



ELIMINATING BLIND SPOTS

Xavier Rousseau, Senior Security Research Engineer
xrousseau@ixiacom.com

Penetration Tester for French Department of Defense

Trainer for Ethical Hacking Team and Security
(Organizational and Technical)

8 years experiences in

Security System Integration

Main focus on IPS / WAF / DLP / Vulnerability Scanner /
PenTest Tools / Audit / SOC

Member of several beta-test programs (IPS)

Technical evaluation of Security Controls (R&D)

Security Architect

Security Advisor for Orange Business Services'
customers

Business Developer and ISO-27001 Consultant

Now, working for **visibility and Network Test**
company as Senior Security Research Engineer

Used to evaluate security controls (5 years)

IPS, NGFW, Sandboxes, WAF, SLB, Proxy

Worked on Cyber Security Project and Cyber Range

Devised test methodologies


Delivered Training and ProServ

Working with Bank, Industry, Military, Defense
Contractors, Government, Network Equipment
Manufacturers



ELIMINATING BLIND SPOTS

SOMETHINGS WRONG WHEN...

- In less than 24 hours, a hacker knows more about a compromised network than most the IT people
 - At a minimum, they know more about the vulnerable assets and how they are maintained
- How do I know this?
 - Every breach report ever...
 - How does a hacker steal your valuable information from you if you are watching it like a Hawk?
 - Contest: Try to build a security policy from scratch into an IPS and let see ;)



SOMETHINGS WRONG WHEN...

- Why ?
 - Basics still not applied (password still the main issue...)
 - Lack of experts
 - Trust level in the security infrastructure is too high
 - Security rules not aligned with assets
 - Security policy not up to date (organizational and technical)
 - Technologies (NGFW, Sandbox, SIEM, ...)
 - Gartner, NSS, ...
 - No one is prepared about what will happen



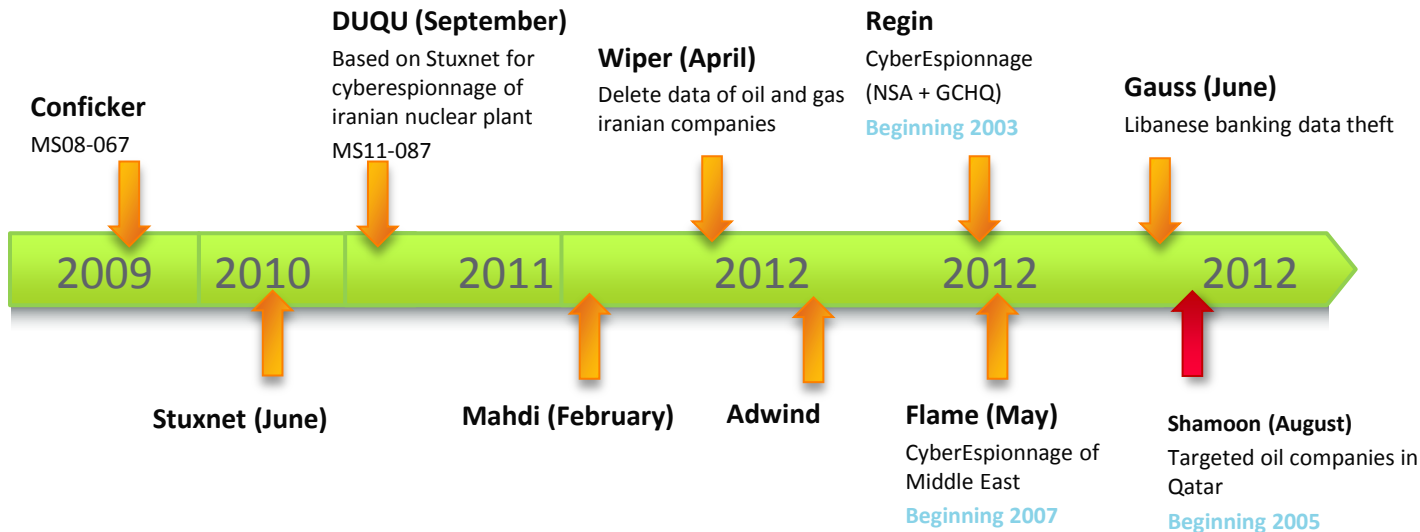
WHAT DOES VISIBILITY HAVE TO DO WITH SECURITY?

