Cooking Cybersecurity

Why we all need new recipes to be successful

Olivier Ménil
Business Development Manager Security

proximus

About me

More than 20 years in security (in various functions including technical ones ☺)

- I have a passion about (cyber) security & I like cooking!
- Experience in start-up, own company, integrators & vendors
- National and international speaker for Security Conferences
- No criminal record (yet)!

Agenda

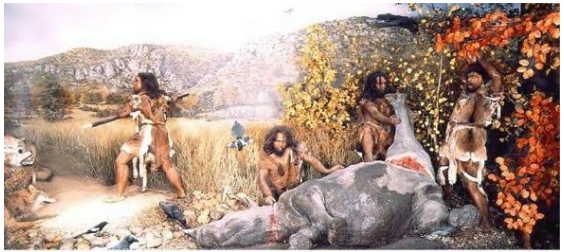
- Setting up the scene
- How to (learn to) cook ?
- Why cooking and cybersecurity have so much in common ?
- Examples
- Conclusion

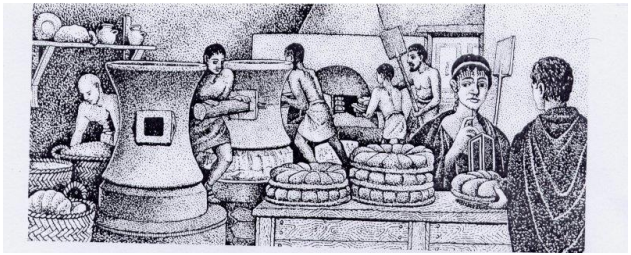
proximus

Setting up the scene

Setting up the scene

- Cooking is very old and is a critical component of mankind!

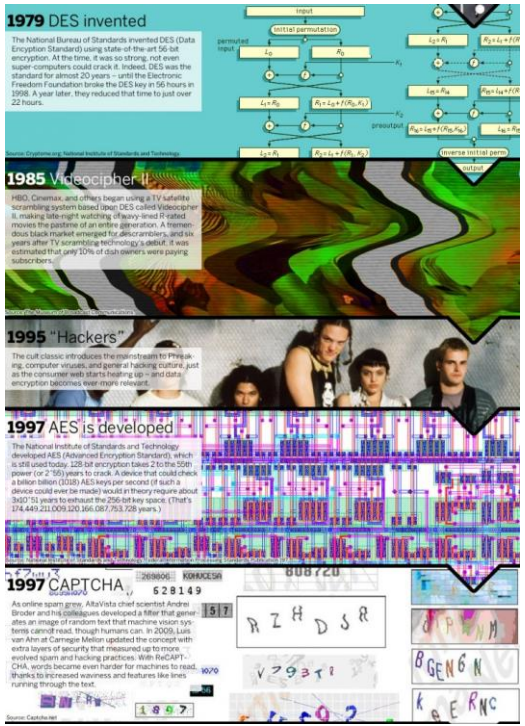




proximus

Setting up the scene

- Cybersecurity is not that old but think about the CIA principle … especially the C!



How to (learn to) cook ?

proximus

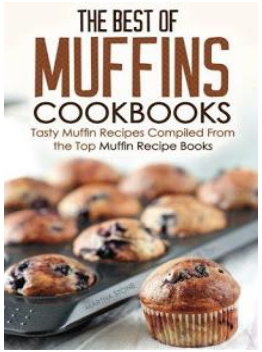
How to (learn to) cook ?

- The basic elements for cooking are obvious:
  - Ingredients
  - Tools
  - Location / facilities
  - Recipes
  - … but please don’t forget the most important!

How to (learn to) cook ?

How to become a chef ?

- There are key elements to be successful:
  - Learning
  - Training
  - Testing
  - Passion
  - Accept failures and challenges
  - Bottom up approach (stay humble)



Why cooking and cybersecurity have so much in common ?

