APRIL 2020

E-BOOK

DWELL TIME AS A CRITICAL SECURITY SUCCESS METRIC

ARMOR

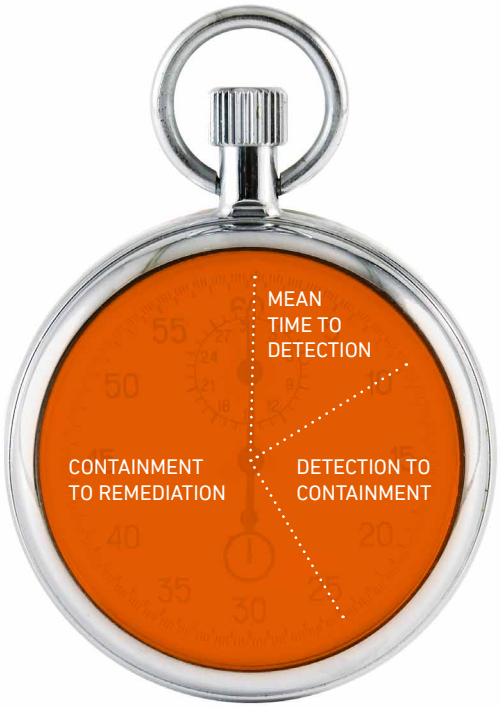
INTRODUCTION

Five days. By Armor estimates, it takes just 5 days for a threat actor to perpetrate a successful breach of your security defenses and complete his or her objective of stealing data from your environment. Those same 5 days can change an organization's fortunes for the worse and put the security team, including the CISO and even the CIO, on very thin ice.

However, security teams across organizations from the smallest business to the largest enterprise—and the security industry at large—seem to be skirting the issue. We talk about how dwell times need to come way down from their 78-days average, but we don't implement the changes needed to really do so. In fact, we define dwell times in different ways. And we certainly don't report on dwell times openly.

It's high time that security teams and security providers redefine how they measure the performance of their security programs (architectures, policies, and processes) against today's cyberthreats. "Dwell Time," defined as the time from the point a threat successfully enters your environment to when the threat is completely remediated, represents the best measure of the overall effectiveness of your security team in combating threats.

COMPONENTS OF DWELL TIME



DWELL TIME = TIME (INITIAL INTRUSION TO ERADICATION)

EXECUTIVE HIGHLIGHTS

1. Dwell time is more than just a metric; it is a catalyst for a proactive security philosophy built around a common objective.

2. Organizations should pursue reductions in dwell time, defined as the period from when a threat successfully enters the network environment to the time the threat is completely removed from that environment.

3. Dwell time should align to the entire lifecycle of an attack as best represented by the Cyber Kill Chain® (Lockheed Martin). Phases 4 through 7 represent the opportunity security teams have to disrupt the threat actor's processes.

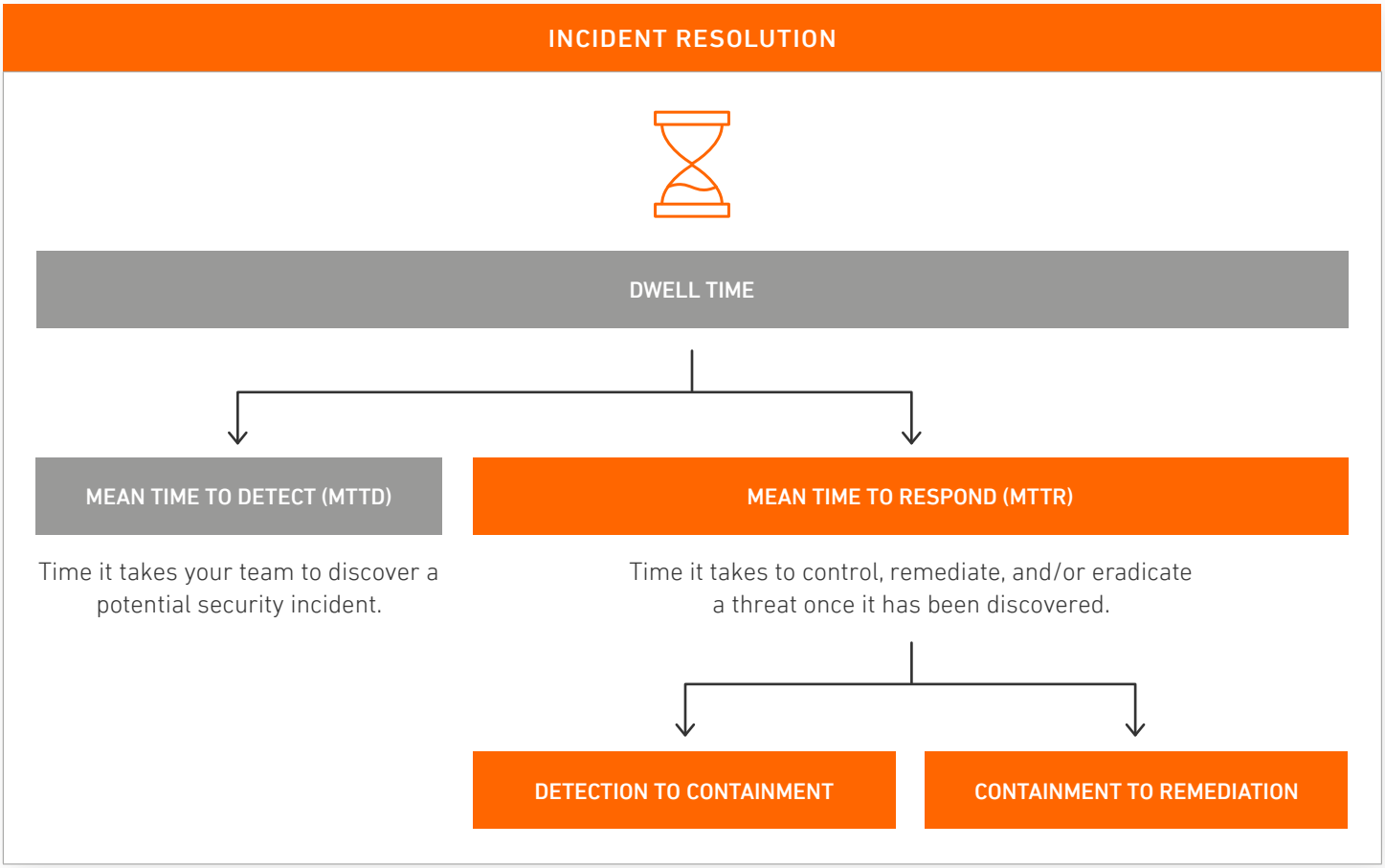
4. MSPs, managed detection and response (MDR) providers, and security-as-a-service providers should retool their processes, systems and infrastructure to align to and report on dwell time for their customers. They should also report on dwell time as a standard industry metric and critical security outcome.

