HERJAVEC
GROUP

Buyer's Guide to Managed Security Services

How to select a transformative security partner in a crowded provider landscape

HERJAVEC GROUP

Buyer’s Guide to Managed Security Services

Table of contents

A Paradigm Shift in Cybersecurity 3

MSS Adoption Drivers:
Making Sense Of Security 4

Deciphering Between Providers,
From Detect To Protect 5

Key Criteria When Evaluating MSSPs 6

Service Delivery: Find The Best Fit 12

Why Herjavec Group? 13

A Paradigm Shift in Cybersecurity

From a technology problem to a global business driver

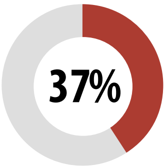
In the world of cybersecurity, there are monumental changes, yet much remains the same. Defenders and adversaries exist in a seemingly endless game of chess—each trying to outwit the other, hiding their techniques, and vying to take the lead.

The trend of cybersecurity as a business driver rather than a technology issue has been developing for some time. However, given the current threat climate and change in how businesses operate with imperatives like cloud-first, Bring Your Own Device (BYOD) programs, and work-from-anywhere, organizations are at a tipping point in how they handle the balance of security and digital transformation.

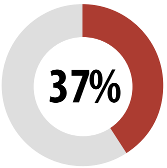
As the threat surface expands to an often unmanageable size, organizations are in a continuous struggle to defend against persistent, sophisticated crimes. Short on staff, overrun with alerts, and constrained by budget, IT and security teams need a better way to become more than a technology cost center and support real business change.

Remaining in the adversary's shadow is a dangerous position—now is the time for change. Managed Security Services (MSS) are a popular way to move ahead by addressing common security pain points that stand in the way of strategic security objectives. This eBook examines the different benefits that Managed Security Services Providers (MSSPs) offer, and will help you understand what to look for when choosing the right provider for your organization.

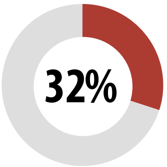
In the last 12 months, security incidents caused the following negative impacts to businesses:



Disrupted business activities[1]



Reduced employee productivity



Deployment of IT resources to triage and remediatite issue

[1] *Herjavec Group. "Managed Security Services Trends." 2020*

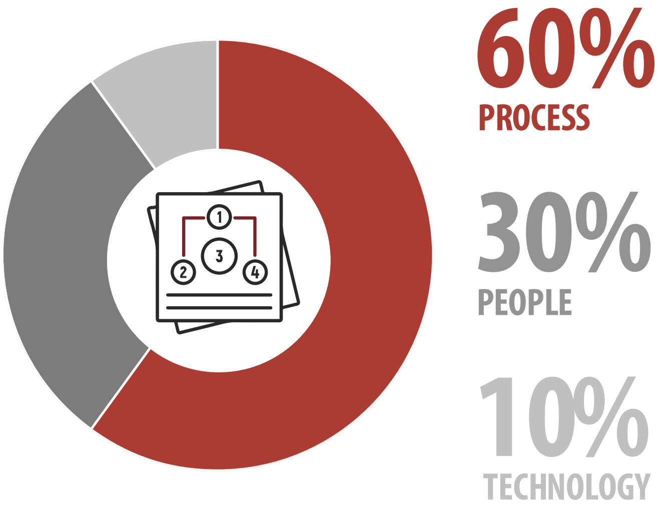
Remaining in the adversary's shadow is a dangerous position—now is the time for change.

MSS Adoption Drivers: Making Sense of Security

In times when security was seen as an IT function rather than a strategic business function, organizations tapped MSSPs to deliver and maintain security technologies, or simply throw alerts over the wall for the organization to firefight. The deluge of alerts as a symptom of sophisticated, cybercrime threats has made this approach not only unmanageable, but has diluted any value it once brought to security operations.

MSSPs have had to reimagine how to bring value and stay relevant. Now, services are structured to provide benefits through security insights and interpreting security requirements so that organizations can prioritize their efforts and focus on direct risk impacts.

The Composition of MSS



Drivers behind MSS adoption include the need for:

- Access to trained security analysts and specialized experts beyond in-house capabilities
- Threat-centric approach that spans people, process, and technology for faster detection and response to disrupt and block attacks 24/7/365
- Improved cybersecurity ROI from enhanced technology utilization and process optimization
- Executive metrics to measure progress and identify what risks remain to the organization in order to communicate effectively to board/executive level
- Immediate availability of hands-on incident response when a breach occurs

In a 2020 survey of IT and cybersecurity professionals[2] , we found these to be the top challenges that enterprises struggled with when managing their security operations:

Shortage of in-house cybersecurity skills

Cost and complexity of building in-house security operations

Lack of true 24x7 security coverage

Slowness in time to detect, notify, and respond to security events

Inadequate visibility into overall security posture

Inability to proactively identify emerging threats across the environment

[2] Herjavec Group. "Managed Security Services Trends." 2020

Deciphering Between Providers, From Detect to Protect

Enterprises now widely accept that it is no longer a matter of if a breach will happen, but when. Now, more than ever, enterprises are turning to MSSPs to play a critical role in the mitigation of these security incidents.

