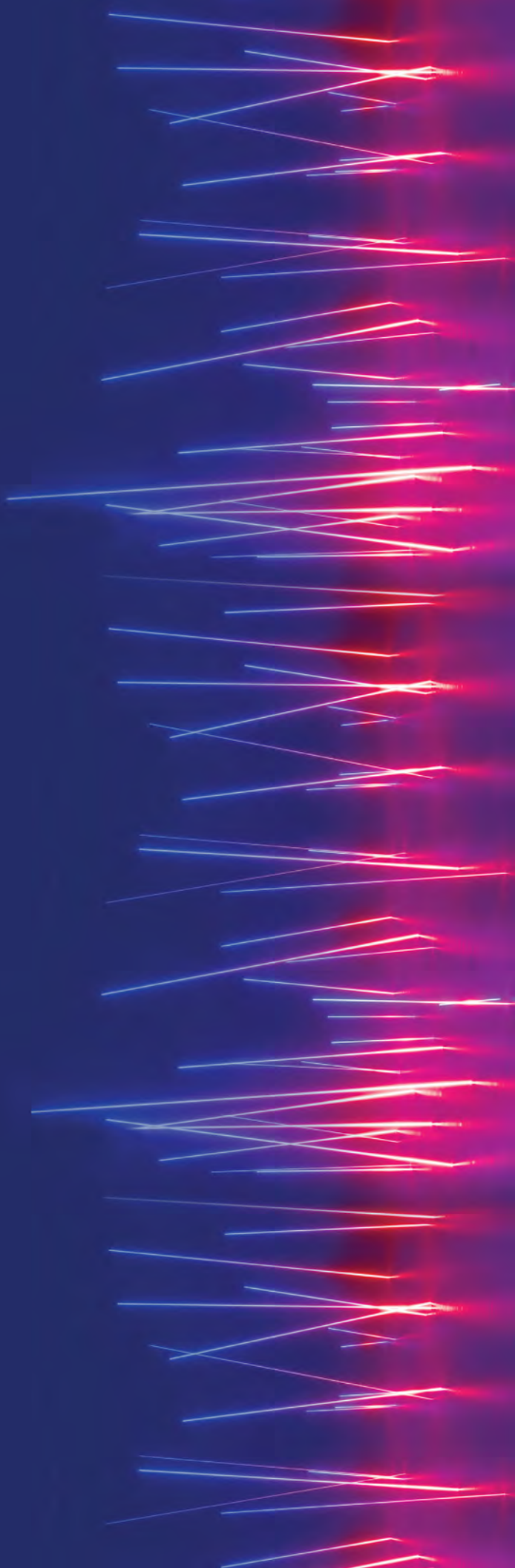
KPMG

Evolving to prosilience

Moving from reactionary defense to proactive, automatic enterprise cyber defense

A 2019 concept brief



kpmg.com

Executive summary

Our adversaries hold the "upper hand." There aren't enough qualified cyber individuals and resources to successfully protect the enterprise. Organizations are constantly playing "catch-up," and reactive responses do not adequately address the threat. The playing field needs to change by evolving defense from reactive to proactive resilience: ***Prosilience.***

Prosilience is "cyber resilience with consciousness of environment self-awareness and the capacity to evolve automatically."[1] KPMG's Prosilience Reference Architecture incorporates new disruptive techniques in concert with preemptive threat intelligence to build the foundation for intelligent automation and cyber convergence. Prosilience delivers a powerful, cyber resilient enterprise that facilitates optimal mission outcomes.

[1] "Moving Beyond Resilience to Prosilience," Summer Fowler, Carnegie Mellon University, Software Engineering Institute, February 27, 2017

Deploying prosilience

KPMG's Prosilience Reference Architecture **(Figure 1)** consists of three phases, each of which incorporate two technology elements:

Phase 1

Define the enterprise baseline using a smart baselining (SB) approach

— Real-time situational awareness

— Advanced adversary pursuit (aka Intelligent Hunting)

Phase 2

Automatically protect the enterprise

— Automatic zero-day and unpatched applications protection

— Actionable predictive threat intelligence

Phase 3

Automate response and remediation

— Security orchestration, automation, and response

— Automation of actionable information

Deployment of prosilience entails two distinct dimensions:

— Technology/Capability integration: Enabling the tools to work together in the context of the enterprise environment

— Operational integration: Adjusting and deploying operational procedures and training the cyber workforce to effectively operate the integrated prosilience capabilities

Phase 1
Define the baseline

— Cyber situational awareness

— Adversary pursuit

Phase 3
Automate response and remediation

— Security orchestration, automation, and response

— Automating actionable information

Phase 2
Automatically protect the enterprise

— Auto protect

— Predictive threat intelligence

Figure 1: *Prosilience Reference Architecture steps*

Phase 1

Phase 1 incorporates SB combined with Intelligent Hunting. SB moves the vulnerability paradigm from what is *unknown* to what is *known* (Figure 2).

