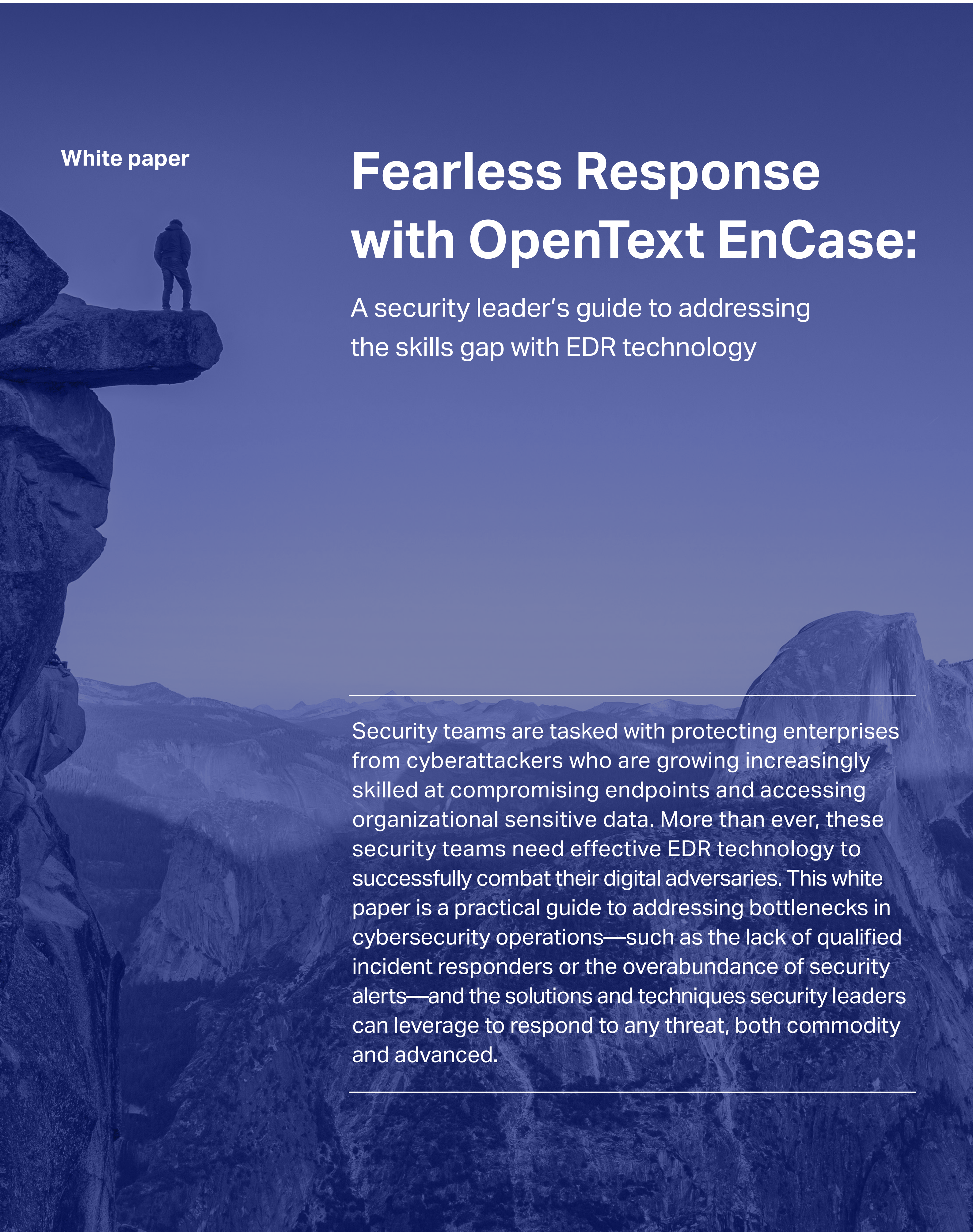
opentext™



White paper

Fearless Response with OpenText EnCase:

A security leader's guide to addressing the skills gap with EDR technology

Security teams are tasked with protecting enterprises from cyberattackers who are growing increasingly skilled at compromising endpoints and accessing organizational sensitive data. More than ever, these security teams need effective EDR technology to successfully combat their digital adversaries. This white paper is a practical guide to addressing bottlenecks in cybersecurity operations—such as the lack of qualified incident responders or the overabundance of security alerts—and the solutions and techniques security leaders can leverage to respond to any threat, both commodity and advanced.