5. Threat Intelligence is critical to identifying unknown threats missed by traditional technologies and tools, and it is a key component of any effort to reduce dwell times.

DWELL TIME AS A CRITICAL METRIC

Dwell time represents a powerful metric for security teams to use in today's cyberthreat landscape to assess the entire operational process of your security program from architecture to engineering to operations and incident response. Dwell time is also a transparent measure to assess how well your team, or the services of a service provider, prevents, detects, and neutralizes threats.

No other measure is as comprehensive or meaningful for organizations today than dwell time. Regardless of whether your organizations have an established in-house security program or you leverage a managed service provider, you should be assessing the performance of your security program by this measure.



DEFINING DWELL TIME

Dwell time, at its core, is an admission that proactive controls have failed. Though one would expect that "dwell time" would be straight-forward and understood across the industry, there are actually competing definitions on what dwell time refers to.

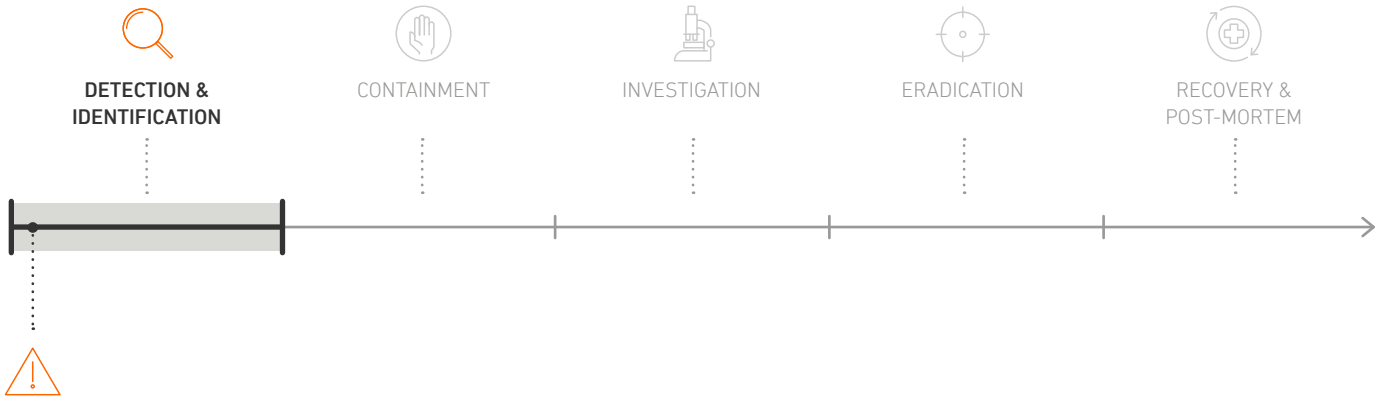
One cited definition comes from FireEye's M-Trends 2020 Report where dwell time is defined as:

> **Dwell time is calculated as the number of days an attacker is present in a victim network before they are detected. The median represents a value at the midpoint of a data set sorted by magnitude, from internal detection to external notification.**
>
> — FireEye/Mandiant

FireEye calculates dwell time and the containment time of an incident. The dwell time refers to the length of time from the initial compromise through the point of notifying stakeholders. The containment time refers to the period between collecting live response data and the eventual remediation. The organization may choose to define remediation as simple containment (preventing the threat from moving laterally), or full restoration of service (threat eliminated, system returned to normal).

