Seekurity

STATE OF INFORMATION SECURITY

Contact us on +(52) 55 81958834 or email us at Info@Seekurity.com
or at 911@Seekurity.com if your business is under attack and need an urgent quote.

Seekurity for Information Security and Cybersecurity SAS de C.v. is an information security consulting firm based in the heart of Distrito Federal, Mexico City.

We offer a full Information security consultation services for Industrial, governmental and non-governmental business
We deliver detailed, comprehensive and customizable report at the end of each security engagement.
Our reports typically include an executive summary, detailed technical findings with well defined proof of concepts and recommended remediation steps.

OUR SERVICES

[-] PENETRATION TESTING

[-] PHYSICAL PENETRATION TESTING

[-] CMS TESTING AND HARDENING

[-] VULNERABILITY ASSESSMENTS

[-] SECURITY RESEARCHES

[-] MALWARE ANALYSIS

[-] DATA PRIVACY AND COMPLIANCE

[-] INCIDENT MANAGEMENT

[-] RISK MANAGEMENT

[-] OSINT - OPEN SOURCE INTELLIGENCE

[-] PHISHING ANALYSIS

[-] ANTI-FRAUD SOLUTIONS

[-] SOCIAL ENGINEERING ENGAGEMENTS

[-] CYBER SECURITY MONITORING

[-] VOIP SECURITY AND SOLUTIONS

[-] INTERNET OF THINGS - IOT

[-] FREE/LIBRE OPEN SOURCE SOFTWARE

PENETRATION TESTING

We are offering black-box, white-box security penetration testing and source code audit for Desktop, Mobile and Web applications against recently found vulnerabilities, OWASP top 10 and our own 0-days vulnerabilities found which are based on our great experience in information security field.

After each engagement we are delivering a very detailed reports which typically include an executive summary, detailed technical findings with well defined proof of concepts and recommended remediation steps.

PHYSICAL PENETRATION TESTING

The primary objective for a physical penetration test is to measure the strength of existing physical security controls and uncover their weaknesses before bad people are able to discover and exploit them.

Physical penetration testing, or physical intrusion testing, will reveal real-world opportunities for malicious insiders or bad actors to be able to compromise physical barriers (ie: locks, sensors, cameras, mantraps) in such a way that allows for unauthorized physical access to sensitive areas leading up to data breaches and system/network compromise.

CONTENT MANAGEMENT SYSTEMS SECURITY HARDENING

Content Management Systems like Wordpress, Drupal, Joomla, etc. made the process of starting a business easier but CMSes can't be secure from its own.

We are offering you a dedicated security testing and hardening to make sure your business safe and secure we also offering tips for best practices and CMS issues remediation.

VULNERABILITY ASSESSMENTS

A vulnerability assessment is the process of identifying, quantifying, and prioritizing/ranking the vulnerabilities in a system. Examples of systems for which vulnerability assessments are performed include, but are not limited to information technology systems, energy supply systems, water supply systems, transportation systems, and communication systems.

We offer you such assessments which may be conducted on behalf of a range of different organizations, from small businesses up to large regional infrastructures.

SECURITY RESEARCHES

Our expert researchers are working continuously to create, discover and identify new attacks before the bad people do, after that we address our findings responsibly to the appropriate vendors and give them enough time to make sure the discovered vulnerabilities are successfully patched, after making sure everything is okay we publish an advisory along with a public security awareness to prevent incidents and widespread abuse.

We love Security Researches and we are always keeping our knowledge base up-to-date.

MALWARE ANALYSIS

Malware Analysis is the study or process of determining the functionality and potential impact of a given malware sample such as a virus, trojan horse, rootkits, ransomwares or backdoors.

We offer you this service if you are noticing an unusual activity on your systems or experiencing strange functional misbehaving. Our experts can detect, analyze and clean your business infected assets and remove any Advanced Persistent Threat (APT) infections.

DATA & INFORMATION SECURITY

PRIVACY AND COMPLIANCE

Our experts can implement all forms of data security technologies like Disk encryption, Software versus hardware based mechanisms for protecting data, Backups, Data masking, Data erasure, Intellectual property, National Data Protection and Privacy Laws based on LFPDPPP, Privacy Assessment based on ISO 27000 International standards and finally Payment Card Industry Data Security Standard (PCI-DSS).

We help your business getting properly certified.

