Orange
Cyberdefense

Human & Tech: Times of Change

Your checklist to combine culture and technology for greater security outcomes

1 Where and how to start when it comes to human & tech balance?

☑ **Know yourself:**
It is crucial to have a good overview of the "current state" of your organization to make the good strategic choices.

- **A comprehensive maturity assessment can help.**

☑ **Know the context of your organization:**

- **What and where are your valuable assets?**
- **What type of threats?**
- **What business model, etc.?**

-The objective is to prioritize and have a more risk-based approach to your investments – instead of reactive approach.

-By having the fundamentals in place and by implementing technology correctly you will:

- **Save time**
- **Become more cost-efficient**
- **Increase security significantly**
- **Have more time for the security specialists to focus on more interesting tasks, which helps retaining your employees.**

2 How SOAR is a good example of the human & tech balance?

✓ **Design your own processes:**

It is important to define and design your processes before doing an automation project.

✓ **How can SOAR technology help you?**

This technology can support your business cases by facilitating integration between applications and playbooks that replicate existing processes:

- Hundreds of use cases: network security, forensic, malware analysis, analytics & SIEM, IAM, Vulnerability Management…
- Incident management processes with actions such as categorisation, notification, investigation, response and closure.
- New employee onboarding and compliance.

✓ **Adapt SOAR technology to your context**

SOAR technology comes with playbooks and standard integration but it's up to you to adapt them to your organization. This needs development and maintenance cost.

Once in place, automatic playbooks will have to be monitored like other automatic task.

✓ **3 keys areas to consider in the human and tech balance:**

1. Customer service: some key questions

Do we want to improve the time to respond to a breach ? How much ?

2. Efficiency: some key questions

Do we plan to lower the error rate? Do we want to introduce new KPI?

3. Expertise: some key questions

Do we want to free our cyber experts time for other projects ? Or avoiding hiring more of them and focusing on our core business?

✓ **Automation can save time and prevent analysts from quicky burning out**

- The triage process is a repetitive activity which needs to interact with multiple applications and is prone to human errors.
- SOAR tooling is particularly interesting because it's an opportunity to free tiers 1 engineer time, to reduce the error rate and to improve the service quality.
- Customers also report that it's easier for them to buy a service or an application than to hire new tiers 1 employee.

3 What are the best practices for employee security awareness?

✓ **The "Compliance check" approach is not sufficient**
Some digital learning-sessions a few times a year doesn´t help to transform your organization into a security aware culture.

✓ **Know why you are doing it and for who**
it is important to define your context and what goals you want to achieve

- What is your business context and where are your vulnerabilities?
- What are the different stakeholder groups, and what level of security awareness do they need to have?
- Stakeholder groups can be different groups that are very important to security, but don't necessarily work with it (HR, Finance…)

✓ **Define specific learning approaches for every stakeholder**
It is crucial to differentiate between awareness, training, and education – and ensure that the different stakeholder groups receive the relevant learning approach - or they will lose interest.

✓ **Before implementation, you should ensure that you have:**

- Management support ("Tone at the top").
- Resources (dedicated budget and resources).
- Material and tools: do you create the content yourself? Outsource it (or hybrid)? How to you deliver it (learning platform, gamification, courses, etc.).
- Communication: what do you communicate, how and when.

✓ **When you have implemented the program, you need to ensure** that it stays relevant and effective,– as culture is built over time.

- Collect feedback and improve.
- Find measurable areas to see if the program is effective (reported incidents, phishing resilience, surveys, etc.).
- Manage changes in program, success indicators and factors, and go on (Plan-Do-Check-Act).

✓ **The goal is to build a "security by reflex" culture where :**

- People think "just a little" about security in everything they do.
- People know where to report when they see something suspicious.
- People praised for reporting it and not shamed.

3 What are the best practices for employee security awareness?

✓ Personalize the learning content and use marketing techniques

- For example, distributing awareness training to users involved into an incident.
- Take inspiration from the marketing teams who are often slicing the information to the reader to be more digest and maximize the efficiency.

✓ Automate the way you deliver content when it’s possible

- This use case can be automatized with a playbook in SOAR : from an incident, we can associate a user and then sending him learning content in pieces.
- Any enhancement can be tracked and help the user to train his reflex.

If you want to know more about these topics, discover our solutions:

Ethical Hacking

CISO as a Service

Awareness & Training