According to Gartner, "By 2025, 50% of organizations will allow third parties to go beyond pure monitoring for security breaches but also provide mitigation using remotely accessible security technologies, up from 15% today."[3]

Depending on your goals, there are a variety of provider types for MSS:

- Security pure-play
- Network services or telecommunications
- System Integrators
- IT Outsource
- Consultancy firms

While the end goal of protection is clear, confusion arises when reviewing capabilities that span from detection to stopping a breach.

Beyond the foundational detect & respond, predict, prevent, and protect services, industry-leading MSSPs typically offer some or all of the following advanced services:

- Managed Endpoint & EDR
- Managed Secure Gateway
- Managed Identity
- Vulnerability Scanning
- Threat Hunting
- Threat Modelling
- Managed Phishing Service

When evaluating MSSP services, many organizations consider flexibility in utilizing existing security technology investments and accelerating the operational effectiveness of current security solutions clear advantages. But they often find that how those goals are achieved varies greatly from provider to provider.

Consider your in-house capabilities and existing security stack. MSSP engagement models range from commoditized technology management-driven to heavily customized and consultancy-led.

We asked: What are the most important Managed Security Services to your company?

26%
Managed detection and response

25%
Managed SIEM

14%
Firewall management

[3] *Herjavec Group. "Managed Security Services Trends." 2020*

Key Criteria When Evaluating MSSPs

When evaluating MSSPs, you'll want a provider who can:

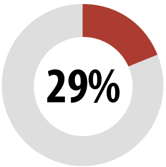
- Increase visibility and help you better understand your risk exposure
- Work with you continuously to improve your security program
- Provide actionable intelligence
- Ensure you gain control of threats
- Help you enable your hybrid workforce
- Act as an extension of your in-house team
- Improve the ROI of your existing cybersecurity investments

Increase visibility and help you better understand your risk exposure

The perimeter has evaporated, diluting the effectiveness of bygone security controls that were built and deployed when the perimeter was well-defined. Now, adversaries can find their way in through a slew of entry points, gaining a foothold and escalating privileges until they reach their intended target. Enterprises are left in a reactive mode, hastily buying yet another point solution to keep the lights on after an attack—creating silos of technologies that address immediate dangers, rather than risk exposure on the whole.

> “As security stacks grow, visibility decreases. Yet, to have a strong security posture, enterprises need to be able understand their security infrastructure, gather data, and put context around security incidents.

While all MSSPs work with enterprises to improve visibility, approaches differ, relying on a specific set of tools or a broader range of options. Consider a vendor-agnostic provider that can step back from the solution-centric marketing messages. These unbiased partners can advise on the combination of tools, technologies, procedures, and methodologies your organization truly needs to achieve real-time visibility, and determine current detection ability and existing gaps.



of organizations we surveyed have no visibility into overall security posture[4]

> “**Unbiased partners can advise on the combination of tools, technologies, procedures, and methodologies your organization truly needs to achieve real-time visibility, and determine current detection ability and existing gaps.**

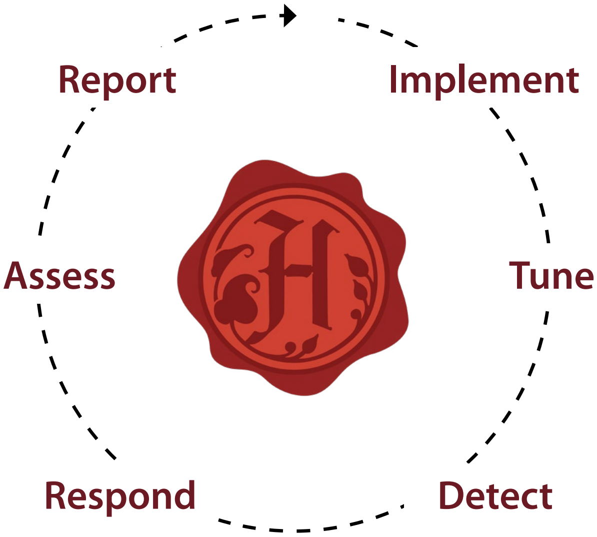
[4] Herjavec Group. *“Managed Security Services Trends.” 2020*

Key Criteria When Evaluating MSSPs

Work with you to continuously improve your security program

Security programs cannot be static. There should always be continuous, measurable improvement, evolving with the dynamic threat landscape and increasingly sophisticated attacks. What worked yesterday may not work tomorrow.