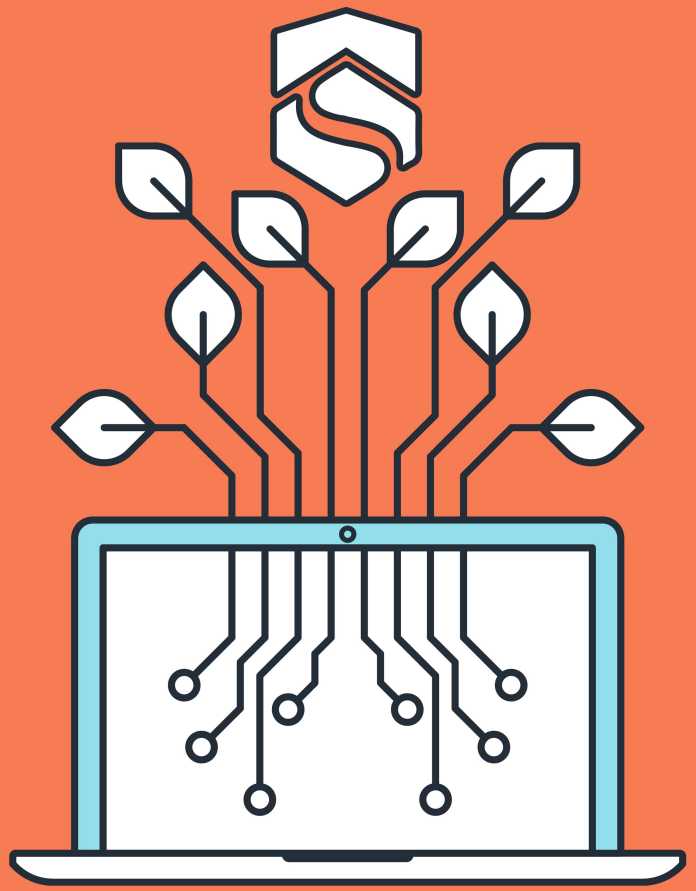
INCIDENT MANAGEMENT

Incident Management is all about describing the activities of an organization to identify, analyze, and correct hazards to prevent a future re-occurrence.

We help you managing, controlling and preventing incidents that affects the company severely, your customers and damage the reputation of your business.

RISK MANAGEMENT

Risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions. This process is not unique to the IT environment; indeed it pervades decision-making in all areas of our daily lives. We identify, evaluate and assess existing risks that may arise in the future.



Open-Source Intelligence (OSINT)

Open-source intelligence (OSINT) is all about intelligence of information collection from publicly available sources.

In the intelligence community (IC), the term "open" refers to overt, publicly available sources (as opposed to covert or clandestine sources); it is not related to open-source software or public intelligence. We offer a comprehensive information gathering-based investigations to serve all your needs because a piece of information means a lot.

PHISHING ANALYSIS

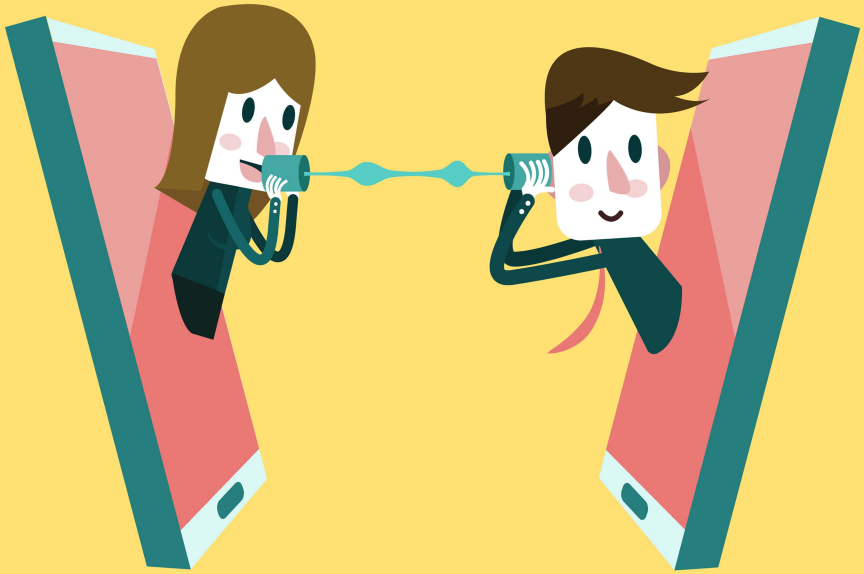
Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details , (indirectly money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication and it is one of many examples of social engineering techniques used to deceive users, and exploits weaknesses in current web security.

