towards proactive approaches to prevent security incidents. It is critical that we embrace this solution and service offering as a key discussion with our customers and equally important that we embrace and skill ourselves as well in these areas as these are key even for our regular operations and any application development.”*

**Balaji Uppili,**  
COO, GS Lab | GAVS



*“It’s time we move towards real-time on anything we do. The vulnerabilities must be detected as soon as they come into the system, not after three or six months. I don’t think today’s digital transformation can afford to wait for any periodic checks. Everything must be instantaneous and real-time.”*

**S Chandra,**  
SVP and Head of IP and Infra, GS Lab | GAVS



*“As we continue our journey in Information Technology where Financial transactions, Personal Communications (mail, audio, video etc.) and dependency of day-to-day life increases on information technology, AAA (Audit, Authorization and Authentication) becomes a must to detect, identify and deal with potential cybercrimes. Cybersecurity is a MUST to enable us to deal with threats. It will continue to gain more importance.”*

**Asit Shah,**  
Vice President & General Manager, GS Lab | GAVS

# What's New In Cyber Security Tech



## Quantum Cryptography implemented for the first time

An international team has successfully implemented an advanced form of quantum cryptography for the first time. Moreover, encryption is independent of the quantum device used and therefore even more secure against hacking attempts.



## Linux Tool Aims to Guard Against Supply Chain Attacks

Security firm Chainguard has launched a Linux distribution called Wolfi, a simple, open-source way for organizations to defend the cloud against attacks. It is designed specifically for how digital systems are actually built today in the cloud.



## Thinking like a cyber-attacker to protect user data

MIT researchers have shown that a component of modern computer processors that enables different areas of the chip to communicate with each other is susceptible to a side-channel attack. They reverse-engineered the on-chip interconnect to study how this kind of attack would be possible and used this knowledge to develop 2 mitigation strategies.



## Secure communication with light particles

Quantum computers offer many novel possibilities, but they also pose a threat to internet security since they make common encryption methods vulnerable. Based on the so-called quantum key distribution, researchers have developed a new, tap-proof communication network. The new system is used to exchange symmetric keys between parties in order to encrypt messages so that they cannot be read by third parties.

# Secure Application Development Practices For Startups

A session by Mr. Kannan Srinivasan at the NASSCOM Event

When you think of startups the first things that come to your mind are Uber, Airbnb, Lyft, Paytm etc. They all had a unique idea supported by an application which is simple to use, reliable and most of all secure. There are other startups that started with great ideas but failed miserably due to poor information security practices.

Startups have very limited to no time to focus on information security due to lack of skilled resources and/or additional funds to invest in security tools. At a high level their reasons for not following information security are justifiable however regulations such as GDPR, HIPAA, PDPA, etc. are very stringent on the data security requirements and they levy a huge penalty for not adhering to the security and privacy principles.

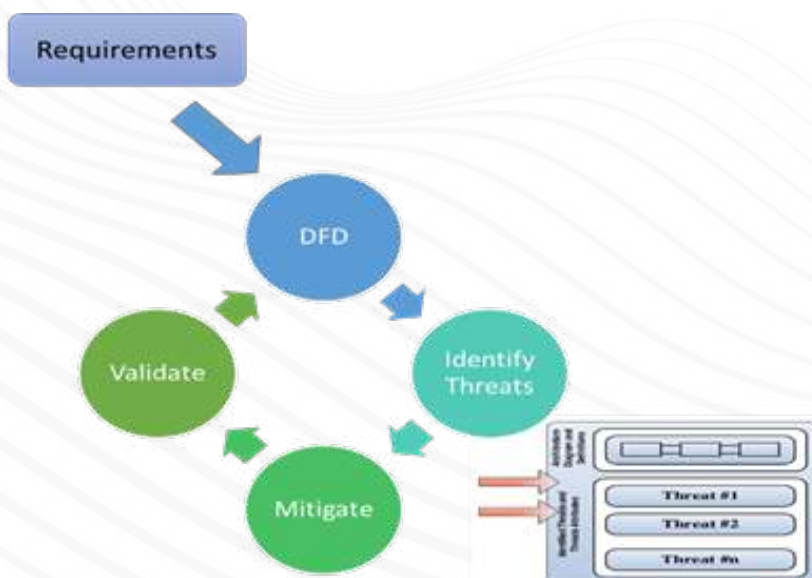
Larger companies are no exception, as any lapse in the security process even once can lead to major breaches leading to penalties and a dent in their reputation. British Airways recently paid a hefty 183 million penalty for breaching client data. SQL injection vulnerability in Starbucks code resulted in loss of one million financial data records. Well, the list goes on and on but the attack vector is mostly similar. Increased adoption of microservices, cloud and DevOps have all increased the threat vectors of the application.

We recently conducted a session at the NASSCOM Centre of Excellence IoT & AI to guide startups on how to build and deploy secured products. It was recommended to have the following structure for security process



**Threat modeling:** Think Ahead on what can go wrong, weigh the risks and act accordingly. The following aspects are taken care as part of threat modelling:

- o Structured process to identify and enumerate potential threats
- o Help security team with an analysis of what security controls are to be put in place
- o Collaboration between Security Architects, Security Operations, Network Defenders, SOC
- o Threat modeling helps threat intelligence analysts identify, classify, and prioritize threats



**Coding and Testing:** Create and enforce developers to use secure coding practices. Secure coding practices should address the following areas:

- Input validation
- Authentication
- Authorization
- Cryptography
- Logging and Auditing
- Output Encoding
- Session Management

Static Application Security Testing (SAST) software inspects and analyzes an application's code to discover security vulnerabilities without executing code. These tools are frequently used by companies with continuous delivery practices to identify flaws prior to deployment.