An MSSP that leverages a feedback loop will ensure your security program remains effective in the current threat climate by making enhancements on a regular basis.



Provide actionable intelligence

Oftentimes we plan security programs in the context of what we know exists, and even with threat feeds, it is often an overwhelming task to make the intelligence actionable. The key is to work with an MSSP that defends customers around the globe, so that what exists is a much broader scope. Using deeper sharing abilities across network, endpoint and other telemetry, allows providers to leverage intelligence that is more insightful than your everyday indicator of compromise (IoC). Along with these learnings, MSSPs gain insights on adversary tools, tactics, and procedures (TTPs) as well as information on geographical and vertical attacks and apply that directly to protect individual organizations.

Key Criteria When Evaluating MSSPs

Ensure you gain control of threats

It can take months to detect an attack. All the while a stealthy adversary quietly collects data and looks for confidential material or credentials to allow them to move laterally across the environment. And once an adversary successfully evades detection and attacks, the problem balloons as organizations are not always prepared with detection capabilities required to stop advanced persistent threats from remaining inside the network.

MSSPs with active threat hunting capabilities will keep your organization from experiencing these challenges by assuming adversaries are already in your system and initiating investigations to uncover them. They will go beyond point-in-time scanning of signatures and 24/7 automated tools, which alone won't keep up with advanced threats. MSSPs that are well-positioned to handle today's sophisticated threats have expert, hands-on analysts to proactively hunt and protect your business.

Effective threat hunters are difficult to find and retain. MSSPs use their hard-learned lessons from the SOC to find today's stealthiest threats that put your organization at risk.

Help you securely enable your hybrid workforce

No one could have predicted the way we transitioned to the remote work environment. VPNs were overwhelmed, split tunnelling was accepted, and employees connected to the network with any device they had at home. As a result, many enterprises were forced into compromising on their security program until things shifted back. What happened though was not a return to normal, but an acceptance that we now have a hybrid workforce that has to be secured without impeding their ability to work.

Finding an MSSP that can secure any workforce, no matter the location, is essential. MSSPs should have time-tested experience, allowing them to refine their technology and processes for a range of customer environments. By choosing a long-standing MSSP with a proven track record, you will feel confident that your technology stack will deliver the same level of security efficacy for remote employees as it does in the corporate environment.

Key Criteria When Evaluating MSSPs

Ask Yourself:

✓ **Does the MSSP operate with the mindset that people are the new perimeter?**

No matter where your employees work, they will always be the weakest link in your security. Of all cyber threats facing organizations, our 2020 survey showed that two of the top three threats used social engineering to exploit employees.

We asked:
What are the most concerning threats to your organization?

73% Ransomware

57% Loss of customer data

39% Email account compromise

36% Compliance findings/fines

✓ **Do they offer holistic services that go beyond technology to protect?**

Even with the best technology, organizations will benefit from training in their security operations for an added layer of defense. Managed Phishing Services help prevent employees from being exploited using techniques such as reviewing IOCs, email attachments, and URLs within sandbox environments.

Secure in and out of the office with an MSSP that also provides:

Endpoint Tool Management to automate regular routines like installing patches, deploying software, imaging and deploying OS, managing assets, software licenses, etc., for streamlined security

Engineering to provide expertise on deploying, configuring, and managing ATP, DLP, Email, Firewall, Endpoint, IDS, NAC, SIEM, UBA tools & more

An inventory of assets within the environment to know exactly what you are protecting

Key Criteria When Evaluating MSSPs

Act as an extension of your in-house team

The well-known cybersecurity skills shortage is getting worse, and the effects are measurable. 70% of ISSA members believe their organization has been impacted by the global cybersecurity skills shortage . And the problem isn't confined to a lack of people, but also expertise—63% of respondents have only worked in cybersecurity for less than three years. Combined with the sheer number of alerts and false positives generated by disparate security tools, ill-fated analysts have come to accept slow mean time to detection (MTTD) and mean time to remediation (MTTR).

Technology alone doesn't disrupt threats. Instead, it requires a blend of best-of-breed technology and human experts. MSSPs solve this challenge by augmenting in house capabilities--often referred to as an "extension of your security team." This, however, can be misleading as some providers are less specialized and address the broader IT ecosystem, while others live and breathe security.

