# ABNORMAL BEHAVIOR DETECTION IN THE ENTERPRISE

## A HACKER'S VIEW OF ENTERPRISE SECURITY

BY: DAVE KENNEDY

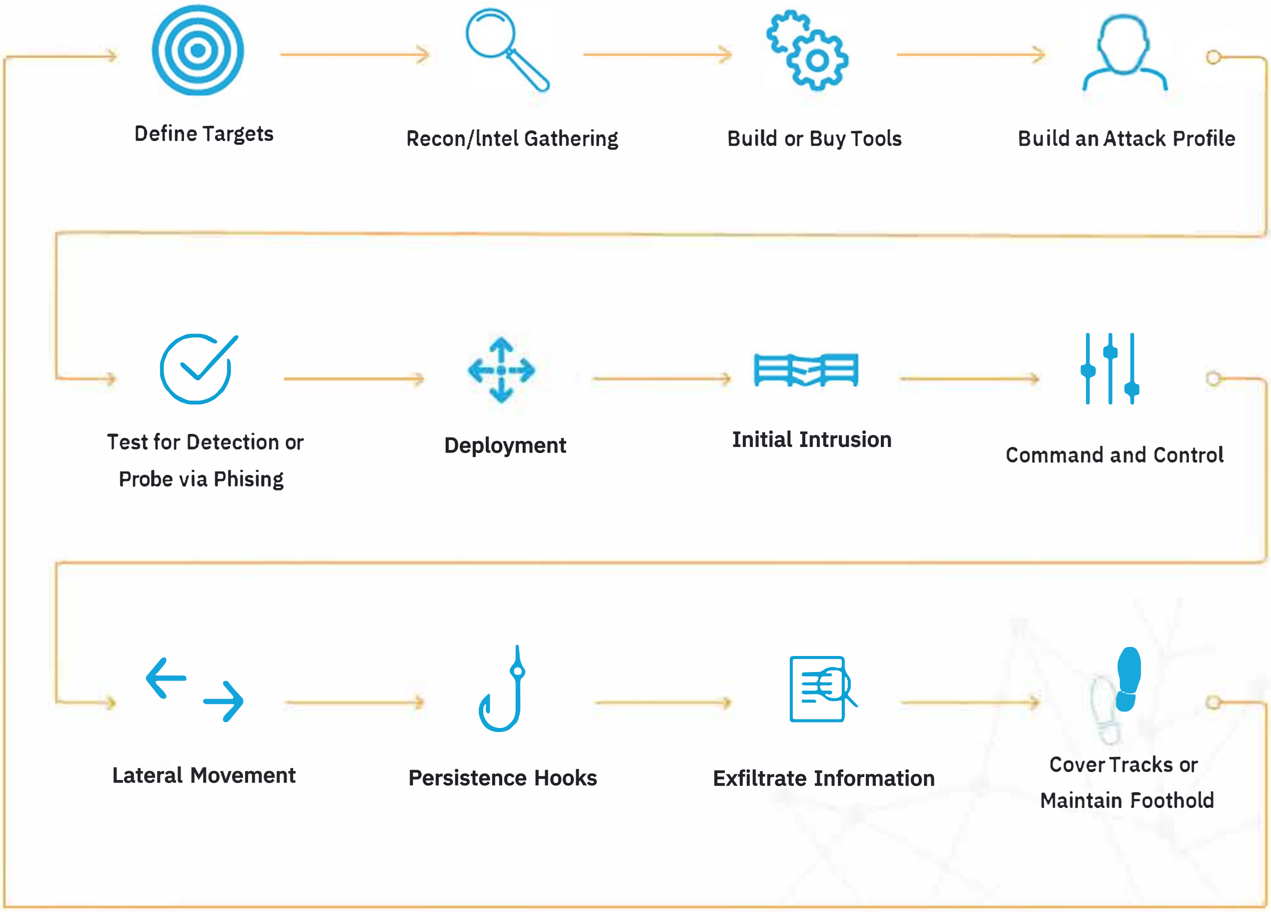
Most enterprises struggle with the ability to detect attack vectors that are designed to evade most enterprise defenses. The shifting tactics of the attackers are troublesome for most companies due to the nature of how the attacks work and the inability to change dynamically with the attack vectors. Traditional technology such as Anti-Virus, Intrusion Prevention Systems, and Firewalls are a base level of security when it comes to defending against what most attackers focus on.

