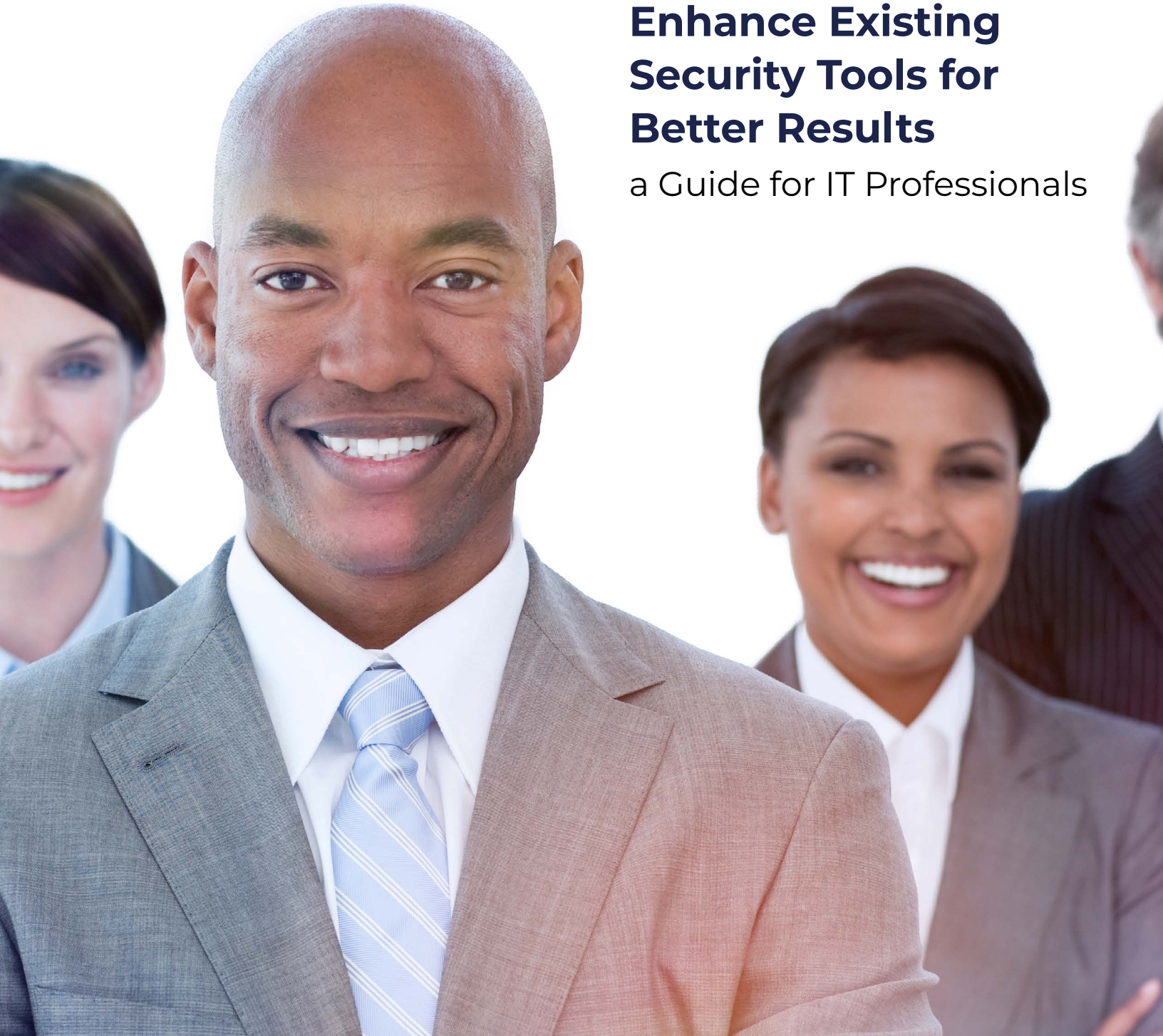
CISO GLOBAL

A **CISO GLOBAL** WHITE PAPER

XDR

Enhance Existing Security Tools for Better Results

a Guide for IT Professionals



Growing Security Demands and Restricted Resources

With IT resources already stretched, how do you address ever increasing security demands from your leadership, board, end users, and constantly evolving attack types?

You probably don't have enough internal team members to keep eyes on all the diverse security feeds generated by your IT estate, but endpoints, networks, firewalls, cloud architectures, the Dark Web, DNS records and more must all be kept under constant review.