Dynamic application security testing (DAST) is a method of AppSec testing that examines an application while it is running, without knowledge of the application's internal interactions or designs at the system level, and with no access or visibility into the source program.

Testing should consider the following OWASP Top 10 Vulnerabilities

- o Injection
- o Broken authentication
- o Sensitive data exposure
- o XML external entities (XXE)
- o Broken access control
- o Security misconfigurations
- o Cross site scripting (XSS)
- o Insecure deserialization
- o Using components with known vulnerabilities
- o Insufficient logging and monitoring

**Deploy & Monitor:** Perform Vulnerability Assessment of the infrastructure and Penetration Testing to ensure that there are no vulnerabilities in the production environment that can be exploited.

The best part is there are multiple opensource tools that are available to address the above mentioned process.

A few pictures from the recent Nasscom event:



### About the Speaker

Kannan has over 21 years of experience in Cybersecurity and Delivery Management. He is a subject matter expert in the areas of Cloud security, infra security including SOC, Vulnerability Management, GRC, Identity and Access Management, Managed Security Services. He has led various security transformation engagements for large banks and financial clients.



# Cybersecurity as a Service (CaaS)

## A Cognitive GS Lab | GAVS Model

With the harmful consequences and high costs of security breaches, organizations are having to fight a constant battle to stay safe and keep their data secure.

As Cybersecurity is an essential need of business, here is how GS Lab | GAVS CaaS is structured to offer a phenomenal service.

### Highlights

- 75 customers onboarded
- 10000+ events monitored per day
- 1000+ applications integrated with IAM/IDAM solution
- 15000+ mobile devices managed
- 100+ trained & certified cybersecurity professionals
- 1000+ SSO connectors developed for multiple on-prem & cloud end-points
- 80000+ endpoints are managed
- 50+ Provisioning adapters developed for multiple on-prem & cloud end points

### Key SOC Locations

US (NY, NC, FL) | India

### Recognitions



GAVS has been announced as a winner of the 2022 Fortress Cyber Security Award by the Business Intelligence Group in the 'Authentication & Identity' category.



GS Lab has been recognized as OneLogin's Global Integration Partner for 2021.

With our expertise in product engineering, we are an ideal partner to implement & integrate OneLogin's Unified Access Management Solution within your ecosystem.

# GS Lab | GAVS Cybersecurity Services Areas

| Infra Security  | Digital IDM   | GRC  | Vulnerability Mgmt   | Data Privacy  | BCMS  | Cloud Security  |
|---|---|--|--|---|---|---|
| <ul style="list-style-type: none"> <li>• SOC</li> <li>• Datacenter security</li> <li>• System Security</li> <li>• Infra &amp; Network Security</li> <li>• Security Engineering</li> <li>• End point security</li> <li>• Encryption</li> </ul> | <ul style="list-style-type: none"> <li>• PIM/PAM</li> <li>• RBA/RPA</li> <li>• Tools &amp; Automation</li> <li>• IDM/ IAM</li> <li>• User Lifecycle Management</li> <li>• User Behavior Analysis (UBA)</li> <li>• RBAC, ABAC &amp; Adaptive Access Control</li> </ul> | <ul style="list-style-type: none"> <li>• Identity Gov/ IMA</li> <li>• Gov/ Gov</li> <li>• Risk Management</li> <li>• Compliance</li> <li>• Testing</li> <li>• Policies &amp; Standards</li> <li>• Data Security Governance</li> <li>• Audit &amp; Certification</li> <li>• Training &amp; Awareness</li> <li>• Security Assurance</li> </ul> | <ul style="list-style-type: none"> <li>• SIEM</li> <li>• SAST</li> <li>• Vulnerability Assessment</li> <li>• DAST</li> <li>• Penetration Test</li> <li>• Infra vulnerability scan</li> <li>• Application Security</li> <li>• Mobile &amp; Container Security</li> <li>• Customer Identity Access Mgmt. (CIAM)</li> </ul> | <ul style="list-style-type: none"> <li>• Privacy implementation (GDPR, CCPA, PDPB)</li> <li>• Data classification</li> <li>• Privacy policies and standards</li> <li>• PIA</li> <li>• DPIA</li> <li>• Privacy incident management</li> <li>• HIPAA</li> </ul> | <ul style="list-style-type: none"> <li>• BCMS implementation</li> <li>• DR Program Management</li> <li>• BCP policies and standards</li> <li>• BIA</li> <li>• BCP: Plan and testing</li> <li>• DR plan and testing</li> </ul> | <ul style="list-style-type: none"> <li>• Cloud Security Assessment &amp; architecture</li> <li>• SecOps</li> <li>• Cloud Governance</li> <li>• Security Testing</li> <li>• Cloud Data Security</li> <li>• Regulatory&amp; standard compliance</li> <li>• User &amp; developer awareness</li> <li>• DevSecOps</li> <li>• Incident Management &amp; response</li> <li>• KPI Monitoring &amp; Reporting</li> </ul> |

Healthcare | BFSI | Pharma | Hi-Tech | E-Commerce | Manufacturing | Ed-Tech | ISV

Copyright © 2022 GS Lab and/or GAVS as applicable. All rights reserved.

