Introduction to Cyber warfare
&
Blue Team tactics

by Binu Balachandran

About Me

- An Indian Air Force Veteran
- 23 Years of Experience out of which, 12 years Cyber Security
- Been with EY for almost 5 years
- Extremely passionate about this stuff we call blue team

Linkedin: https://www.linkedin.com/in/binu-balachandran/

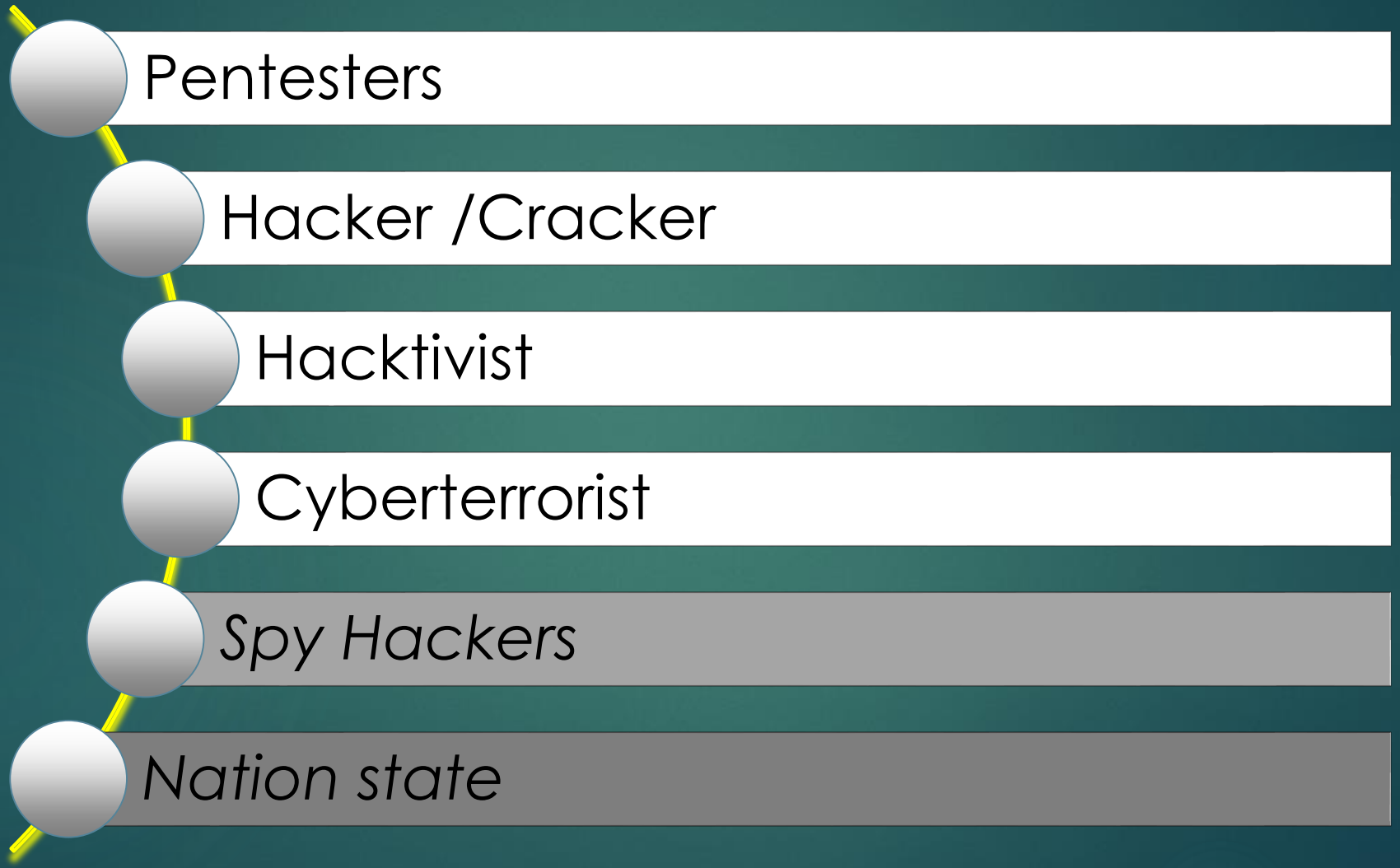
Cyber Warfare

Cyberwarfare

"Actions by a nation-state to penetrate another nations computers or networks for the purposes of causing damage or disruption."

Richard A Clarke - Former National Coordinator for Security, Infrastructure Protection and Counter-terrorism for the United States

Differentiator : Motive



Strategy

- Highly Anonymous
- Deniability
- Maximum control

Attack Scale

- Difficult to identify private or state sponsored hacking.
- Citizens of other regions and countries can also volunteer.