We offer services for identity thefts cases, usually or commonly for enterprises whose their clients could be affected by phishing emails, financial loses and Identity theft for companies.

Internet services can be used to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme.

Research suggests that online scams can happen through social engineering and social influence. It can occur in chat rooms, social media, email, message boards, or on websites.

Our highly trained experts analyze, eliminate and control internal threats, design and customize security controls to prevent any appearance of old or new threats through our peerless Anti-Fraud solutions built with love in **Seekurity**.



SOCIAL ENGINEERING ENGAGEMENTS

Social engineering refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

We offer Onsite and Remote Social Engineering engagements includes but not limited to social engineering campaigns, spear-phishing, pretext calling through spoofing and physical deception.

CYBER SECURITY MONITORING

The protection of computer systems from the theft or damage to the hardware, software or the information stored on them, as well as from disruption or misdirection of the services they provide. It includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection and due to malpractice by operators, whether intentional, accidental, or due to them being tricked into deviating from secure procedures.

We offer a super monitoring services against recent attacks and real-world updates.

VOIP SECURITY AND SOLUTIONS

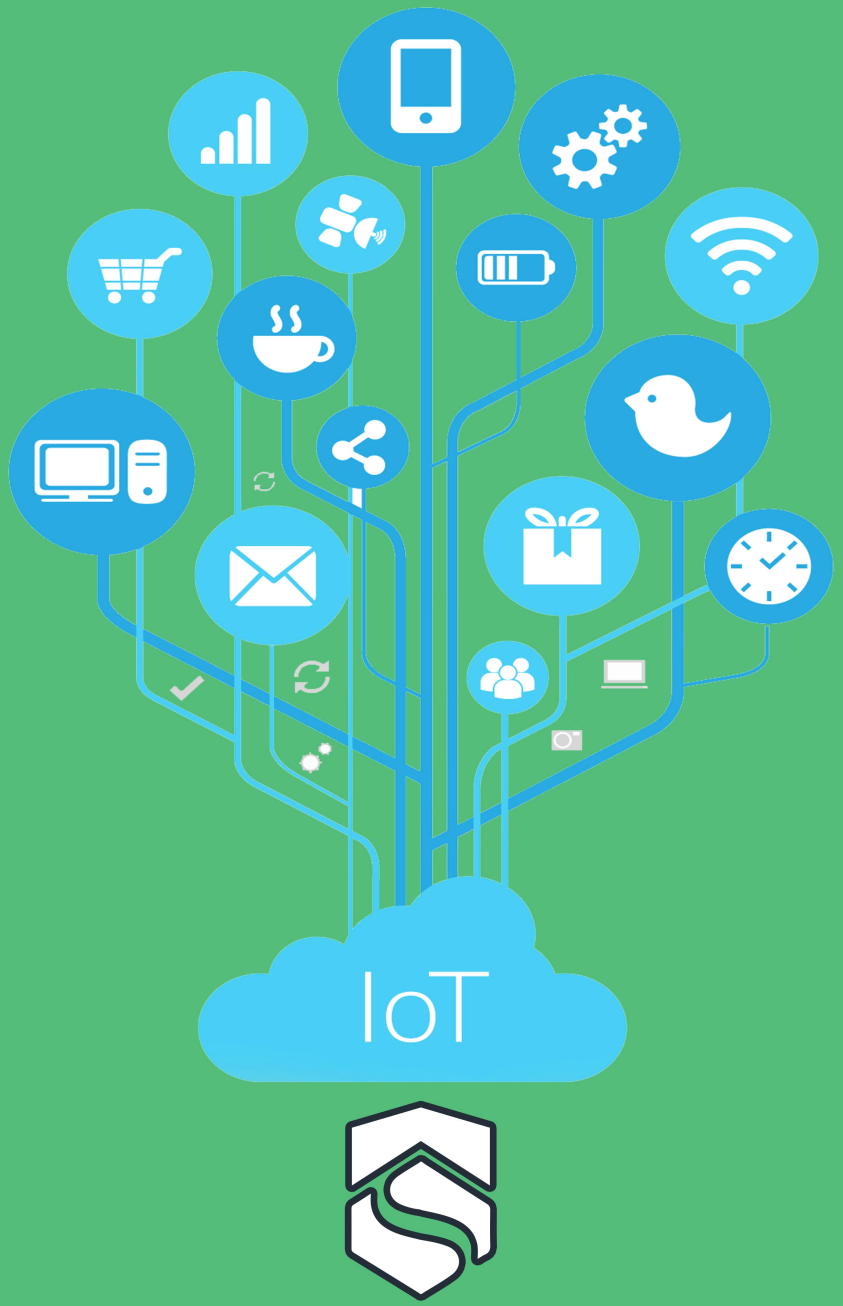
What is VoIP?