# GS Lab | GAVS Cybersecurity Services

|   |   |
|---|---|
|  <h3>Consulting – RoadMap &amp; Strategy</h3> <ul style="list-style-type: none"> <li>• CISO- Level Gap Analysis</li> <li>• Strategy &amp; Advisory Services</li> <li>• CISO level reporting</li> <li>• Security program design</li> <li>• Security controls and compliance</li> <li>• SIEM Audit and Compliance</li> </ul>   |  <h3>Implementation</h3> <ul style="list-style-type: none"> <li>• Analysis of existing environment</li> <li>• Solution engineering</li> <li>• Implementation Roadmap</li> <li>• Customization and implementation</li> <li>• Deployment</li> </ul>  |
|  <h3>Support &amp; Maintenance</h3> <ul style="list-style-type: none"> <li>• Deploy &amp; Maintain solutions</li> <li>• Training &amp; Knowledge Transfers</li> <li>• 24x7 production support activities</li> <li>• Incident Management tickets</li> <li>• Upgrades the product solution</li> <li>• Migrations and Enhancements</li> <li>• Documentations</li> </ul> |  <h3>Product Engineering</h3> <p><b>Product Engineering Lifecycle covered</b></p> <ul style="list-style-type: none"> <li>• Design</li> <li>• Architecture</li> <li>• Development - SaaS based, Micro-services, UI</li> <li>• QA (Manual and automation)</li> <li>• L1/ L2/ L3 Support</li> </ul> |

# Our full line-up of Managed Security Service



## Business Outcomes

-  Effective usage of security tools for improved ROI
-  Reduction in security incidents / data breaches
-  Operational Excellence across the value chain
-  Compliance to privacy and regulatory requirements
-  Security transformation through automation
-  ^ 30% cost savings using GAVS' remote 24/7 SOC model

# Staying on top of cyber threats with our CISO Advisory Services

### CISO's Challenge Areas:

- Market trend aligned Cybersecurity strategy and implementation roadmap
- Adherence of good governance practices across all aspects of Cybersecurity giving holistic risk posture
- Cost optimization & continuously improve the services by leveraging AI / ML

### Industry Trends

- Thought leadership on Market trends (Ex: Gartner predictions)
- Provide insights on emerging Information Security regulations
- Help to make right decisions on Digital initiatives
- Help on Cybersecurity cost optimization programs & Cybersecurity Budgets.
- Advisory on new tools & processes for technology upgrade

- Quarterly connect with CxOs to highlight current trends and focus areas

### Strategic Initiatives

- Support to choose right tools/products
- Help to implement right cyber defence solutions
- Adoption of SASE model
- Perform Cyber risk quantification
- Develop digital identity strategy

- Double click view of all strategic initiatives

### Audit & Compliance

- Support to implement an effective governance regime and ensure the correct level of security for your business
- Support to perform Security health check – using an industry-standard framework (NIST)
- Provide inputs to Information security management system (ISMS) implementation
- Advise on third party risk assessment

- 100% adherence to compliance requirements

### Cybersecurity Operations

- Adoption of AI/ML use cases to improve security operating
- Threat detection assessment – using a custom threat model
- Review application, network, infrastructure, endpoints and recommend suggestions

- 30% cost reduction through adoption of AI/ML and optimization

# IP led Acceleration



## ZIF Zero Incident Framework

AIOps based TechOps Platform Zero Incident Framework™ (ZIF™) that enables proactive detection and remediation of incidents helping organizations drive towards a Zero Incident Enterprise™

ZIF helps:

- Auto-discover an application and understand the dependencies between the various components
- End-to-end monitoring of all the devices, infrastructure components and applications,
- Baseline the acceptable performance behavior of these components and alert any potential abnormal patterns, through machine learning.



## IdentityDesk

IdentityDesk is a complete user lifecycle and access management solution that helps your IT team streamline the end users' journey — from provisioning to change management to de-provisioning.

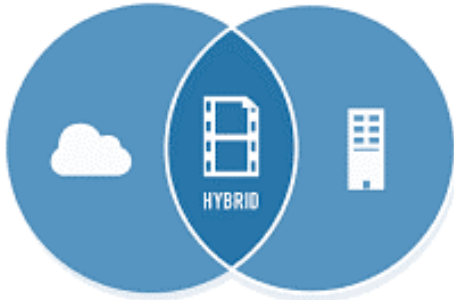
It helps:

- Improve overall security posture and achieve higher levels of compliance
- Reduce operational costs by automating the complete process
- Support your business processes around user on boarding, departures, etc.