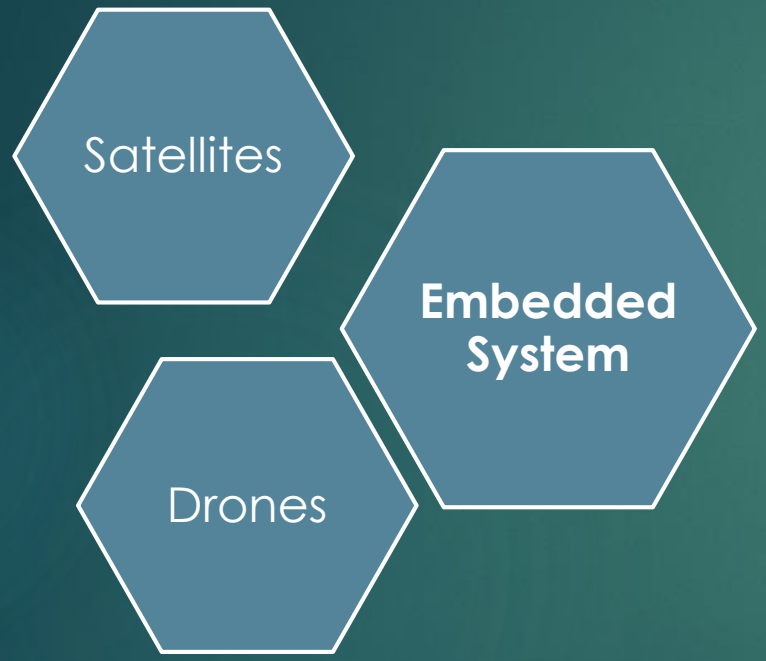
Most Important Phase

Attack Progression, aka the "Cyber Kill Chain"

Most successful attacks

Humans are still the weakest link

New Ammunitions of Cyberwarfare



Blue Teaming

Blue Team

"Blue Team refers to the internal security team that defends against both real attackers and Red Teams. Blue Teams should be distinguished from standard security teams in most organizations, as most security operations teams do not have a mentality of constant vigilance against attack, which is the mission and perspective of a true Blue Team.."

Daniel Miessler – Information Security professional & Writer

Understand Your Business

Know your Ground

Team selection

- Security first mind-set
- Enthusiastic
- Investigative Mind-set
- Good Communication

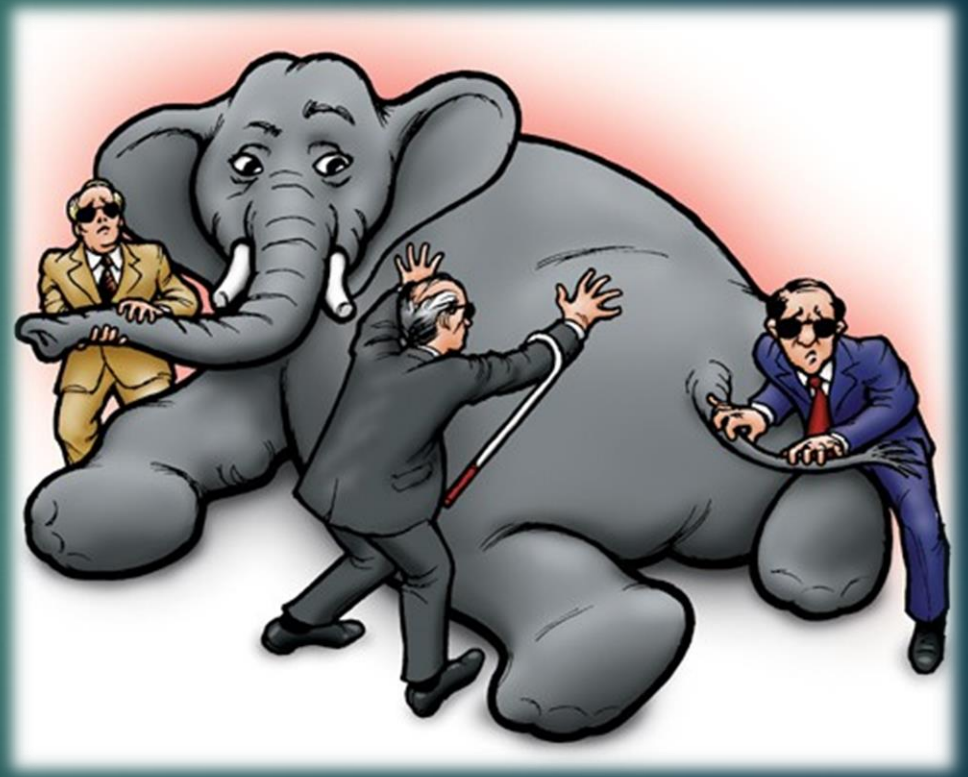
Incident Response Plan

SIEM – "Security Information and Event Management"

