deepwatch

7 Questions to Ask Your MSSP

You've hired your Managed Security Services Provider (MSSP) to secure your perimeter. But are you getting the value you deserve from your investment? Do you have a true partnership with your provider or are you simply getting alerts thrown your way with little or no context?

FIND OUT IF YOU ARE GETTING YOUR MONEY'S WORTH FROM YOUR MSSP INVESTMENT. WHEN IT COMES TO SECURITY ALERT MANAGEMENT AND EMERGING SECURITY RISKS, ASK YOURSELF THESE SEVEN QUESTIONS TO GET ANSWERS.

Question 1

How does my current MSSP strengthen my ability to detect and respond to actual security incidents?

WHY IT MATTERS

Threat dwell time increases the cost of a breach. In 2020, it took an average of 287 days to identify and contain a breach, costing $1.26M more than breaches contained in 200 days or less.

THE DEEPWATCH APPROACH

With a named Squad assigned to monitor your environment 24/7/365, when we find a threat in your environment, the Squad will validate and enrich the data indicating the threat, drastically lowering false positives, and providing a ticket that is both thorough and aligned to your environment's unique situation.

Question 2

What data does my current MSSP use for detection?

WHY IT MATTERS

Not all data sources provide the same value. The wrong data sources can lead to alert fatigue, increased storage costs, and wasted time investigating false positives. Focusing on the right data sources assures that you are focused on the right places when breaches occur.

THE DEEPWATCH APPROACH

Deepwatch uses our Maturity Model to help you prioritize the best data sources available in your environment, recommends missing data sources of high value, and ensures all data sources are tuned for maximum security fidelity.

Question 3

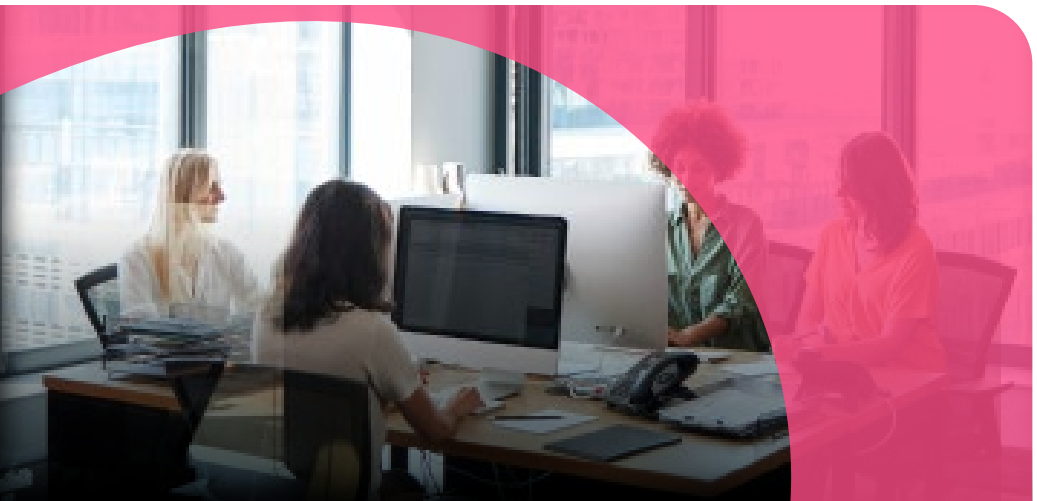
How does my current MSSP help me get more value from my security investments and tools?

WHY IT MATTERS

Despite spending on average $18.4M on security investments, a recent survey of cybersecurity professionals found that only 39% of respondents felt they were getting the full value from those investments.[2]

THE DEEPWATCH APPROACH

Deepwatch integrates your existing security tech stack and workflows seamlessly with your Deepwatch services to optimize security fidelity and mitigate security risks.



Question 4

What data does my current MSSP use for detection?

WHY IT MATTERS

In a recent survey, 43% of CISOs noted a lack of skilled staff as their biggest stumbling block in rapid incident detection and response.[3]

THE DEEPWATCH APPROACH

Deepwatch recruits top cybersecurity talent from the U.S. to support your Deepwatch cybersecurity services. Your named Squad is always watching and ready to respond 24/7/365 with multiple ways to communicate, including a mobile application and Slack channel. This allows you to make the most efficient use of your limited staff, focusing them on your more proactive projects and opportunities. The squads at Deepwatch receive on-going training and education to augment and optimize your team resources.

Question 3

How does my team and my current MSSP work together during a security incident?

WHY IT MATTERS

When a security incident occurs, it is important that your team knows who to call, what the communication flow is, and how incidents will be processed for the fastest resolution.

THE DEEPWATCH APPROACH

Deepwatch provides a named Squad of U.S.-based security experts who monitor your environment 24/7/365, including a Customer Success Manager. Your Squad knows your environment, and you can communicate with them anytime, anywhere.

Question 4

Does my current MSSP detect evasive threats that escape the security stack?

WHY IT MATTERS

In a recent survey, 63% of IT Security practitioners said they have observed a security control reporting an attack was blocked, when it actually failed to do so.[2]

THE DEEPWATCH APPROACH

Deepwatch doesn't just monitor one security control, all of them are monitored to identify security problems throughout the environment to help eliminate incorrect reporting from any one tool. Deepwatch continually innovates on detection technologies and processes to ensure that when protective controls fail, the Squad will detect and respond to evasive threats. Proactive threat hunting, advanced threat detection, and data enrichment techniques are used to investigate abnormal activity that may be malicious.

Question 7

How does my current MSSP help me understand and improve my security posture?

WHY IT MATTERS

Every hour, there are 7 businesses in the United States getting hit by ransomware attacks.5 A comprehensive security program is tablestakes to running a successful business today. Your MSSP should have a vested interest in helping you make security improvements to stay ahead of evolving threats. If they bill by the hour or ticket, your security maturity is not their priority.

THE DEEPWATCH APPROACH

Deepwatch has a patented, proprietary Security Maturity model to help customers strengthen their security posture and measure their progress year over year with their Deepwatch SCORE and Squad.

UNPARALLELED SECURITY SERVICES FROM AN MDR PARTNER YOU CAN TRUST

The security of your organization is too important to trust to vendors who claim they can help, but when it matters most–you are just a number. Your current MSSP is falling short and you deserve better. You deserve a true security partner that assigns named security experts to your organization that work to understand the nuances of your environment and risk profile and become an extension of your team.**You deserve Deepwatch.**

We work closely with each and every one of our customers to help them amplify their detection capabilities, get more from their current security investments, and provide expert guided responses to stay a step ahead of threats.

SQUAD MODEL

We assign a team of highly capable security professionals to work with you. These “squads” are named resources who support you on a daily basis as an extension of your team.

DEEPWATCH PLATFORM

We deliver comprehensive coverage via the industry’s most advanced cloud SecOps platform backed by a team of world class security experts.

MATURITY MODEL

We assess your overall security posture at onboarding through proprietary algorithms that objectively score your maturity level. This benchmarks your security posture against industry peersand provides a well defined roadmap to improvement. And it aligns our team and yours on the highest priorities.

PROVEN ENTERPRISE EXPERTISE

We deliver a comprehensive view of your security posture and vulnerabilities by flexibly ingesting new data sources and new content. We leverage proprietary and comprehensive content libraries and response playbooks.

deepwatch

To learn more about Deepwatch MDR and how we provide improved detection and reduced risk for our customers, **visit www.Deepwatch.com or reach out to us at sales@Deepwatch.com.**

ABOUT DEEPWATCH

Deepwatch helps secure the digital economy by protecting and defending enterprise networks, everywhere, every day. Deepwatch leverages its highly automated cloud-based SOC platform backed by a world class team of experts who monitor, detect, and respond to threats on customers' digital assets 24/7/365. Deepwatch extends security teams and proactively improves cybersecurity posture via its Squad delivery and patented Security Maturity Model. Many of the world's leading brands rely on Deepwatch's managed detection and response security.

SOURCES

1. IBM Cost of a Data Breach Report: https://www.ibm.com/security/data-breach
2. Ponemon Study: 53 Percent of IT Security Leaders Don't Know if Cybersecurity Tools are Working Despite an Average of $18.4 Million Annual Spend: https: //www.businesswire.com/news/ home/20190730005215/en/Ponemon-Study-53-Percent-of-IT-Security-Leaders-Don%E2%80%99t-Know-if-Cybersecurity-Tools-are-Working-Despite-an-Average-of-18.4-Million-Annual-Spend
3. More Than Half of CISOs Around the World Concerned About the Cybersecurity Skills Gap: https://securityintelligence.com/news/more-than-half-of-cisos-around-the-world-concerned-about-thecybersecurity-skills-gap/
4. Unit 42 Ransomware Threat Report, 1H 2021 Update: https://www.paloaltonetworks.com/blog/2021/08/ransomware-crisis/
5. U.S. Suffers Over 7 Ransomware Attacks An Hour. It's Now A National Security Risk: https://www.npr.org/2021/06/09/1004684788/u-s-suffers-over-7-ransomware-attacks-an-hour-itsnow-a-national-security-risk