# Curated Security Technologies Expertise & Alliances

| SIEM      | Endpoint & Data Security | Digital Identity                     | VA & PT / Config Audit | Threat Intelligence | Standards and Compliance |
|-----------|--------------------------|--------------------------------------|------------------------|---------------------|--------------------------|
| Azure     | Symantec                 | SAVIYNT onelogin                     | QUALYS RAPID7          | DARKTRACE           | HIPAA                    |
| AVAST     | McAfee                   | SailPoint Arcon                      | appvance.ai Nessus     | Email Security      | HITRUST                  |
| splunk    | SOPHOS                   | ForgeRock CYBERARK                   | KALI SF                | SOPHOS              | OWASP                    |
| Radar IBM | cybereason               | Azure Active Directory Ping Identity | DevSecOps              | Email Security      | ISO                      |
| seceon    | TREND MICRO              | BeyondTrust                          | Hdiv sonarqube         | SOPHOS              | CMS                      |
| RSA       | Windows Defender         | airwatch okta                        | Checkmarx BLACKBUCK    | Microsoft Intune    | NIST                     |
| LogRhythm | VARONIS                  |                                      |                        | Lookout             | PCI DSS                  |

## Services on cloud, Hybrid and On-premises IT Infra



### Why GS Lab | GAVS?

- ✓ Priority to problem statement rather than the catalogue of services
- ✓ Be a part of challenging requirements driving towards success
- ✓ Seamless delivery excellence Right First Time
- ✓ Security services powered by AI & Automation
- ✓ Cross functional SMEs to meet the needs of the customers

**For more details, please visit: <https://www.gavstech.com/service/security-services/>**

*We would like to acknowledge the efforts of Sundaramoorthy S, Gayatri Rairkar, Karthikeyan Manoharan, Shivakumar D, Yuvaraj Arumugam and Kannan Srinivasan in creating this article.*



# Role of Adaptive Authentication in Access Management for Cybersecurity

Sundaramoorthy S

Since access management is a key challenge for major entities which have numerous corporate applications as part of the enterprises, let me discuss how Adaptive Authentication plays a key role in handling the Access Management issues seamlessly.

A basic authentication with user id and password is enough to unlock the system when it is a standalone system, but when systems are connected to network which holds business critical data, the system needs multiple layers of security to ensure the systems are safe.

When Remote and Hybrid work culture is an opportunity for the Hackers to penetrate through the Networks, Multi-Factor Authentication (MFA) is the solution for securing the systems. MFA is reliable when there is limited number of users in the enterprise, with the increased utilization of cloud and Software as a Service type models, corporate enterprises need next level of authentication mechanisms to ensure Network Security.

As we need to accept the fact that CHANGE is continuous, lets discuss about Adaptive Authentication which is currently in trend.

## What is Adaptive Authentication?

Adaptive Authentication is a type of dynamic Multi Factor Authentication (Risk based Authentication) which could be implemented in such a way that the Identity Service Provider (IDP) will select multiple different Authentication mechanisms and additional mechanisms to verify the user based on the user's Risk Profile, behavior, organization's Access Security Policies and the type of the target which user is trying to access.

## How does Adaptive Authentication work?

Adaptive Authentication works in multiple ways based on the capabilities of the Identity Service Provider -

1. Organization-wide static policies could be defined based on the risk levels of the user such as role, department, location, and work schedules
2. Creating dynamic policies where the system will utilize it based on the complexity of the target and User Behavioural Analytics along with static policies
3. Utilizing the location and IP of user to step up the Authentication factors if required based on the criticality

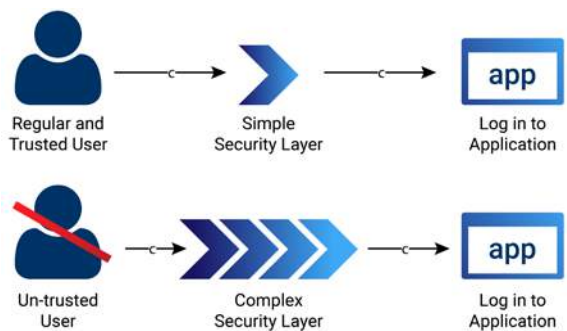


Fig 1.1: How Adaptive Authentication work based on User Types

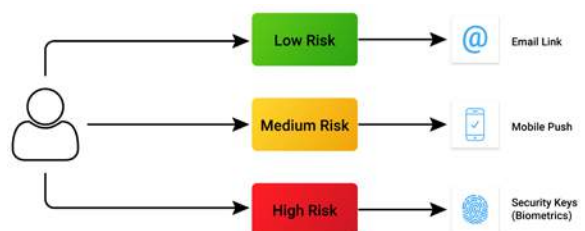


Fig 1.2: How Adaptive Authentication work based on Policies

A typical Adaptive Authentications system should provide multiple verification mechanisms, it should support Multi Factor Authentications through -

1. SMS / Text Verification
2. Authentication App
3. Email Verification
4. Phone call verification to predefined, verified phone number
5. OTP Tokens
6. Push notifications in mobile devices
7. Smart cards
8. Face recognition & Biometrics

