#0000FF, #FF0000, #A020F0, # or #000000?

#0000FF

- CSIRT -> Cyber Security Incident Response Team
- CERT -> Computer Emergency Response Team

- Officially a Reactive team handling incidents
- Usually works at a high organizational level
  - The ones to call, when everything else has failed
  - Or S*** has hit the fan
- Often compared to a fire brigade

Reaction vs. Day Job

- Work on detection cases
  - Create SIEM rules
  - Develop detection mechanisms for crazy components
- Work on actual detections
  - Talk to people
  - Resolve FPs
- Expand monitoring capabilities
  - Add new logs
  - Add new systems to SIEM

- Handle actual Emergencies / Incidents

Is it an Incident / Emergency ?

Network-wide malware breakout

Is it an Incident / Emergency ?

Hacker submitting a crit vuln in perimeter

Is it an Incident / Emergency ?

Potential DC compromise

Is it an Incident / Emergency ?

Really bad finding in pentest

Is it an Incident / Emergency ?

Systems affected by fresh 0-Day

Is it an Incident / Emergency ?

Security contractor submitting

a crit vuln in perimeter

Is it an Incident / Emergency ?

New highly critical CVE for software you use

Is it an Incident / Emergency ?

Public vuln report via Twitter

Aspects in Classification

- Guidelines, Rules and Laws
- Affected systems
- Exposure
- Personal experience
- References
  - CVEs, publications

Aspects in Classification

- How much work will it be to fix?
  - Do I have to fix it myself?
- Will I get into trouble due to the fact that the issue exists?
- Who caused the issue?
- What are my capabilities?

Threat or Incident / Emergency?

- Who makes the decision
  - Blue team may call incident if it thinks necessary
  - Formal escalation
  - Other related team makes the call
- Rules defining who takes care of reports coming from specific sources
  - I.e. public researchers, red team, contractors, pentests
  - With rules on what has to be reported upwards

- Blue team has to rely on the fact that they will be informed
  - If necessary

Responsibilities & Politics

- Every team needs a job
- Every team needs to prove that they're good at their "job"
- Every team needs big fish
  - Showing you "solved" an issue is always good
- In some companies Security is still a prestigious area
  - More Cyber Cyber more promotions

Real World Situations

- “It’s not an incident because it was reported by one of our partners!”
  - “Maybe somebody else also found it but didn’t report it?”
  - “Nope, not an incident”
- “It may be an incident but we’re going to resolve it!”
  - “But…we’re the ones with the knowledge in that area”
  - “Well, we’ll manage”
- “Have you fixed the issue?”
  - “Nope”
  - “Ok” ……a week later ….. “Have you fixed the issue?”
  - “Nope”
  - “Ok” ……a week later ….. “Have you fixed the issue?”
  - “Nope”
  - “Ok” ……a week later ….. “Have you fixed the issue?”
  - “Nope”
  - “Ok” ……a week later ….. “Have you fixed the issue?”

Pure #0000FF

- Only do Detect and Respond
  - “Don’t think, just wait”
- Following the “fire brigade” comparison they lack the fire inspector
  - Which would be preventive work

- Basically a very perverted role, where you sit, see stupid things happening but it’s your job to wait until something goes really really wrong, because only then may you step in

Ouchies...

- How about we show them how to do things properly?
  - Not our job
- How about we write a few guides on how to ensure secure operations
  - Not our scope
- How about we recommend a new process?
  - Not Cyber enough
-

Pure #0000FF

- A Blue team is an important role!

- But: Does it make sense to have a team that practically focuses on watching potential misuse of known issues?
  - Which could easily have been fixed?

#FF0000

- Preventive team
- Seeking for issues in company systems
  - Reports them
  - Partially tracks the fixes

- According to some Blue teams “an easy job”
  - Defending is hard, not attacking

Pure #FF0000

- In theory the same as a global scale quality assurance program
- Only makes sense, when reports are being taken serious
  - Which in large corporations often is a major issue
  - → Aspects in Classification
- Has to contain the process of not only fixing specific issues but understanding structural problems and must address these
  - Oversight

#0000FF vs. #FF0000

- Title of the slide actually makes no sense at all
  - It should never be a vs. but always an &
  - Even when fighting each other in a specific scenario: It’s a game, it’s training, it’s not more than a NERF war!

- A fire brigade only copes due to the combination of having the actual firefighters
  - Who put out fires when something has gone wrong
- And the fire inspectors
  - Which make sure that nobody impregnates their walls with flammable oil, because it’ll make them waterproof

#0A20F0

- A blend #FF0000 and #0000FF
- A purple team is usually referred to as one of two things
  - A functional role bringing red and blue together
  - A hybrid team, which has both blue and red capabilities
- A way of combining both preventive and reactive work

#FF00FF vs #A020F0

- Should probably be a #magenta team not a #purple team
- But we’re Hackers, so let’s just throw in some #green

Thoughts

- Defense only works when you can scale the attack surface
  - Otherwise you'll never be able to handle all alerts
- Offense only makes sense when you actually learn from the findings
  - And fix them

- Offense is simply a way scaling the attack surface
  - Down to something that defense is capable of handling

- Thus the combination is a simple necessity

In Summary

#0000FF: :-(

#FF0000: :-/

#FF00FF: :)

I’d be happy to hear some opinions :)