As an attacker myself, I focus my efforts on ensuring that when I go after a target, the implants (malware/ backdoors) do not get detected by Anti-Virus and other technologies. Some companies have invested in Sand boxing technologies that focus on the virtualization and identification of abnormal patterns. These are highly predictable and easy to circumvent. Still to this day, most compromises occur from direct executables infection. That means that most of the attack vectors regardless if it's a Macro-enabled excel document or visiting a malicious website attempt code injection in order to download an executable in order to compromise the system. This is the majority of attacks that we see today in the industry.

Executable infections are problematic because they range from ransomware infections all the way to targeted attacks from nation states. With the majority of the "noise" being from executables, it's never been more important for us as an industry to understand the best approach to protecting against the largest risk factor we have. While our endpoints tend to be the infection origination for a breach, the methods for infection need to be understood and protected against. The question is, how do you protect yourself against the largest population of attacks, and then move onto the more advanced methods for compromise.

This brings us to the topic of "known good" or what is also known as application whitelisting. Most organizations struggle with the ability to baseline their images and ensure a consistent number of workstations/endpoints that have the same configuration across the enterprise. The concept of known good takes a companies normal operations and documenters deviations in order to understand what the enterprise needs to operate. Any deviations are then either prohibited or monitored in order to ensure they are not malicious in nature. For those that are not familiar with application whitelisting, it's the concept of baselining your organization and then from there only allowing what is normal. Normal is defined by the baseline configurations and documented deviations and monitored from there.

## Life cycle of an Attack



The concept of known good is nothing new, but if your main infection method is through executables and you understand what your environment is doing -you can literally cut out 90% of your "noise" which is the main methods for exploitation and then monitor on deviations to that. This industry is focused too much on individual attacks and not on how to reduce the overall noise of an organization and focus/prioritize on the best methods for reduction of noise and minimization of risk.

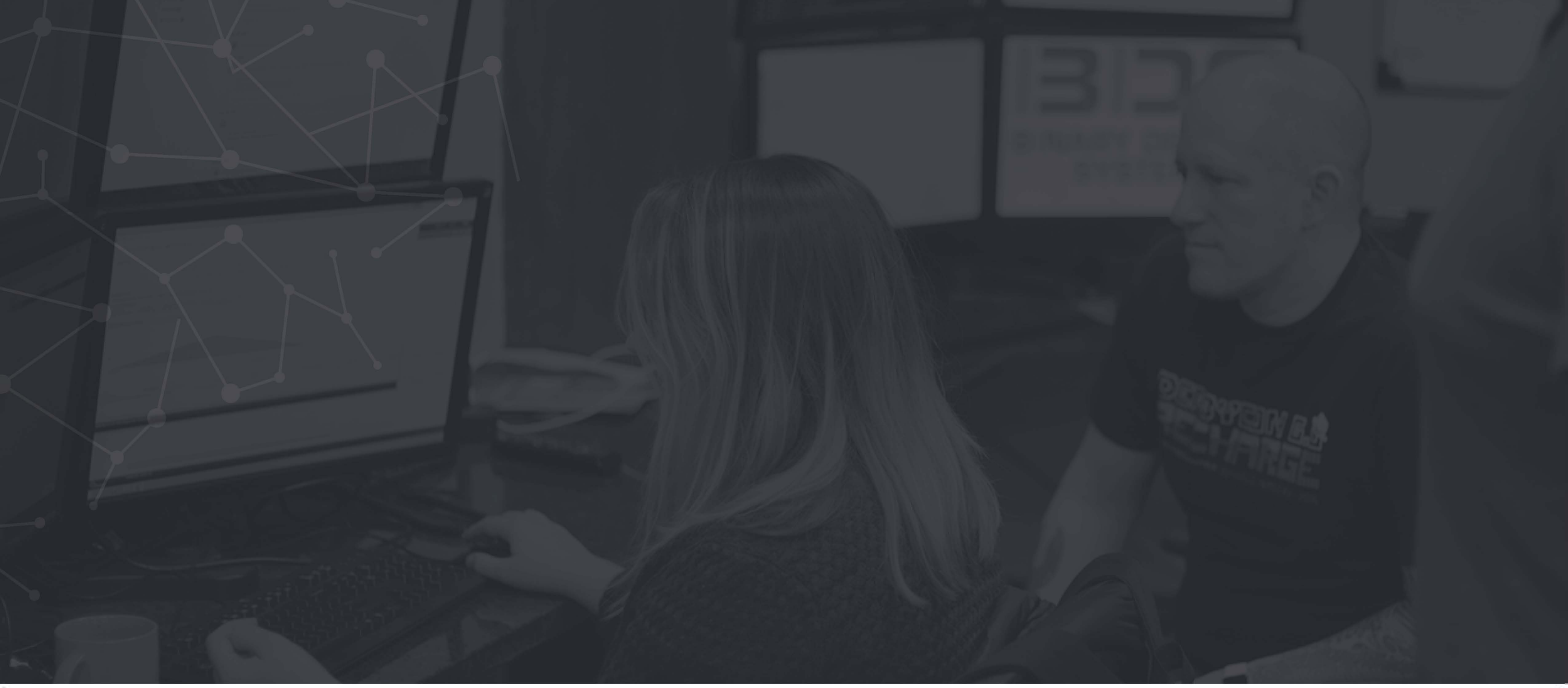
There's no question that application whitelisting is difficult. It's a GOOD difficult. It means that when you baseline your enterprise, you have an understanding of what your environment looks like. It means that you can now look for deviations of patterns and recognition of behavior. Most security programs are not anywhere near this level. Once you've performed and implemented known good - it becomes significantly easier to prohibit directed attacks against you.