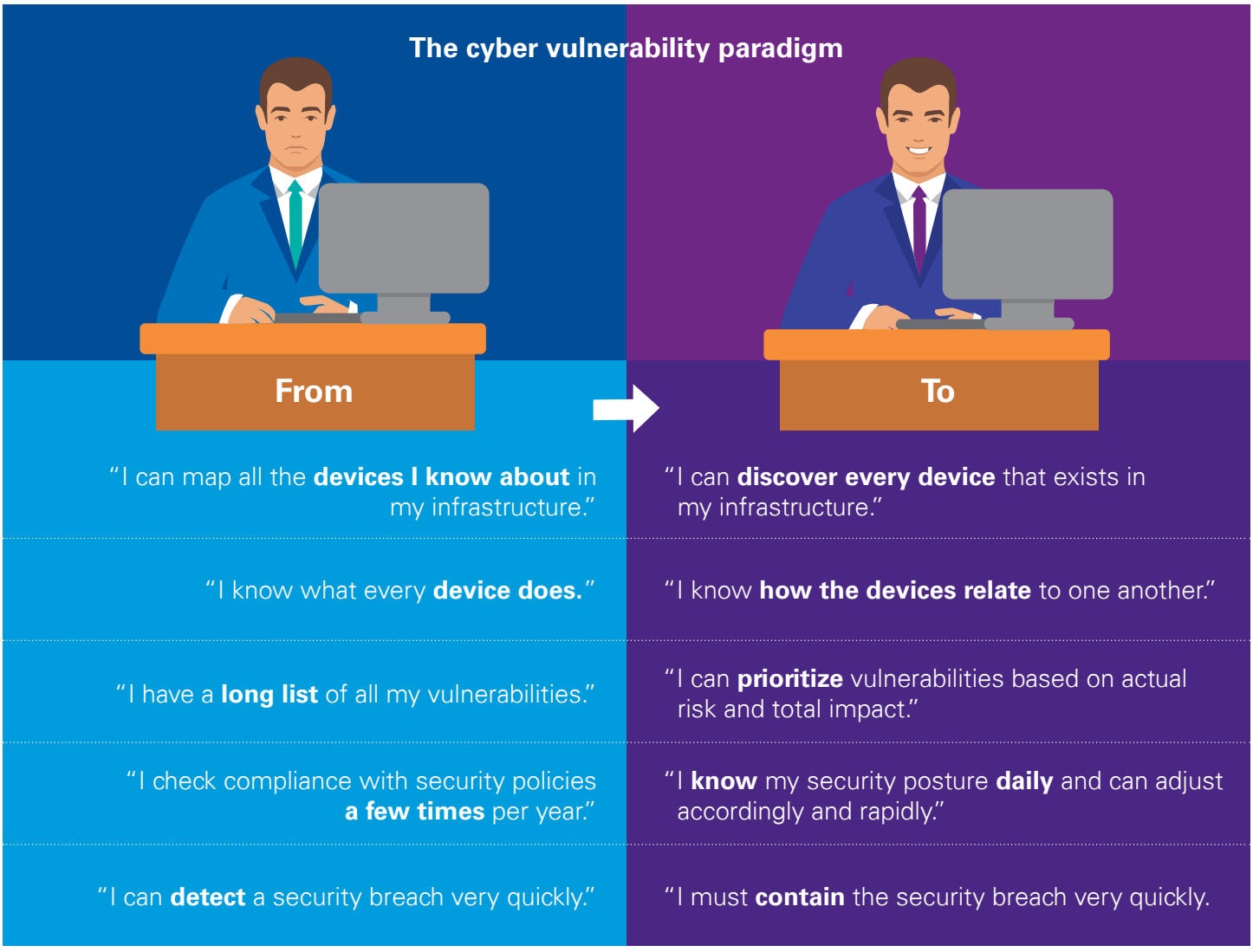
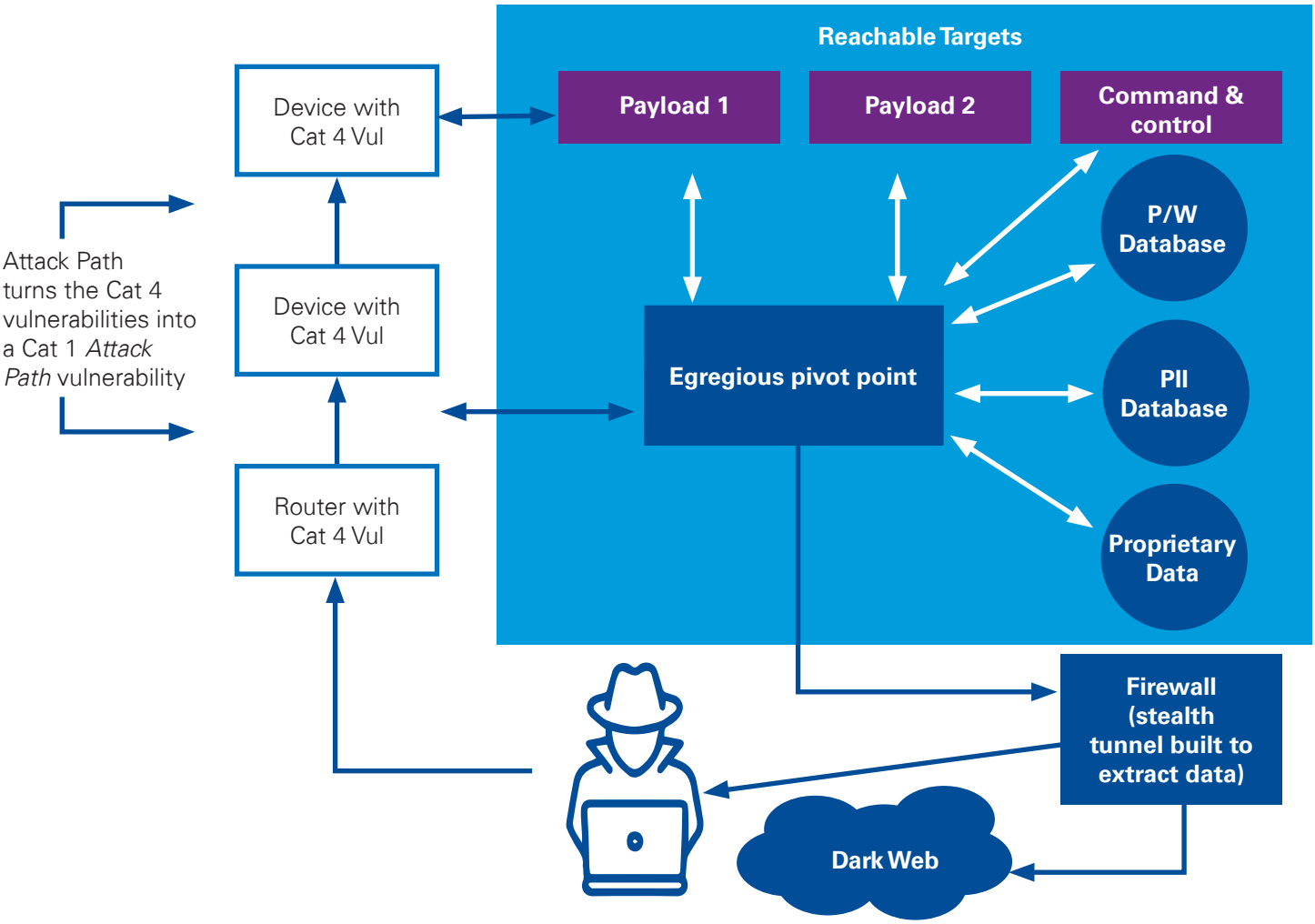