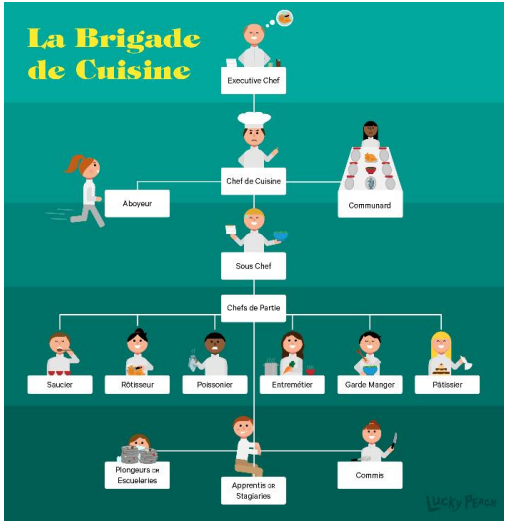
Why cooking and cybersecurity have so much in common ?

- In fact all previous elements can be easily compared:
  - Ingredients & tools -> devices
  - Location & facilities -> infrastructure / connectivity / datacenter / cloud
  - Recipes -> configuration and policies
  - Cooks -> Cybersecurity specialists
  - Training -> training
  - Tasting -> auditing / pentesting
  - Dressing -> finetuning

proximus

How cooking and cybersecurity have so much in common ?

- Furthermore … even the way how cooking is regulated in a professional kitchen can be compared:



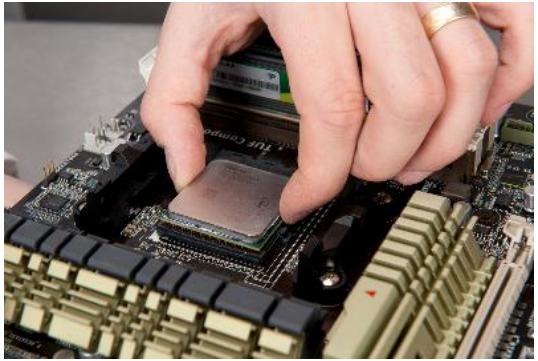
- Clear roles and responsibilities
- Segmentation, risk control and management

Examples

proximus

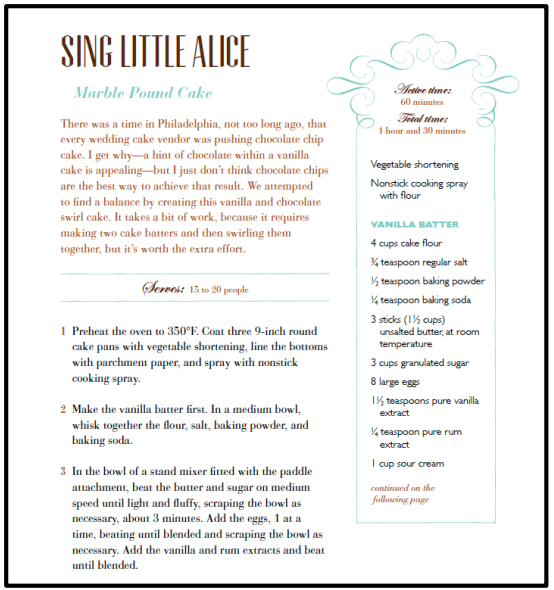
State of the art / best of breed / industrialisation

- Cooking is like cybersecurity: “standardized” or “à la carte”

Implementation / configuration

- It MUST be precise, accurate, exact …. In fact perfect!
- Why do you think in cybersecurity we all like to use … cookbooks?



SING LITTLE ALICE

Marble Pound Cake

Active time: 60 minutes
Total time: 1 hour and 30 minutes

There was a time in Philadelphia, not too long ago, that every wedding cake vendor was pushing chocolate chip cake. I get why—a hint of chocolate within a vanilla cake is appealing—but I just don't think chocolate chips are the best way to achieve that result. We attempted to find a balance by creating this vanilla and chocolate swirl cake. It takes a bit of work, because it requires making two cake batters and then swirling them together, but it's worth the extra effort.

Serves: 15 to 20 people

1 Preheat the oven to 350°F. Coat three 9-inch round cake pans with vegetable shortening, line the bottoms with parchment paper, and spray with nonstick cooking spray.

