THE EVOLUTION OF CYBER THREAT HUNTING

MEASURING THE DIRECT AND INDIRECT BENEFITS OF HUNT

The term hunt has been largely accepted in the cybersecurity community, and we believe this particular definition is useful because it's durable: whatever your current state, and however your capability changes, it applies. The hunt mentality, hunt approach and hunt capability is something that everyone can use.

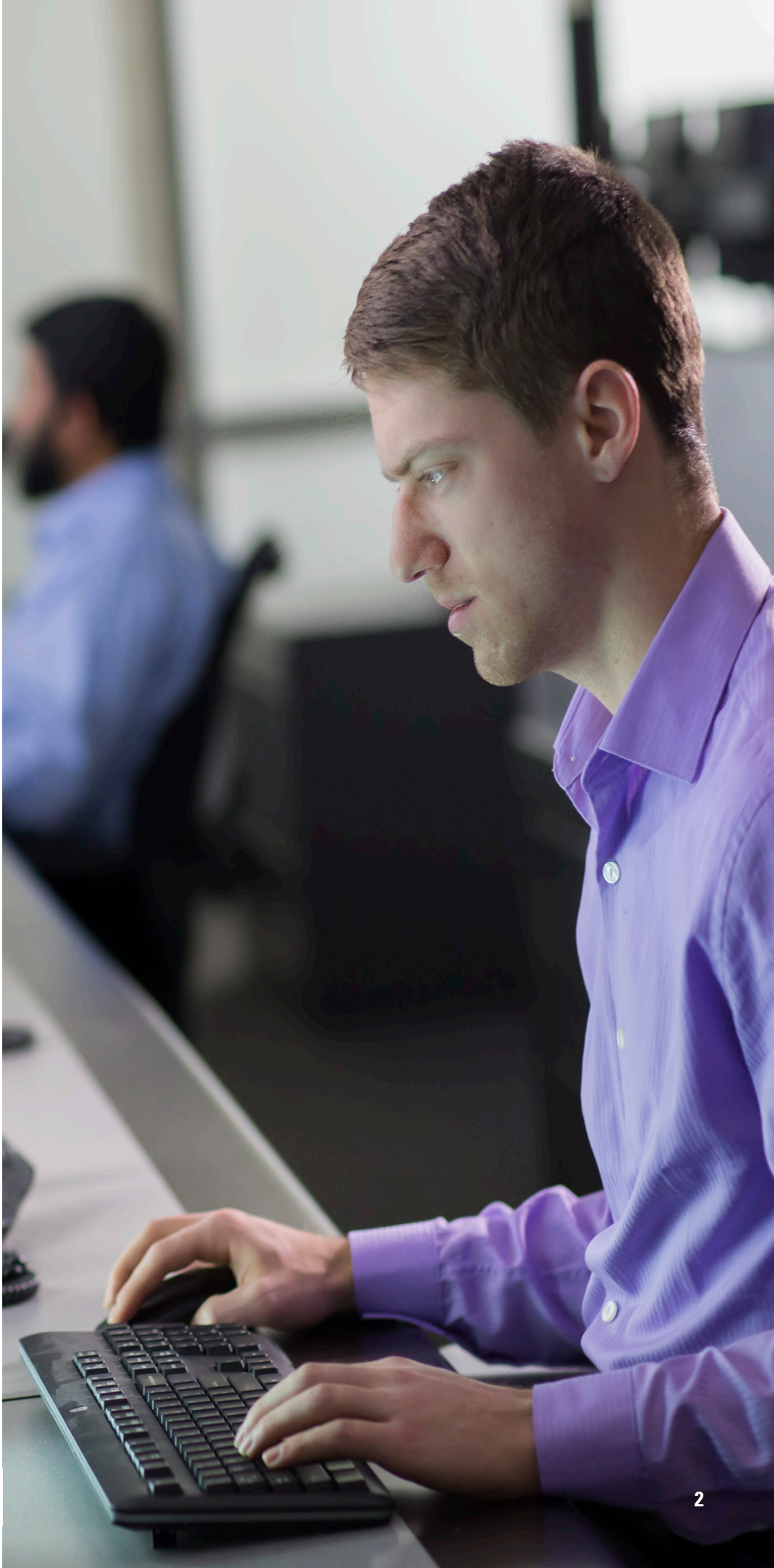
MOTOROLA SOLUTIONS

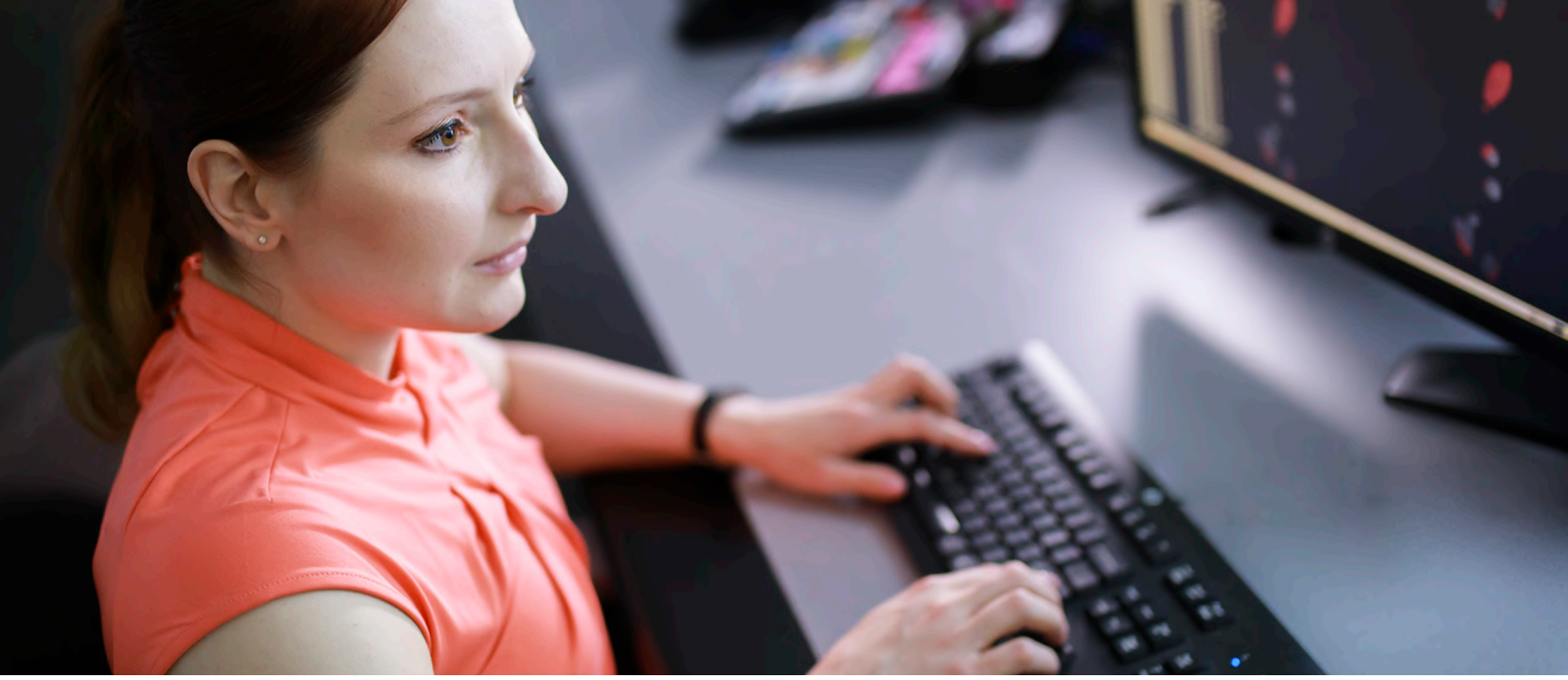
INTRODUCTION

Determined attackers get past even the best defenders. Given the current state of cybersecurity, preventing all attacks is simply impossible. Attacking is faster and cheaper than defending, and attackers only need to succeed once to cause significant damage. Meanwhile, perfect defense would require preventing a constant stream of diverse attacks every single time. A subset of attackers will likely go undetected, and the longer they stay that way, the greater the potential cost.

All is not lost, though. By acknowledging the uncomfortable truth that a compromise will happen, organizations can minimize the associated costs through cyber threat hunting. Hunting means focusing resources on detecting attackers who have managed to get inside your network and escape detection despite defensive measures you already have in place. Organizations that embrace and practice this concept can find attackers faster, which lowers remediation cost.

This concept also creates indirect benefits by building a cycle of continuous improvement for existing steady state security teams. Accepting this definition of cyber threat hunting puts an organization in the best position to begin advancing the maturity of their security operations, proactively mitigating attacks, and minimizing damage and cost.