CrowdStrike followed this lead and similarly defined dwell time as: "...the period between when a malicious attack enters your network and when it is discovered."

DWELL TIME AS DEFINED BY FIREEYE, CROWDSTRIKE, AND OTHER MSSPS

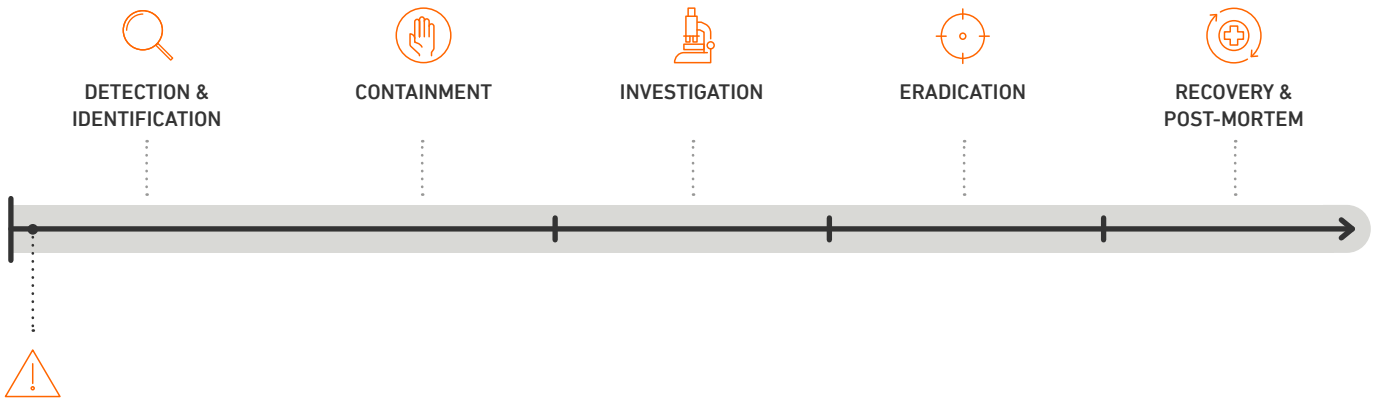


However, other organizations, including Raytheon and Armor, advocate for a different definition of dwell time. In their report "Cyber Dwell Time and Lateral Movement: The New Cybersecurity Blueprint," Raytheon stated:

> **Cyber dwell time begins when an attacker enters your network and continues until you eject them or they leave (presumably after having completed the intended actions).**
>
> — Raytheon

At Armor, we believe dwell time should closely align to the Lockheed Martin Cyber Kill Chain® and encompass the period from when a threat successfully enters the network to the time the threat is completely removed from that environment. This change in thinking rallies the entire team around one quantifiable standard to calculate the effectiveness of your security strategy, programs, and overall security posture.