- It's not a matter of “**IF**” you'll get hacked, rather a matter of **WHEN**...
- Average time between compromise and discovery, 99 days

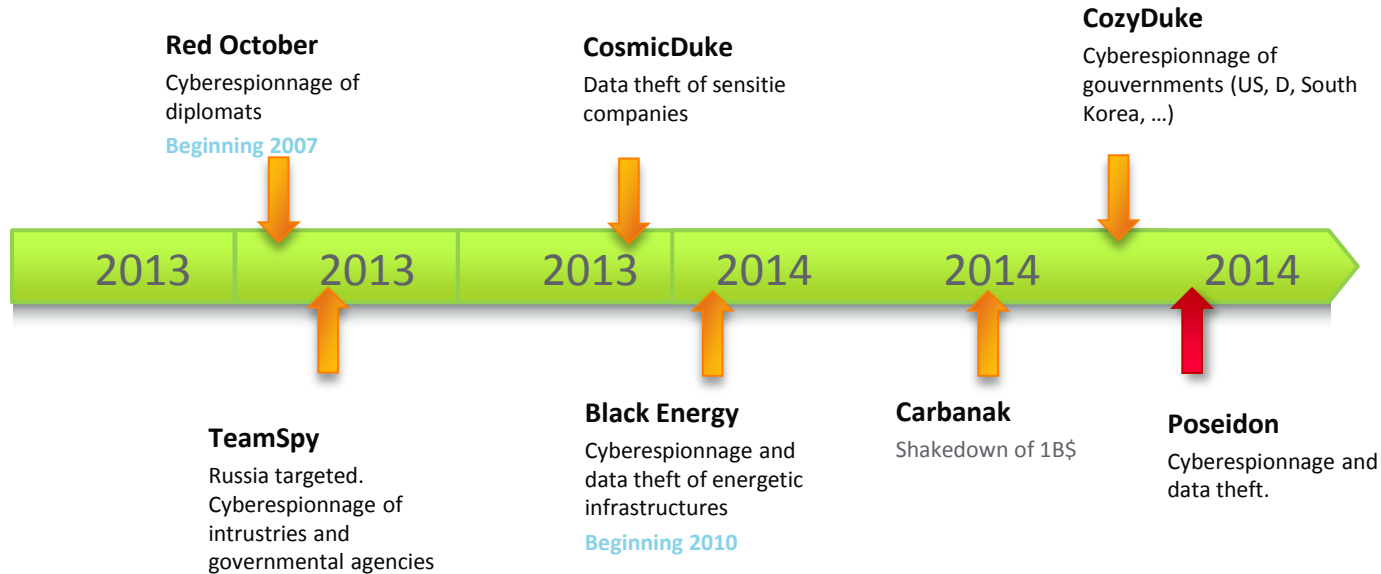


- Visibility will help **reduce** amount of time between compromise and discovery

WHAT DOES VISIBILITY HAVE TO DO WITH SECURITY?



WHAT DOES VISIBILITY HAVE TO DO WITH SECURITY?



WHAT TO DO?

- Continuously monitor and assess your DEPLOYED tools, processes, and people (PDCA)
 - Not up-to-date, immature, insuitable, not trained
- Why? Obvious but nothing changed
 - New vulns, tools, leak every day
 - New attack methods created every day
 - No silver bullet solution, find out where weaknesses exist and shore up
 - Audit not enough, PoC not enough/immature
 - Changes are happening daily
 - Policy
 - Configuration
 - Patches/Updates



WHAT TO DO?