Figure 2: *Moving the cyber vulnerability paradigm delivers improved, actionable, and real-time cyber situational awareness.*

Critical for Real Time SA is understanding how every device relates to one another. Many times devices with Cat 3 & 4 vulnerabilities are not mitigated due to time, cost or other factors as the ATO focus is on remediating Cat 1 & 2 vulnerabilities. Adversaries seek the Cat 3 & 4 devices to build an attack path, and that attack path in-and-of-itself then becomes a Cat 1 vulnerability. (Figure X below). This is why it's imperative to instantaneously and automatically have attack path visualization, model access flow, identify egregious pivot points and reachable targets.



Phase 1, cont.

The next **Phase 1** element is *Intelligent Hunting*. The average "dwell" time during which threats are present before they are discovered is 101 days.[2] Intelligent Hunting is the art of deploying an advanced adversary pursuit methodology, using live memory analysis, that automatically identifies concealed threats residing in the uncontested conceded space. Why "uncontested"? The stealthy adversary knows these spaces are impervious to ordinary, traditional scanning tools—hence, uncontested. Intelligent Hunting complements SB by rapidly finding the hidden threats and, consequently, delivering an accurate, real-time, embedded threat situational-awareness picture.

[2] "EMEA Attack Dwell Time Hits 175 Days," Phil Muncaster, Info Security Magazine, April 4, 2018.

Phase 2

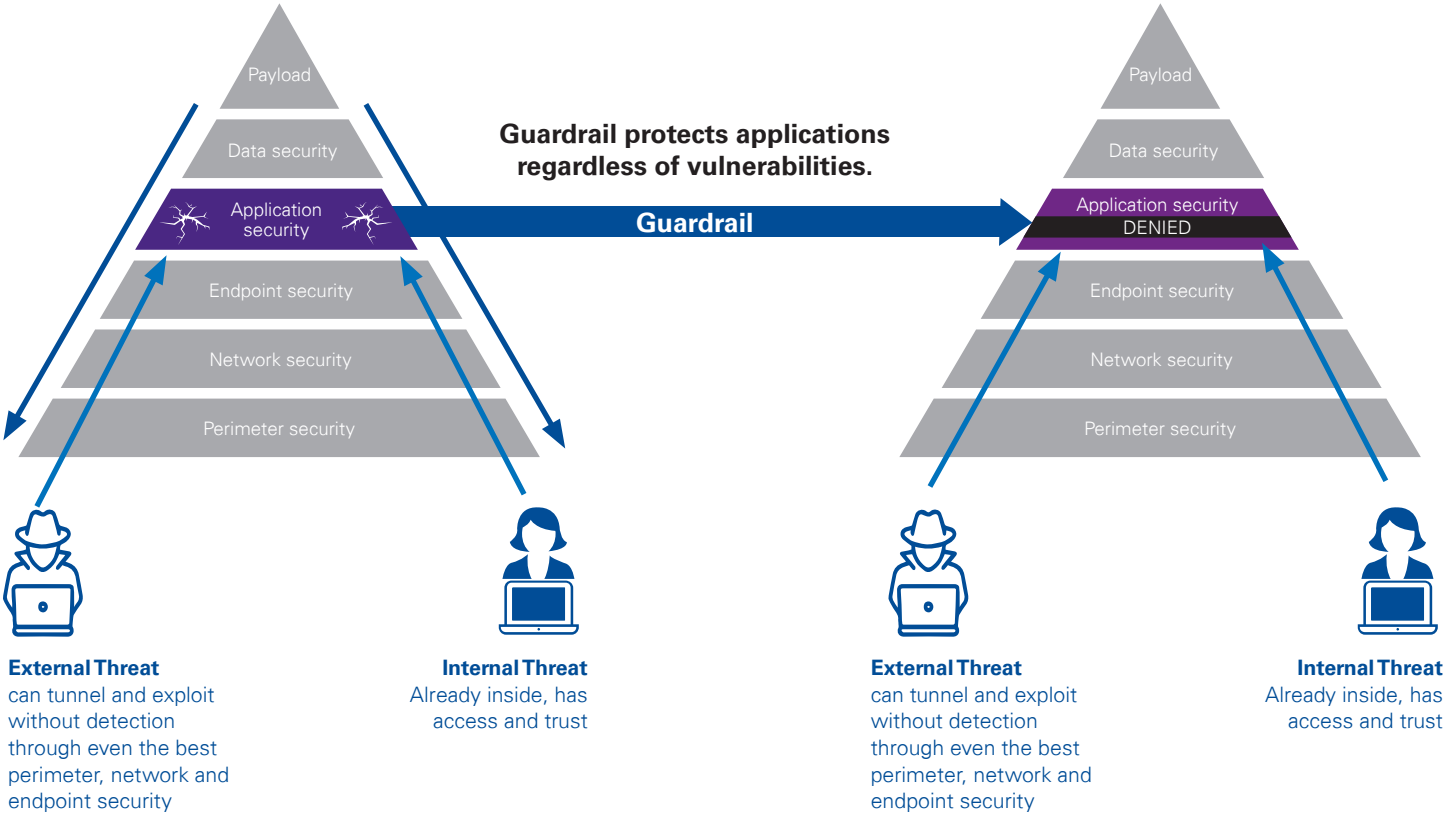


Figure 4: *Cracks in the application security layer present the most sought-after entry point.*

Phase 2 provides the ability to automatically protect the enterprise by combining automatic zero-day and unpatched applications protection with actionable predictive threat intelligence. Applications tend to be some of the most vulnerable, if not the most vulnerable, of all elements in an enterprise **(Figure 4)**. Cracks in the Defense in Depth (DiD) Application Layer present the most sought-after entry point.