THE DETECTION/RESPONSE SPECTRUM

Organizational capabilities to detect and respond to cyber threats can be loosely modeled as a spectrum, ranging from basic to advanced. Basic capabilities include built-in operating system and application features, user self-reporting and fundamental information technology (IT) response processes such as a helpdesk-driven approach. Security teams may choose to simply wipe and reload suspicious systems based on general anomalies. Technology at this end includes things like commodity anti-virus and host intrusion detection services.

As you move to the more advanced end of the spectrum, organizations tend to have larger security teams that include dedicated cybersecurity analysis and response personnel. Capabilities will expand to include purpose-built security technology and processes for analysis, tuning and response. Advanced teams typically exercise their capabilities periodically, evaluating their effectiveness, and often augment their sensor stack with aggregation, correlation and analytics.

Each individual organization has some steady-state security capability on this spectrum comprised of power users, IT staff, security operations centers and incident response teams. Organizations can conduct in-house studies to see where they fall on the detection/response spectrum, or they can hire security consulting experts to assist with this. For the purposes of this whitepaper, we'll use the basic description of the model.

Steady-state security's position on this spectrum can improve. However, improving detection and response maturity is notoriously difficult. These teams have limited resources and must meet requirements beyond detection and response, including risk management, updates and patching, regulatory compliance, training, controls implementation, departmental metrics and more.

