The 2018 Managed Security Report is based on the results of a comprehensive online survey of IT and cybersecurity professionals conducted in July and August of 2018.

The report reveals the latest trends and attitudes towards managed security, answering why organizations invest in security outsourcing, what challenges they are facing, and what requirements companies are prioritizing.

Faced with challenges such as the persistent cybersecurity skills gap, lack of 24x7 security coverage, increasing security threat pressure, and the cost and complexity of in-house security operations, many organizations are turning to outsourcing of cybersecurity processes and systems.

Popular managed security services include security monitoring, threat detection and response, security systems management and orchestration, and threat hunting - all working in concert to help organizations protect their data and systems, safeguard investments, and meet compliance regulations.

We would like to thank AlienVault, an AT&T company, for supporting this unique research.

We hope you will enjoy the report.

Thank you,

Holger Schulze
Organizations continue to struggle with the security skills gap. More than half of the respondents (55%) said a shortage of cybersecurity skills in-house is the biggest security operations challenge. This is followed by a lack of 24x7 security coverage (42%), slow speed of incident response (32%), and the cost and complexity of building in-house teams (32%).

What are the biggest security operations challenges for your IT organization?

- Cybersecurity skills shortage in-house: 55%
- Lack of 24x7 security coverage: 42%
- Speed of incident response issues: 32%
- Cost and complexity of building in-house: 32%
- Lack of detection and response capabilities: 30%
- No visibility into overall security posture: 30%

Speed of deployment and provisioning issues 22%  |  Lack of customization of correlation rules and reports 13%  |  Not able to meet compliance requirements 12%  |  None 3%  |  Not sure/Other 17%
Most organizations (58%) are still sourcing their security operations programs in-house. Increasingly popular sourcing alternatives include a hybrid of in-house and outsourced services (16%), outsourcing to a managed security service provider (12%), and outsourcing to a managed threat detection and response provider (5%).

How is your security operations program currently sourced?

<table>
<thead>
<tr>
<th>Source of Security Operations</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>In-house</td>
<td>58%</td>
</tr>
<tr>
<td>Hybrid of in-house and outsourced</td>
<td>16%</td>
</tr>
<tr>
<td>Outsourced to a managed security service provider</td>
<td>12%</td>
</tr>
<tr>
<td>Outsourced to managed threat detection and response provider</td>
<td>5%</td>
</tr>
<tr>
<td>No security program in place</td>
<td>8%</td>
</tr>
<tr>
<td>Not sure/Other</td>
<td>1%</td>
</tr>
</tbody>
</table>
Only 36% of organizations are on the confident end of their in-house security team’s ability to keep up with threats by maintaining the right security skills and competencies. The remaining 64% - and majority of organizations - are at best somewhat confident their in-house security operations can keep up with today’s evolving threat.

If you are currently NOT outsourcing security operations to a third-party service provider, how confident are you that your organization can keep up with today's evolving threats by maintaining the right skills?

64% of organizations not currently outsourcing security operations are, at best, somewhat confident.
DRIVERS FOR MANAGED SECURITY

Organizations not currently using managed security say a number of factors would drive them to sign up for a managed service. These include a lack of internal security personnel/expertise (47%), desire to move to 24x7 security coverage (44%), cost savings (42%), breach protection (33%), need for faster response to incidents (32%), and a lack of security domain expertise in-house (30%).

If you’re NOT currently using a managed security service provider, what would drive you to sign up for a managed service?

- Lack of internal security personnel/expertise: 47%
- Moving to 24x7 security coverage: 44%
- Cost savings: 42%
- Breach Protection: 33%
- Speed of response to incidents: 32%
- Lack of security domain expertise in-house: 30%
- Meeting regulatory compliance mandates: 26%
Of the organizations not currently outsourcing security management to a third-party service provider, nearly 40% say they are either likely or very likely to do so within the next 12 months. On the other hand, only 29% said they are unlikely or very unlikely to do so.

If you are NOT currently outsourcing security management to a third-party service provider, how likely are you to do so in the next 12 months?

- Very Unlikely: 15%
- Likely: 14%
- Very Likely: 39%

Likely or very likely to outsource security to a services provider 39%
When asked what managed security services organizations would consider outsourcing to a security service provider, two-thirds of the respondents said monitoring and threat detection. Other security services considered suitable for outsourcing include compromise assessment/forensics (59%), incident response (56%), endpoint protection (49%), network protection (46%), perimeter protection (45%), and application protection (42%).

**What managed security services would you consider outsourcing to a security service provider?**

- **Monitoring & threat detection**: 66%
- **Compromise assessment/forensics**: 59%
- **Incident response**: 56%
- **Endpoint protection**: 49%
- **Network protection**: 46%

Perimeter protection 45% | Application protection 42%
The most commonly outsourced advisory service is penetration testing (77%). Others include security assessment (66%), cyber exercises/red team operations (58%), education and training programs (42%), and compliance (36%).

What security advisory services would you consider outsourcing to a security service provider?

- Penetration testing: 77%
- Security assessment: 66%
- Cyber exercises/red team operations: 58%
- Education/training programs: 42%
- Compliance: 36%

Not sure/Other: 3%
Expected Savings from Outsourcing

Organizations not currently outsourcing security operations to a third-party service provider have a range of expectations with regard to anticipated time and cost savings from outsourcing. The most frequently selected response ranges from 10% to 25% in cost savings from outsourcing security operations.

If you are currently NOT outsourcing security operations to a third-party service provider, what is your organization’s expectation for time and cost savings?