Contents

56.8% of surveyed incident responders reported that the top impediment to effective IR at their organization was a **"shortage of staffing and skills"**

Executive summary

Modern digital adversaries have more access than ever to advanced tools, tactics and procedures. The result is an increase in effectiveness at compromising enterprise networks and stealing sensitive data. New research from the SANS Institute indicates that resource limitations are reaching critical mass, citing that a staggering **77.3 percent of security incident response (IR) teams are comprised of five members of less.**[1] With this reality, it is becoming clear that security leaders should expect *more* from their EDR technology in order to successfully combat digital adversaries, who benefit from scales that are already tipped heavily to their advantage.

Although attackers are increasingly skilled at compromising endpoints and infiltrating the machines that IR groups are tasked with protecting, **security teams can *confidently* and *comprehensively* respond** to any cyberthreat, both commodity and targeted attacks, with OpenText™ EnCase™.

Securing the modern enterprise requires doing more with less

Resource scarcity and long-term concerns for security leaders

A recent OpenText sponsored SANS Institute research report illustrates the impossible job of providing security to an organization with limited resources. Industry insiders and experts were polled on issues specific to SOC and IR teams, including notable successes, weaknesses and new patterns to consider, as well as a general inventory of incident response (IR) happenings. The result is a tremendously important and accurate look at today's cybersecurity climate.

56.8 percent of survey respondents reported that the top impediment to effective incident response at their organization was a shortage of staffing and skills.[2] This is a well-known and documented concern in the industry, but has failed to gain attention and, in turn, downstream capital, outside of the SOC.

Although related, the resource concern noted by the SANS Institute is a problem that has two separate drivers:

1. **Not enough people.** There is not enough human power in the enterprise security organization, often quantified by job vacancies and unfilled security roles.
2. **Not enough skilled people.** Often less-than-ideal resumes are considered for unfilled security roles, or security leaders are open to staffing their teams with more junior candidates

Cybersecurity Ventures predicts that **there will be an astounding 3.5 million cybersecurity job openings by 2021**[3], further supporting the lack of human power. In North America, one possible explanation is that accredited universities have only recently begun to offer degrees in cybersecurity-related fields. Most programs are nascent and promising, but currently not producing enough candidates to fill the available positions in cybersecurity across the globe. The result leaves security leaders with open positions that often go unfilled for weeks, months or even years.

Continuing to cause an impediment to effective IR, the lack of fully-qualified candidates has led to a lack of skills. Security leaders are adjusting hiring practices to be more inclusive of less-qualified or junior security personnel. This means teams are a more "junior" and less technical demographic than in years past, leaving a gap in expected contribution from team members that security leaders are expected to adjust to and overcome. It is interesting to note that a lack of qualified IR personnel has led to an increase in partnerships with trusted third-party security consulting services as a short-term solution to staffing concerns.

Endpoint detection and response technology can and should be relied upon to contribute to more of the security workload when considering the lack of qualified IR personnel at present. By prioritizing and "boiling up" the most relevant and critical security information first and automating manual and repetitive tasks, security leaders can begin to tip the scales back towards balance in the fight against modern digital adversaries.

Also, indicative of the scarcity of resources in the SOC, 48.2 percent of survey respondents in the same incident response survey conducted by the SANS Institute reported that the lack of budget for tools and technology was a primary impediment to effective IR at their organization.[4] With a generous Information Security team being a mere 10 percent or less of the overall IT budget, which is a fraction of the overall enterprise budget, CISO's are frequently the last-in-line when it comes to acquiring resources that enable their cause.[5]

And yet, the Information Security group is ultimately responsible for *defensively protecting* organizational intellectual property, sensitive customer and employee data, managing compliance and, where applicable, the demands of regulators. The group must also avoid a headline breach that would result in the loss of consumer trust, fines and potentially irreparable brand damage. Budgets should skew towards becoming more substantive and needed resources should be made more available given the tangible revenue implications tied to the charter of a security leader. Because security teams are revenue-defending and fight to avoid losses and theft rather than generate net-new revenue for the enterprise, the push will always be an uphill battle.