DWELL TIME AS DEFINED BY ARMOR AND RAYTHEON

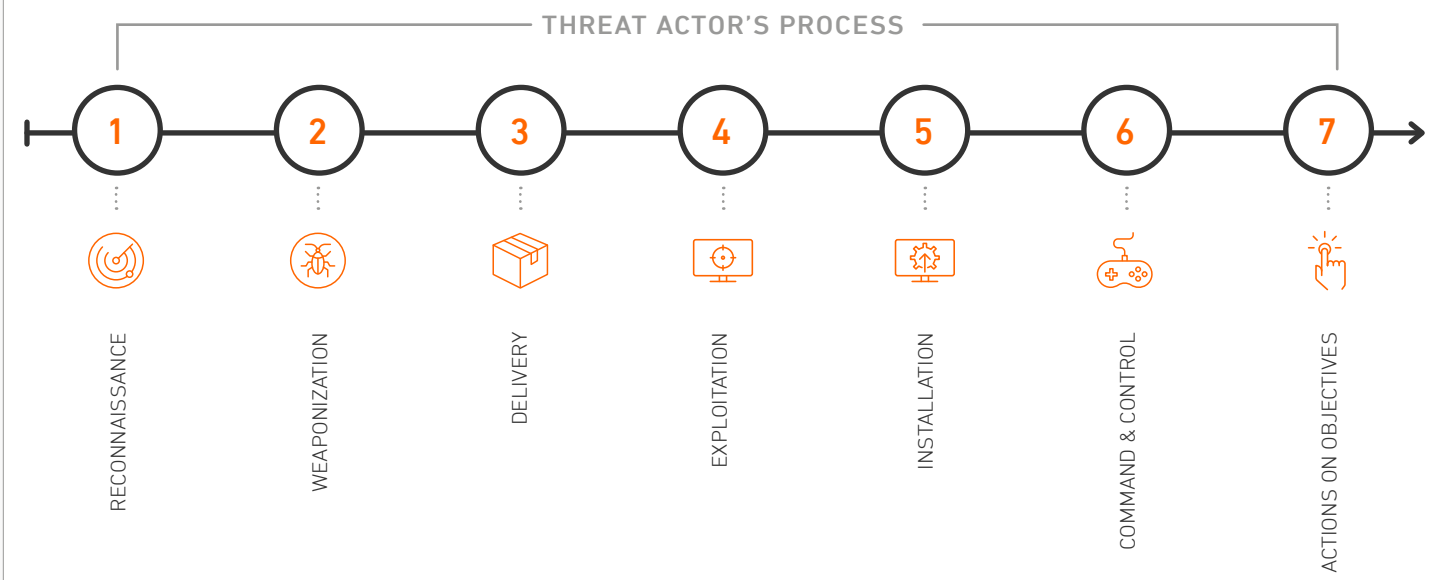


DWELL TIME AND THE CYBER KILL CHAIN

If you're in information security, you likely know about the Cyber Kill Chain articulated by Lockheed Martin. The Kill Chain represents the lifecycle of a threat (the process the threat actor conducts) from beginning to end. In this model, phases 4 through 7 represent the opportunity security teams have to disrupt the threat actor's efforts.

Though the characteristics of each threat and movement through the process will be unique, each threat must be looked at in its entirety.

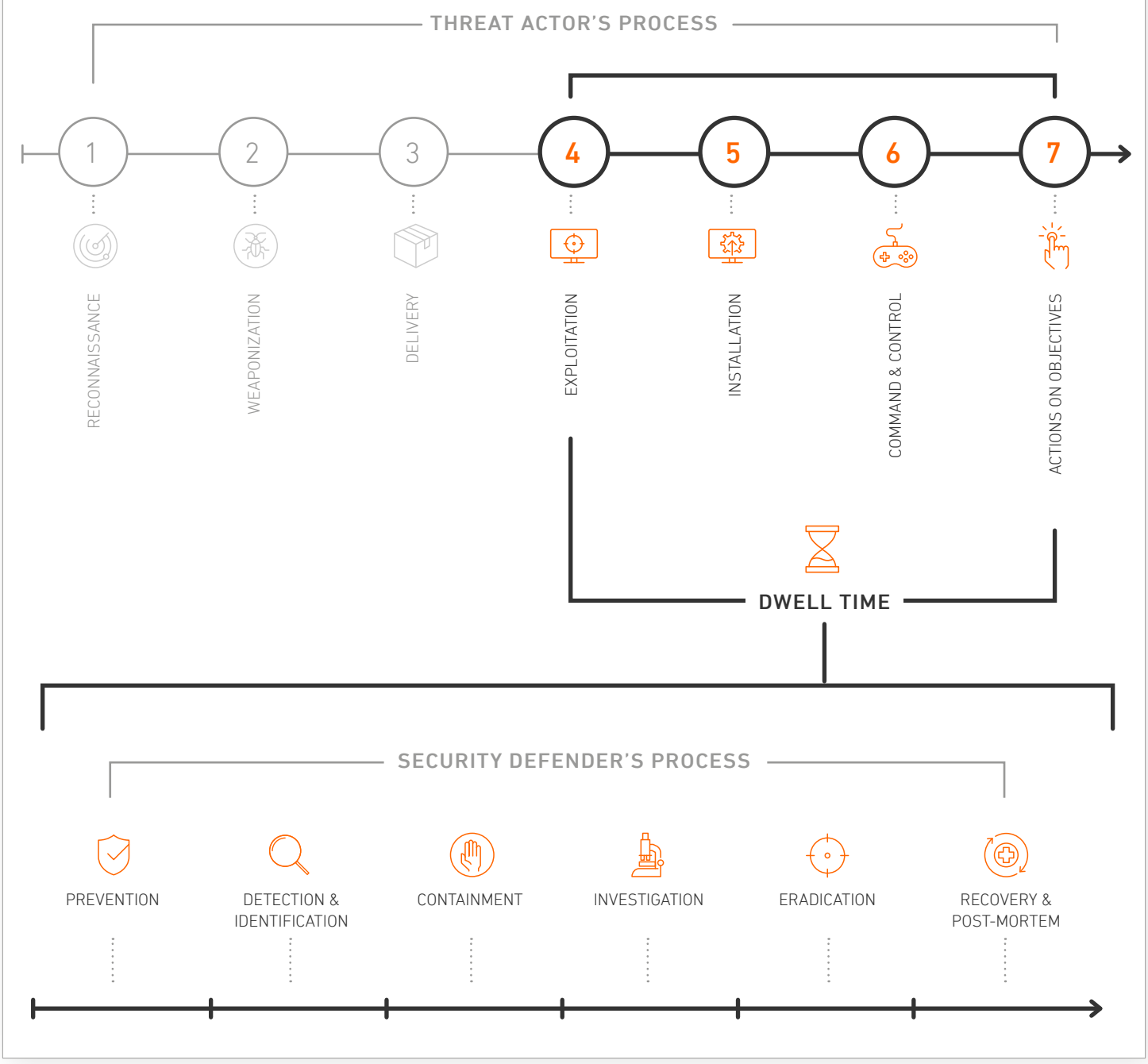
LOCKHEED MARTIN CYBER KILL CHAIN



This is a fundamental premise for why Armor believes that dwell time must be representative of the entire period that a threat is present within an organization and poses risk, from the time the threat successfully penetrates network defenses to the time the threat is completely removed from the environment.