- 45%: More than 75%
- 27%: 51-75%
- 6%: 26-50%
- 15%: 10-25%
- 7%: Less than 10%
MANAGED SECURITY BENEFITS

Organizations are reporting a number of benefits from outsourcing their security operations to third-party service providers. The most common benefit is more flexible capacity and scalability, cited by 24% of the respondents. Other benefits include reduced cost and complexity (21%), improved security and quality of protection (19%), improved regulatory compliance (18%), and accelerated deployment and provisioning (16%).

If you are currently outsourcing security operations to a third-party service provider, what benefits have you realized?

- More flexible capacity/scalability: 24%
- Reduced cost and complexity: 21%
- Improved security and quality of protection: 19%
- Improved regulatory compliance: 18%
- Accelerated deployment and provisioning: 16%

Improved performance 15% | Increased efficiency of incident response 15% | Increased agility 15% | Increased geographic reach 14% | Increased employee productivity 13% | Better customization to meet my needs 10% | Aligned cost model with usage 5% | Not sure/Other 15%
Managed security is not a panacea - using third-party service providers for security operations can also present a number of challenges for organizations. At the top of the list, by a wide margin, are cost issues, cited by 37% of the respondents. That was followed by efficiency issues (21%), lack of integration (18%), and lack of agility issues (17%). Nearly one quarter of the organizations (23%) report having no challenges with security service providers.

If you are currently outsourcing security operations to a third-party service provider, what challenges are you experiencing with that arrangement?

- Cost issues: 37%
- Efficiency issues: 21%
- Lack of integration: 18%
- Agility issues: 17%
- Performance issues: 16%
- Security posture issues: 15%
- Availability and business continuity issues: 15%

Flexibility/scalability issues: 13%  |  Speed of deployment and provisioning issues: 12%  |  Regulatory compliance issues: 11%  |  Complexity issues: 11%  |  Geographic reach issues: 10%  |  Employee productivity issues: 8%  |  Time to market issues: 6%  |  Not sure/Other: 12%
MSSP SELECTION FACTORS

A variety of factors go into selecting the right managed security services provider (MSSP). The most important, according to 61% of the respondents, is 24/7 coverage of security operations. Other important criteria include cost and complexity (53%), expertise of security analysts (52%), competence in threat detection and incident response (41%), and the stability and reputation of the company (40%).

What factors are most important to you when selecting a managed security services provider (MSSP)?

- 24x7 coverage of security operations: 61%
- Cost and complexity: 53%
- Expertise of security analysts: 52%
- Competence in threat detection and incident response: 41%
- Stability and reputation of company: 40%
- Ability to integrate/leverage our security technology stack: 37%
- Flexibility: 34%
- Analyst experience: 34%
- Breadth of capabilities: 33%
- Ability to offer customized approach: 30%
- Business and vertical domain expertise: 27%
- Ability to customize compliance reporting: 21%
- Turnkey solution: 18%
- Location/Proximity: 18%
- Leadership: 13%
- Company size: 9%
- Not sure/Other: 2%
Managed security capabilities hold different levels of value for organizations. Deemed most valuable is rapid identification and remediation of attacks (77%). Other prioritized capabilities include 24x7 monitoring and analysis (75%), security posture reports to identify vulnerabilities and risks (67%), security policy and controls management (56%), and ensuring regulatory compliance (45%).

How valuable are the following managed security capabilities?

- **Rapid identification and remediation of attacks**: 77%
- **24x7 monitoring and analysis**: 75%
- **Security posture reports to identify vulnerabilities and risks**: 67%
- **Security policy and controls management (firewall, IPS management)**: 56%
- **Ensuring regulatory compliance**: 45%

Not sure/Other 1%
Security information and event management (SIEM) is one of the most important capabilities an MSSP needs to provide, according to about two-thirds of the respondents (65%). Other important capabilities include alerting, event correlation, and management (64%), network monitoring (62%), threat hunting (52%), security orchestration, automation and response (50%), intrusion detection and intrusion prevention systems (42%), and endpoint monitoring (41%).
Flat, all-inclusive pricing is the most attractive model for 8 out of 10 organizations. The most attractive pricing model for organizations is a multi-year, flat, all-inclusive contract (41%). Next was an annual, flat, all-inclusive contract (36%) followed by consumption-based pricing (23%).

What MSSP pricing model would be most attractive to your organization?

- Multi-year, flat, all-inclusive contract: 41%
- Annual, flat, all-inclusive contract: 36%
- Consumption-based pricing: 23%
Organizations will be investing more in managed services over the next year. More than half of the respondents (53%) said their budget for managed security will increase by an average of 14% over the next 12 months.

How is your budget for managed security changing over the next 12 months?

- 53% Budget will increase
- 38% Budget will stay the same
- 9% Budget will decrease
Eight of 10 organizations allocate 25% or less of their security budgets to managed security.

If you are using a mix of in-house and managed security service providers, what percentage of your security budget is allocated for managed security services?

- 33% of respondents allocated 1-15% of their security budget to managed security services.
- 29% allocated 16-25%.
- 14% allocated 26-50%.
- 6% allocated 51-75%.
- 1% allocated more than 75%.
AlienVault®, an AT&T Company, has simplified the way organizations detect and respond to today’s ever evolving threat landscape. Our unique and award-winning approach, trusted by thousands of customers, combines the essential security controls of our all-in-one platform, AlienVault Unified Security Management®, with the power of AlienVault’s Open Threat Exchange®, the world’s largest crowd-sourced threat intelligence community, making effective and affordable threat detection attainable for resource constrained IT teams.

www.alienvault.com
This report is based on the results of a comprehensive online survey of 385 IT and cybersecurity professionals conducted in July and August of 2018. It reveals the latest trends and attitudes towards managed security, answering why organizations invest in security outsourcing, what challenges they are facing, and what requirements companies are prioritizing. The respondents range from technical executives to senior managers and IT security practitioners, across the spectrum of company sizes and industries, representing a balanced cross-section of organizations.