[2] "EMEA Attack Dwell Time Hits 175 Days," Phil Muncaster, Info Security Magazine, April 4, 2018.

[3] Zero-Day attacks take advantage of the never-seen-before vulnerabilities that are found in-the-wild.

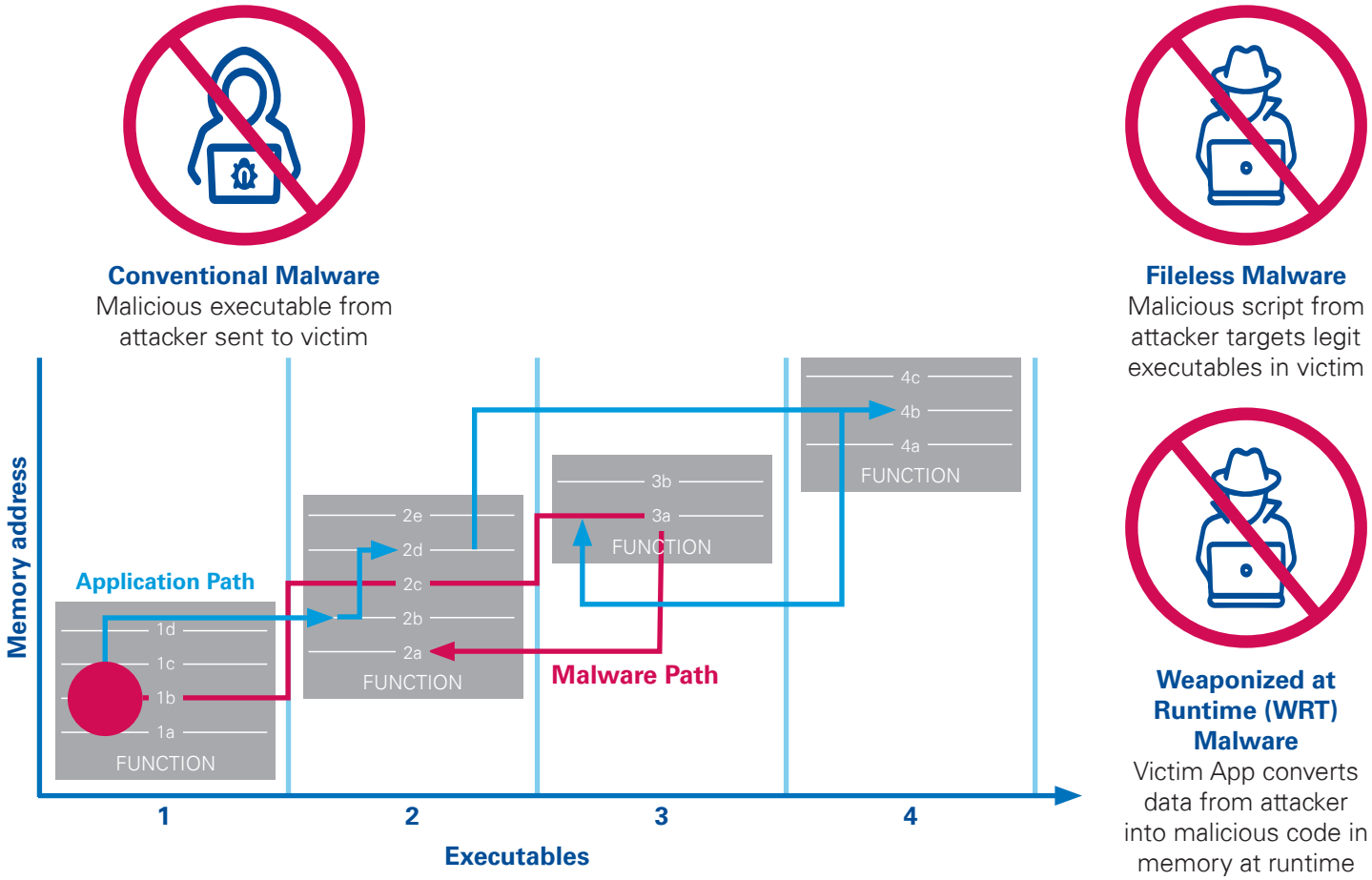


Figure 5: *Malware always maps to CPU memory differently compared to approved applications; Guardrail only allows acceptable applications to be processed; all malware, regardless of type, is immediately recognized, stopped and recorded.*

Phase 2 incorporates a "guardrail" methodology, which focuses on application code, not attacker techniques, to automatically protect the Enterprise **(Figure 5)**. This methodology secures the application stack through its full lifecycle, from disk-to-processes-to-CPU memory, with protection kicking in within milliseconds. Most importantly, guardrail binary code methodology detects attacks at the memory level and only enables developer's application code to execute, not the attacker's malware, so zero-day attacks are rendered impotent. Also, since attacker intent is stopped instantly, unpatched applications are now fully protected, which negates the risk of falling behind with the latest application patches/updates.