Even during any response phase, the threat actor may still have an opportunity to perform actions on objectives, making it critical to add this time into the overall calculation for dwell time.

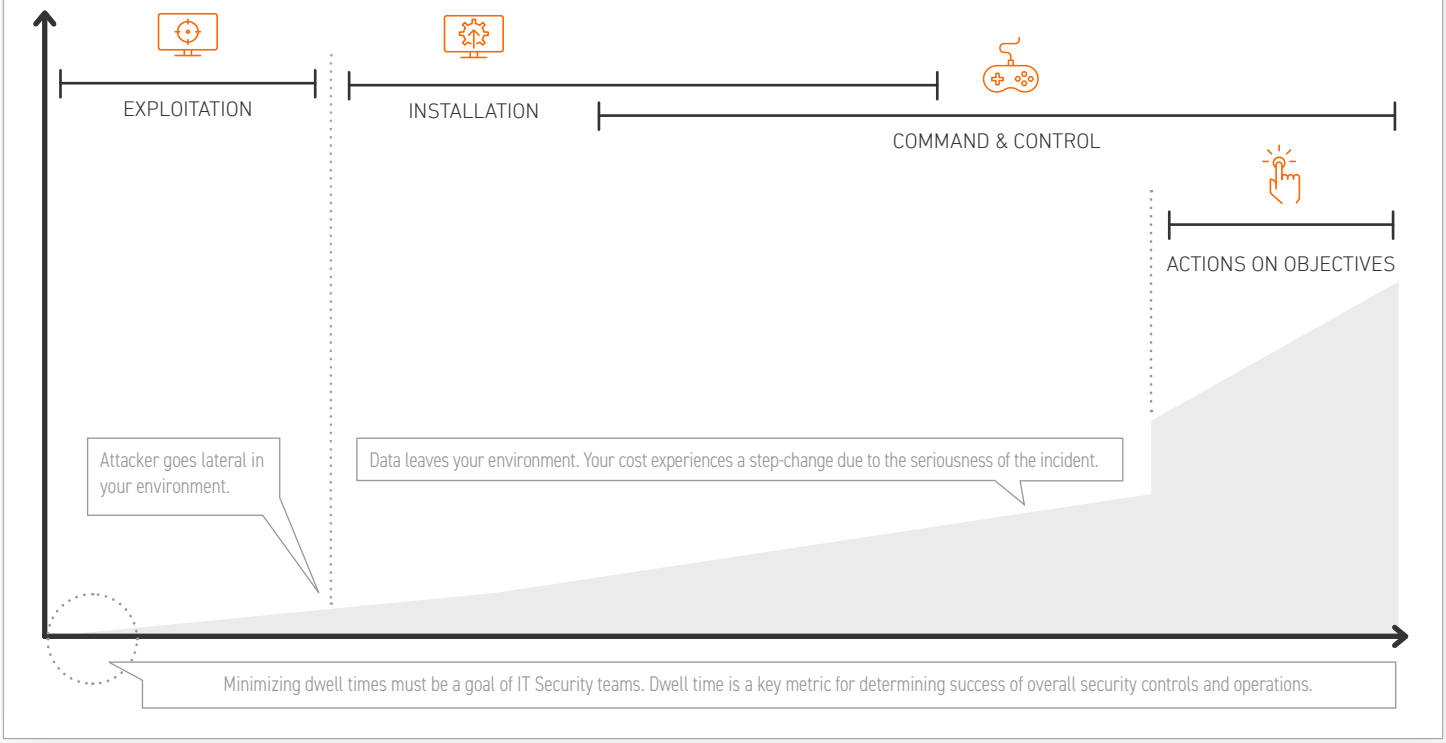
THREAT ACTOR'S PROCESS VS. SECURITY DEFENDER'S PROCESS



THE COST OF EXTENDED DWELL TIMES

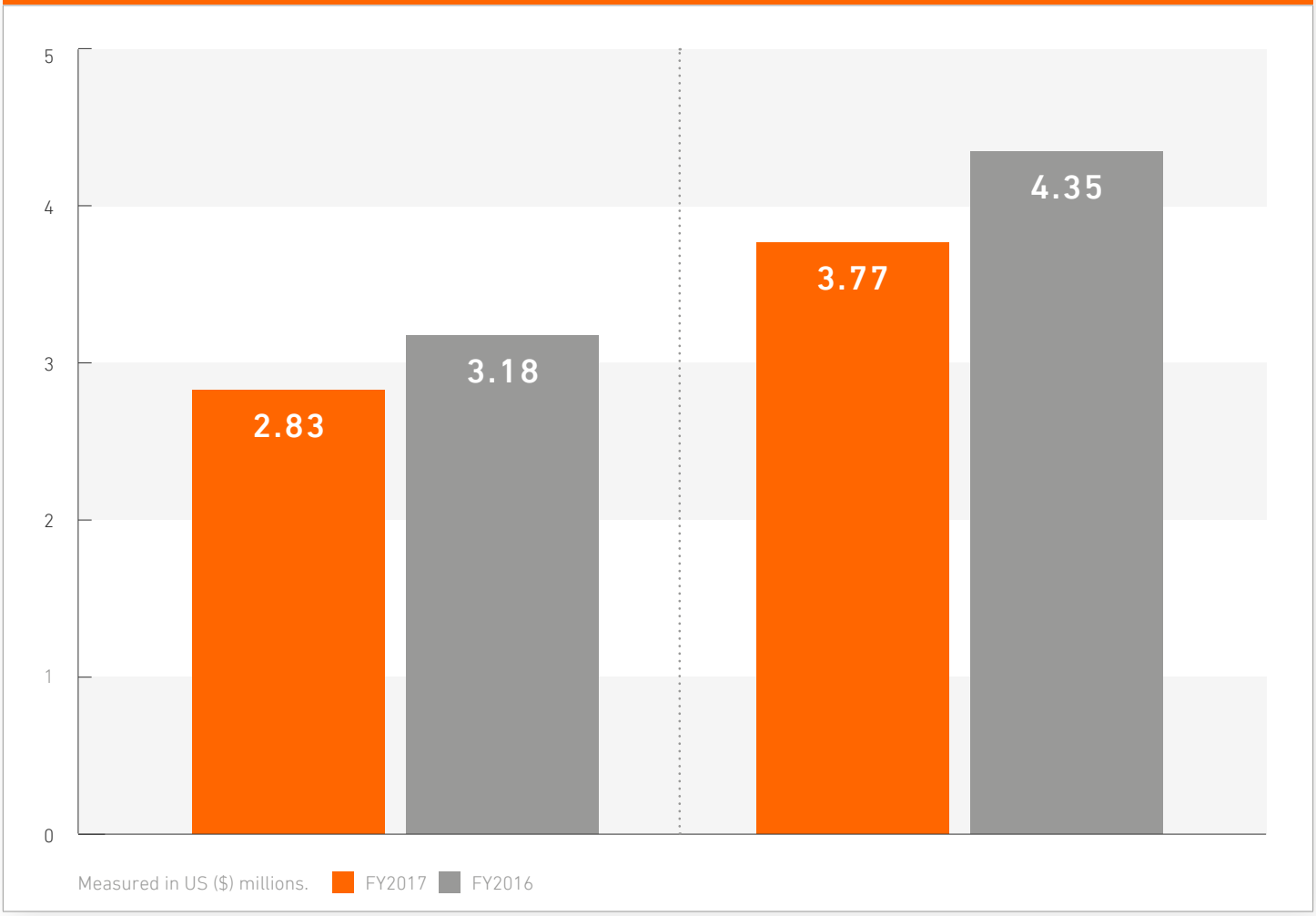
The longer a threat actor is able to operate unfettered in your environment, the more likely the actor is able to achieve actions on objectives, the final stage of the Cyber Kill Chain. For businesses, shorter dwell times mean reduced risk of a data breach, a malware outbreak, or their machines getting ensnared in a botnet or held hostage by ransomware. In turn, this also means lower chances of downtime, regulatory compliance penalties, and hefty lawsuits and costs stemming from a cyberincident.

CYBER KILL CHAIN AND COST OF AN INCIDENT



The importance of minimizing costs can't be overstated. This correlation of time and cost is articulated in Ponemon Institute's "2019 Cost of Data Breach Study: United States" report and depicted in the chart below:

RELATIONSHIPS BETWEEN 'MEAN TIME TO CONTAIN' AND 'AVERAGE COST'



While dwell time has been generally declining year over year, it's still unacceptable. Currently measured in days, the average dwell time varies depending on who you ask. Ponemon Institute cites 191 days from the point of detection to the point of remediation with the time from detection to remediation being 66 days. FireEye reported a median dwell time of 56 days in its "M-TRENDS®: A View From the Front Lines 2019" report. However, that dwell time reflects its narrower definition, which only considers initial penetration to detection and alerting, and doesn't include response and recovery periods.

This is a problem because mid-level threat actors are attacking vulnerable workloads within minutes and only need 4 to 6 days to infiltrate a network and then less than a day to ultimately carry out their main goal of exfiltrating data. Because we know from experience that a threat actor will not stop in their efforts to achieve actions on objective until they are actually kicked out of an environment, not counting the time it takes from the point of detection or alerting of the threat to its eradication from the environment underrepresents the period of time a threat actor has to operate.

DWELL TIME AND SECURITY SERVICE PROVIDERS

If you utilize the services of a MSP, managed detection and response (MDR) provider or security-as-a-service provider today, this section should help you understand how your provider may or may not address dwell time and the value that provider delivers in helping to reduce risk to your organization.

Talking the Talk, Not Walking the Walk

We performed an anecdotal review of 8 MSPs, MDRs, and SECaaS combined to look at:

1. Do they talk about dwell time, mean-time-to-detection, mean-time-to-response or other similar metric in content on their website or collateral?
2. Do they provide any actual metric for how they perform in terms of dwell time, mean-time-to-detection, mean-time-to-response or similar metrics?