How to improve the odds of increasing InfoSec resources

- ✓ Security leaders should work to improve the "soft skills" in business that lead to more conversations that educate stakeholders from adjacent areas of the enterprise
- ✓ Track KPIs and metrics that the board will understand and value
- ✓ Accurately and realistically portray risks to senior management
- ✓ Have a plan for how to efficiently leverage resources that come to the InfoSec team on day one

Resource scarcity and real-world impacts

The 2013 Target breach still serves as a reminder that the issues security groups dealt with in 2013 still exist and with potentially significant impact today. A careful study of the bad luck of organizations from the past can help shore up defenses for a more secured future, ensuring organizations know what to focus on and where to direct attention.

If left unaddressed, a compromise will continue to grow and fester in IT networks until it eventually escalates into a data breach. If sensitive data is stolen, brand trust is compromised, regulatory penalties are inbound and organizations must begin a lengthy and difficult recovery process.

Target breach details

- Attackers accessed the Target network via a third-party vendor with an initial phishing email.
- Malware was used to compromise log in credentials.
- Alerting technology correctly identified suspicious activity of hackers.
- Due to the "vast numbers of technical events", the alert was missed by the InfoSec team.[6]
- The compromise continued unaddressed and grew into a data breach, impacting approximately 70 million individuals.[7]

Every compromise should be addressed, and any effort to get ahead of resource and staffing concerns will likely pay immediate and long-term dividends for security leaders in today's climate. The unfortunate reality is that compromise is an everyday occurrence that is troubleshooted in the SOC. Compromise does not necessarily equate to an instant or acute data breach but, if left undiscovered, could certainly escalate into that scenario.

The great news is that technology exists to address these problems and help alleviate the looming sense of concern and anxiety related to security event visibility and validation.

The role of EDR technology in addressing the skills gap

While effective against legacy vulnerabilities, protective perimeter security technologies are not a guarantee of total threat prevention. Prevention technologies are dependent on history and context for success. Legacy vulnerabilities from the past still exist, and prevention technologies that monitor known and legacy threats are an important layer in a successful security strategy.

When it comes to present cybercrime, advanced and targeted attacks are the primary means of inflicting damage. Advanced and targeted attacks often leverage campaign-style tactics, with extensive reconnaissance, multiple breach tactics, command and control with compromised credentials, privilege escalation and, eventually, data exfiltration. In other words, prevention technologies exist to address legacy vulnerabilities and are less effective against net-new, zero day, advanced and targeted attacks.

Savvy security leaders address zero-day threats, APT malware, theft by a privileged insider and nation-state sponsored attacks with endpoint detection and response (EDR) technology. EDR is the last line of defense for an organization against digital theft and focuses on uncovering and remediating a benign compromise before it escalates into a more intrusive data breach.

There is not enough time in the day or human power available for security teams to comfortably manage the workload ***without*** **the assistance of EDR technology.**

Threat detection and the need for continuous endpoint visibility

While the focus of this white paper is on Fearless Response, there is one simple truth to remember—organizations cannot respond to a threat that was not first detected. Security teams must see everything, even if it means dealing with the byproduct of managing too many security alerts. Security leaders cannot risk missing the proverbial "needle in a haystack" threat that becomes a more serious security issue.

Additional industry research by the Verizon Risk Team in the annual Data Breach Investigations Report indicated that 56 percent of eventual breaches take weeks or even months to develop and go undiscovered by InfoSec teams.[8] Any effort to reduce the mean-time-to-detection (awareness of the security vulnerability) and the mean-time-to-response (restoring trust to a previously compromised host) will pay dividends for security leaders in finding more success.

Threat detection with OpenText EnCase

- ✓ Policy-based rules for detection of advanced and targeted attacks
- ✓ Behavioral "triggers" that indicate endpoint compromise
- ✓ Custom anomaly detection builder
- ✓ Corral detections and events from other sources and EnCase as a single pane of glass for response with SIEM, IPS, IDS and network alerting technologies

Security leaders should err on the side of caution and aim for 100 percent visibility and detection of threats. While this may not be totally achievable at present as a guiding principle and methodology, it will surface more events and detections that require response, any of which could be a disaster if left unaddressed. Once a security team has maximum visibility and is detecting as close to 100 percent of potential threats as possible, ***there will be too many alerts.*** This is a necessary byproduct of visibility, but still an issue that needs attention because it creates an exorbitant amount of security events.