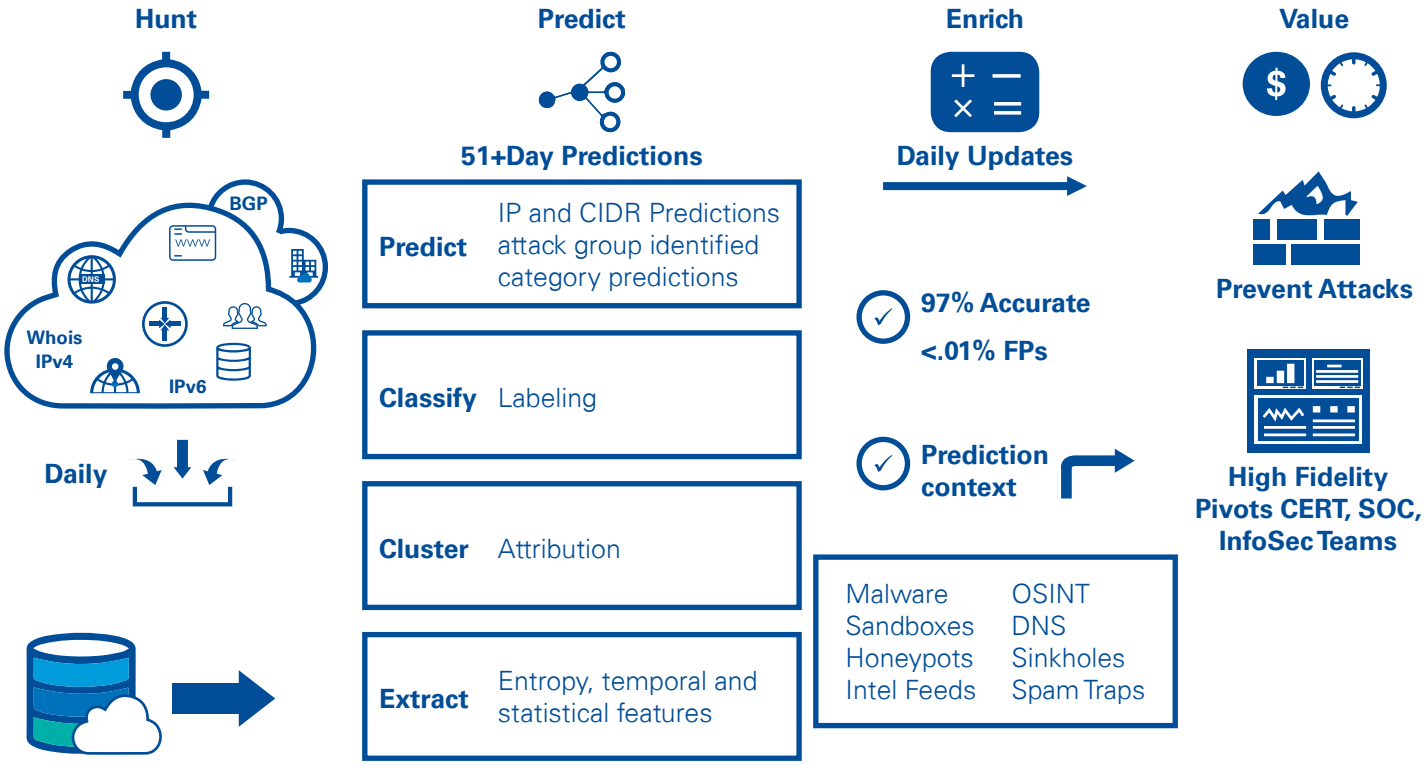
The guardrail methodology further protects applications and critical infrastructure from advanced fileless[4] and memory-based attacks that bypass conventional security, and it protects against WRT malware. This approach effectively detects and precisely addresses threats that attack at the memory level during runtime. It is not dependent on the policies, whitelisting, or rules and tuning requirements that characterize previous generations of protection.

[4] "What is a Fileless attack?", Maria Korolov, *CSO Magazine,* Oct 9, 2017, see https://bit.ly/2JPszR6

Phase 2, cont.

Phase 2 also exploits the "shadow infrastructure," which is the hidden infrastructure where adversaries stage and test their attack code before launch. The end result is Actionable Predictive Threat Intelligence (APTI)—a new, better early-warning system of threat intelligence **(Figure 6)**. This is accomplished by leveraging existing, deployed sensors and other "tools" that autodetect the buildup of cyberattack infrastructures during their creation and deliver a better "anticipated threat" picture. When combined with a predictive algorithm, the result is an APTI capability that enables cyber defenders to "get ahead" of threats that have yet to materialize.

Combining APTI with the guardrail methodology results in robust, automatic threat protection for an enterprise.



The prediction difference

— Prediction accuracy

- Classifier Accuracy: 97 percent
- False-Positive Rate: 0.007 percent

— Forward-deployed visibility

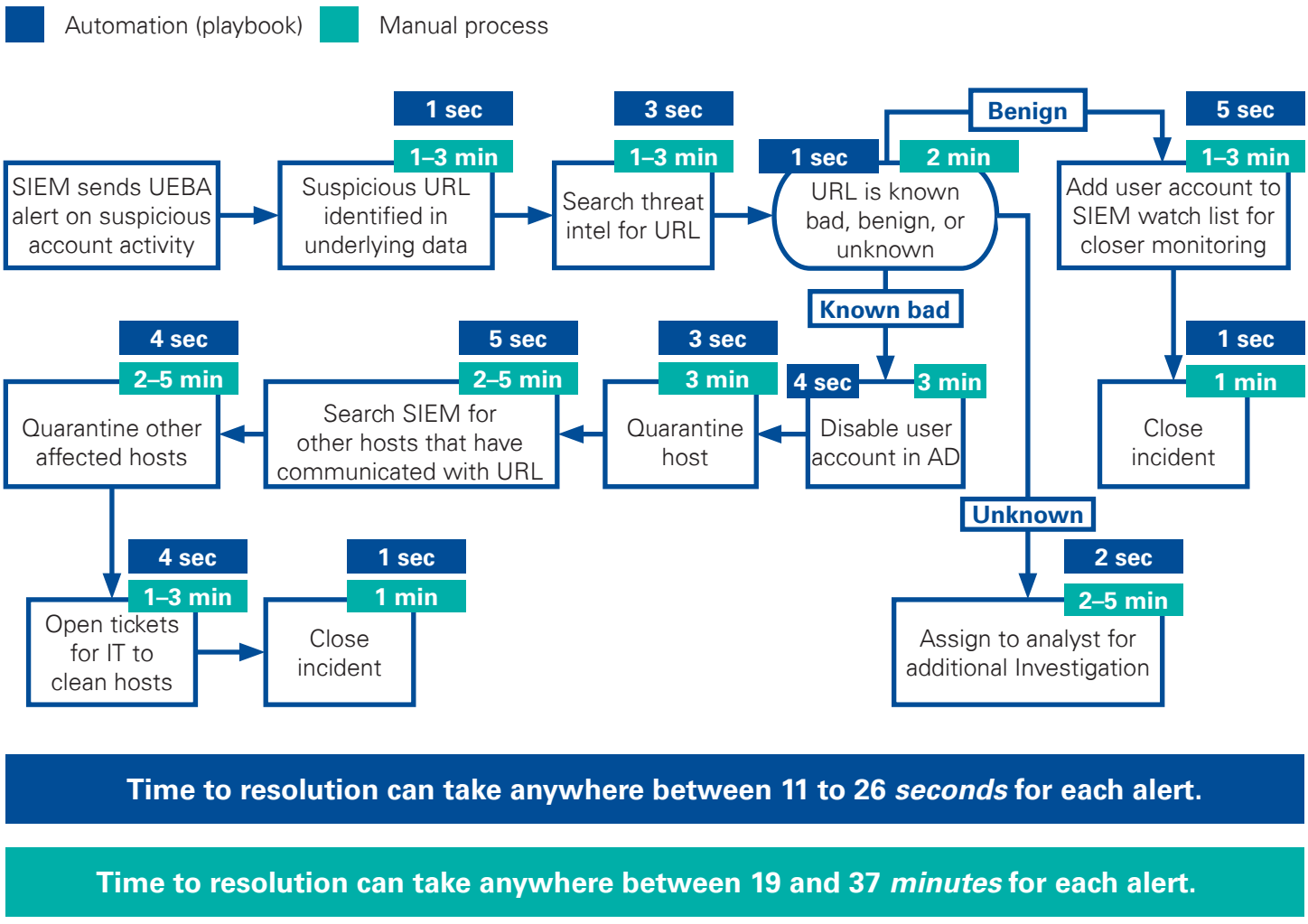
Fifty-one-day average prediction before attack launch

