THE EVOLUTION OF **THREAT HUNTING**

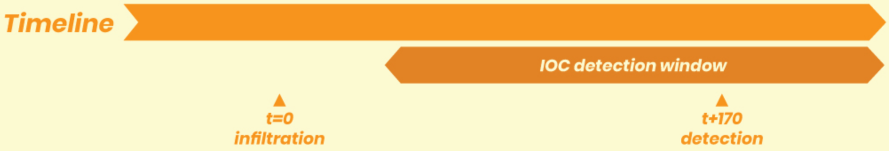
> "The process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions."
>
> ***Cyber Threat Hunting***

Depending on who you ask, threat hunting has been around for upwards of 20 years, with the job title, "threat hunter," originating in the last 5-6 years. Today, there are nearly 1000 profiles on Linkedin with either a headline or job title matching the term

IOC Detection

Initially, hunters sought to identify Indicators of Compromise (IOCs). At its simplest, an IOC is evidence that an attack of some sort has occurred. Examples of IOCs include malware infection, unexpected outbound traffic from an internal asset, large outbound data transfers, etc.

170 Days The average dwell time before a company detects a threat.



Timeline

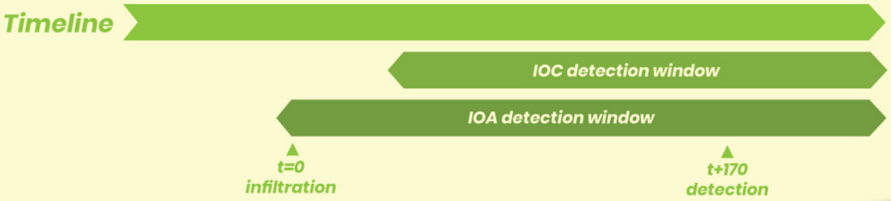
IOC detection window

t=0
infiltration

t+170
detection

IOA Detection

This IOC shortcoming has lead infosec teams to move up their detection capabilities, focusing not on "What has happened," but to "What is happening." While IOA detection helps to identify threats sooner in the process, its Achilles' Heel is that detection is still only possible after an initial infiltration event has occurred.



Timeline

IOC detection window

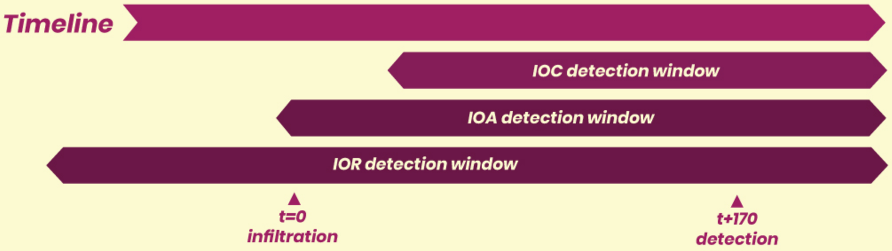
IOA detection window

t=0
infiltration

t+170
detection

IOR Detection

In light of these challenges, threat hunting teams are increasingly turning their attention to indicators that are observable before the adversary has infiltrated the organization - Indicators of Risk (IORs). IORs tell the threat hunter whether the organization is vulnerable to a particular type of attack, not whether or not an attack is happening right then.



Timeline

IOC detection window

IOA detection window

IOR detection window

t=0
infiltration

t+170
detection