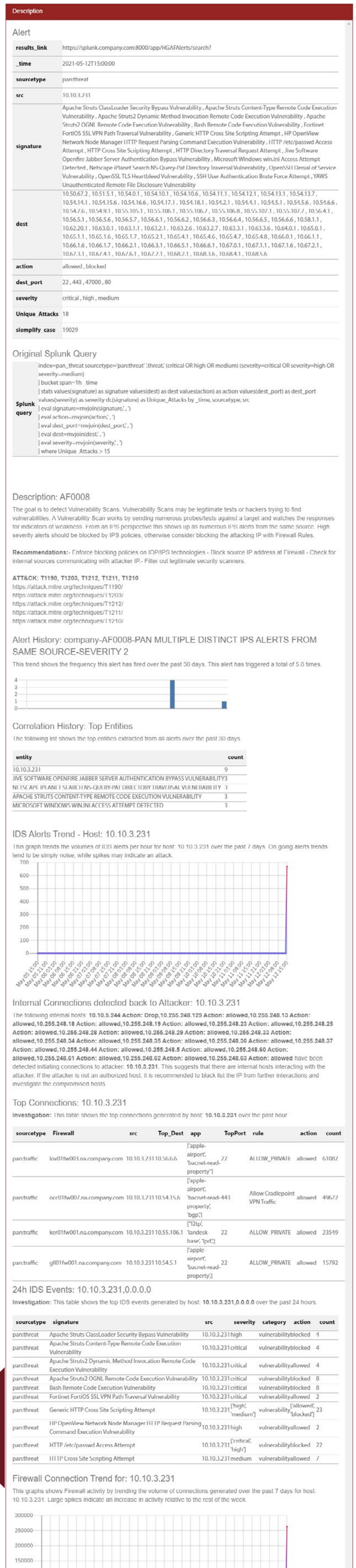
ASK: Do you have experts available 24/7/365?

Another consideration when evaluating MSSPs is the availability of human experts. It is a tremendous benefit to have access to security experts, but without the need to recruit, retain, and train FTEs. When reviewing service offerings, seek out MSSPs that have a SOC with 24/7 security monitoring. This "always on" service delivers value through timely logging, alerting, enrichment, and escalation to drive containment and remediation efforts needed to improve MTTD and MTTR.

Improve the ROI of your existing cybersecurity investments

When information security is fully managed by an internal team, organizations can face unforeseeable costs from issues with staffing, hardware, maintenance, licensing, and more. MSSPs can improve your cyber ROI, not only through predictable costs, but by reducing risk through continuous improvement, industry benchmarking, and efficient automation.

> "
> 70% of ISSA members believe their organization has been impacted by the global cybersecurity skills shortage.



Description

Alert

results_link	https://splunk.company.com:8000/app/HGAFAlerts/search?
_time	2021-05-12T15:00:00
sourcetype	pan:threat
src	10.10.3.231
signature	Apache Struts ClassLoader Security Bypass Vulnerability , Apache Struts Content-Type Remote Code Execution Vulnerability , Apache Struts2 Dynamic Method Invocation Remote Code Execution Vulnerability , Apache Struts2 OGNL Remote Code Execution Vulnerability , Bash Remote Code Execution Vulnerability , Fortinet FortiOS SSL VPN Path Traversal Vulnerability , Generic HTTP Cross Site Scripting Attempt , HP OpenView Network Node Manager HTTP Request Parsing Command Execution Vulnerability , HTTP /etc/passwd Access Attempt , HTTP Cross Site Scripting Attempt , HTTP Directory Traversal Request Attempt , Jive Software Openfire Jabber Server Authentication Bypass Vulnerability , Microsoft Windows win.ini Access Attempt Detected , Netscape iPlanet Search NS-Query-Pat Directory Traversal Vulnerability , OpenSSH Denial of Service Vulnerability , OpenSSL TLS Heartbleed Vulnerability , SSH User Authentication Brute Force Attempt , YAWS Unauthenticated Remote File Disclosure Vulnerability
dest	10.50.67.2 , 10.51.5.1 , 10.54.0.1 , 10.54.10.1 , 10.54.10.6 , 10.54.11.1 , 10.54.12.1 , 10.54.13.1 , 10.54.13.7 , 10.54.14.1 , 10.54.15.6 , 10.54.16.6 , 10.54.17.1 , 10.54.18.1 , 10.54.2.1 , 10.54.4.1 , 10.54.5.1 , 10.54.5.6 , 10.54.6.6 , 10.54.7.6 , 10.54.9.1 , 10.55.105.1 , 10.55.106.1 , 10.55.106.7 , 10.55.106.8 , 10.55.107.1 , 10.55.107.7 , 10.56.4.1 , 10.56.5.1 , 10.56.5.6 , 10.56.5.7 , 10.56.6.1 , 10.56.6.2 , 10.56.6.3 , 10.56.6.4 , 10.56.6.5 , 10.56.6.6 , 10.58.1.1 , 10.62.20.1 , 10.63.0.1 , 10.63.1.1 , 10.63.2.1 , 10.63.2.6 , 10.63.2.7 , 10.63.3.1 , 10.63.3.6 , 10.64.0.1 , 10.65.0.1 , 10.65.1.1 , 10.65.1.6 , 10.65.1.7 , 10.65.2.1 , 10.65.4.1 , 10.65.4.6 , 10.65.4.7 , 10.65.4.8 , 10.66.0.1 , 10.66.1.1 , 10.66.1.6 , 10.66.1.7 , 10.66.2.1 , 10.66.3.1 , 10.66.5.1 , 10.66.6.1 , 10.67.0.1 , 10.67.1.1 , 10.67.1.6 , 10.67.2.1 , 10.67.3.1 , 10.67.4.1 , 10.67.6.1 , 10.67.7.1 , 10.68.2.1 , 10.68.3.6 , 10.68.4.1 , 10.68.5.6
action	allowed , blocked
dest_port	22 , 443 , 47000 , 80
severity	critical , high , medium
Unique_Attacks	18
siemplify_case	19029