Voice over Internet Protocol (Voice over IP, VoIP and IP telephony) is a methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. The terms Internet telephony, broadband telephony, and broadband phone service specifically refer to the provisioning of communications services (voice, fax, SMS, voice-messaging) over the public Internet, rather than via the public switched telephone network (PSTN).

To make sure that you VoIP and Internet telephony services could not be attacked we test your the security of your VoIP systems against a lot of vulnerabilities for example but not limited to:

- Interception of calls.
- Denial of Service Attacks.
- Theft of Service.
- Exfiltration of data via media session.
-Malware embedded in signaling and media session.

We also design and implement security measures for all types of VoIP solutions.

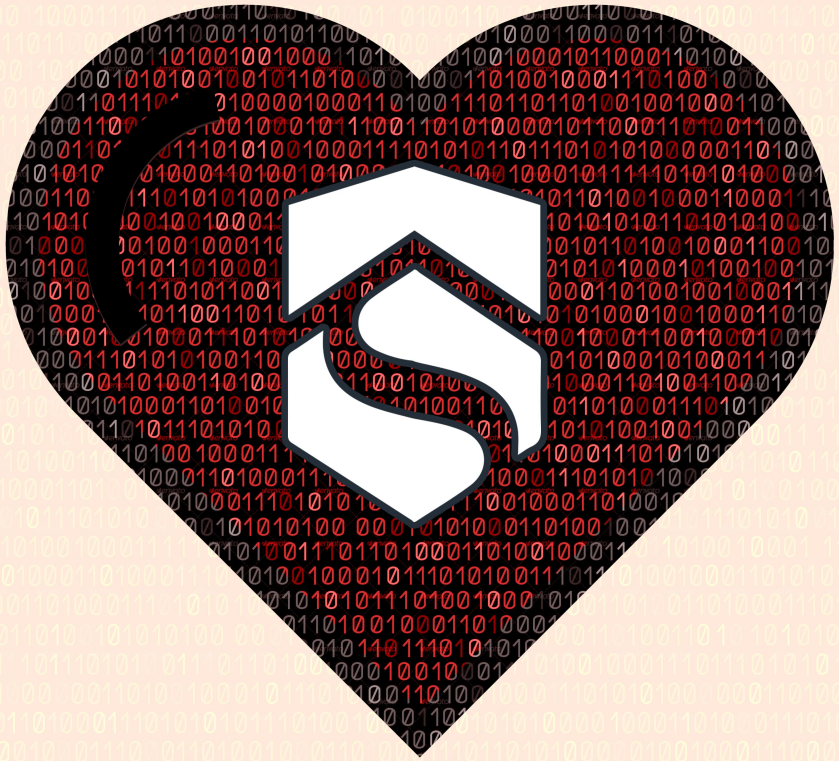


Internet of Things (IoT)

The Internet of things (stylized Internet of Things or IoT) is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items—embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data.
In 2013 the Global Standards Initiative on Internet of Things (IoT-GSI) defined the IoT as "the infrastructure of the information society." The IoT allows objects to be sensed or controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention. -“Wikipedia”

Recently IoT became more important industry (if not critical) because of its sensitive nature and involvement in humans life these “connected things” have to be tested against security bugs and vulnerabilities periodically.

In **Seekurity** we are doing many researches on IoT and embedded devices. We are also offering security testing services to projects based on Arduino, Raspberry PI and other logic boards. Contact us for more information!



FLOSS

Free/Libre Open Source Software

PROUDLY SUPPORTING FLOSS

Because Seekurity adores Free/Libre Open Source Software and Creative Commons (CC) based projects we are offering a free Security testing, Vulnerability Assessments and a Long Term Security Support (LTSS) free of charge to any eligible Free and Open Source Project.

Visit our website for more information or email us at:
Info@Seekurity.com

Seekurity is looking forward to be a service to you soon!

ACKNOWLEDGMENTS

Seekurity is proudly rewarded and acknowledged by tons of high-profile companies.