The average SOC receives 10,000 security alerts per day, 80 percent of which are false positives.[9] Many larger enterprises and organizations are reporting numbers that are much higher, with 27 percent of IT teams dealing more than a million threats per day.[10] On average, IR teams are comprised of 2-5 members, and with those data points in mind, the math does not add up.[11] There simply is not enough time in the day or human power available for security teams to comfortably manage the workload ***without*** **the assistance of EDR technology.**

Fearless Response with OpenText EnCase Endpoint Security

With OpenText™ EnCase™ Endpoint Security, both experienced and junior IR teams are enabled to confidently and comprehensively respond to any threat, including legacy vulnerabilities, targeted external attacks and insider threats.

Avoid manual wipe and reimage with surgical, over-the-wire remediation

The success IR teams are having against cyberattacks is real and tangible, and surprisingly being accomplished with a heavy reliance on manual processes for remediation. 53 percent of organizations are continuing to "reimage or restore compromised machines from a gold baseline" as a preferred remediation method.[12]

An over-reliance on manual processes leads to lengthy response times and growing, not shrinking, queues of security alerts that require IR attention and insight, ultimately creating disruption to the business and processes. For example, manual remediation involving wipe and reimage almost always requires physical possession of the device, formatting the hard drive and re-installing a profile with files and systems access. Adherence to this process or a remediation workflow that is similar is not scalable or suggested for enterprise security needs.

Advantages of remote, network-enabled response capabilities with OpenText EnCase

- ✓ Global access to any endpoint connected to the network
- ✓ Surgical remediation—only interact with the affected systems and information
- ✓ Avoid endpoint downtime or lengthy business disruption due to compromised systems
- ✓ Asynchronous monitoring of non-traditional employees with intermittent connectivity to the corporate network
- ✓ Quarantine compromised endpoints to reduce lateral spread
- ✓ Determine incident scope and identify similarly compromised endpoints
- ✓ Kill malicious processes and delete the corrupted files that spawn them
- ✓ Reset impacted registry keys which enable advanced threats to survive a reboot in memory

Simplified for confident use by Tier I security analysts

With the lack of qualified IR personnel readily available to fill open positions in the SOC, security leaders can bring the breadth, depth and access of EnCase to the less-technical staff on their team. EnCase enables junior security analysts to have an immediate and palpable impact on security operations, especially relative to event triage and Tier I response.

EnCase offers security-first workflows and an intuitive UI that was purpose-built for immediate contribution and impact by junior security analysts. Tier I analysts can take guided and non-permanent actions that disrupt the effect and lateral spread of malware until Tier II/Tier III resources are available for more advanced investigation and response.

For example, take an Advanced Persistent Threat (APT) that is detected on the corporate network. That detection is packaged as a security event and flagged as needing more analysis. A Tier I analyst can quickly verify the alert, understand why that alert is malicious or suspicious, quickly act to isolate the endpoint and send this detection up the internal chain for further review by a Tier II or Tier III responder.

Amplify the abilities of expert power-users with suggested workflows and builders for junior personnel

We have covered that there are fewer experts available to assist CISOs in today's fight against cyber-attackers, and that **savvy security leaders are shifting their focus to maximize the contributions of their valuable experts.**

IR power-users can supplement EnCase's out-of-the-box threat detection rules with additional custom anomaly rules for maximum threat detection. The detection needs of security teams differ wildly by industry, organizational type, common attack vectors and innumerable other variables. The ability to deploy custom detection rules will cast a wider and more targeted net for better visibility into potential vulnerabilities. One-size-fits-all security panaceas seldom work as advertised, and the ability to customize detection after deployment is a key component of success.

EnCase easily integrates with adjacent security technologies for maximum operational efficiency, including:

- SIEM
- IPS
- IDS
- Threat intelligence sources
- Dynamic analysis/ sandboxing
- Security orchestration
- Commonly used OSTs
- + Open and RESTful API with documented SDK for on-demand integrations

These additional and targeted anomaly rules create new events and detections that get routed to Tier I analyst queues for high-level triage and simple response.