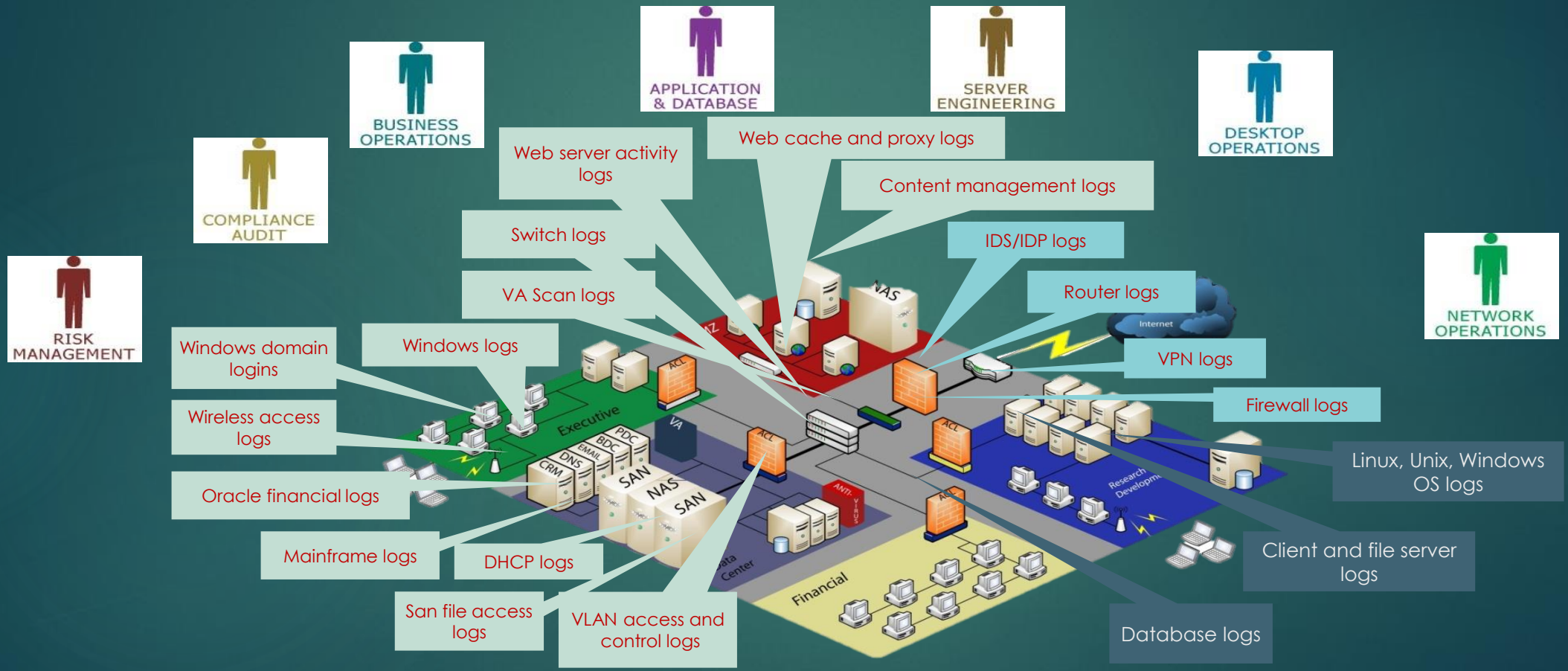
View what's happening on your Infrastructure through a different lens

- Intrusion Detection only understands Packets, Protocols and IP Addresses
- Your Endpoint Security sees files, usernames and hosts
- Your Service Logs show user logins, service activity and configuration changes.
- Your Asset Management system sees apps, business processes and owners

None of these by themselves, can tell you what is happening in terms of securing the infrastructure – but together, they can…



SIEM transform data into actionable knowledge and intelligent Information



Red Team Vs Blue Team

Threat logic

Threat logic is a formulated thought process comprised of the following:

- What's the nature of the alert?
- What type of machine did it happen on (Server, laptop, etc)?
- What data do I have to formulate a better hypothesis of the activity?
- What may have occurred prior to the alert & shortly after?
- What are the Indicators of Compromise (IOC)
- Which stage in the Cyber Kill Chain
- What questions can I not answer?

Cyber Kill Chain

Threat Hunting

- Focuses less on the tools and more on the threat hunter's knowledge .
- Skills must be deep and diverse, including penetration testing, threat intelligence, network and host forensics, risk modelling and analytics and incident response.
- Threat Intelligence Sources are critical to mature threat hunting teams, and should ideally leverage commercial AND open source intelligence feeds to adequately cover business risks.

Questions Anyone?