Original Splunk Query

Splunk query

```
index=pan_threat sourcetype='pan:threat' ',threat.' (critical OR high OR medium) (severity=critical OR severity=high OR
severity=medium)
| bucket span=1h _time
| stats values(signature) as signature values(dest) as dest values(action) as action values(dest_port) as dest_port
values(severity) as severity dc(signature) as Unique_Attacks by _time, sourcetype, src
| eval signature=mvjoin(signature,' , ')
| eval action=mvjoin(action,' , ')
| eval dest_port=mvjoin(dest_port,' , ')
| eval dest=mvjoin(dest,' , ')
| eval severity=mvjoin(severity,' , ')
| where Unique_Attacks > 15
```

Description: AF0008

The goal is to detect Vulnerability Scans. Vulnerability Scans may be legitimate tests or hackers trying to find vulnerabilities. A Vulnerability Scan works by sending numerous probes/tests against a target and watches the responses for indicators of weakness. From an IPS perspective this shows up as numerous IPS alerts from the same source. High severity alerts should be blocked by IPS policies, otherwise consider blocking the attacking IP with Firewall Rules.

Recommendations:- Enforce blocking policies on IDP/IPS technologies - Block source IP address at Firewall - Check for internal sources communicating with attacker IP.- Filter out legitimate security scanners.

ATT&CK: T1190, T1203, T1212, T1211, T1210
https://attack.mitre.org/techniques/T1190/
https://attack.mitre.org/techniques/T1203/
https://attack.mitre.org/techniques/T1212/
https://attack.mitre.org/techniques/T1211/
https://attack.mitre.org/techniques/T1210/

Alert History: company-AF0008-PAN MULTIPLE DISTINCT IPS ALERTS FROM SAME SOURCE-SEVERITY 2

This trend shows the frequency this alert has fired over the past 30 days. This alert has triggered a total of 5.0 times.

Correlation History: Top Entities

The following list shows the top entities extracted from all alerts over the past 30 days.

entity	count
10.10.3.231	9
JIVE SOFTWARE OPENFIRE JABBER SERVER AUTHENTICATION BYPASS VULNERABILITY	3
NETSCAPE IPLANET SEARCH NS-QUERY-PAT DIRECTORY TRAVERSAL VULNERABILITY	3
APACHE STRUTS CONTENT-TYPE REMOTE CODE EXECUTION VULNERABILITY	3
MICROSOFT WINDOWS WIN.INI ACCESS ATTEMPT DETECTED	3

IDS Alerts Trend - Host: 10.10.3.231

This graph trends the volumes of IDS alerts per hour for host: 10.10.3.231 over the past 7 days. On going alerts trends tend to be simply noise, while spikes may indicate an attack.