> Red teams and pen testers can help organizations understand when they are no longer able to detect and respond to network intrusions.

For those teams seeking to determine their current state, it's important to start off by enlisting assessment teams to test their abilities. Red teams and pen testers can explore the cyber spectrum on a friendly basis, helping organizations understand when they are no longer able to detect and respond to network intrusions. Other ways to gauge steady-state effectiveness include using risk assessment frameworks or using exercise-based evaluations.

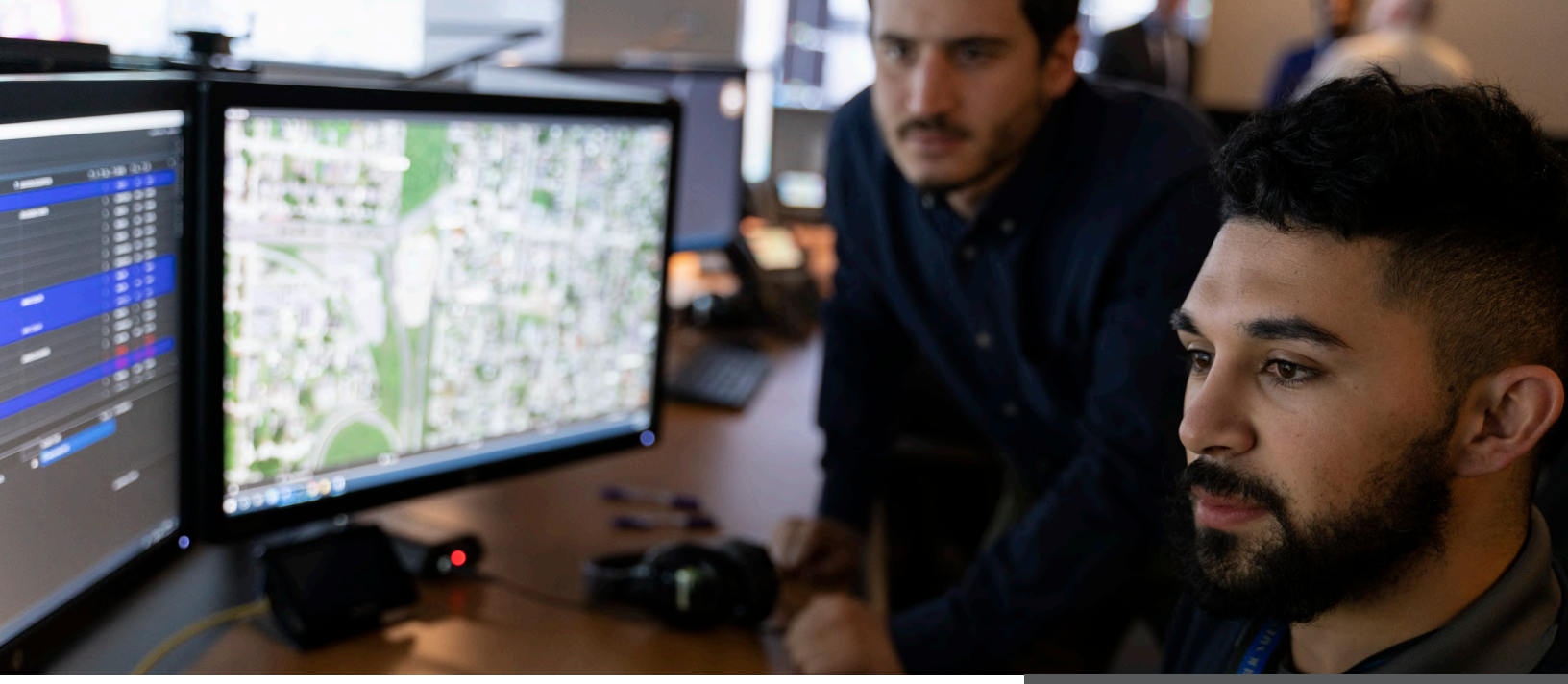
A CLOSER LOOK AT THE THREAT SPECTRUM AND ADVANCED ATTACKERS

There's a similar model that exists parallel to the detection and response spectrum, capturing a range of attackers from basic to advanced. Irrespective of where an organization's security lies on the detection and response spectrum, there are attackers and adversaries further along the threat spectrum. Less sophisticated attackers are caught by steady-state security. All one needs to do is turn on the news to see the frequency of cyber attacks to understand that you cannot prevent everything. The reality is that no matter how much you prepare, or how good your defenses are, there's always someone who's a step ahead.

This threat spectrum is dynamic and continues to advance at a rapid pace. Sophisticated attackers such as nation-states or well-funded researchers, and a vibrant community of offensive-minded cyber enthusiasts, continue to push the boundaries. Meanwhile, these advances become more well-known and accessible to less sophisticated attackers. Even the most novice attacker today has more capability than the sophisticated attackers of a decade ago.

Moreover, dwell time – the length of time that attackers have access to networks before detection and containment – is still shockingly long. According to a 2020 report on data breaches, malicious data breaches took the longest, an average of 315 days, to identify and contain. [1] If these threats have not been detected and responded to by steady-state security, they advance along the spectrum, inflicting damage in the way of lost data, downed systems and reputational harm.

