Abstract:
Cybersecurity Analytics and Operations in Transition

Challenges, Plans, Successes, and Strategies

By Jon Oltsik, ESG Senior Principal Analyst
July 2017
Introduction

Research Objectives

In order to assess organizations’ cybersecurity analytics and operations plans, successes, and struggles, ESG surveyed 412 IT and information security professionals representing mid-market (500 to 999 employees) and enterprise-class (more than 1,000 employees) organizations in North America and Western Europe. All respondents were involved in the planning, implementation, and/or daily operations of their organization’s security analytics and operations.

The survey and overall research project were designed to answer the following questions:

- How are enterprise organizations doing security analytics today? Are they building SOCs? If so, how?
- What challenges do organizations face with security analytics?
- Do organizations have the right skills and personnel for security analytics?
- How are cybersecurity analytics requirements changing? What’s driving these changes?
- What role does SIEM play for security analytics today and in the future?
- What other cybersecurity analytics technologies are enterprises researching, testing, piloting, or deploying?
- How are organizations integrating threat intelligence with their cybersecurity analytics strategies?
- Are organizations deploying host- and network-based security analytics tools? If so, are these used independently or as part of a more integrated cybersecurity analytics architecture?
- What is the relationship between cybersecurity analytics and incident response automation and orchestration?
- How do these requirements vary by company size and industry?
- Are organizations using professional and/or managed services as part of their cybersecurity analytics strategy? If so, for what purposes?
- Are organizations building a cybersecurity analytics architecture? If so, what are the piece parts and how do they come together?
Research Methodology

To gather data for this report, ESG conducted a comprehensive online survey of IT and information security professionals responsible for/familiar with their organization’s cybersecurity analytics and operations processes, technologies, and strategies in North America (United States and Canada) and Western Europe (United Kingdom and Germany) between March 27, 2017 and April 7, 2017. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 412 IT and information security professionals.

Please see the Respondent Demographics section of this report for more information on these respondents.

Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.
Respondent Demographics

The data presented in this report is based on a survey of 412 qualified respondents. Figures 1-5 detail the demographics of the respondent base.

Respondents by Current Responsibility

Respondents’ current responsibility in shown in Figure 1.

**Figure 1. Respondents by Role**

Which of the following best describes your current responsibility within your organization? (Percent of respondents, N=412)

- Security management, 1%
- Security staff, 1%
- Cybersecurity analysis and/or operations (i.e. security analyst, threat intelligence analyst, forensic investigator, etc.), 1%
- Senior security management (e.g., CSO, CIO, VP-level, Director-level), 7%
- IT staff, 4%
- IT management (e.g., Director of IT), 39%
- Senior IT management (e.g., CIO, VP of IT, etc.), 47%

Source: Enterprise Strategy Group, 2017

Respondents by Number of Employees

The number of employees in respondents’ organizations is shown in Figure 2.

**Figure 2. Respondents by Number of Employees Worldwide**

How many total employees does your organization have worldwide? (Percent of respondents, N=412)

- 2,500 to 4,999, 15%
- 5,000 to 9,999, 24%
- 10,000 to 19,999, 12%
- 1,000 to 2,499, 23%
- 500 to 999, 12%
- 20,000 or more, 13%
- 5,000 to 9,999, 24%
- 10,000 to 19,999, 12%
- 1,000 to 2,499, 23%
- 500 to 999, 12%
- 20,000 or more, 13%

Source: Enterprise Strategy Group, 2017
Respondents by Industry

Respondents were asked to identify their organization’s primary industry. In total, ESG received completed, qualified respondents from individuals in 19 distinct vertical industries, plus an “Other” category. Respondents were then grouped into the broader categories shown in Figure 3.

**Figure 3. Respondents by Industry**

![Pie chart showing the distribution of respondents by industry.]

- **Manufacturing**: 24%
- **Financial (banking, securities, insurance)**: 17%
- **Retail/Wholesale**: 15%
- **Health Care**: 7%
- **Government (Federal/National, State/Local)**: 7%
- **Transportation & Logistics**: 6%
- **Business Services (accounting, consulting, legal, etc.)**: 8%
- **Consumer Packaged Goods**: 5%
- **Education**: 5%
- **Other**: 6%

**What is your organization’s primary industry? (Percent of respondents, N=412)**

Source: Enterprise Strategy Group, 2017

Respondents by Annual Revenue

Respondent organizations’ annual revenue is shown in Figure 4.

**Figure 4. Respondents by Annual Revenue**

![Bar chart showing the distribution of respondents by annual revenue.]