Internal Connections detected back to Attacker: 10.10.3.231

The following internal hosts: **10.10.5.244 Action: Drop,10.255.248.129 Action: allowed,10.255.248.13 Action: allowed,10.255.248.18 Action: allowed,10.255.248.19 Action: allowed,10.255.248.23 Action: allowed,10.255.248.25 Action: allowed,10.255.248.28 Action: allowed,10.255.248.29 Action: allowed,10.255.248.33 Action: allowed,10.255.248.34 Action: allowed,10.255.248.35 Action: allowed,10.255.248.36 Action: allowed,10.255.248.37 Action: allowed,10.255.248.44 Action: allowed,10.255.248.5 Action: allowed,10.255.248.60 Action: allowed,10.255.248.61 Action: allowed,10.255.248.62 Action: allowed,10.255.248.63 Action: allowed** have been detected initiating connections to attacker: **10.10.3.231**. This suggests that there are internal hosts interacting with the attacker. If the attacker is not an authorized host, it is recommended to black list the IP from further interactions and investigate the compromised hosts

Top Connections: 10.10.3.231

Investigation: This table shows the top connections generated by host: **10.10.3.231** over the past hour

sourcetype	Firewall	src	Top_Dest	app	TopPort	rule	action	count
pan:traffic	lov01fw003.na.company.com	10.10.3.231	10.56.6.6	['apple-airport', 'bacnet-read-property'']	22	ALLOW_PRIVATE	allowed	61082
pan:traffic	occ01fw007.na.company.com	10.10.3.231	10.54.15.6	['apple-airport', 'bacnet-read-property', 'bgp',]	443	Allow Cradlepoint VPN Traffic	allowed	49672
pan:traffic	ker01fw001.na.company.com	10.10.3.231	10.55.106.1	[''l2tp', 'landesk base', 'lpd',]	22	ALLOW_PRIVATE	allowed	23549
pan:traffic	gll01fw001.na.company.com	10.10.3.231	10.54.5.1	['apple airport', 'bacnet-read-property',]	22	ALLOW_PRIVATE	allowed	15792

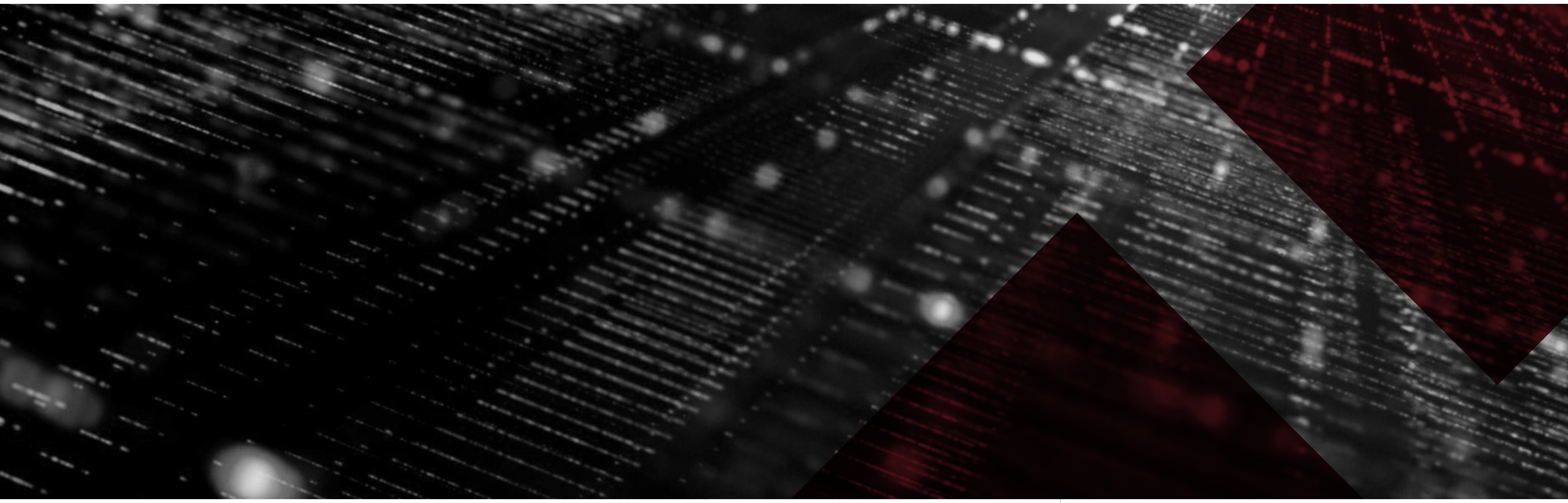
24h IDS Events: 10.10.3.231,0.0.0.0

Investigation: This table shows the top IDS events generated by host: **10.10.3.231,0.0.0.0** over the past 24 hours.