The results were disappointing. Though 7 of the 8 vendors talked about dwell time and the importance of reducing it as much as possible, only one vendor talked about its operations being designed with dwell time in mind. However, not a single vendor actually published any specific dwell time statistics on its website or in marketing collateral.

Measuring dwell time is a crucial metric and operating tenet that providers must strive to deliver on beyond the apparent lip service being paid. Dwell time also represents a clear way for organizations to prove the real value of their protection to customers beyond simple counts of events processed and alerts generated for the customer to then address.

Paying Lip Service to Dwell Time

Seven of 8 security service providers mention the importance of reducing dwell time. However, zero of 8 actually publish any specific dwell time statistics.

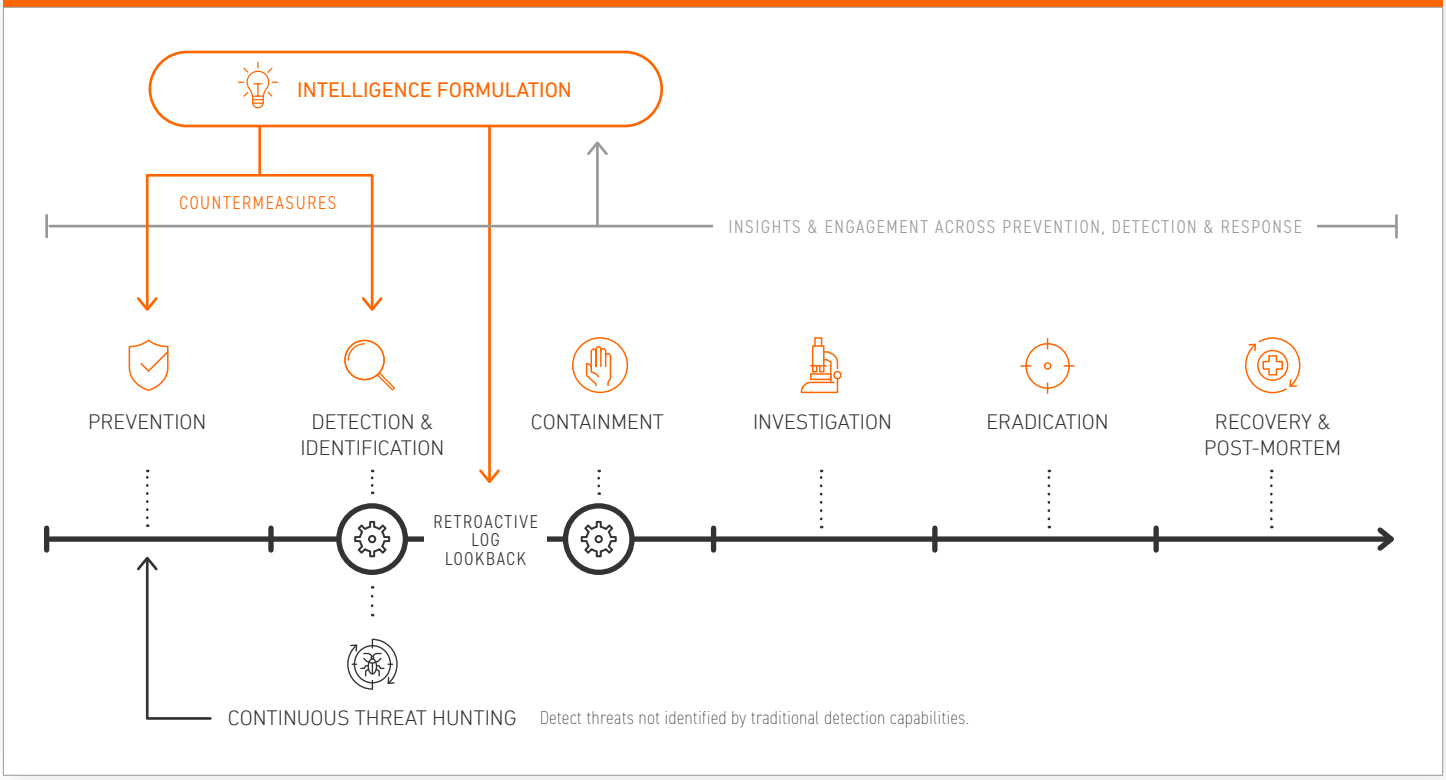
REARCHITECTING YOUR SECURITY PROGRAM TO ADDRESS DWELL TIME

Dwell time is not just a metric. It's a proactive security philosophy and culture that drives unified change across all security operations to achieve a common objective: Minimize the opportunity a threat actor has to cause harm to your organization.

Our security experts have put together the suggestions on the next page to help you and your security team drive toward operating and measuring your security program by dwell time. It's important to note that these suggestions are borne out of Armor's own strategies and design elements of our cloud security threat detection and response platform. In other words, they are proven.

If you use a managed service provider, it's imperative you ask them about these same areas and their commitment to and reporting on reducing dwell time.

SECURITY PROGRAM DESIGNED AROUND DWELL TIME AS AN OPERATING PHILOSOPHY



SUGGESTIONS TO REDUCE DWELL TIME

LEVERAGE HARDENED CIS SERVER BUILDS

Make sure that all servers are hardened out of the box and adherent to CIS standards. This makes it extremely difficult for threat actors to even initiate their Cyber Kill Chain.