However, just because attackers may have advanced past steady state security doesn't mean that they're so far ahead that they can't be caught. How "advanced" an attacker is must be judged relative to the sophistication and capabilities of their target. Through hunt practices, there is a chance to not only catch more threats but catch them faster.



DEFINING HUNT: FINDING ATTACKERS OTHERS MISSED

We define hunt simply and broadly: hunt is a capability – people, processes and technology – that is further along the detection/response spectrum than steady-state security. Hunt is designed to find attackers everyone else missed. This is a more focused capability, unencumbered by the other aspects of broader security.

Hunt teams can get in front of attackers who made it past that initial layer of detection. These teams are also tasked with implementing a hunt capability. They are typically smaller groups with a concentrated focus on detecting and responding to attackers who are more advanced than steady-state defenders.

These threat hunters adopt the assumed breach mentality: instead of fixating on whether a compromise has occurred, they are already plotting how to find the attackers.

The term hunt has been largely accepted in the cybersecurity community, and we believe this particular definition is useful because it's durable: whatever your current state, and however your capability changes, it applies. The hunt mentality, hunt approach and hunt capability are something that everyone can use.

This form of hunt can be implemented in a lot of different ways. For example, organizations can charter new internal teams, they can bring in an external hunt team, or they can tap into their existing security teams and empower them with part-time or full-time focus toward hunt tasks and responsibilities.

Pitching the value of hunt to stakeholders can be as clear and straight-forward as saying, "We need this capability that's further to the right of the detection and response spectrum, and we need these resources and this charter to implement hunt in a very precise way because it's going to result in concrete benefits for the business."

PEOPLE, ACHIEVING HUNT THROUGH PROCESS AND TECHNOLOGY

Besides being durable, this definition is useful because it's flexible: there are multiple ways to achieve it. Vendors have taken the popularity of the hunt term and used it to promote tools and technologies throughout the enterprise. By defining hunting holistically as a capability, rather than a device, though, organizations are empowered to get the most out of their existing tools (technology) by enhancing their processes and staff (people).

Depending on the state of an organization, a hunt team may be best served attending advanced training, hiring new experts, or improving their analysis and triage.

HOW HUNT RELATES TO SCOUT FORCE OR SKUNK WORKS

The hunt definition is also useful because it parallels time-tested concepts. It evokes the image of a scout force in front of the main body, detecting and responding to threats before the larger, slower force can bring their capability to bear. It also has similarities to advanced research teams like the famous Skunk Works – thinkers pushing the envelope of what was possible using new and existing technology to gain an edge on an ever-changing adversary[4].

WHAT HUNT ISN'T

It's important to distinguish hunt from other cybersecurity practices.

PEN TESTING, RED TEAMS AND VULNERABILITY ASSESSMENTS

Penetration tests, red teams and vulnerability assessments are designed to emulate attackers to assess controls and help train steady-state security teams. Hunt is strictly looking for actual attackers. These other tools can help determine positioning on the defense spectrum, and have their place in a security program, but they are quite distinct from hunt.

INCIDENT RESPONSE

Incident response (IR) teams are very closely related to hunt, though also distinct in that they focus on the investigation, containment and eradication of already-identified threats. IR is by definition reactive, whereas hunt is a proactive pursuit of an assumed threat. IR and hunt skills overlap significantly, so much so that many organizations use incident responders as hunters when they are not actively responding. IR may also be employed after hunters identify a threat.

HUNT BENEFITS

(DIRECT) SAVE MONEY BY FINDING ATTACKERS FASTER

The sooner attacks are discovered, the faster they can be mitigated, and the less damage done. Companies that embrace hunting can accrue financial benefits by reducing monetary losses resulting from cyber attacks. That type of damage can cost upwards of $3.8 million dollars on average. [2] Managing incidents is expensive and only gets worse the longer an attacker stays on a network undetected.