sourcetype	signature	src	severity	category	action	count
pan:threat	Apache Struts ClassLoader Security Bypass Vulnerability	10.10.3.231	high	vulnerability	blocked	4
pan:threat	Apache Struts Content-Type Remote Code Execution Vulnerability	10.10.3.231	critical	vulnerability	blocked	4
pan:threat	Apache Struts2 Dynamic Method Invocation Remote Code Execution Vulnerability	10.10.3.231	critical	vulnerability	allowed	4
pan:threat	Apache Struts2 OGNL Remote Code Execution Vulnerability	10.10.3.231	critical	vulnerability	blocked	8
pan:threat	Bash Remote Code Execution Vulnerability	10.10.3.231	critical	vulnerability	blocked	8
pan:threat	Fortinet FortiOS SSL VPN Path Traversal Vulnerability	10.10.3.231	critical	vulnerability	allowed	2
pan:threat	Generic HTTP Cross Site Scripting Attempt	10.10.3.231	['high', 'medium']	vulnerability	['allowed', 'blocked']	23
pan:threat	HP OpenView Network Node Manager HTTP Request Parsing Command Execution Vulnerability	10.10.3.231	high	vulnerability	allowed	2
pan:threat	HTTP /etc/passwd Access Attempt	10.10.3.231	['critical', 'high']	vulnerability	blocked	22
pan:threat	HTTP Cross Site Scripting Attempt	10.10.3.231	medium	vulnerability	allowed	7

Firewall Connection Trend for: 10.10.3.231

This graphs shows Firewall activity by trending the volume of connections generated over the past 7 days for host: 10.10.3.231. Large spikes indicate an increase in activity relative to the rest of the week.



Evaluate MSSPs with 3 Investment-Optimizing Questions

✓ Do you provide assessments, testing, and re-testing before choosing technologies?

Red team operations and penetration testing and re-testing using real-world adversary tradecraft to assess an organization's security posture is an integral part of identifying areas of improvement. Before making recommendations on what people, processes, and technologies are needed, MSSPs should do their due-diligence to get to know your unique environment so that budget is not wasted on superfluous or ineffective investments.

✓ Do you use threat modeling?

One area of differentiation between providers is their threat intelligence and active threat hunting services. To reduce risk and improve cyber ROI, organizations need to shift from reactive to proactive security. For many enterprises, dedicating in-house staff to this is not possible as they are consumed by alert investigation. Instead, organizations can lean on MSSPs to provide systemic and structured processes through threat modeling to anticipate cyber attacks. Using frameworks like MITRE ATT&CK, plus methodologies and tools, providers are better suited to identify, quantify, and prioritize industry-specific threats.

✓ Do you use SOAR integration with automated workflows and playbooks?

Leveraging a SOAR platform saves resources, time, and talent with automated, pre-defined playbooks. Through the wide and deep integration of SOAR solutions, security programs benefit from efficiencies of improved detection, notification and response times, standardized processes, and enhanced content development across verticals and geographies.

Service Delivery: Find the Best Fit

Beyond evaluating MSSPs on the key criteria we've outlined, the final, and potentially most important factor you will need to judge providers on is their service delivery.

There are three common models that range in flexibility:

Black Box

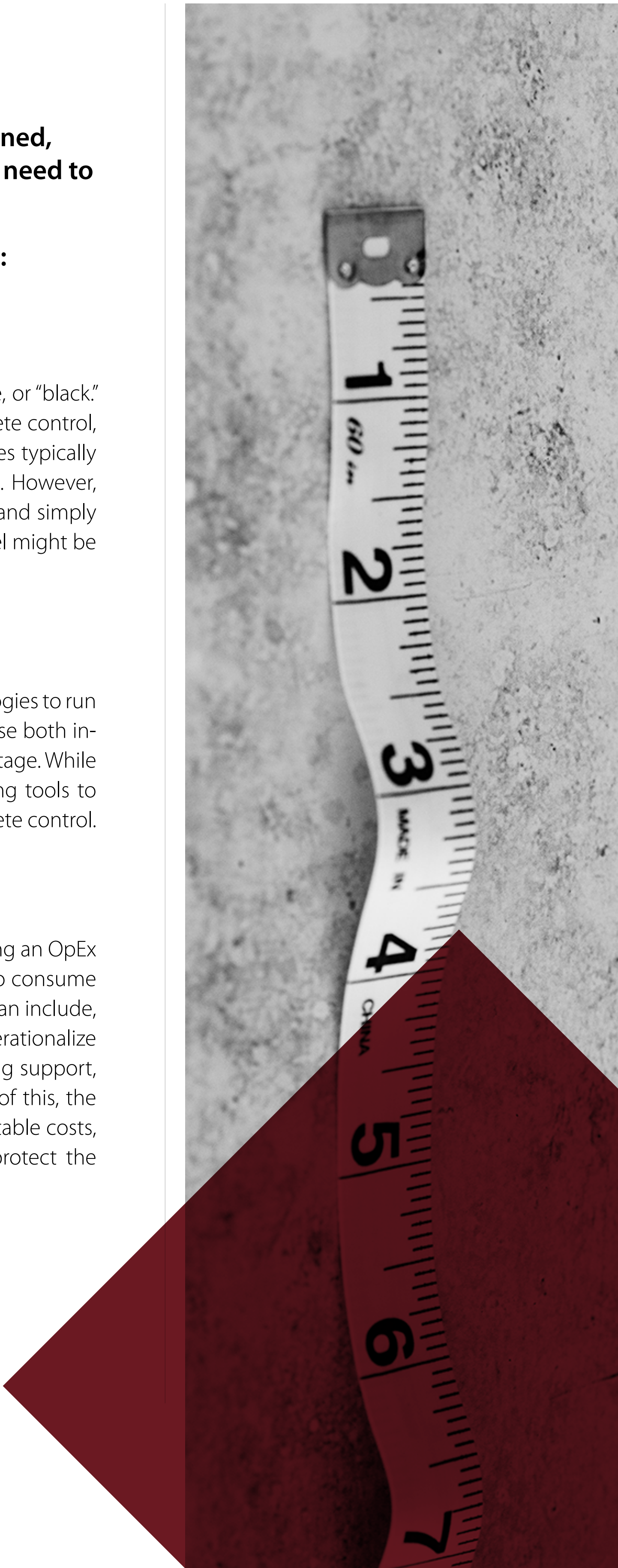
Black Box implementation gets its name from being opaque, or "black." Meaning, the MSSP provides the technology and has complete control, while the customer remains hands-off. These days, enterprises typically want more visibility into their data than black box provides. However, if the in-house team is less concerned about access to logs and simply wants to be updated on events, this hands-off delivery model might be the right fit.