Let's take an example of how to configure known good. Let's take a basic example. Most attackers (based on Binary Defense research 98.7 percent) do not utilize code signing certificates. If you implement a program that blocks any executable that is not code signed, you can eliminate 98.7 (on average) of risk in your environment.

> *Example:*
> *Microsoft deploys a patch. Is code signed by Microsoft. Allowed. Malware – not code signed, is blocked.*

In this simplistic example, if you block anything that is not code-signed and allow exceptions based on deviations. Known Good becomes a much easier process to handle.

I am personally a huge advocate, but I'm not alone. Penetration Testers/Researchers/Red Teamers all agree that by baseline your configuration you can drastically reduce your attack surface.



Let's assume that you have bought into the concept of application whitelisting and "Known Good" and have it implemented appropriately. Now comes the detection and deviation of patterns. Attackers are smart. They realize that organizations that have implemented Known Good will become much more difficult for exploitation. They need another way for exploitation.

There are multiple other ways to gain access to a system that does not require exploitation of executables. PowerShell is a fantastic example. There are patterns within an enterprise that you can baseline, similar to known good that can help you detect these types of attacks.

Did you know that there are fourteen different variations to EncodedCommand which are used for PowerShell detection bypasses?

-e
-ec
-en
-enc
-enco
-encod
-encode
-encoded
-encodedc
-encodedco
-encodeecom
-encodedcomm
-enodedcomman
-encodedcommand

There's great research on PowerShell injection as a main method for exploitation by Palo Alto Networks on methods for exploitation using PowerShell

http://researchcenter.paloaltonetworks.com/2017/03/unit42-pulling-back-the-curtains-on-encodedcommand-powershell-attacks/

Binary Defense focuses on “Known Good” as well as enhanced detection and prevention capabilities around obscure behavioral attack vectors. While known good may seem daunting, our Endpoint Detection and Response platform focuses on Known Good protection (in an easy manner) as well as multiple other phases of an attack. All the way from methods of compromise, all the way to lateral movement and further compromise of systems.

Let Binary Defense help you with get to the point where attackers move on, based on your level of protection.

> Understanding abnormal behavior in an environment is a tough challenge but not impossible. This article focuses on thinking differently about how to detect indicators of compromise within an organization.

Dave Kennedy
Chief Technology Officer
Binary Defense