IMPLEMENT AN AGGRESSIVE PATCHING PROGRAM

Most major malware outbreaks happen because threat actors can exploit vulnerabilities in unpatched software. An aggressive patching program can eliminate known vulnerabilities and thwart the large number of commoditized exploit kits (along with their accompanying malware payloads) that target them.

USE ON-ACCESS SCANS FOR ANTI-MALWARE TOOLS

On-access scans have the advantage of detecting malware infections much earlier than on-demand or scheduled scans by automatically scanning for malware every time a new connection occurs. Previous scheduled scans can leave you vulnerable for the duration of time between each scan.

INTEGRATE EDGE-BASED TRAFFIC SHAPING

By integrating edge-based traffic shaping, you can prevent known-bad infrastructure from connecting to your infrastructure based on the consensus of the cyberthreat research community.

DEPLOY A 'ZERO TRUST' MODEL FOR SERVER PROVISIONING

A Zero Trust model assumes no one (neither outsiders nor authorized end users) can be trusted. As such, apply rigorous segmentation that prevents threat actors from moving laterally with ease. For example, for websites, implement a highly segmented multi-tiered architecture. In this case, a web server would be configured to have limited communications with the application server, which, in turn, would have limited communications with the database server.

INTEGRATE THREAT INTELLIGENCE FOR VALUE

Proactive threat intelligence operations are another critical component to ultimately reduce dwell time, and this entails the monitoring and research of activities within and beyond your network edge to identify potential areas of concern and risk as well as instrument protections before an attack takes place. Considered in the context of the Cyber Kill Chain, the idea is to "push left" to thwart attackers earlier in the process. Organizations must have this capability to be effective in reducing dwell time, either in-house or through their managed services provider.

USE ADVANCED ANALYTICS AND CORRELATION

Poorly designed security information and event management (SIEM) systems tend to report thousands of events that are, in fact, only part of a handful of events or even just a single event, thereby causing confusion and preventing incident responders from taking the right course of action. If operating security in-house, use a SIEM that correlates information exceptionally well and tells you exactly what's going on. This enables you to quickly analyze an event and respond accordingly. If you are leveraging a managed services provider, be sure to investigate how their backend "platform" and SIEM function, what types of analysis are performed on incoming event data, how intelligence is collected and applied across their processes, and what response levels are included in their core offering.

SECURITY ORCHESTRATION AND AUTOMATION

Assess your security program's processes and workflows to identify areas where a security orchestration, automation, and response (SOAR) solution can be applied to you advantage. If just starting out, automation may make more sense to pursue initially to get some quick wins and experience before embarking on more complex orchestration projects. Research vendor options in this field that may accelerate your organization's operations.

For instance, organizations may be able to automatically triage events and reduce these events from touch by humans, automatically retrieve related threat intelligence information to speed decision-making, and orchestrate various workflows that allow security teams to focus their energies on more critical and complex initiatives.

With the challenge in finding and retaining security talent as well as in managing and remediating alerts, security teams must pursue strategies to standardize, automate, and even orchestrate processes within their organizations. This is equally true for MSSPs and service providers who must be able to scale processes across large client bases. These organizations must be adopting approaches that work to minimize the response burden for their customers as much as possible, as many organizations simply do not have the expertise and resources to respond effectively to incidents within the 5-day window required for a determined threat actor to realize their objectives.

GATHER THREAT INTELLIGENCE

It's important to recognize that "detection" doesn't just mean the myriad of devices that organizations have invested in and installed in their environments. Detection also entails regular threat hunting performed to identify potential threats that the technologies in place may have missed. It's a critical component of the dwell time equation. Absent threat intelligence-gathering, organizations lack the additional assurance that a threat or threat actor has not gotten past your traditional controls and isn't already present in the environment.

CONCLUSION

Five days is all a knowledgeable threat actor needs to inflict considerable harm on an organization and put IT and IT Security in turmoil. Dwell time represents a proactive security philosophy and culture that drives unified change across all security operations to achieve a common objective. Unfortunately, most organizations as well as security service providers are failing when it comes to actually operating by this philosophy. As a consequence, estimates suggest dwell times for many organizations to be upwards of 191 days.

Organizations and service providers that drive toward operations centered around dwell time—architectures, policies, and processes—have an opportunity to make meaningful enhancements to their security posture and maximize the investments made in their current security programs.

ABOUT ARMOR

Armor is a global cybersecurity software company that simplifies protecting your data and applications in private, public, or hybrid cloud—or in an on-premise IT environment. Armor Anywhere provides technology to detect and respond to threats and can be activated in minutes. Armor also helps organizations comply with major regulatory frameworks and controls. Armor's cybersecurity experts monitor customer environments 24/7/365 and, if an attack takes place, helps customers respond quickly and effectively. Wherever you are on your cloud journey, Armor can help. We make cybersecurity simple.

ARMOR.COM | (US) +1 844 682 2858 | (UK) +44 800 500 3167