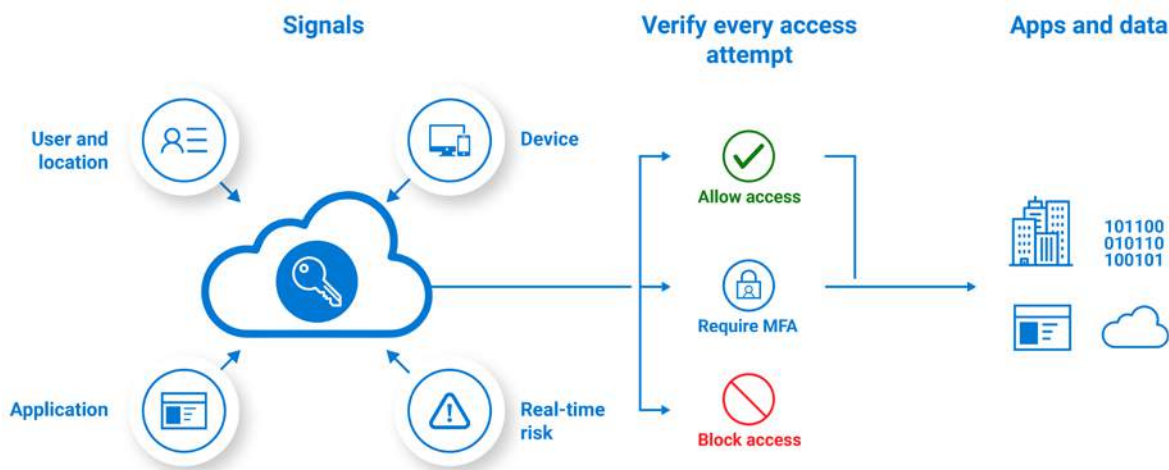


Fig 1.3: How Adaptive Authentication work with multiple layers of Security

## Difference between MFA and Adaptive Authentication

Multifactor Authentications is the popular at present. However, the Adaptive MFA or Adaptive Authentication or Risk Based Authentication is the Future of Authentications.

When compared to MFA, Adaptive MFA utilizes dynamic factors such as User Behavioural Analytics (UBEA), location, multiple types of authentications and other dynamic attributes of the users, devices or applications which requests the access to the target to improvise the security. This is a must to ensure the Network Security to remain competitive for global businesses.

- Risk-based authentication triggers only in elevated-risk situations and helps avoid unnecessary long authentication processes
- Security adaptive multi-factor authentication for users requesting access to sensitive and critical applications and data
- Easy to deploy and maintain for the corporates
- Context-based authentication solves the BYOD (bring your own device) security challenges

Adaptive Authentication is a much-required technology to handle the modernized cyber-attacks.

## Key Benefits

- Frictionless Authentication
- Defends cyber-attacks with add on layer of security scrutinizing
- Comprehensive security layer by analyzing the risk factors and consumer behavior
- Secure access to customers, partners, and employees regardless of their location

## About the Author

Sundar has more than 13 years of experience in IT, IT security, IDAM, PAM and MDM project and products. He is interested in developing innovative mobile applications which saves time and money. He is also a travel enthusiast.



# 3D: DANE-DNSSEC-DNS

Aravindh Subramanian

DNS is vulnerable - Cannot be trusted, No improvements since 1983 and usage of functionality and quantity has widened.

Risks | No DNS - no webpage

| Wrong DNS - wrong webpage

Beside, Security fails with Opportunistic Encryption which leads to unauthorized and compromised certificates, Man-in-the-Middle attacker may downgrade session to non-TLS at the time of email communications.

## ISPs are stripping encryption from netizens' email – EFF

Civil liberties body in shock blog



12 Nov 2014 at 18:23, John Leyden

Some ISPs are removing encryption from customers' connections to email servers – threatening the privacy of their communications – claims civil-liberties group the Electronic Frontier Foundation.

Incidents in the US and Thailand over recent months have seen service providers intercepting their customers' data to strip a security flag (called STARTTLS) from email traffic, the group says.

The STARTTLS flag is used by email software to request encryption during the process of talking to another server or client.

Without this flag, email is sent in the clear, as a blog post by the Electronic Frontier Foundation (EFF) explains.

By stripping out this flag, these ISPs prevent the email servers from successfully encrypting their conversation, and by default the servers will proceed to send email unencrypted. Some ISPs do this in order to monitor for spam originating from within their network and server.

Hacker can intercept TLS communication by mapping certificate from the way of MITM and improper configurations accepts self-signed certificates.

DANE is vow technology that might change our present and future. It's a DNSSEC trust scheme for X.509 certificates provides encrypted email communications.

DANE – DNS based Authentication of Named Entities

provides, layered security by fastening the X.509 certificate of a website to the DNS. This another channel provides details about X.509 certificate to the user who can use to validate certificate.

DANE uses DNSSEC —> DNS turn into policy channel —> DNSSEC affix trust layer

DNSSEC - DNSSEC abbreviates "DNS Security Extensions" DNSSEC adds security to the DNS by embodying public key cryptography into the DNS hierarchy. When carried out via an attack on a networks or an ISP's infrastructure, all of the entity's users are affected. This is often referred to as DNS cache poisoning, DNS malware borne attacks, Man in the Middle attacks and DNS redirection / DNS spoofing.

## NCDRC's take on DNSSEC and DANE

We have tested DNSSEC validation on our resolvers by using Bind9, Mozilla, Chrome and Gateway which means our resolvers always validate queries for domains that have been signed using DNSSEC. Users automatically benefit as fast as a domain is signed using DNSSEC. Nevertheless NCDRC moving to DANE.

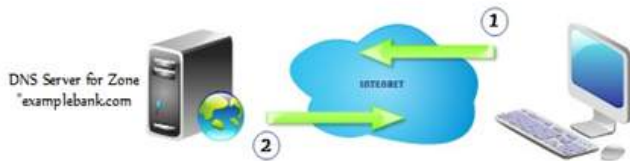
So far techies deploying DNSSEC on their domain names – "sign" domain names or ask Registrar for DNSSEC (Enable DNSSEC validation on originations/ ISP DNS resolvers). World really needs lots of DNS resolvers. Beside, ask ISP about DNSSEC and support on their ISP DNS resolvers.