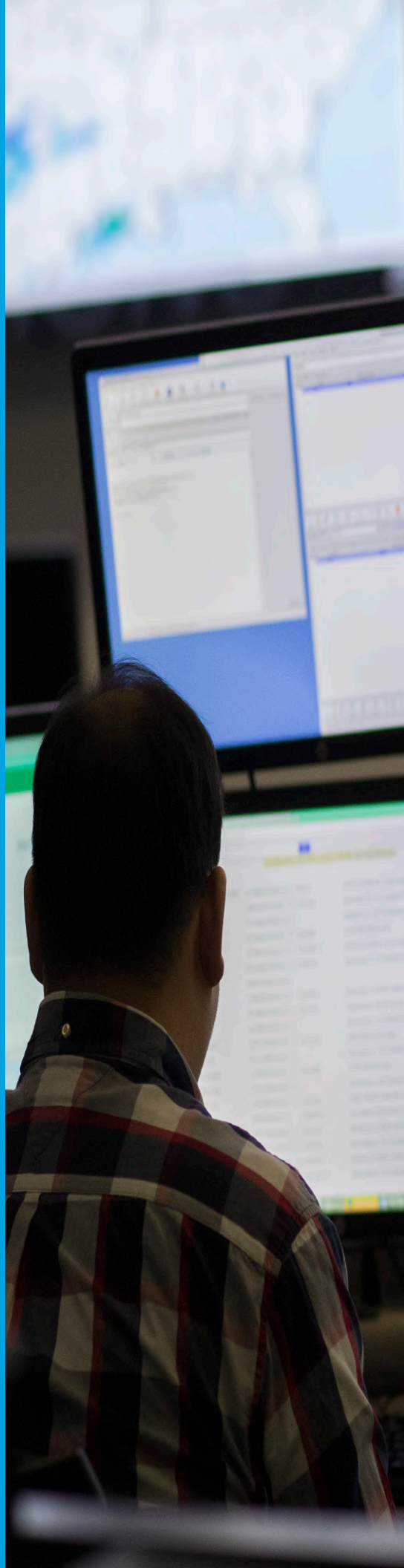
By catching more attackers and catching them faster, remediation costs can be reduced. Organizations with incident response teams and IR testing compared to those that did not have teams or testing in place saved an average of $2 million. [3] These direct benefits will also improve the business case to the board, non-security, or non-IT-related professionals.

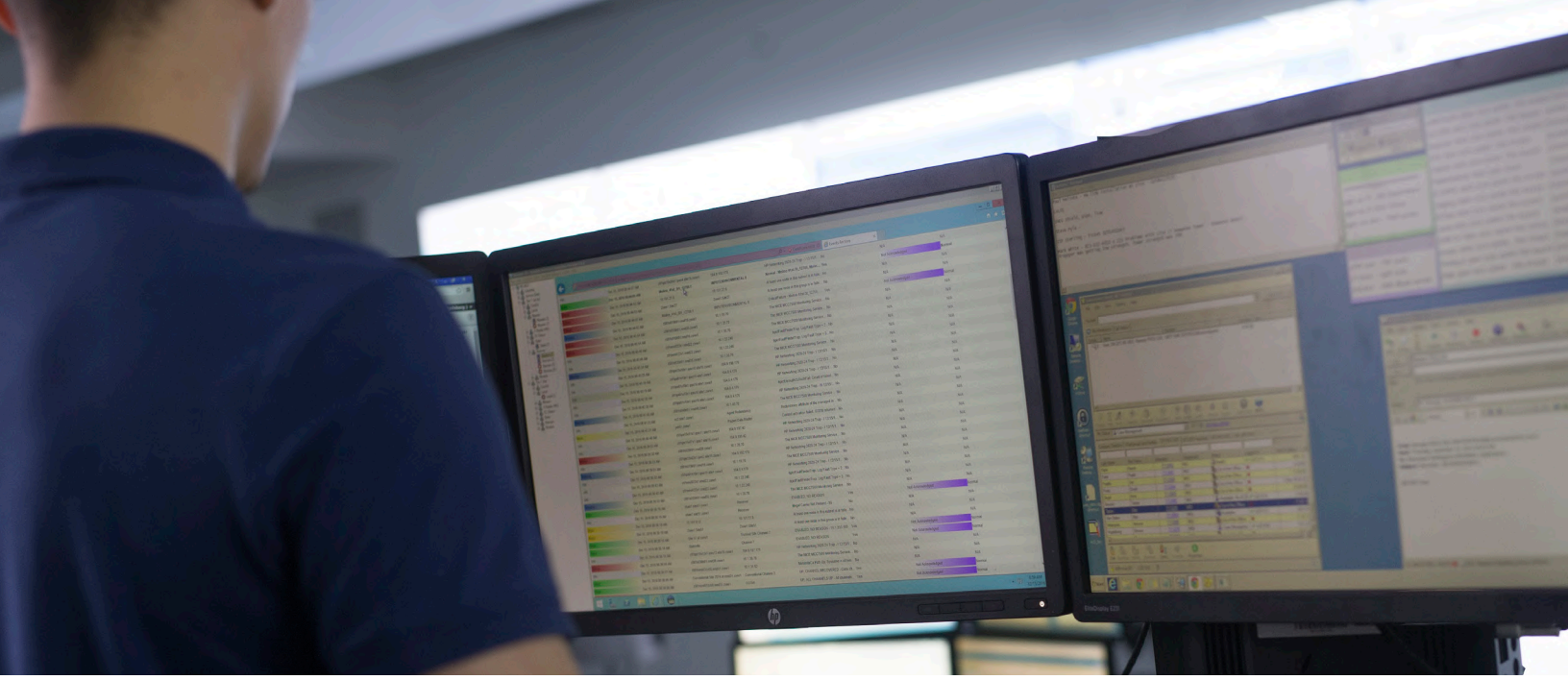
(INDIRECT) THE PHYSICS OF HUNT IMPROVE SKILLS

Beyond the direct effects, organizations also benefit indirectly. The biggest indirect benefit is that steady-state security typically improves in the presence of a hunt capability. In the same way that nation-state level research trickles down to less sophisticated attackers, hunt's advanced capabilities trickle down to steady-state security teams. Hunt's investments in things like newer technology and improved processes will eventually be adapted by steady-state security.