2 Make the vanilla batter first. In a medium bowl, whisk together the flour, salt, baking powder, and baking soda.

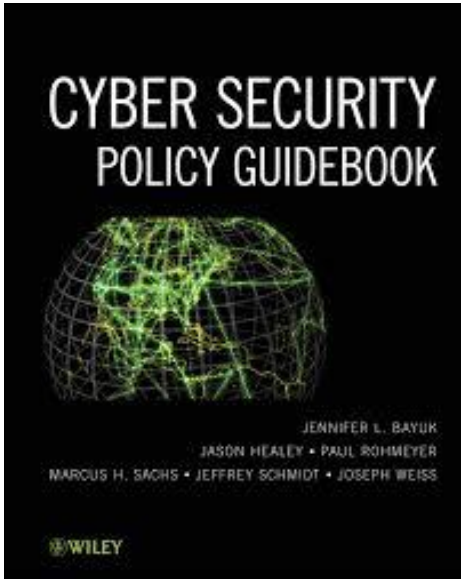
3 In the bowl of a stand mixer fitted with the paddle attachment, beat the butter and sugar on medium speed until light and fluffy, scraping the bowl as necessary, about 3 minutes. Add the eggs, 1 at a time, beating until blended and scraping the bowl as necessary. Add the vanilla and rum extracts and beat until blended.

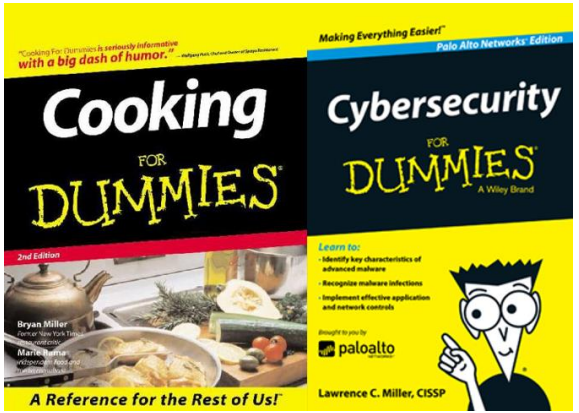
Vegetable shortening
Nonstick cooking spray with flour

VANILLA BATTER

4 cups cake flour
¾ teaspoon regular salt
½ teaspoon baking powder
¼ teaspoon baking soda
3 sticks (1½ cups) unsalted butter, at room temperature
3 cups granulated sugar
8 large eggs
1½ teaspoons pure vanilla extract
¼ teaspoon pure rum extract
1 cup sour cream

continued on the following page

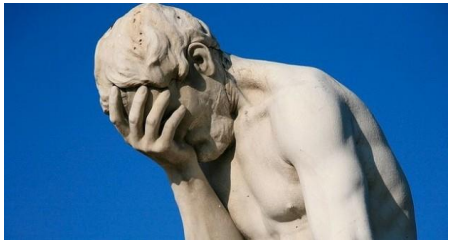




Old ingredients … New recipes

- Modern cooks like to (re)use forgotten ingredients
- … it’s exactly the same for cybersecurity!

Remember …. Logs?