Recent days naive techies debates on DNSSEC vs. Secure Sockets Layer (SSL)

Both DNSSEC and SSL depend on public key cryptography. DNSSEC deals with "where", and SSL deals with "how" and "who".



Testing results: Below image explains the process of with DNSSEC and without.



a. Simple DNS query, no DNSSEC

- 1 DNS Request for "examplebank.com"
- 2 DNS response for "123.0.24.025.026"



b. Simple DNS query intercepted, no DNSSEC

- 1 DNS Request for "examplebank.com"
- 2 DNS response for "123.024.025.026" Compromised
- 3 False DNS response sent to user by 3rd party resulting in attack scenario. Client has no indication of false DNS data



c. DNS query with DNSSEC thwarting invalid responses

- 1 DNS Request with DNSSEC option for "examplebank.com"
- 2 DNS response with valid DNSSEC signature "123.024.025.026"
- 3 DNS response with no DNSSEC signature or invalid signature dropped by the client

Below image is the proof of concept tested on Mozilla Firefox browser with DNSSEC validator



DANE is targeted by Security providers, Government or Private Email users with known security needs, Online-Payment sites, insurance providers, banks, Enterprises and Internet of Things

DANE is de facto standard technology.

This article was originally published in National Cyber Crime Reference Handbook II Edition.

## About the Author

Aravindh is experienced in Offensive Security and Cloud-centric cybersecurity strategies to achieve cost benefits that reduce risk and exposure to threats. He empowers healthcare organizations avoid potential financial loss from their data being misused in the cloud and from being non-compliant.

In his leisure time, he loves road trips and listening to music.



# Malware Analysis Benefits Incident Response

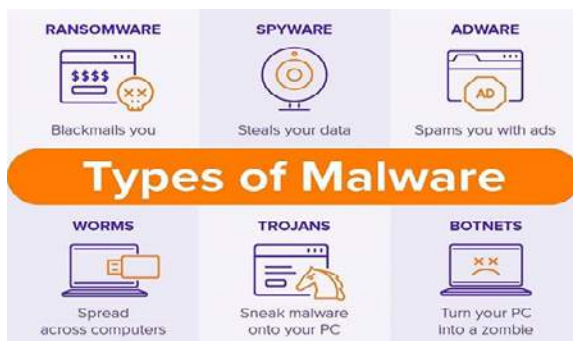
Vishnu Raj



## What is Malware?

Malware (MALicious softWARE) is an intrusive software that tries to execute unauthorized commands in the target system. The malware can exfiltrate data causing severe impacts on the target that falls victim. Malware attack vectors could be trojan horse or virus which are localized to infected system and worms which could infect the entire network.

Over the years, variety of malware attack vectors that can sneak their way into the IT exoskeleton of a company and malwares like rootkits, keyloggers, spyware, file infectors, ransomware etc. are used to compromise the targets effectively.



## Incident Response

On an imminent security breach, incident response helps in reducing the loss of intellectual property and critical private data. Incident response programs strive to limit the damage of an attack, along with the cost of recovery. Incident response plan has several components like resource identification, preparation to technical investigation and containment, but malware analysis is one distinct area of security that has become increasingly beneficial to the process.

It helps responders understand the extent of a malware-based incident and identify additional hosts or systems that could be affected. Actionable information from malware analysis can help an organization more effectively mitigate vulnerabilities exploited by malware and help prevent additional compromise.

## The Value of Malware Analysis for Successful Incident Response

Malware analysis is applicable to all phases of incident response. The phases include preparation, detection and analysis, containment and eradication, and post-incident activity. Organizations should have their teams properly trained and equipped with responders who can quickly and effectively perform malware analysis. Without these resources, it's hard to identify malware as the root cause of an incident. They may also take longer to contain incidents or fail to completely understand and eradicate malware from their networks, causing incremental damage and loss over time. The phases of incidence response are discussed in the picture below.

## Phase of Incident Response



### What if an Incident Occurs?

When malware is the source of a breach, knowledge of its capabilities and behaviour are crucial to effective incident response. Fast and reliable malware analysis can reveal the functionality of the malicious code. It can identify any changes the malware may have made to affected systems, and it can provide preliminary host and network-based indicators for detection signatures.

Malware analysis requires in-depth reverse engineering of malicious code and unknown software for a deep understanding of its capabilities, intent, attack vector, motivation, and tactics. Organizations should not be scrambling to find and equip malware analysts in the wake of a breach. With malware analysis, incident response program helps ensure a more swift and effective response and containment.

### Advanced Malware Threats through Incident Response -> Value of Technical Indicators

The malware used in advanced threats are often undetected by common antivirus and network-based detection solutions. Targeted attacks using unique

malware can successfully compromise the intended target.

Malware analysis reveals technical indicators that can be used to spot additional infections and compromised resources. These technical indicators contain forensic artifacts unique to the malicious code. They can relate to the way the malware behaves or the code itself and can be identified on a host or network.