The existence of a hunt team bent on finding things that steady-state security missed creates healthy competition. This new tier also gives steady-state security analysts an increased path for professional development. Overall, the hunt capability can pioneer new or better training, people and staff.

As steady-state security teams get pulled along the detection and response spectrum, they also create this constructive pressure to push the hunt team forward. In turn, the hunt team must be ready to innovate because they don't want to be rendered irrelevant by these steady-state improvements. This physics of hunt (of hunt pulling steady-state along, who then push hunt forward) concept is the gift that keeps on giving. Ultimately, organizations can create this environment for continuous improvement by moving both hunt and steady-state capabilities further along on the spectrum.





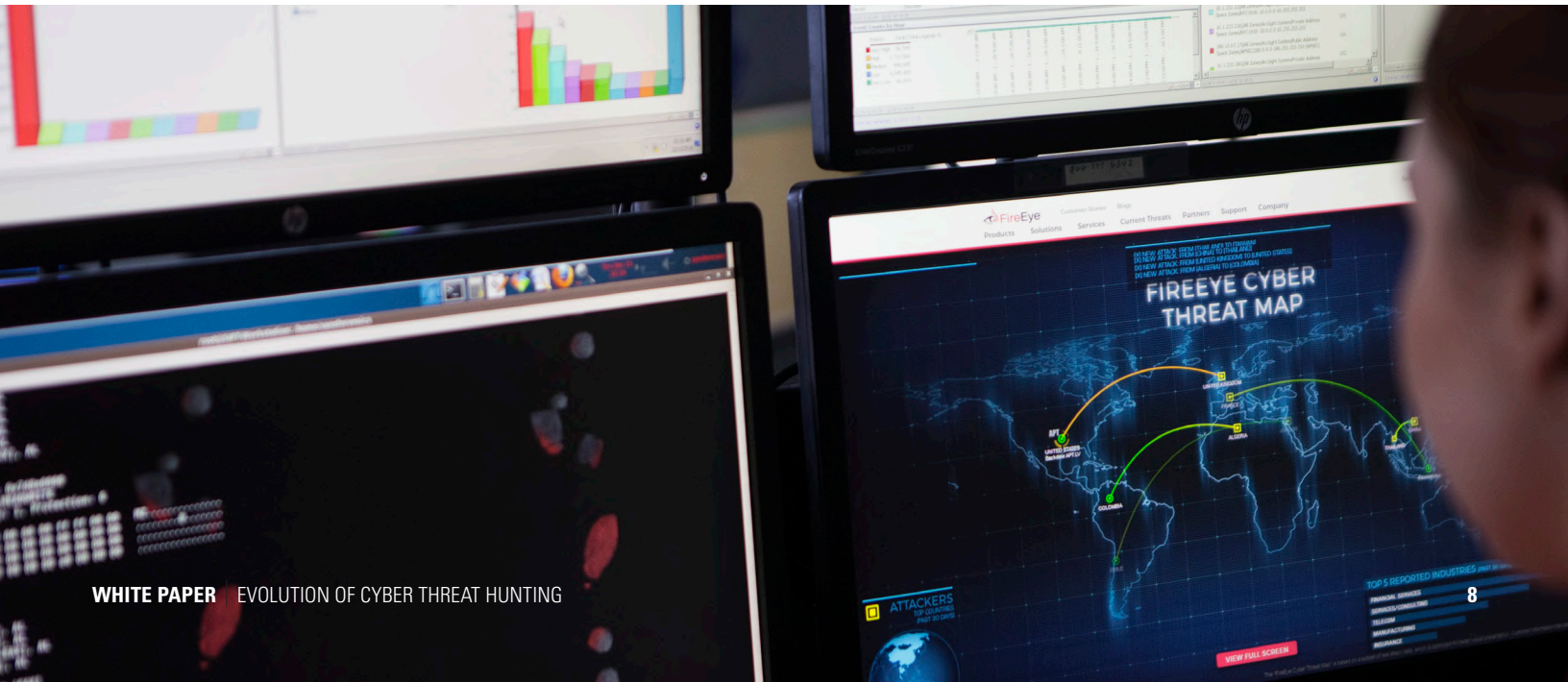
ANYONE CAN HUNT

Hunting is not just for organizations with mature security operations and big budgets. Anyone can embrace the concept of hunting to advance their security posture. All an organization needs to do is to start dedicating just a few more resources toward discovering active cyber attackers.

A smaller organization with little to no steady-state security can implement hunting using just the basics, such as dedicating someone part-time to threat detection if there is no one doing this now. Even outsourcing a specialized team for a hunt focused engagement can expose existing staff to new concepts, techniques and technologies. As long as these individuals are focused on detecting undiscovered threats, they can use relatively unsophisticated and fundamental techniques and still be considered to be hunting.

On the more advanced end with dedicated security staff and well-funded budgets, an organization can start the same way: commit time and resources to the hunt practice. Assemble a hunt team, give them the resources they need and hold them accountable to hunt centered metrics.