Easily integrate with adjacent security technologies for maximum operational efficiency

Defense-in-depth (DiD) is a standard practice and widespread methodology for securing an enterprise. It often "takes a village" and different security technologies to achieve enterprise protection and digital safety. Security leaders tend to leverage a variety of security solutions to meet their needs. With many layers of endpoint, network, data analytics, intelligence and response solutions overlapping each other for the desired 100 percent coverage.

This preference by security leaders means that security technology vendors should work well with adjacent security technologies, share information easily between tools and provide easy access between the separate UIs with minimal cumbersome operations.

EnCase easily integrates with a wide variety of adjacent security technologies. Where there is not integration pre-built out of the box, the EnCase RESTful API and Software Development Kit can be used for on-demand and less traditional integrations.

This makes it possible to automate as much as makes sense in the SOC. Mission-critical tasks still require manual review and analysis by a human incident responder, as too much automation can kill good tasks and cause more disruption.

Automation through integrations makes the whole worth more than the sum of its parts as the technology works together effectively and streamlines security operations.

Prioritize alert response with embedded threat intelligence and context

Security event volumes are worrisomely high, and every event requires triage and review to successfully mitigate a security issue. Approximately 80 percent of events are false positives, but security leaders must err on the side of caution.[13] This need for caution creates the unwanted but necessary byproduct of too many security events for incident response teams to analyze and address.

With EnCase, security teams can rapidly prioritize response based on threat criticality. With file reputation analysis and dynamic analysis into all security alerts with accompanying threat scores, incident responders have the context that is needed to successfully evaluate and prioritize valid threats, while dramatically reducing the number of false positives that require 1:1 investigation. Security teams can quickly address serious and high-priority alerts first, with the higher threat scores indicating strong supporting evidence for verified malicious or suspicious activity. From there, Tier I analysts can work backwards and steadily address threats that are less critical until eventually the only remaining alerts are false positives.

Fully assess advanced and targeted attacks with a comprehensive DFIR/Tier III feature-set

To be truly successful as a security group, InfoSec teams should prioritize the ability to uncover and remediate advanced and targeted attacks. Advanced nation-state sponsored cyberattacks often closely resemble the tactics used by privileged insiders that abscond with the sensitive data they were entrusted with, meaning that a focus on Digital Forensic Incident Response (DFIR)-style investigations is one of the only proven methods for detection and response. Bad actors will compromise users and fraudulently use credentials and privileges to eventually access the sensitive data.

In addition to identity and access management protocols, Tier III investigative solutions are one of the only proven methods for uncovering, fully assessing and remediating advanced and targeted attacks.

Respond fearlessly and recover forensically with OpenText™ | EnCase™ Endpoint Security

Questions?

opentext.com/security encase@opentext.com

OpenText offers the gold standard in digital investigations and is a winner of the 2019 SC Magazine "Best Computer Forensic Solution" award for the tenth year running. Examiners can investigate everywhere with unrivaled support for devices, operating systems, cloud sources and encryption technologies, ensuring that evidence is never out of reach in a critical investigation. OpenText provides the leading threat detection and incident response solutions on the market that enable quick detection and remediation of compromised endpoints by efficiently and forensically returning them to a trusted state with comprehensive and surgical remediation.

As the most widely supported forensic solution available to address the most demanding modern investigation needs, teams can rely on OpenText.

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: opentext.com.

Connect with us:

- OpenText CEO Mark Barrenechea's blog
- Twitter | LinkedIn

Sources

[1] SANS, *SANS 2019 Incident Response (IR) Survey: It's Time for a Change*, July 31, 2019.

[2] Ibid.

[3] Cybercrime Magazine, *Cybersecurity Jobs Report 2018-2021*, May 31, 2017.

[4] SANS, *SANS 2019 Incident Response (IR) Survey: It's Time for a Change*, July 31, 2019.

[5] Ibid.

[6] New York Times, *Target Missed Signs of a Data Breach*, March 13, 2014.

[7] Ibid.

[8] Verizon, *2019 Data Breach Investigations Report.*

[9] DarkReading, *Security Analysts Are Only Human*, February 21, 2019.

[10] Imperva, Survey: 27 Percent of IT professionals receive more than 1 million security alerts daily, May 28, 2018.

[11] SANS, *SANS 2019 Incident Response (IR) Survey: It's Time for a Change*, July 31, 2019.

[12] Ibid.

[13] DarkReading, *Security Analysts Are Only Human*, February 21, 2019.

opentext.com/contact