This guide summarizes various challenges you face in your role as a technologist that are addressed by XDR, and how it enables you to deliver the security your organization needs, within your available resources, without ripping and replacing the solutions you already have.

Challenges, Capabilities, Benefits

The Challenge	XDR Capability	The Difference
Slow Time to Remediate (TTR) and restricted visibility of complete attack strategies.	Retaining logs and monitoring your entire environment, XDR correlates and analyzes telemetry for improved visibility of all events and their interactions. Custom playbooks automate common remediation tasks.	Improved visibility and understanding, and vastly accelerated TTR, including against layered attacks. XDR typically responds in just minutes.
Tech portal overload and siloed security information.	See all your security events and how they relate to one another, in one place and one format.	Improved understanding of security events and accelerated decision-making, without data incongruence or portal overload.
Inability to monitor your entire IT estate all the time, resulting in limited visibility into attacks, or failure to completely remove attackers from the network.	All alert types, including those from cloud platforms, are triaged in the CISO Global SOC and passed to expert analysts for further action.	Reduced dwell time and improved visibility with accelerated understanding of, and response to, events across your environment.
Inability to monitor the Dark Web for your organization's information.	Continuous Dark Web monitoring for your company's information, with remediation support if it's detected.	Assurance that if any corporate information has been exfiltrated and posted to the Dark Web, you will know about it ASAP.
Active Directory is notoriously difficult to monitor, but AD attacks can lead to disastrous account takeovers and privilege escalation, making it a favorite target for attackers.	Any suspicious AD activity is flagged to an expert analyst in the CISO Global SOC, 24/7/365.	Early identification and response to AD attacks, denying this attack vector to attackers seeking an easy way in.
Weakening of firewalls, as rule exceptions accumulate and some alerts are switched off.	Automatic firewall log analysis raises alerts for any suspicious activity.	Improved firewall effectiveness and RoI. Prompt detection of and response to firewall-related security events.

The Challenge	XDR Capability	The Difference
Lack of resource to monitor domain registrations that could be used to spoof your website.	Retaining logs and monitoring your entire environment, XDR correlates and analyzes telemetry for improved visibility of all events and their interactions. Custom playbooks automate common remediation tasks.	Improved visibility and understanding, and vastly accelerated TTR, including against layered attacks. XDR typically responds in just minutes.
No resource to watch for unauthorized DNS configuration changes.	See all your security events and how they relate to one another, in one place and one format.	Improved understanding of security events and accelerated decision-making, without data incongruence or portal overload.
Inability to detect anomalous behaviors potentially indicating a covert attack.	All alert types, including those from cloud platforms, are triaged in the CISO Global SOC and passed to expert analysts for further action.	Reduced dwell time and improved visibility with accelerated understanding of, and response to, events across your environment.
Lack of resource to keep logs correlated and under ongoing review, risking missing new attack types.	Continuous Dark Web monitoring for your company's information, with remediation support if it's detected.	Assurance that if any corporate information has been exfiltrated and posted to the Dark Web, you will know about it ASAP.
Lack of clarity on what devices are connected to your network.	Any suspicious AD activity is flagged to an expert analyst in the CISO Global SOC, 24/7/365.	Early identification and response to AD attacks, denying this attack vector to attackers seeking an easy way in.
Bad actors' increasing focus on covert attacks.	Automatic firewall log analysis raises alerts for any suspicious activity.	Improved firewall effectiveness and RoI. Prompt detection of and response to firewall-related security events.
Lack of expertise and resource to ensure rapid triage, response and remediation.	Lack of expertise and resource to ensure rapid triage, response and remediation.	Attacks are essentially reversed, protecting operational uptime and restoring order on all protected endpoints, almost as if they never happened.

Next Steps

XDR does all this without additional in-house resource. Through automation, it will also free you of routine security monitoring, releasing time in your team for more valuable work.

Discover the difference XDR can make for you, your organization and your team: call us today at 866-430-2595 or email sales@ciso.inc.

CISO GLOBAL

CISO Global is an industry leader as a global cybersecurity and compliance provider. We are rapidly expanding by assembling whole teams of world-class cybersecurity, secured managed services, and compliance experts who utilize the latest technology to create innovative solutions. CISO solutions protect the most demanding businesses and government organizations, mitigating continuing and emerging security threats and compliance obligations.

AICPA SOC
aicpa.org/soc4so
SOC 2® Type II Audited