Technical indicators include traditional forensic artifacts such as MD5 checksums, malware compile times, file size, name, path locations and registry keys. Technical indicators include domain names, IP addresses, email addresses, URIs or URLs, or any suspicious network communication. Advanced malware analysis techniques such as memory forensics analysis, identification of running process components, and imported/exported libraries used by an executable, are used to find the technical indicators.

### Post-Incident Activity

Post-incident activity is probably the most important phase. During this phase, information learned by malware analysis should be documented and included in the incident summary reports or separate malware analysis documents for dissemination. The

information should be used to help prevent future malware-based incidents of similar nature and bolster the capabilities to defend against future threats.

- Identify and understand the type of malware and its functionality.
- Finding how the system is infected and define the severity of the attack.
- How cybercriminals communicate with the malware.

## Malware Analysis

Malware analysis is the process of extracting information from a malware to study the origin, function, and impact of the malware. The main objectives of malware analysis are to:

Malware analysis is an important constituent in the incident response plan and various use cases for malware analysis is shown in the diagram below.

### Use cases for Malware Analysis

#### Case 1: Incident response and management

- If a organization detects or suspect a malware infection in their system, the incident response team performs malware analysis.
- This process helps to find the impact, root cause analysis and recover the system from the infection.

#### Case 2: Indicator of compromise extracion

- The cybersecurity team performs a massive malware analysis to find out the new indicators of compromise (IOC).
- This IOP can be used in security systems or devices to prevent the future threats.

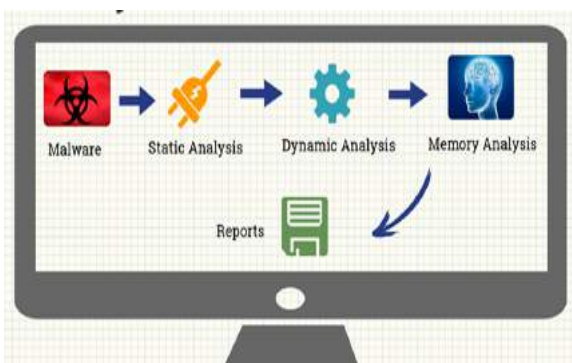
#### Case 3: Threat alerts

- The malware analysis solution provides highly reliable alert in the threat cycle thus making it easier to focus on the threat, prioritize and save time and resources.

#### Case 4: Malware research

- Malware analysis is performed by researchers to gain an understanding to the new techniques, malware vectors and tools used by the cybercriminals.

## Types of Malware Analysis



- **Static Analysis:** Static analysis is analyzing the software without executing it. It is simple but it cannot analyze sophisticated malware. Details like file type, encoded binary file, file obfuscations can be determined in static analysis.
- **Dynamic Analysis:** Dynamic analysis is executing the malware and observing its behavior while the infected system is isolated from the network. The responses to the malware requests are simulated to monitor the behavior. Dynamic analysis helps to remove the infection and focuses on consecutive activities, file system, registry, network, and system calls.

- **Memory Forensics:** Using a memory image to determine information about the programs, operating system, and state of the infected system. It involves memory acquisition and memory analysis. Memory forensics helps to congregate information like past and current network connections, keystrokes entered, open files and registry associated with the process, rootkit detection, code injection and other forensic artifacts.

## Automating Malware Analysis

Automated solutions simplify malware analysis greatly by helping the analysts to check files, suspicious URLs, endpoints, and memory dumps at scale, instead of doing it manually. Automation saves time, effort and helps overcome the skills shortage. Automated solutions aren't complicated, so beginner analysts can use them too.

Besides automation, practices that can be implemented for malware protection:

- Scanning systems regularly
- Employing security best practices like firewalls and anti-phishing prevention
- Creating regular backups
- Updating systems and applications regularly
- Employing measures to prevent social engineering attacks

## Importance of Malware Analysis in an Organization

With malware causing so many security breaches, strong analysis is required for effective incident response. So, organization should conduct 24/7 security threat research, vulnerability analysis and incident response. An incident response program that includes expert malware analysis helps responders identify malware-based incidents and understand their ramifications. Actionable information and early intelligence from malware analysis can help an organization be more aware and help prevent additional compromise.

## References:

- [https://informationsecurity.report/Resources/Whitepapers/51e831f9-aeef-41a4-b2e9-5162a2ac5f65\\_How%20Malware%20Analysis.pdf](https://informationsecurity.report/Resources/Whitepapers/51e831f9-aeef-41a4-b2e9-5162a2ac5f65_How%20Malware%20Analysis.pdf)

## Sources:

- <https://www.researchgate.net/profile/Mariwan-Ahmad/publication/340770783/figure/fig1/AS:882090539233283@1587318181208/Types-of-Malware-7.jpg>
- <https://www.yeahhub.com/wp-content/uploads/2017/01/malware.png>