<table>
<thead>
<tr>
<th>Revenue Range</th>
<th>Percent of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than $25 million</td>
<td>1%</td>
</tr>
<tr>
<td>$25 million to $49.999 million</td>
<td>2%</td>
</tr>
<tr>
<td>$50 million to $99.999 million</td>
<td>4%</td>
</tr>
<tr>
<td>$100 million to $499.999 million</td>
<td>18%</td>
</tr>
<tr>
<td>$500 million to $999.999 million</td>
<td>19%</td>
</tr>
<tr>
<td>$1 billion to $4.999 billion</td>
<td>23%</td>
</tr>
<tr>
<td>$5 billion to $9.999 billion</td>
<td>18%</td>
</tr>
<tr>
<td>$10 billion to $19.999 billion</td>
<td>7%</td>
</tr>
<tr>
<td>$20 billion or more</td>
<td>6%</td>
</tr>
<tr>
<td>Not applicable (e.g., public sector, non-profit)</td>
<td>3%</td>
</tr>
</tbody>
</table>

Source: Enterprise Strategy Group, 2017
Respondents by Region

Geographic region in which respondents’ organizations operate is shown in Figure 5.

Figure 5. Respondents by Region

Respondents by region. (Percent of respondents, N=412)

- Western Europe, 39%
- North America, 61%

Source: Enterprise Strategy Group, 2017
Contents

List of Figures .......................................................................................................................................................................... 3
Executive Summary ................................................................................................................................................................. 4
    Report Conclusions .......................................................................................................................................................... 4
Introduction ............................................................................................................................................................................ 6
    Research Objectives ..................................................................................................................................................... 6
Research Findings ............................................................................................................................................................. 7
    The Current Cybersecurity Analytics and Operations Landscape ................................................................. 7
    Cybersecurity Operations Staffing and Skills ................................................................................................. 12
    Security Analytics and Operations Technology .......................................................................................... 14
Moving Toward a Security Operations and Analytics Platform Architecture (SOAPA) .................................................... 16
    Operationalizing Threat Intelligence ................................................................................................................... 17
    Automation and Orchestration ............................................................................................................................. 19
    Artificial Intelligence ........................................................................................................................................ 20
Future Security Analytics and Operations Plans ............................................................................................................... 22
Conclusion ............................................................................................................................................................................. 24
    Recommendations for Cybersecurity Professionals .................................................................................. 24
    Recommendations for Cybersecurity Vendors ........................................................................................... 26
Research Methodology ......................................................................................................................................................... 28
Respondent Demographics ................................................................................................................................................... 29
    Respondents by Current Responsibility ........................................................................................................ 29
    Respondents by Number of Employees ............................................................................................................ 29
    Respondents by Industry .................................................................................................................................. 30
    Respondents by Annual Revenue ....................................................................................................................... 30
    Respondents by Region ..................................................................................................................................... 31
List of Figures

Figure 1. Cybersecurity Analytics and Operations Climate: Today versus 24 Months Ago ................................................................. 8
Figure 2. Reasons Security Analytics and Operations Has Gotten More Difficult .............................................................................. 9
Figure 3. Security Analytics and Operations Objectives ...................................................................................................................... 10
Figure 4. Security Analytics and Operations Challenges .................................................................................................................. 11
Figure 5. Size and Skillsets of Security Analytics and Operations Staff .............................................................................................. 12
Figure 6. Plans for Recruiting or Hiring Security Analytics and Operations Staff .................................................................................. 13
Figure 7. Ability to Recruit or Hire Security Analytics and Operations Staff ....................................................................................... 13
Figure 8. Total Security Data Collected Monthly ............................................................................................................................... 14
Figure 9. Total Products and Services Used to Support Security Analytics and Operations Efforts ......................................................... 15
Figure 10. Types of Products and Services Used to Support Security Analytics and Operations Efforts .............................................. 15
Figure 11. Security Analytics and Operations Integration Approaches .................................................................................................. 16
Figure 12. Security Analytics and Operations Integration Efforts ......................................................................................................... 17
Figure 13. Threat Intelligence Program Objectives ............................................................................................................................ 18
Figure 14. Priorities for Security Analytics and Operations Automation and Orchestration ............................................................. 20
Figure 15. Supporting Security Analytics and Operations with Machine Learning ........................................................................... 21
Figure 16. Security Analytics and Operations Spending Plans ........................................................................................................... 22
Figure 17. Security Analytics and Operations Plans ............................................................................................................................... 23
Figure 18. Respondents by Role ....................................................................................................................................................... 29
Figure 19. Respondents by Number of Employees Worldwide ............................................................................................................. 29
Figure 20. Respondents by Industry .................................................................................................................................................... 30
Figure 21. Respondents by Annual Revenue .......................................................................................................................................... 30
Figure 22. Respondents by Region .................................................................................................................................................... 31