- Eight-to nine-week average for phishing, proxy, and botnet attacks
- Twelve-week average for malware, spam, and scanners

Phase 3

Phase 3 provides automated response and remediation by combining Security Orchestration, Automation, Response (SOAR) with capabilities that automate actionable information. SOAR combines processes and tools working in concert to automate otherwise disparate, tedious, time-consuming security tasks. SOAR quickly discerns the criticality and legitimacy of an alert, understands context and takes corresponding corrective actions, and initiates automatic remediation. SOAR's primary benefit is moving alert detection and remediation from *minutes/hours* to seconds, thereby significantly reducing cost per alert and increasing resilience **(Figure 7)**.

SOAR automation reduces alert resolution from minutes to seconds.



Time to resolution can take anywhere between 11 to 26 *seconds* for each alert.

Time to resolution can take anywhere between 19 and 37 *minutes* for each alert.

Figure 7: *Example of alert/remediation time reduction moving from manual process to SOAR automation*

Phase 3 also incorporates automating the extraction and correlation of actionable threat information. There is a mountain of excellent, actionable data available via commercial and government threat reports **(Figure 8)**. The challenge is trying to keep up with the sheer volume of reports—typically more than 5,800 per month, with 195 unique, unstructured formats identifying more than 9,500 threat indicators. In the face of this deluge, the tasks of manual data collection, analysis, and correlation are overwhelming, and many reports are missed. The solution is to implement automation to reduce time-consuming review tasks and orchestrate a process to establish a shared knowledge base that captures actions throughout the automated reports review process. The result is a shift from manual extraction and correlations of actionable information to automating the data extraction process, which enhances the effectiveness of human watch standers **(Figure 9)**.

