INVISIBLE SECURITY

The geopolitical divides which our societies are facing have transformed cybercrime into an extremely lucrative business. Its “border-less and visa-free” characteristics are being further fueled by increasing global inequality in wealth and the scale of digital processes, connections, devices and exploitable data. At the same time, cybercrime techniques are increasing in complexity and sophistication thanks to a growth in computer skills and education programs, and global access to technology and networks. Attacker tools are being commercialized and commoditized, with vast improvements in user interfaces, training and support.

In this complex political and economic context, the addition of emerging technologies, such as artificial intelligence, will open another dimension within the cybersecurity playground. Increasing maturity in AI capability is potentially creating unprecedented attack scenarios, catching defenders completely off-guard. As a result, the negative impact of cybercrime on businesses and societies is expected to grow exponentially.

Security practitioners are overwhelmed by the amount of information

Despite the marketing messages around security automation, the reality of day to day cybersecurity operations is still highly human-centric.

Enterprise networks can generate billions of potential security events per day from a wide range of data sources, including security devices, network appliances, connected objects and mobile applications.

This ever-increasing volume of alerts puts an unsustainable strain on security analysts and diminishes the speed and accuracy with which they can process threat data.

This is further aggravated by the worldwide shortage of appropriately skilled security practitioners. A deficit that is currently growing 25%[1] a year, from a cybersecurity workforce gap of 4 million in 2019.

Make the visible invisible to make the invisible visible

AI techniques are now being applied to assist with the prioritization of security alerts and automation of responses, with machine learning models being trained to identify unusual behavior patterns that may not be identified by pre-set rules. Such approaches will significantly reduce the workload on security teams.

AI will help drive cybersecurity to the next level - the Invisible Security paradigm. The previously overwhelming levels of visible information will be dealt with automatically, releasing human security analysts to make previously invisible but critical information more visible.

Cybersecurity will have to be decentralized with security intelligence and automation for decision-making

In a world, where digital connections are no longer confined to traditional IT infrastructures, but are able to span multiple industrial and social environments, cybersecurity will have to be decentralized. Security intelligence and decision-making will be automatic and

[1] https://www.isc2.org/Research/Workforce-Study# (2019)
https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx (2018)

executed close to data sources. This will allow the rapid self-adaption of controls to cope with ever-changing threat landscapes, different regional data privacy regulations and the devious skills of cybercriminals.

Classic concepts of strict architectural control and technology governance will no longer work with edge computing that is based on decentralized heterogenous mechanisms. Centralized information security, monitoring and policy enforcement approaches will reach their limits and won't scale as needed.

Decentralized "early stage" detection, reaction and effective counter measures are essential to address the fast-growing number of single attack events, and the complexity of inter-networked infrastructures.

Invisible security will adopt AI in a distributed model across all environments

As the capacity and capability of AI decision-making far exceeds those of human analysts, they will inevitably be exploited, leveraged and orchestrated across multi-agent systems that involve a wide range of other technologies. For such a model to become mainstream and efficient, it needs to be integrated into the layer of Invisible Security that runs efficiently "under the hood" both in centralized and decentralized contexts.

Security intelligence and automated decisions will then serve the continuous evaluation of risks and their treatments[2] according to the impact on delivered services. This process is described by NISTs[3] 5 concurrent and continuous functions: Identify, Protect, Detect, Respond, Recover.

While AI for cybersecurity has largely focused on the Detect and Respond functions until now, it will begin to impact other areas via specialized AI agents:

- **Identify AI,** building a comprehensive view of IT configurations and highlighting their risks,
- **Protect AI,** balancing risk versus services levels, and performing acceptable changes,
- **Detect AI**, differentiating attacks from acceptable behaviors,
- **Respond AI,** performing immediate reactions to identified attacks,
- **Recover AI,** establishing cyber resilience and restoring compromised business functions.

In addition, **Orchestration AI** will provide integration and coordination of all of the above functions in the context of customer business, risk and resilience objectives.

These 6 **Cyber AI** functions will be specialized by IT domains, industry verticals and regulations, and will deliver multiple layers of collaboration between organizations that share common interests. Rather than focusing solely on detecting attacks, this framework will help AI for cyber-defense prevail over AI for cyber-attack.

A distributed AI approach that makes the invisible visible, will bring enterprises an unprecedented understanding about their information systems. It will provide invaluable insights into optimal approaches for visibility, protection, attack detection, response and resilience.

Invisible security will foster technical progress and the evolution of commercial and industrial digital ecosystems, sustaining and safeguarding the advancement of society.

[2] Risk treatment can be mitigation, acceptation, transfer or avoidance.
[3] National Institute of Standards and Technology.

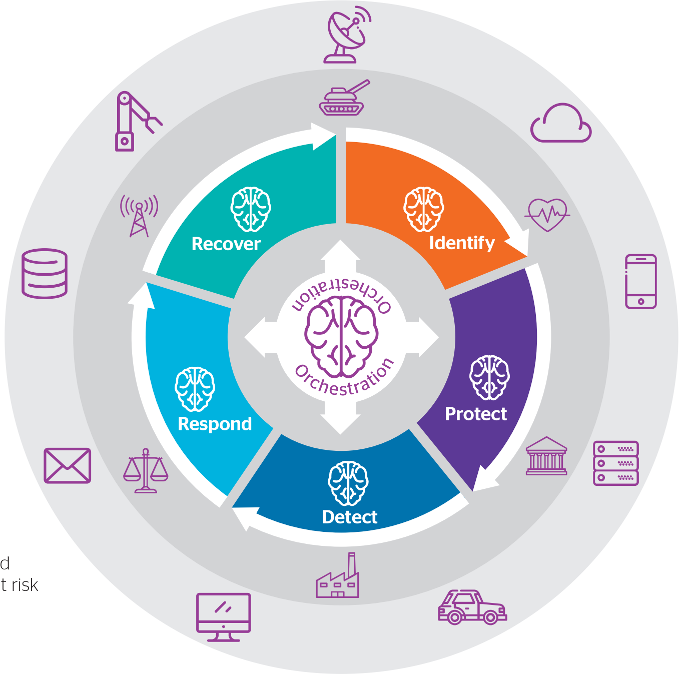

Figure 21: The five concurrent and continuous functions of intelligent risk evaluation and treatment.