## About the Author

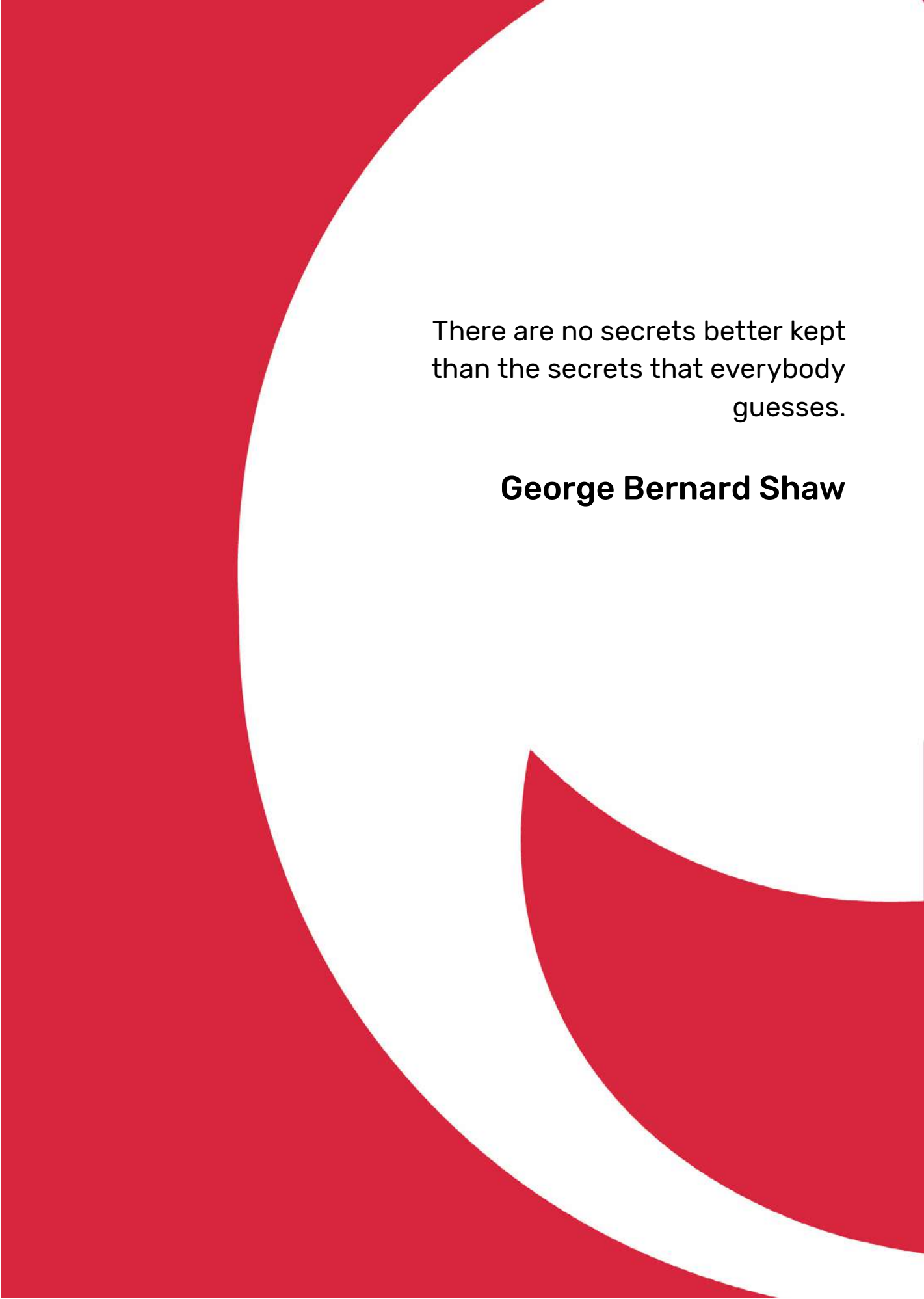
*Vishnu Raj is a part of the GAVS Security Practice (Red Team Member). He's passionate in building secure apps as he believes everyone deserves privacy.*

# InfoSec Champions

We would like to thank all those who have helped us in identifying suspicious cyber activities.

1. Akshay Deshmukh
2. Navneet Pandey
3. Animesh Patel
4. Yogesh Deshpande
5. Vishal Punjabi
6. Tejas Kulkarni
7. Ekta Dravid
8. Pranav Patel
9. Omkar Chogale
10. Antraj Khaire
11. Huzefa Ghadiyali
12. Mayur Patange
13. Suraj Puyad
14. Kartik Karekar
15. Lalit Belwal
16. Tshailendra Naidu
17. Farha Khan
18. Barun Singh
19. Pradeep Patole
20. Kishan Patel
21. Sahil Rangari
22. Rakeshreddy Donthireddy
23. Shubham Raut
24. Prince Patel
25. Deepti Mahato
26. Vishal Mane
27. Anuja Kudale
28. Sagar Rampure
29. Prachi More
30. Ujawala Gaikwad
31. Rushabh Tathod
32. Nirmala Mary
33. Avijit Kalita
34. Deepak Doegar
35. Wafadar Husain Khan
36. Sangeetha Karthikeyan
37. Chandrasekaran N
38. Narasimha Shenoy
39. Trupti Diwate
40. Gurumurthy B
41. Sudarshan Murthy B
42. Sriram Radhakrishnan
43. Sandra Babu
44. Joshua Goldstein
45. Lakshmi Prabhakar
46. Ramya Subramaniam
47. Vignesh Sridharan
48. Kugan Rajendiran
49. Dillibabu Subramaniyam
50. Ruban Salamon

*Note: This is not an exhaustive list.*



There are no secrets better kept  
than the secrets that everybody  
guesses.

**George Bernard Shaw**

# *enGAGE*

GAVS Technologies | [www.gavstech.com](http://www.gavstech.com)

Follow us on:

