Cybersecurity
INSIDERS

2022

XDR REPORT

CRYSTAL EYE XDR

Red Piranha
unified threat management

INTRODUCTION

Evolving security threats, exponential data growth, increased complexity, and a continuing cybersecurity skill shortage has given rise to a new category of security solutions called Extended Detection and Response (XDR). XDR solutions focus on providing technology integration between data sources and security operations to help accelerate detection and response by revealing threats, risks, and attacks that are highly sophisticated or hidden.

Red Piranha has emerged as one of the leaders in the XDR category. Their Crystal Eye platform is one of the first XDR solutions on the market, and offers the convergence of multiple security controls and workflows into a single platform to enhance security operations capabilities.

Red Piranha and Cybersecurity Insiders conducted a comprehensive survey to reveal the latest XDR trends and challenges in managing XDR, what XDR might replace, and how organizations select security technologies and providers.

Key findings include:

- When asked about the most critical security risks to mitigate, organizations see ransomware (79%), network intrusions (72%) and phishing attacks (66%) as the top priorities.
- Among the many challenges organizations are experiencing, the problem of not having enough experienced security staff and skills stands out (79%), followed by insufficient integration (72%) and lack of automation (66%).
- Organizations are looking for XDR to address a variety of challenges: contextualizing and correlating endpoint, network, cloud, identity, user behavior, and email data tops the list of challenges (64%), followed by automation of investigation and remediation (59%).

We want to thank Red Piranha for supporting this important industry research. We hope you find this report informative and helpful as you continue your efforts to protect your organizations against evolving threats.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

RISK PRIORITIES

When asked about the most critical security risks to mitigate, organizations see ransomware (79%), network intrusions (72%) and phishing attacks (66%) as the top priorities.

What are your top risk mitigation priorities?

79%

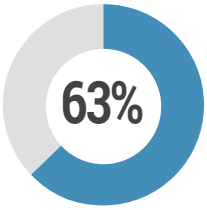
Ransomware

72%

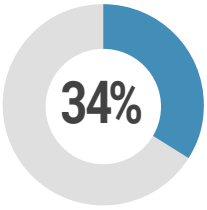
Network intrusion

66%

Phishing



Malware



Supply chain compromise

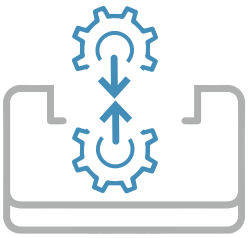
DETECTION AND RESPONSE CHALLENGES

Among the many detection and response related challenges organizations are experiencing, the problem of not having enough experienced security staff and skills stands out (79%). This is followed by insufficient integration (72%) and lack of automation (66%).

Which of the following do you feel are the top Detection and Response challenges for your SOC?

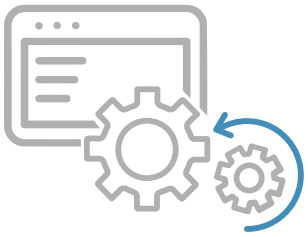
79%

Not enough security staff, skills, or context



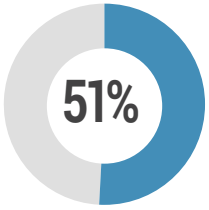
72%

Not enough tool integration

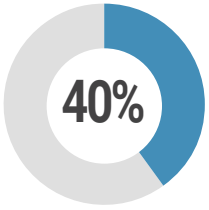


66%

Not enough automation



Alert fatigue from too many false positives

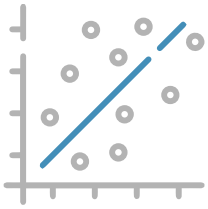


Inadequate SIEM visibility of multi-vector attacks

SECURITY CHALLENGES FOR XDR

We asked cybersecurity professionals what security challenges they are looking to address with XDR. Contextualizing and correlating endpoint, network, cloud, identity, user behavior and email data tops the list of challenges (64%), followed by automation of investigation and remediation (59%).

What are the biggest security challenges you are facing that you would look to XDR to solve?

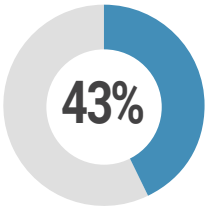


64%

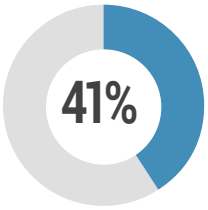
Contextualizing and correlating endpoint, network, cloud, identity, user behavior and email data

59%

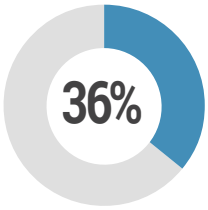
More automation of investigation and remediation process



Lack of an in-house SOC (fully managed 24/7 or hybrid)



Expanding threat surface and lack of visibility



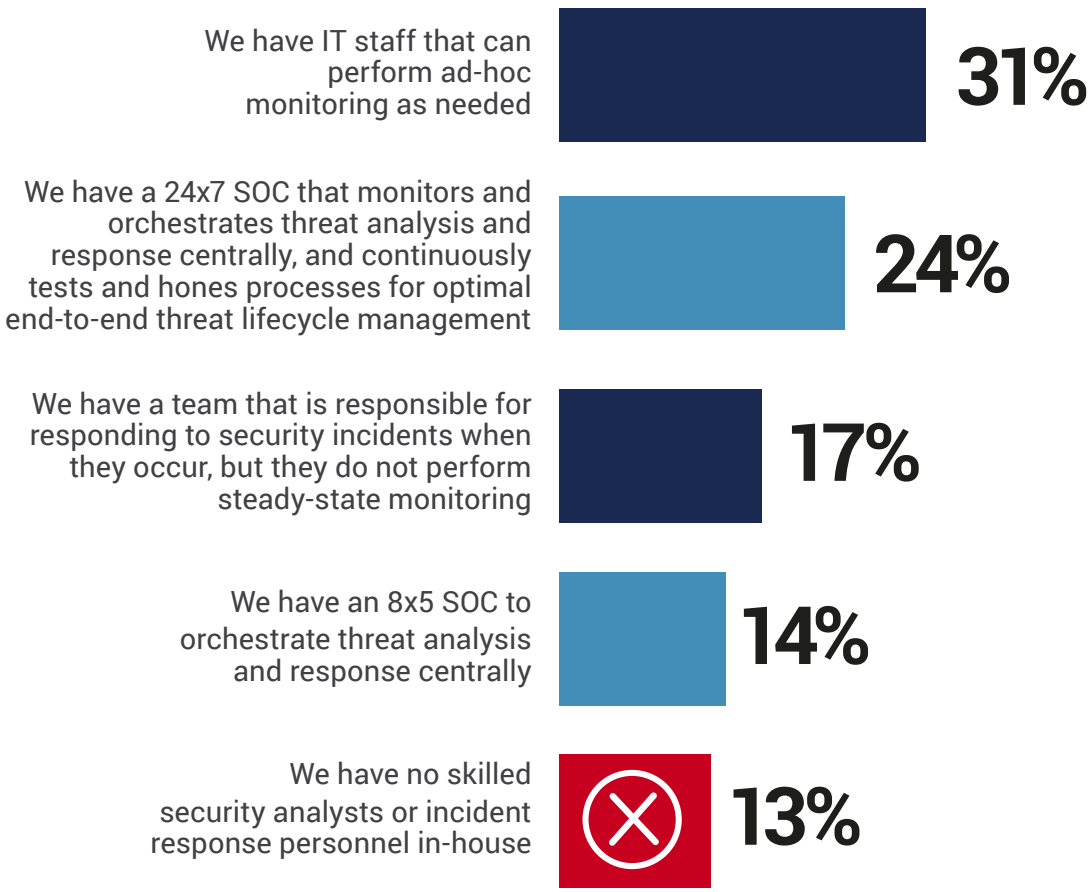
Lack of proper SIEM coverage or SIEM technology altogether

Other 4%

THREAT PREPAREDNESS

Almost a third of organizations (31%) confirm they have only enough IT security staff to perform ad-hoc monitoring as the need arises. Only one-quarter of organizations (24%) have a 24x7 SOC that monitors and orchestrates threat analysis and response centrally, and continuously improves processes for optimal end-to-end threat lifecycle management. An alarming thirteen percent have no skilled security analysts or incident response personnel in-house.

How equipped are your staff and processes to deal with incoming threats?

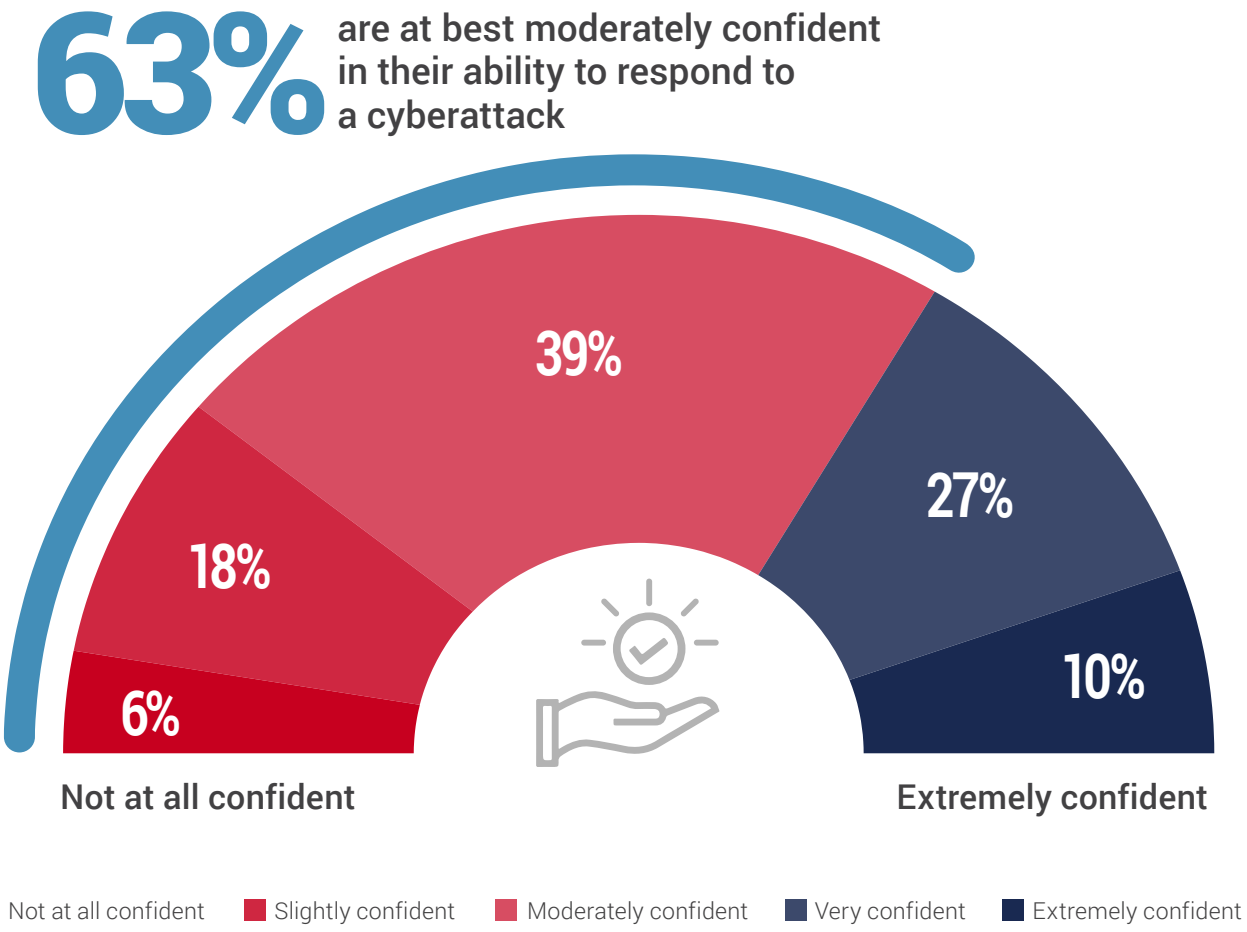


Other 1%

ATTACK RESPONSE CONFIDENCE GAP

A majority of 63% of organizations are not at all to moderately confident in their ability to respond to a cyber attack. This shows an overall need for dedicated, 24x7 security threat detection and response to fill the confidence gap.

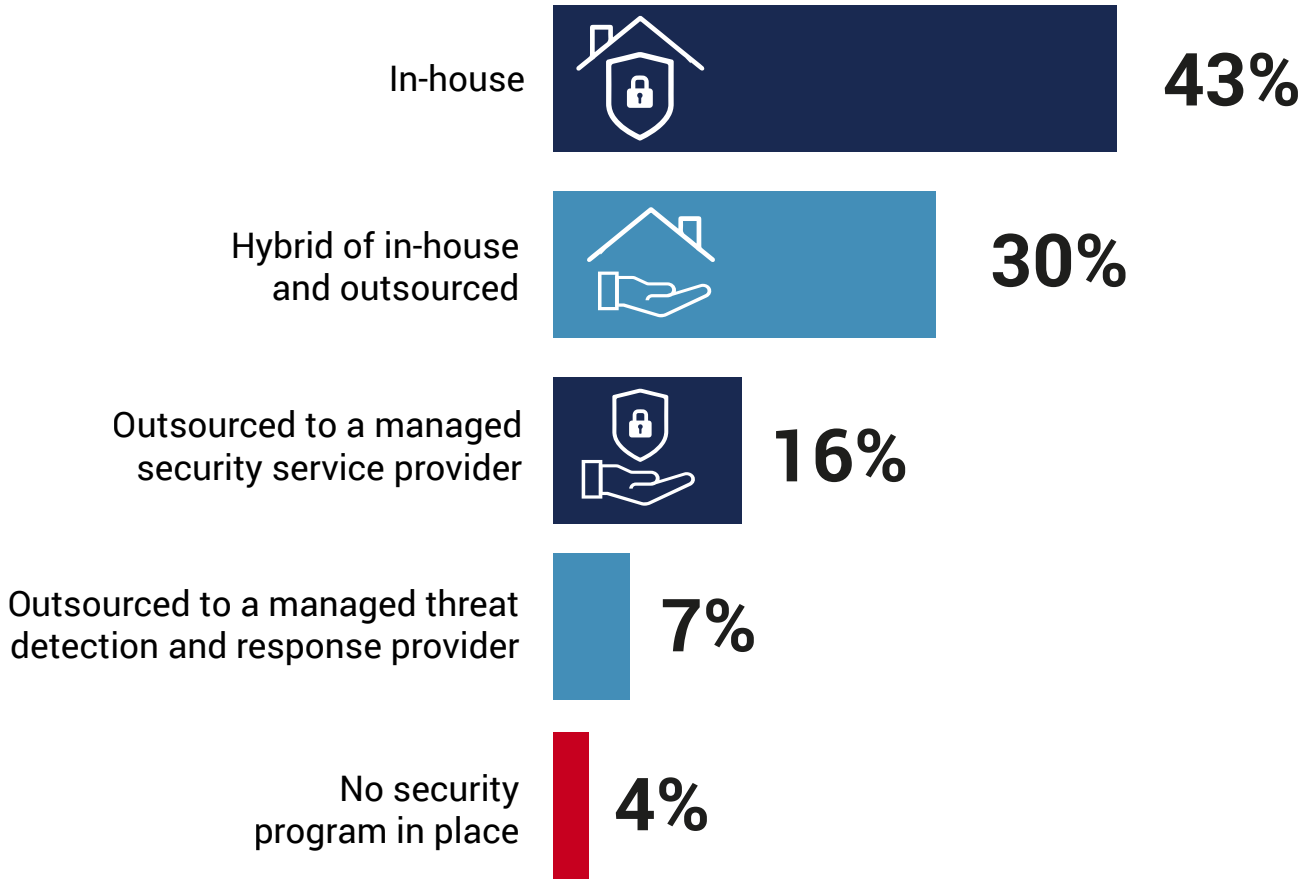
How confident are you in your organization's ability to respond to a cyberattack?



SECURITY OPERATIONS STAFFING

When asked how organizations currently source their security operations, 43% of respondents indicated they operate their security in-house. This is followed by about a third of organizations (30%) that operate in a hybrid model of in-house and outsourced resources. As the cybersecurity skills gap continues to persist, we expect more organizations to outsource security capabilities to a managed service.

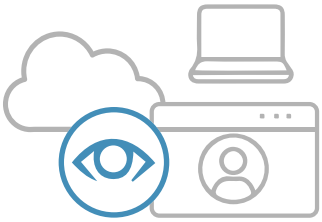
How is your security operations program currently sourced?



CRITICAL XDR FEATURES

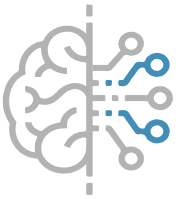
We asked cybersecurity professionals what features they are prioritizing in XDR platforms. The most important capability among security professionals is visibility across endpoint, network, cloud, identity, user behavior and email data (77%). This is followed by analytics to reduce noise and false positives (68%), and integrated threat intelligence to enable threat hunting (65%).

What features are most important to you in an XDR platform?



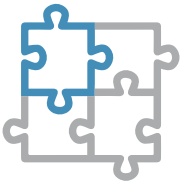
77%

Visibility across endpoint, network, cloud, identity, user behavior and email data



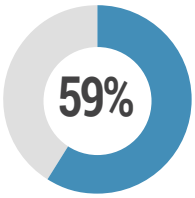
68%

Intelligent analytics to eliminate noise and greatly reduce false positive rates

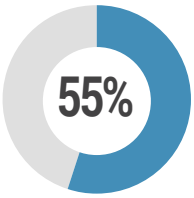


65%

Integrated threat intelligence and contextual information to enable threat hunting



Machine learning driven threat detection and containment



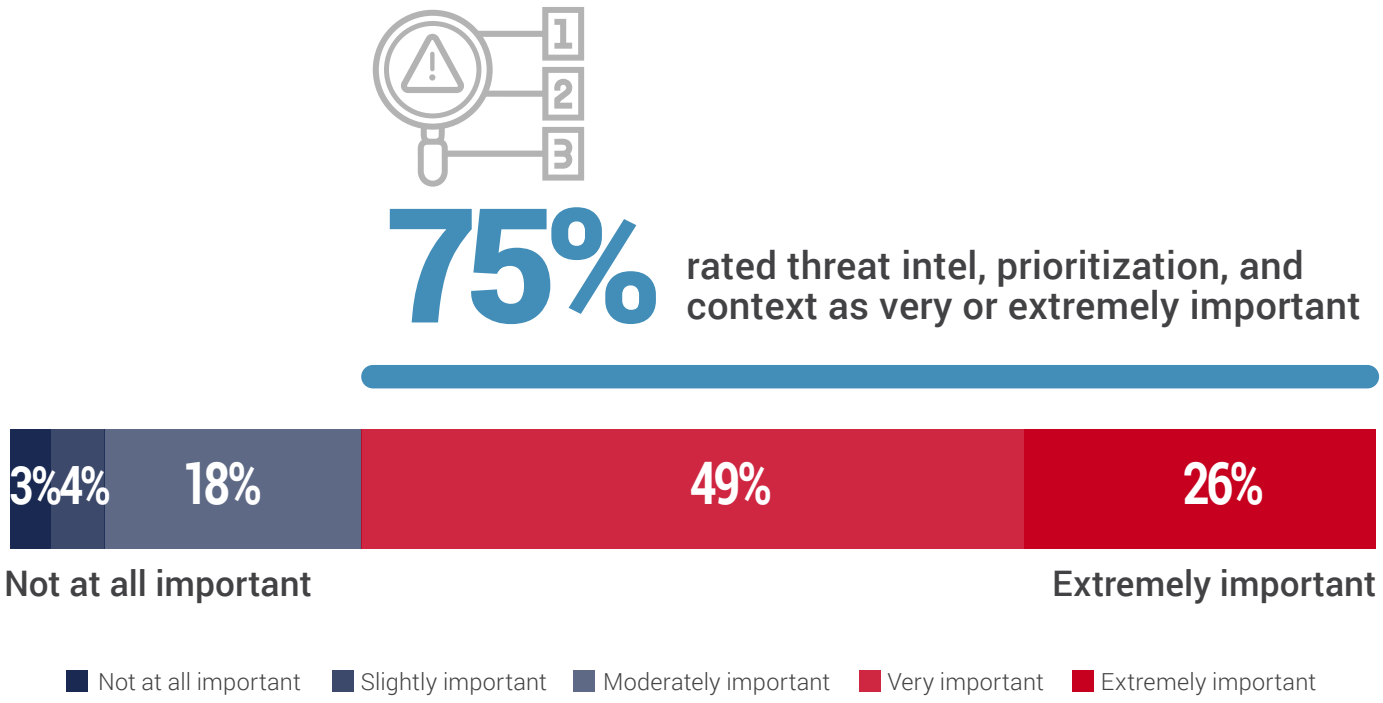
Increased data ingestion for better-quality investigations and responses

Other 4%

THREAT INTELLIGENCE

Threat intelligence and the ability to prioritize and contextualize security observations are becoming increasingly important components of XDR offerings, according to 75% of cyber professionals.

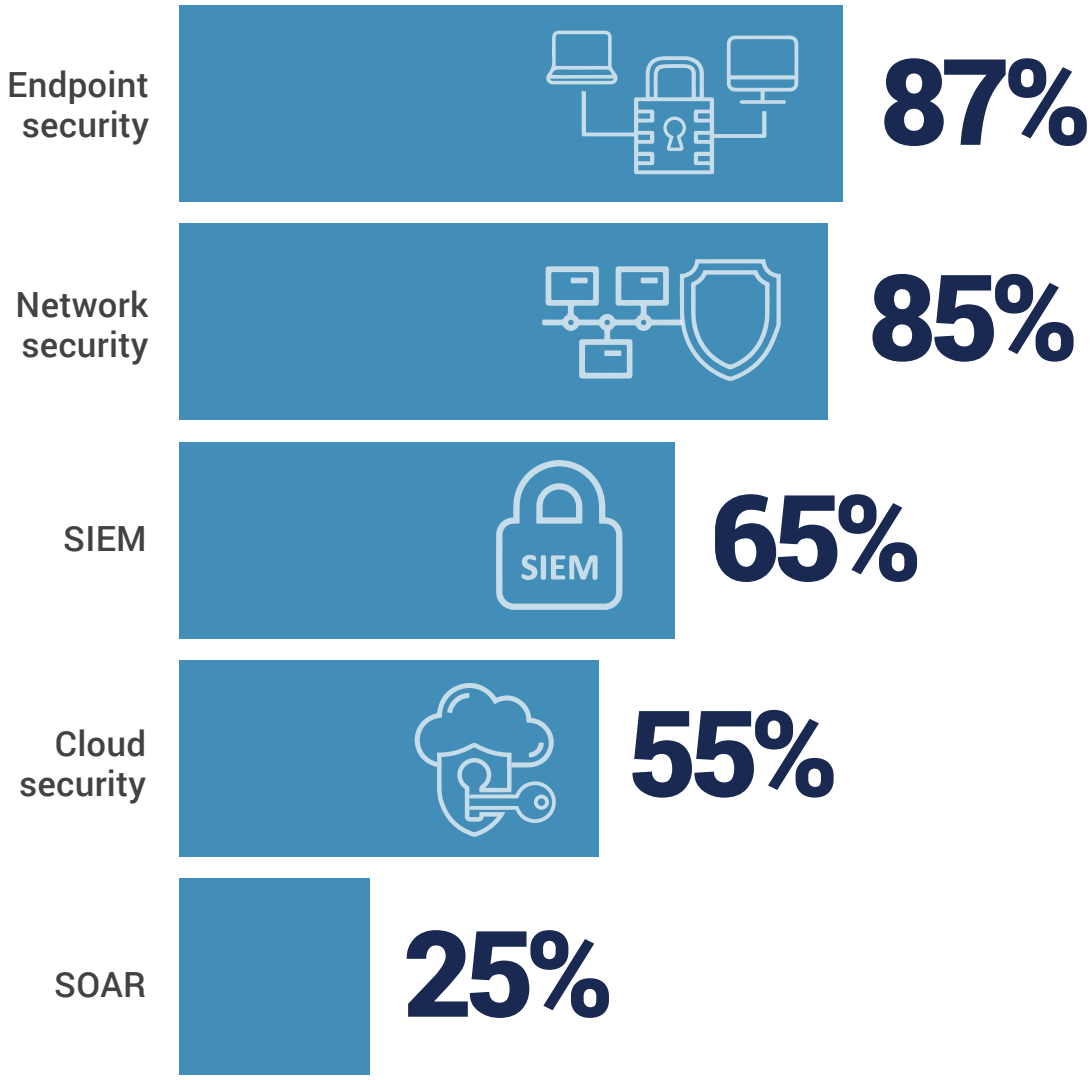
How important is threat intelligence and the ability to prioritize and contextualize security observations as part of an XDR service offering?



SECURITY TECHNOLOGY PRIORITIES

What security technologies are organizations prioritizing in their battle against an ever-evolving threat environment? The top two spots are a virtual tie between endpoint security (87%) and network security (85%), followed by SIEM (65%).

What technologies are you currently leveraging in your security strategy?



WHAT XDR REPLACES

With XDR as the next generation technology for detection and response, what "legacy" technologies is XDR replacing or building on? Cybersecurity professionals see SIEM (56%) and EDR (53%) as the top contenders to be replaced, followed by SOAR (32%).

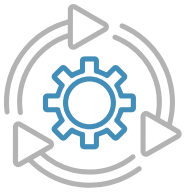
Which of your current technology tools do you expect XDR to replace?

56%

SIEM

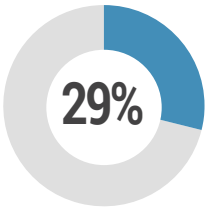
53%

EDR

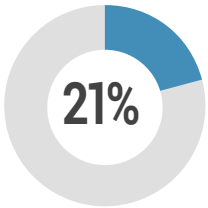


32%

SOAR



NDR



UBA

Other 8%

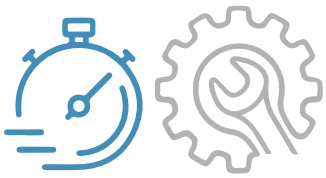
SERVICE PROVIDER SELECTION

When selecting a detection and response provider, most organizations prioritize 24/7 security coverage above all else (59%). This is followed by the speed of incident response (54%) and solution cost (53%).

What are your most important criteria when selecting a managed detection and response provider?

59%

24/7 coverage of security operations

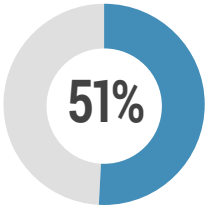


54%

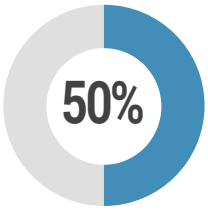
Speed of incident response issues

53%

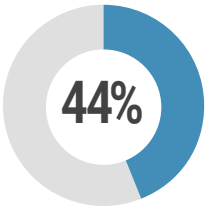
Solution cost



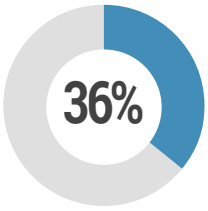
Supported systems or technologies



Ability to integrate/leverage our security technology stack



Automated response capabilities



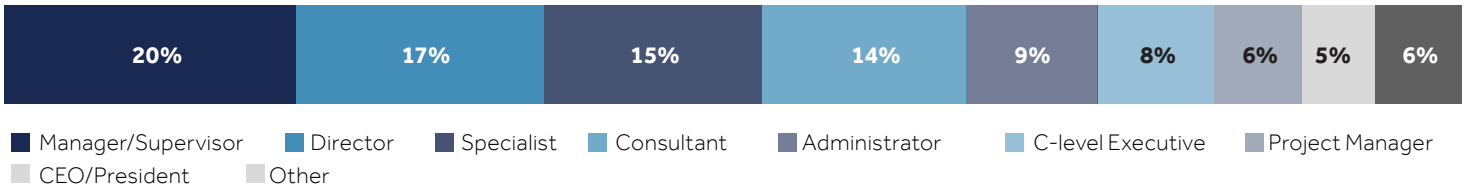
Ability to customize reporting

Reputation of company and leadership 34% | Location/proximity (Ability to interact with a local or regional analyst) 29% | Commitment towards a mean time to contain 24% | Size of their customer base 13% | Other 7%