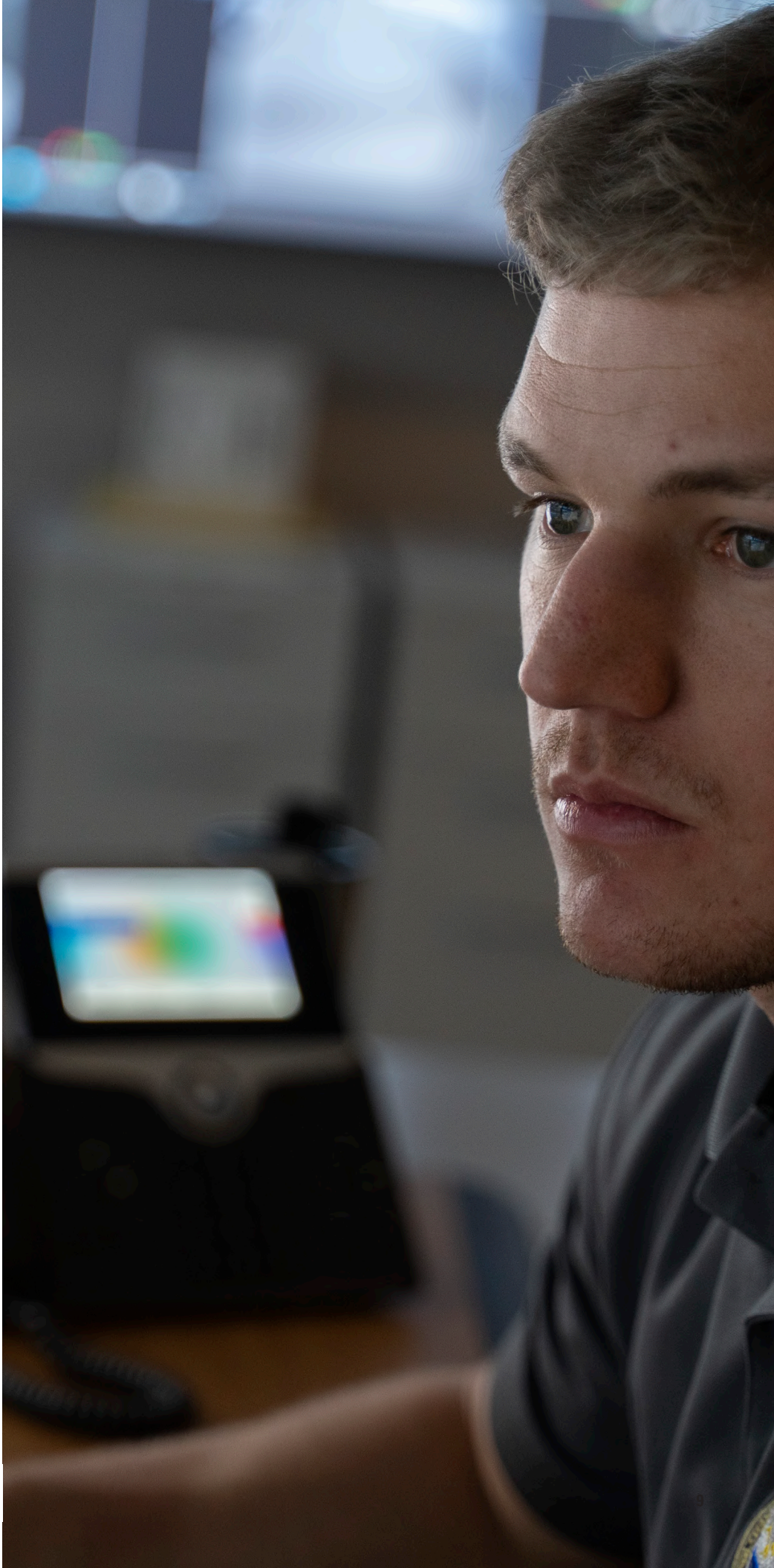
A truly committed organization could send people to advanced training, give them a dedicated budget and acquire more advanced analytics and forensics technologies. No matter the means, developing hunt-specific goals is fundamental to an advanced approach for threat detection. Metrics that are focused on compliance should be flipped to metrics that measure how many adversaries were caught.