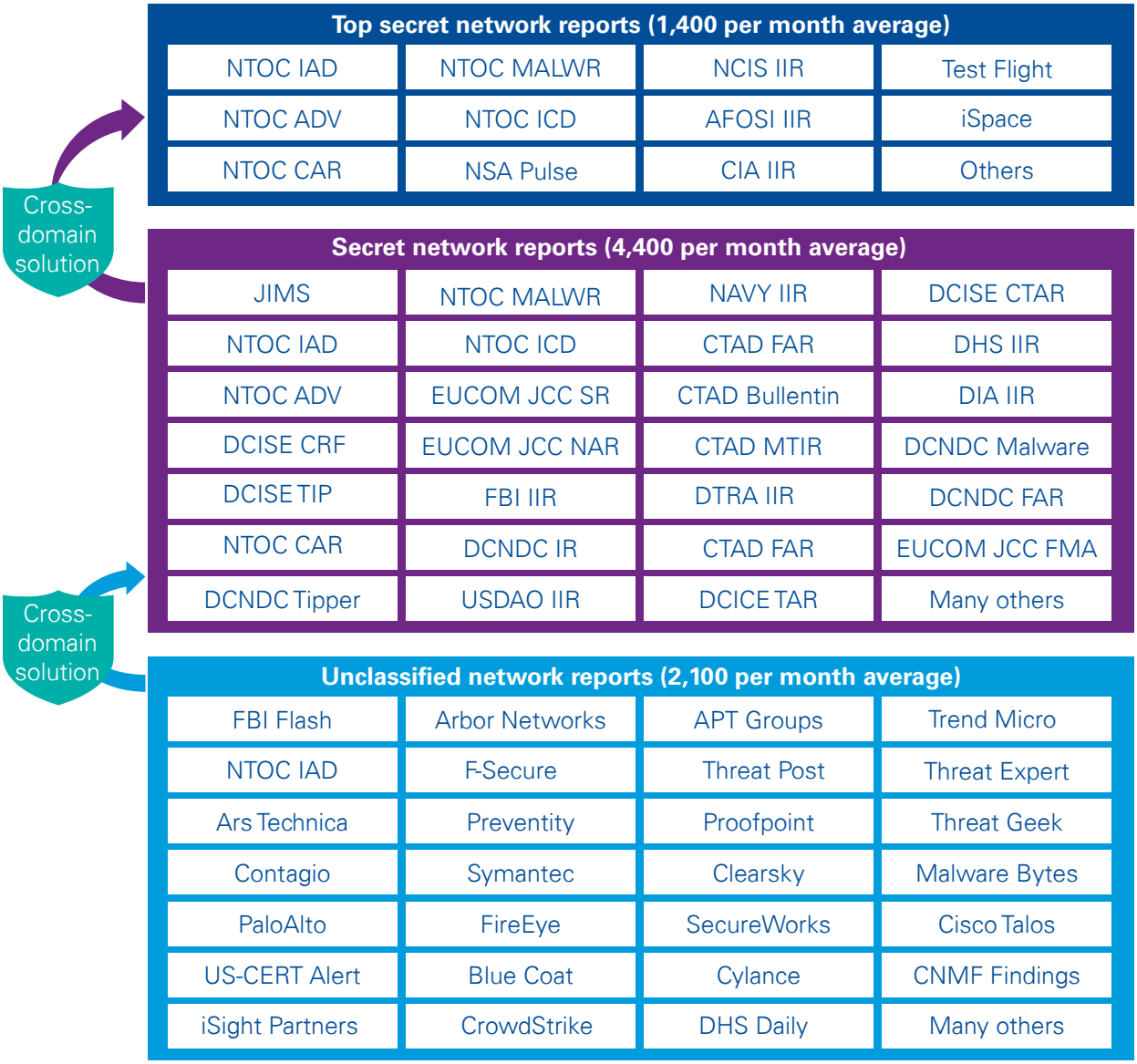


Figure 8: *Example of available cyber threat reports*

Phase 3, cont.

Attempts to manually understand and respond are ineffective

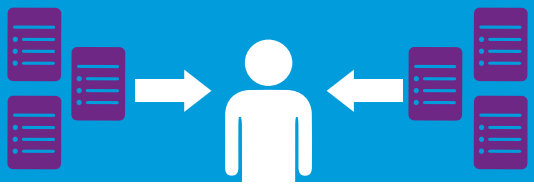
150 Different sources producing cyber intelligence

5800 Reports published every month

2000 + Sensors Tasked with rules and producing cyber alerts

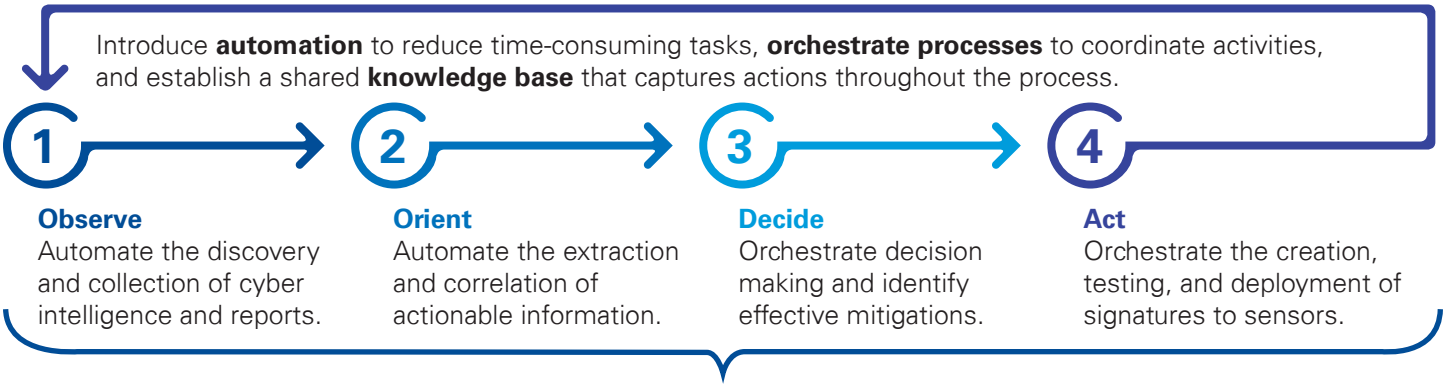
195 Unique formats of unstructured reports

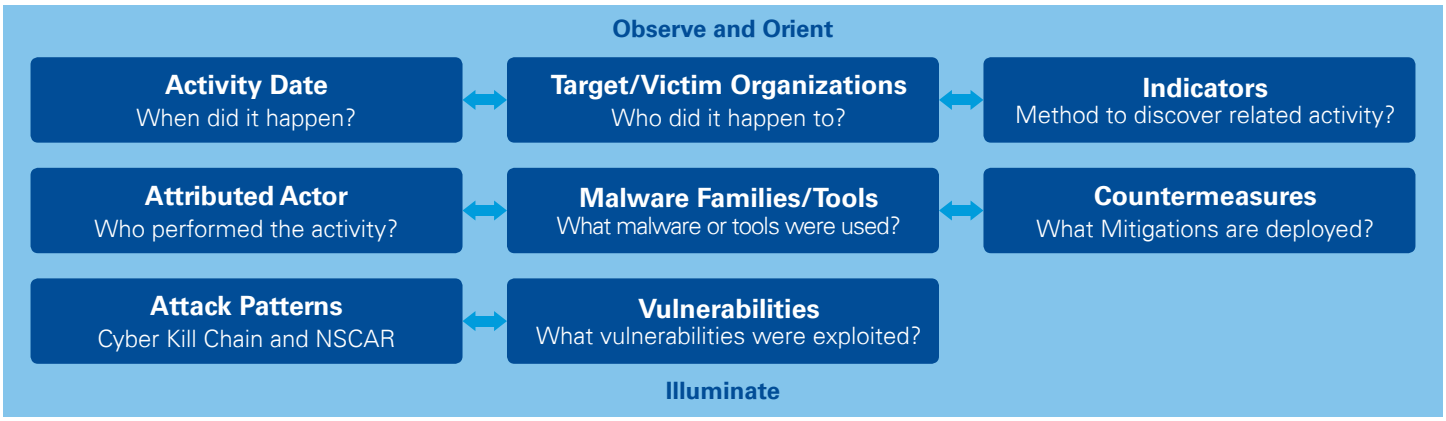
Majority of time spent **manually** Observing and Orienting