METHODOLOGY & DEMOGRAPHICS

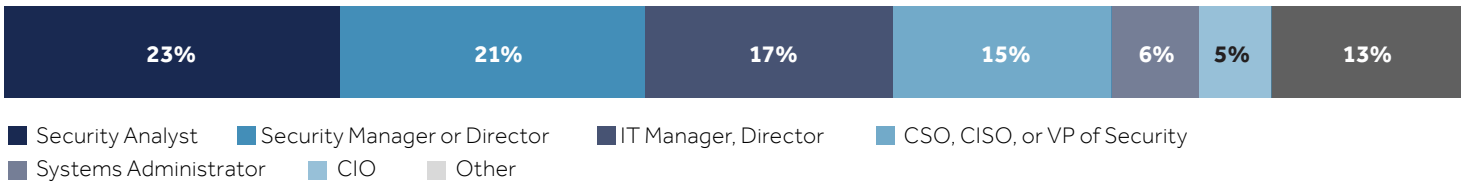
The 2022 XDR Report is based on a comprehensive survey of 227 cybersecurity professionals conducted in April 2022. The respondents range from technical executives to IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

CAREER LEVEL

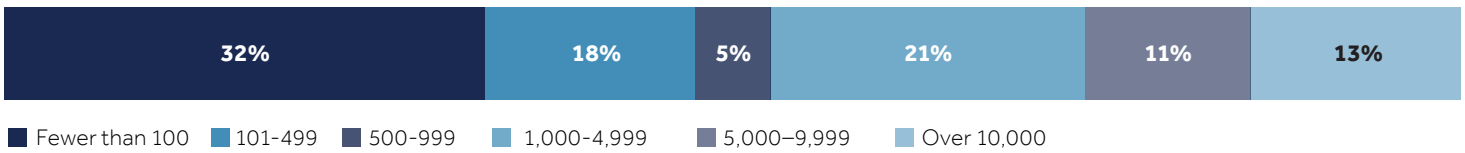


DEPARTMENT

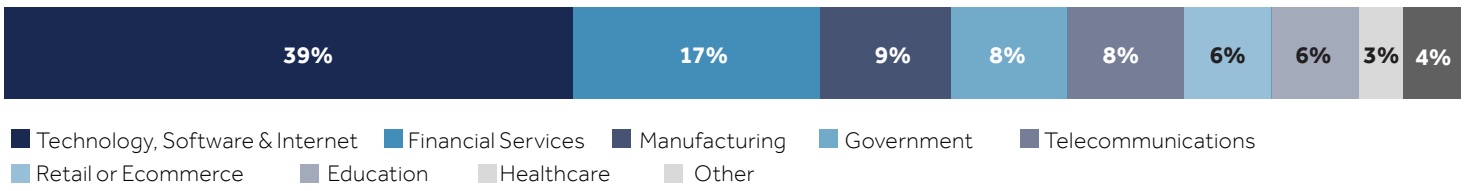
PRIMARY ROLE



COMPANY SIZE



INDUSTRY



Red Piranha is an award-winning cybersecurity vendor based in Australia and is a pioneer in the XDR category. Red Piranha's Crystal Eye XDR platform leads the way in helping organizations to reduce the risk of a security incident, reduce the time to detect & respond to threats and increase the return on investment of cyber spend. Their Consolidated Security Platform is the Swiss army knife of cyber solutions, solving the problem of complexity with their unified approach to security operations efficiencies. They fuse human-machine teaming capability into their platform which extends the integrated services model and delivers increased security outcomes as and when required.

www.redpiranha.net

Cybersecurity
INSIDERS

Cybersecurity Insiders is a 500,000+ member online community for information security professionals, bringing together the best minds dedicated to advancing cybersecurity and protecting organizations across all industries, company sizes, and security roles.

We provide cybersecurity marketers with unique marketing opportunities to reach this qualified audience and deliver fact-based, third-party validation thought leadership content, demand-generation programs, and brand visibility in the cybersecurity market.

For more information please visit www.cybersecurity-insiders.com