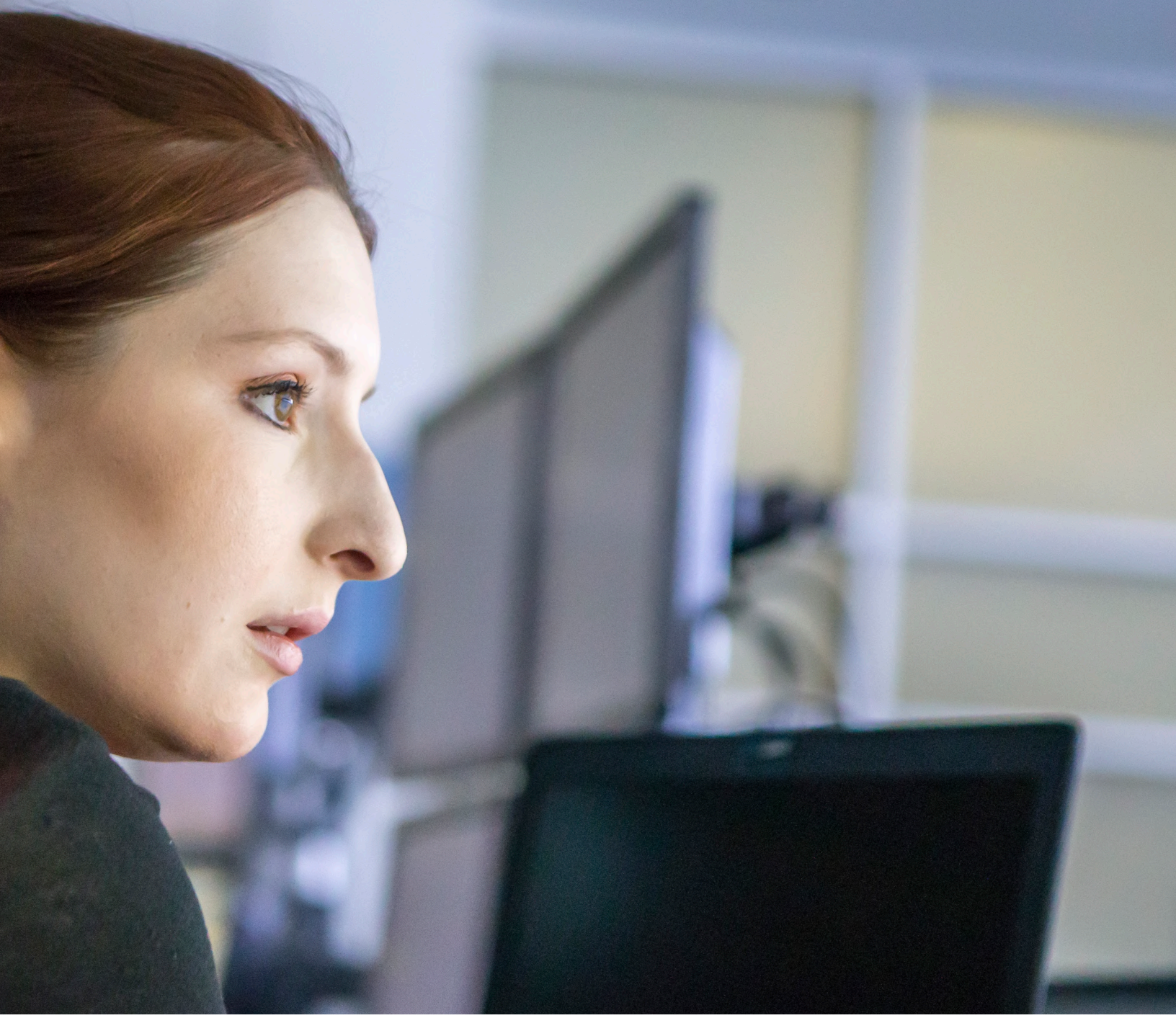


CONCLUSION

By adopting the durable, flexible and holistic definition of hunt as a capability to detect threats steady-state security teams missed, organizations gain real benefits. Hunt goes beyond having a special tool, taking a special course, or completing a checklist. When you redirect the focus to preparing people, processes and technology to catch adversaries that your steady-state security teams missed, the benefits will begin to surface. [5]

The concept of hunting is a powerful way to make the most out of existing resources to find more threats and find them sooner to reduce costs. The push-and-pull of continuous improvement encouraged by embracing hunt ensures that the security posture of an organization is always on the rise. Attackers are constantly improving; defenders need to start hunting to keep up.





ENDNOTES

1. 2020 Ponemon Cost of a Data Breach Study: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf
2. Ibid.
3. Ibid.
4. Definition of Skunk Works. https://en.wikipedia.org/wiki/Skunk_Works
5. Cyber Threat Hunting: Why This Active Strategy Gives Analysts an Edge. https://www.techrepublic.com/article/cyber-threat-hunting-why-this-active-strategy-gives-analysts-an-edge/

BRIDGE THE GAP TO A SECURE CLOUD

Whether you're migrating to the cloud or already there, Motorola Solutions can provide the expertise and solutions you need to keep your organization secure. Explore our other resources to learn more.

Motorola Solutions delivers cloud security, SOC-as-a-Service, managed security, and professional services to commercial and public sector clients. We provide the visibility and control needed for effective cloud, endpoint, and network security to bridge the gap to a modern security approach. ActiveEye℠, our proprietary platform, uses Security Orchestration Automation and Response (SOAR) to optimize and scale Managed Detection and Response (MDR) capabilities across the enterprise. Our US-based cybersecurity experts provide 24/7 monitoring, consulting, and guidance to our customers on their journey to a secure environment. Professional services include penetration testing, exercises and training, vulnerability assessments, threat hunting, and incident response.

Learn more at: motorolasolutions.com/cybersecurity

MOTOROLA SOLUTIONS