Co-Managed

In a co-managed model, the MSSP uses your existing technologies to run the defined security operations. This can be a great way to use both in-house and outsourced cybersecurity resources to your advantage. While the MSSP maximizes the capital expenses and aligns existing tools to better fit your security program, the enterprise retains complete control.

Fully-Hosted

The final service delivery model takes a holistic approach using an OpEx model to provide tool, license, and service under one easy to consume service. Depending on the needs of the enterprise, services can include, VMS, SIEM, MDR, Threat, and SOAR. While the MSSP can operationalize the entire service, from planning and deployment to ongoing support, customers still have full access to the tools in use. Because of this, the scenario has grown in popularity. Enterprises favor its predictable costs, flexibility, as well as access to best-of-breed products to protect the entire infrastructure.



Why Herjavec Group?

For over 16 years, Herjavec Group has defended global enterprises with industry-leading expertise, disciplined processes, forward looking development, and a personalized approach to ensure mutual success. Our integrated, measurable, and threat-centric service portfolio has evolved to become the most holistic offering on the market, spanning Advisory, Professional Services, Managed Services, Identity and Access Management, Digital Forensics and Incident Response.

> Herjavec Group is the rare MSSP that has diversified across consulting, professional services, identity, incident response, and more. Through ongoing investments in talent and R&D, the company consistently ranks among the world's most trusted Managed Security Services Providers.
>
> - Joe Panettieri, Executive VP and Co-Founder of MSSP Alert

We pride ourselves on our customer-centric approach —offering flexible delivery models and a 100% cybersecurity-focused, vendor-agnostic team to ensure the enhancement of our customers' individualized security programs. Supported by 5 global SOCs, we offer 24/7 expert-level threat detection and proactive response to sophisticated threats

To ensure an ongoing, high-level of support, our MSS practice is built on a continuous improvement feedback loop. Recognizing that threats and security programs are always in flux, we are constantly striving improve and accelerate security programs through tuning, assessing, and reporting, and implementing what is right for our customers' environments.

Recognized Industry-Wide

MARKET LEADER IN MSS

CDM CYBER DEFENSE MAGAZINE GLOBAL INFOSEC AWARDS

4 ON THE

MSSP Alert TOP 250 MSSPs

SECURITY SERVICES LEADER

IDC Analyze the Future

MARKET LEADER IN IAM

CDM CYBER DEFENSE MAGAZINE GLOBAL INFOSEC AWARDS

MOST INNOVATIVE SECURITY COMPANY OF THE YEAR

CDM CYBER DEFENSE MAGAZINE GLOBAL INFOSEC AWARDS

F1™

HERJAVEC GROUP

Official Cyber Security Services Provider of Formula 1®

MANAGED SERVICES	24/7 SOC Operations	Managed Detection Response	Security Technology Engineering	Threat Hunting	Digital Forensics & Incident Response
PROFESSIONAL SERVICES	Executive Office of the CISO	Advisory Services	Architecture & Implementation	Identity & Access Management	Assessments & Testing