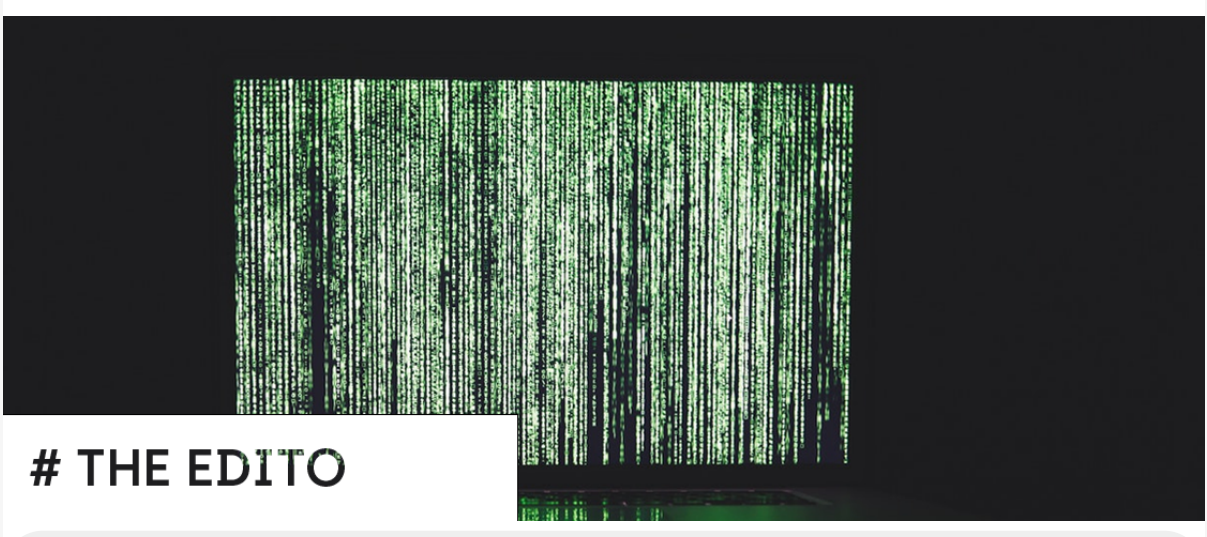
inCyber

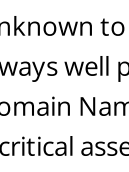
The media hub of the FIC community

November 2021

inCyber Newsletter



THE EDITO



By the Army General (2S) Marc WATIN-AUGOUARD

Founder of the FIC, Former Inspector General of the Armed Forces - National Gendarmerie, he was Director of the Research Centre of the National Gendarmerie Officers School (CREOGN) until 2020.

Alert on the most sensitive "STAD"!

The first aspect—delinquency—is the logical consequence of a 'criminal risk/expected gain' ratio that is very favourable to the predator; the second—inter-state conflict—offers states the possibility of settling their accounts with a certain degree of discretion, favouring "digital banderillas" over "gunboat policy".

These two migrations intersect, since states do not fail to call upon organised criminal groups to act in their place: "*It's not me, it's my sister who broke the calculator*", sang Evariste—who was also a doctor of elementary particles—in the 1960s... Some states have made this song their second national anthem...

Read the edito

CYBER INFO

CYBER RISKS

DNS security, key to Internet resilience?

Unknown to the general public and not always well protected by companies, the Domain Name System (DNS) is nevertheless a critical asset of their information system. Poorly secured, it can become a privileged vector for cyberattacks. When properly configured, it can be a formidable tool against them.

Read the article

HOMELAND SECURITY AND DEFENCE

"Cyber influence warfare": The French Armed Forces unveiled their new doctrine

On 20 October, the Minister of the Armed Forces and the Chief of Staff of the Armed Forces presented the third part of the military doctrine for operations in cyberspace.

Read the article

CYBER RISKS

Cyber insurance: a game where information must be shared

The measurement of cyber risk is currently imprecise due to the fragmentation of information, which prevents the creation of robust financial dykes.

Read the article

OPERATIONAL SECURITY

Data erasure: a resilient process

While antivirus software has become a commonly used protection tool, the sanitization of end-of-life hardware and data is not yet a widespread practice among businesses and individuals.

Read the article

FIC NEWS

FIC Startup Award: applications will open soon!

The FIC Startup Award, organised for the second consecutive year with Atos, aims to encourage innovation and entrepreneurship in the cybersecurity sector. Each year, more than 40 startups apply to a jury that is made up of end users, investment funds, and representatives of the ANSSI and the Ministries of the Interior and of the Armed Forces. Something new this year: in addition to the strengthening of the European dimension (through the candidates and jury members), there will be a new OT-oriented Award. It will enable startups to be recognised for their innovations/solutions capable of meeting the growing challenges linked to the cybersecurity of industrial systems. An application form will be available on the FIC website in early December. Audition sessions will then be organised for the selected startups. In the meantime, do not hesitate to read the various testimonials of former winners.

FOLLOW US!

SAVE THE DATE

Breakfast: "Hardware and software obsolescence: A real resiliency issue"

November 30th, 2021

A 2020 study by NTT's Global Network Insights Report shows that equipment renewal and modernization in Europe is slowing down: 48% of equipment is now old or obsolete, and therefore has unpatched flaws and software vulnerabilities that pose security risks to organizations. As work methods evolve with the widespread use of telecommuting and the proliferation of "intelligent" spaces, exchange platforms and other sharing tools, the obsolescence of equipment and software is a real resilience issue. What risks do they pose to organizations? Are rigorous maintenance and an adapted ISP enough to protect against them? What are the solutions and best practices to prevent and remedy them?

I register!

Webinar: "How to mitigate crypto risks with the right data-driven compliance strategy"

December 1st, 2021

Despite increased adoption of cryptocurrency across the world, some financial institutions continue to hold back from banking cryptocurrency businesses and investing resources to capitalize on its opportunities, in part because of the perception that it is impossible to control for illicit activity.
However, blockchains actually provide unprecedented transparency into criminal financial activity as well as economic activity.
In this presentation, Chainalysis's Compliance Advisory Lead Joosep Vahtras and Account Executive Willem van den Brandeler will share examples of how blockchain data can help flag crypto crime and build data-driven compliance programs.

I register!

INCYBER PARTNERS

blancco tenable Chainalysis

Contact: contact@incyber.fr

Avisa Partners - 17 Avenue Hoche - 75008 Paris - FRANCE

inCyber
The media hub of the FIC community