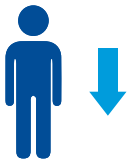


80% of analyst's time spend manually collecting, copying, and pasting

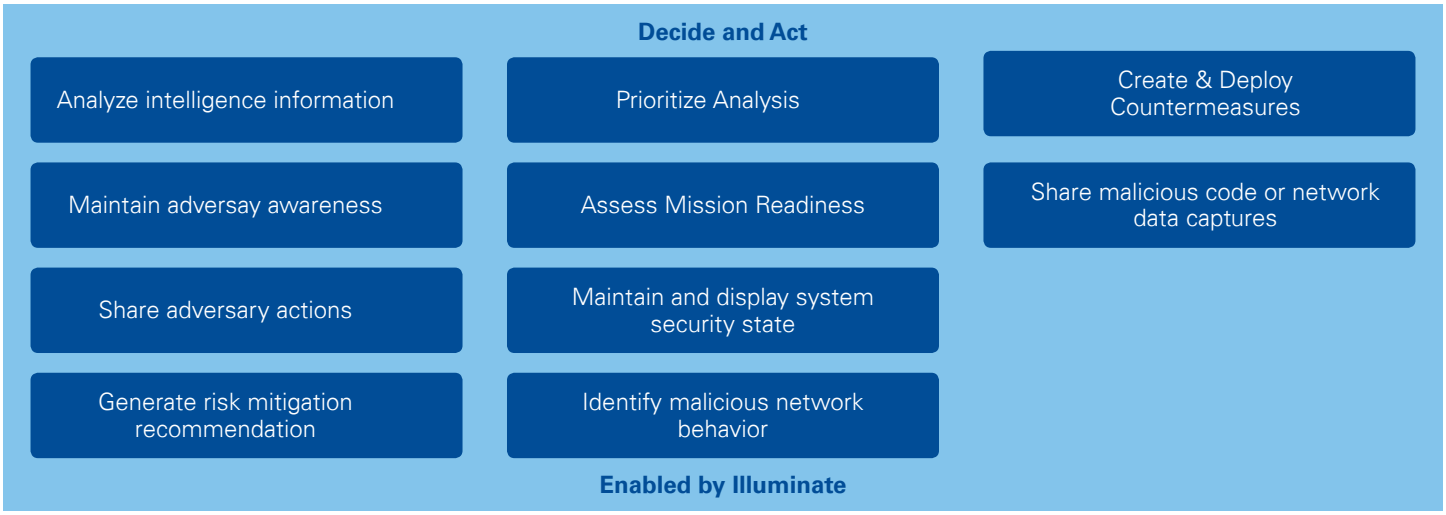
Limited time spent Deciding and Acting







Cyber Analysts now doing more productive DCO activities



Putting it all together— The KPMG advantage

The persistent onslaught of threats requires organizations move at the "speed of cyber," that is evolve from being reactive to proactive in their cyber defense. For this reason, KPMG developed the Prosilience Reference Architecture. Using the reference architecture, KPMG guides clients on how to achieve a prosilience foundation **(Figure 10)**. Key to prosilience deployment is addressing two distinct dimensions:

— Technology/Capability integration: Making the tools work together and in the context of an enterprise environment

— Operational integration: Adjusting and deploying operational procedures and training a cyber workforce to effectively operate the integrated prosilience capabilities

The KPMG Maturity Approach first performs an assessment to determine where the enterprise stands in relationship to the Prosilience Reference Architecture elements. Some of the assessment queries include the following:

— Does the current cyber awareness include real-time graphic depiction of how devices relate to one another? Does it address access flow? Does it visualize all possible attack paths while identifying the egregious pivot points?

— If hunting is deployed, does the organization incorporate an advanced adversary pursuit methodology?

— How are applications protected?

— How is the organization protected against zero-day attacks?

— What is the level of predictive threat intelligence currently in place?

— Is Security Orchestration, Automation, and Response deployed?

— How does the organization analyze and correlate threat reports?

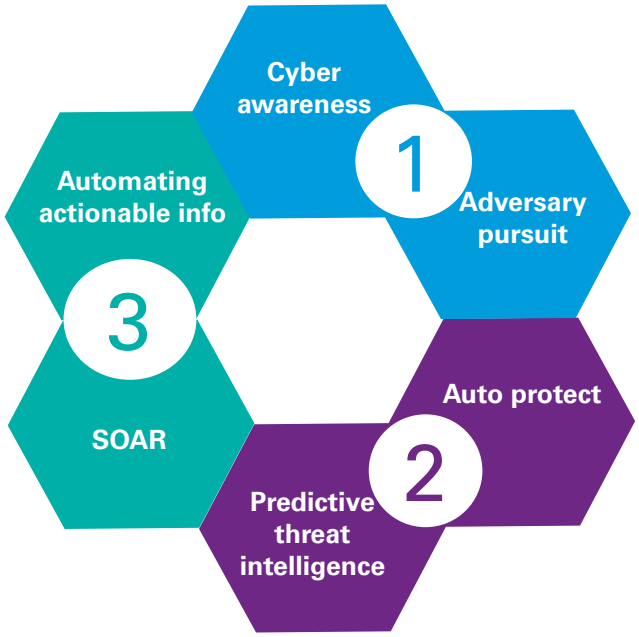


Figure 10: *KPMG Maturity Approach*

Upon assessment completion, we deliver our findings and a roadmap, including architecture and training/procedures recommendations needed to achieve a detailed prosilience foundation. We work closely with our clients to determine if there are existing elements that can be incorporated and/or "tweaked" to preserve existing capital investments whenever possible. We advise clients on the path toward achieving a capable cyber defense position within the constraints of operational requirements, federal regulations, budgets, and time.

The KPMG Advantage brings the experience to guide clients through integrating the six prosilience elements into a cohesive cyber architecture, in alignment with an organization's operational and technical needs, while aiming to minimize disruption. KPMG succeeds when its clients achieve optimal mission outcomes in the most secure manner possible.

About KPMG

KPMG has assisted federal, state, and local governments for more than 100 years. We possess the necessary knowledge, insight, and awareness of cybersecurity standards, legislation, and regulatory implications to address client needs. We help organizations transform their security functions into mission-enabling platforms so they can understand, prioritize, and manage cybersecurity risks; reduce uncertainty; increase agility; and convert risk into advantage.

Contact us

Tony Hubbard
KPMG Government Cyber Security Lead
T: 703-286-8320
E: thubbard@kpmg.com

L. Barry Lyons IV
Director, Government Cyber Security Services
T: 240-306-5555
E: leonardlyons@kpmg.com

kpmg.com/socialmedia