الجمهورية الجزائرية الديمقراطية الشعبية
People's Democratic Republic of Algeria
وزارة التعليم العالي والبحث العلمي
Ministry of Higher Education and Scientific Research
المدرسة العليا للإعلام الآلي - ٠٨ ماي ١٩٤٥ بسيدي بلعباس
Higher School in Computer Science -08 May 1945- Sidi Bel Abbes



**MEMOIRE**

With a view to obtaining the **Master's** degree

Sector : **Computer science**

Specialty: **Computer Systems Engineering (ISI)**

**Theme :**

---

# Security Orchestration and Automation Response (**SOAR**)

---


**Presented by :**

- Ahmed Belhadjadji
- Hichem Selmi


Graduating in **30/09/2021** In front of the jury:

- Mr.**BELFEDHAL** President
- Mrs.**Djihad ANANI** Supervisor
- Ms.**SOUYAH Amina** Examiner

College year : 2020/2021

# Abstract

Digitization and technology have become a familiar thing in our daily lives and an inevitable thing to keep pace with this accelerating world, and it has become necessary for competing companies in this fertile market to devise new technology such as 5G networks and the Internet of Things (IOT) to outperform their peers.

This huge divide in the information technology world (IT) has led to an increase in the flow of data and the difficulty of securing it in this competitive Cyberwarfare because "Who owns the information, he owns the world".

This great conflict in the field of information security has led to the development, diversity and complexity of attacks,Today's attackers are more powerful and intelligent than they have ever been. In their attempts to steal information, conduct fraud, misuse resources, and disrupt systems, attackers are inventive and merciless. They're also patient and have a lot of statistics on their side. Attackers trade information and make research and development investments. They are powerful and organized crime groups.

It is impossible to protect against all cyber intrusions. While a strong defense-in-depth approach is essential, we must not depend on it entirely to protect our assets. As a result, companies' priorities are shifting to integrate quick detection and response, since the manual response is no longer enough to achieve minimum security.

In this project we propose to develop a platform for Network Security Orchestration, Automation and Response (NSOAR) in order to automate the Network incident response against some vicious attacks that can be very harmful for operating systems, network devices and the sustainability of the company's infrastructure.

---

**Keywords :** information technology, data, Cyberwarfare,information security ,Automation,crime,defense,assets,Network Security, Orchestration, attacks,Automation, incident response.

---

# ملخـــص

أصبحت الرقمنة شيئا حتميا لمواكبة هذا العالم المتسارع وأضحت التكنولوجيا شيئا مألوفا في حياتنا اليومية وكان لزاما على الشركات المتنافسة في هذا السوق الخصب التميز على اقرانها من خلال ابتكار تكنولجيا جديدة كشبكات الجيل الخامس وانترنت الاشياء.
هذا الانفتاق العظيم في عالم التكنولوجيا والاتصال ادى الي زيادة تدفق البيانات وصعوبة تأمينها في هذه الحرب التنافسية المشتعلة فمن يملك المعلومة يملك السبق.
هذا الصراع المحتدم في مجال امن المعلومات افدى الى تطور الهجمات وتنوعها وزيادة تعقيدها فالمهاجمون اليوم ليسو هواة يريدون بعض التسلية بل دول وشركات وجمعات اجرامية منظمة تمتلك مايكفي من الحنكة والصبر والتمويل واحدث التكنولوجيات للفتك باكثر الشبكات تأمينا.
اليوم يملك المسؤلون عن امن المعلومات قناعة راسخة بأن الوصول الي الكمال في تأمين شبكاتهم غاية من ضرب المستحيلات لكن الوصول الى امثل الحلول يبقى هدفا مشروعا وعليه فأن السرعة في الاستجابة للهجمات وصدها يعد من اهم العوامل في الوصول الى اكبر قدر من المثالية في تأمين الشبكات.
في مشروعنا للتخرج نسعى للتطوير أداة تساعد في التنسيق واتمتة التصدي لبعض الهجمات التي تضر بأداء الشبكة والأجهزة المتصلة بها .

---

**كلمات مفتاحية :**

التكنولوجيا والاتصال، البيانات ،أمن المعلومات ،الشبكة ،الهجمات ، أتمتة ،تصدي ،تنسيق.

---