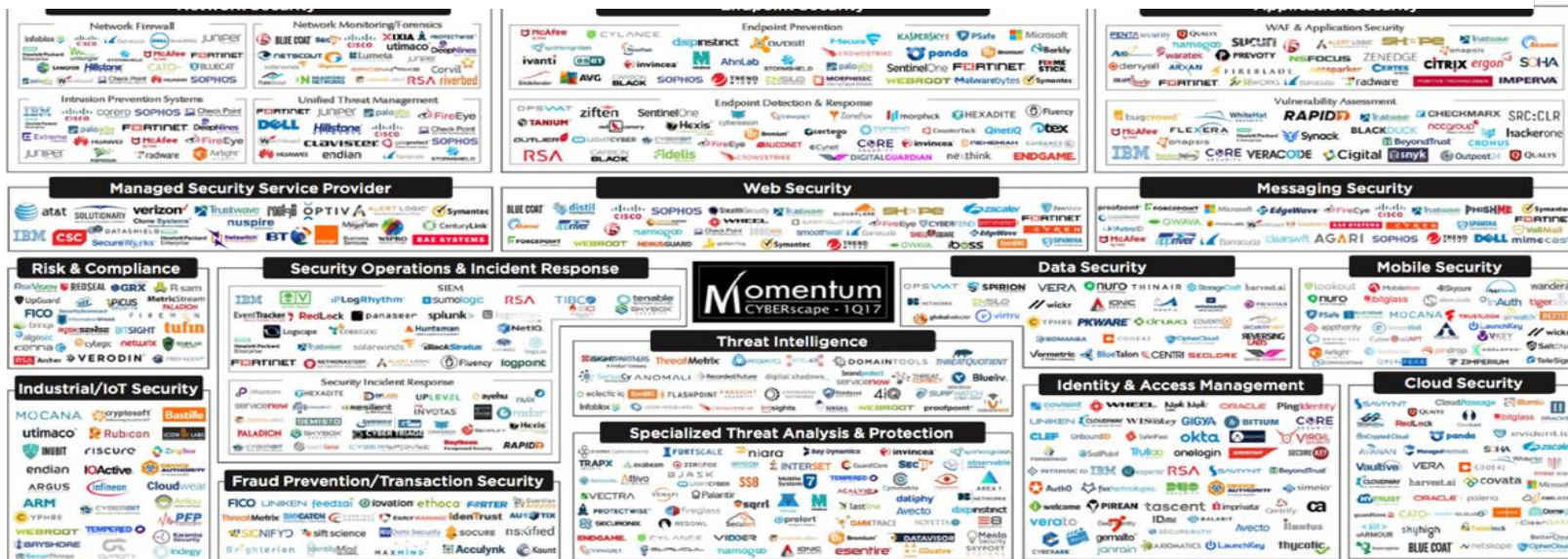
- Get visibility!
 - Flooded by security event (SIEM)
 - Pollution (policy violation, anomaly, execution analysis for an adware...)
 - Discouraging
- Focus on “**lateral movement**”: best compromising indicateur
 - When we are thinking about APT, people say “malware”
 - **46% of compromission didn't use malware...**
 - Attacker still needs human action to get sensitive information (“real-time remote access”)
 - Few examples: twitter, DNS, Ink, ...
 - Unexpected pattern/communication




WHAT TO DO?



The number of vendors that want to help you with network security



WHAT TO DO?

- Place more focus on the **inside of your network**
 - IRL: still focusing on perimeter 
- Know everything you can about your **infrastructure**
 - Especially where the crown jewels reside
 - Who talks to who, (NSA → PRISM), and inspect against black lists
- Monitor ALL DNS and SSL negotiation
 - Collect every DNS query and response, analyze everything against every known black list known to man-kind
 - CN and blacklist
 - Encrypted packet statistics
- Place honeypots inside your network
 - Catch scans, SMB, Active Directory; all the things that are used for lateral movement
 - Inspect with most suitable security engine (protocol/file type dependencies)



MORE THAN 50% OF TRAFFIC IS NOW ENCRYPTED

- Gain insight by decrypting and sending the plaintext through security controls
 - It's the only chance at catching something malicious in an encrypted payload
- Enforcement based on root authority of the certificates
- Block known malicious IP's, Hijacked IP's
 - Don't even start the conversation

TLS1.2



- TLS 1.2 introduced ephemeral keys (but not commonly used...):
 - **requires MiTM for inspection**
 - ephemeral keys are very powerful and provide strong encryption.
- **You cannot store** the network traffic for later review
- Many environments require such capabilities, banking being one of them
- **Out of band inspection is also impossible** and many companies have already invested a lot into out of band inspection tools
- You must have inline device, MiTM, to assist you in viewing the exchanges
- Today MiTM TLS devices are probably only installed in less than 1 – 2 % of networks
- **Hackers can force** all of their TLS communications to use TLS 1.2 and ephemeral keys.
 - Browser prefers this setting
 - Browsers have been removing less secure encryption technologies.
 - In that case, all of the hacker actions will go through your network without inspection.
 - Attackers will have ability to attack high percentage of company's due to the blind spot this new encryption technology brings.

TLS1.3

- TLS1.3 draft **only supports DHE**
- **Removes** a lot of old/weak/deprecated algorithm (SHA-1, RC4, DES, ...)
- **Remove RSA static key usages** (call out-of-band architecture into question)
- **Will make MiTM a necessity** and cause everyone to invest in new tools
 - Complex and costly (not only \$\$\$)
 - We'll see whether that happens or not.
- Stronger encryption techniques might be great for privacy (comes with cost)
- You can't block based on content if you can't see it.
- **Lateral movement** is one of the biggest pain points for both hackers and defenders.
 - Visibility tools can get a view into what is going through your network, even if encrypted. And, you can get more visibility on the inside of your network.
 - Hackers have everything automated up to the lateral movement, this is where they must get visibility into your network and it usually is done manually.

THANK YOU

INFOSEC2017



ixia

The image features a 3D isometric cube in the center, rendered in two shades of blue. The word "ixia" is printed in white on the front face of the cube. The background is a solid blue color with a subtle, repeating pattern of light blue hexagons. The lighting creates soft shadows on the ground plane beneath the cube.