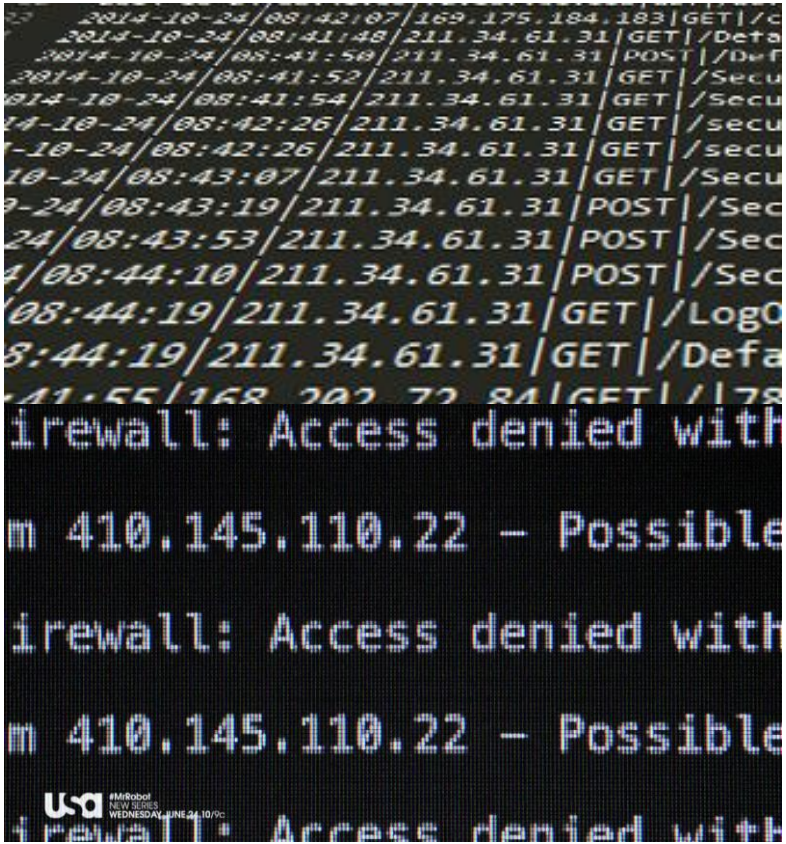


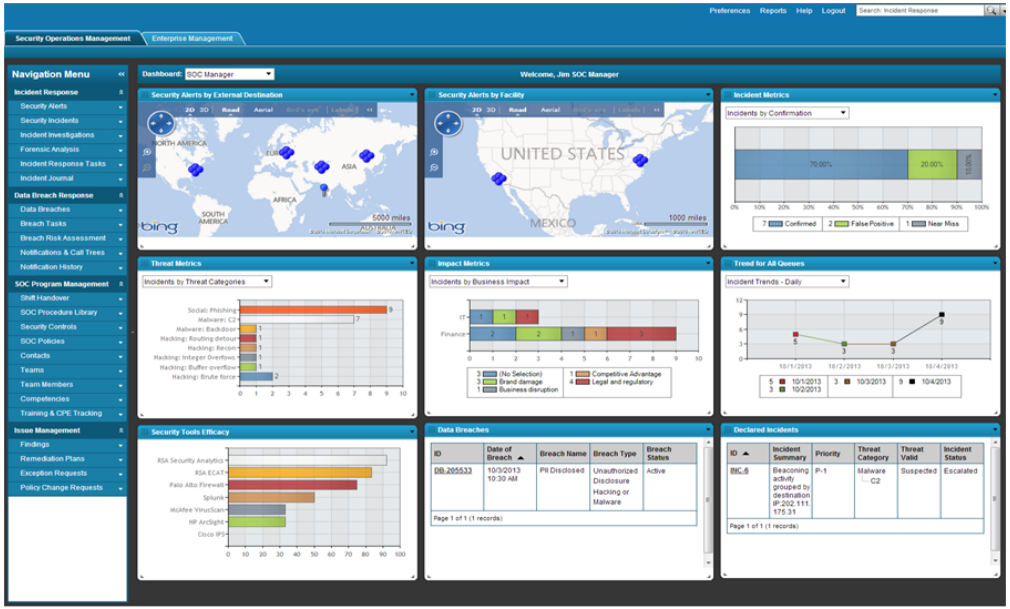
- What was told to us in the 90's ?

3	Log Reduction	* Any	* Any	Any Traffic	NBT bootp rip	drop	None	R70J-A	* Any	this rule helps the LOG files to be tidyier by deliberatly not logging RIP,bootp and NBT
4	* Any	* Any	Any Traffic	NBT microsoft-ds	drop	None	Policy Targets	* Any	There are always some W* hosts around...which shouldn't fill the log	
5	Cleanup Rule	* Any	* Any	Any Traffic	* Any	drop	None			

proximus

Logs …. today … everywhere … for everything!





proximus

Conclusion

Still not convinced?