SANS 2017
SOC Survey
“A Mile of Numbers and a Ton of Stats”

Christopher Crowley
twitter: @CCrowMontance
All Rights Reserved
All Wrongs Reversed
Two Webcasts

- There are two webcasts covering additional aspects of the survey
- Links to those, and the slides for this presentation are at https://bit.ly/crow-soc
- Survey was sponsored by: Carbon Black, Endgame, LogRhythm, NETSCOUT, ThreatConnect, and Tripwire
SOC - Functional Areas

- Steering Committee
- Control Center
- Network Security Monitoring
- Threat Intelligence
- Incident Response
- Forensics
- Self Assessment
SOC - Process Elements

- Inputs
- People
- Technology
- Process
- Artifacts
Caveat Auditor – Survey, not Statistics

- Population size of SOCs globally is not known
- Sample size determination not performed
- Data set example:
  - 38 Respondents from Banking and Finance
  - 11 Respondents from Retail
- Nonetheless, 298 respondents shared their info, so we’ll dig into what we have
The respondents self-identified as being in a particular sector.

I’m going to discuss this, but it is not intended to be a statistically significant representation of that sector as a whole, just the people who responded to this survey.

I’d love to get to the point that we reach data saturation.

Saturation can be simply defined as data satisfaction. It is when the researcher reaches a point where no new information is obtained from further data.
Demographics

- Most of the respondents were from US based companies
  - **54%** listed headquarters in US
  - **21%** European headquarters
- Worldwide operations cited
  - **Cyber & banking** were top industries
- Typical SANS survey respondents are from **government & finance**
Primarily Centralized Architecture

- Centralized into a single SOC center
- Functions in different departments
- Centralized and distributed regionally
- Partial SOCs in regional locations
- Full SOCs distributed regionally
- Some functions multiple cloud providers
- Single cloud provider - all functions
- Multiple cloud providers - all functions
- Single cloud provider - some functions
- Other
Outsourced Components

- 44%—Threat research
- 38%—Digital forensics
- 35%—Security monitoring and detection
- 33%—eDiscovery and legal evidence collection
Further Comparison

• With available survey data, I drilled into some sector-specific (Q2) aspects of the survey results relating to Q10:
  • What activities are you handling in-house? What activities have you outsourced, either totally or in part, to outside services through a managed security service provider (MSSP) or in the cloud? Check only those that apply to your organization
Threat Research Outsourcing by Sector  n=249

- If outsourced, two types:
  - Likely both
    - Cyber, banking, tech
  - Outsource only
    - Gov, Insurance, Utilities

<table>
<thead>
<tr>
<th>Sector</th>
<th>In-House</th>
<th>Outside Services (MSSP, Cloud)</th>
<th>Both</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber security</td>
<td>21</td>
<td>3</td>
<td>15</td>
</tr>
<tr>
<td>Banking and finance</td>
<td>19</td>
<td>5</td>
<td>14</td>
</tr>
<tr>
<td>Technology</td>
<td>12</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>Government</td>
<td>18</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>Insurance</td>
<td>8</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>Utilities</td>
<td>6</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>7</td>
<td>6</td>
<td>5</td>
</tr>
<tr>
<td>Healthcare</td>
<td>8</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>Education</td>
<td>5</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Transportation</td>
<td>2</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>Telecommunications/ISP</td>
<td>7</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>Retail</td>
<td>8</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Hospitality</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Media</td>
<td>5</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Nonprofit/Association</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Thoughts on Threat Intelligence

• I think it *can be* useful. But first:
  • Does org have routine IR handling in the SOC?
• The counterpoint is: what does the org do differently if “Country Cyberforce X” is attacking me versus “Financial Actor B” versus “Amorphous Social Faction 7”?
• Can the org differentiate the threat actor early enough to make a difference?
Digital Forensics Outsourcing by Respondent Sector
n=248

- Overall percentage outsourced is 38% (see slide 7)
- Raw count is interesting, but next slide has more about the likelihood of an industry to outsource
Digital Forensics Outsourcing (sorted by low ratio) by Respondent Sector n=248

- Retail (10%), Government (15%) & Cyber Security (24%), Education (33%) unlikely to outsource partially or wholly
- Outsourced (all or partial) / count responses

<table>
<thead>
<tr>
<th>Sector</th>
<th>In-House</th>
<th>Outside Services (MSSP, Cloud)</th>
<th>Both</th>
<th>(Out+Both) / Sum(all)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retail</td>
<td>10</td>
<td>0</td>
<td>1</td>
<td>0.09091</td>
</tr>
<tr>
<td>Government</td>
<td>22</td>
<td>3</td>
<td>1</td>
<td>0.15385</td>
</tr>
<tr>
<td>Cyber security</td>
<td>31</td>
<td>4</td>
<td>6</td>
<td>0.2439</td>
</tr>
<tr>
<td>Education</td>
<td>8</td>
<td>1</td>
<td>3</td>
<td>0.33333</td>
</tr>
<tr>
<td>Insurance</td>
<td>11</td>
<td>3</td>
<td>4</td>
<td>0.38889</td>
</tr>
<tr>
<td>Utilities</td>
<td>7</td>
<td>1</td>
<td>5</td>
<td>0.46154</td>
</tr>
<tr>
<td>Technology</td>
<td>17</td>
<td>7</td>
<td>8</td>
<td>0.46875</td>
</tr>
<tr>
<td>Media</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0.5</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>9</td>
<td>4</td>
<td>7</td>
<td>0.55</td>
</tr>
<tr>
<td>Telecommunications/ISP</td>
<td>6</td>
<td>3</td>
<td>5</td>
<td>0.57143</td>
</tr>
<tr>
<td>Healthcare</td>
<td>5</td>
<td>2</td>
<td>5</td>
<td>0.58333</td>
</tr>
<tr>
<td>Banking and finance</td>
<td>14</td>
<td>13</td>
<td>8</td>
<td>0.83333</td>
</tr>
<tr>
<td>Transportation</td>
<td>1</td>
<td>0</td>
<td>5</td>
<td>0.83333</td>
</tr>
<tr>
<td>Hospitality</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Nonprofit/Association</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
Thoughts on Digital Forensics

• First, on nomenclature, I differentiate Forensics from analysis performed during Incident Response:
  • The Forensic task is a deep dive assessment of materials to answer specific questions. IR forensics analysis is initial, triage based, and partial analysis due to limited time and scope. Forensics is focused, exhaustive (within the scope of the question) and produces authoritative analysis.
• You’re welcome to disagree with my usage, but that’s how I’m using these words currently.
Thoughts on Digital Forensics

• Interesting that Retail shows less likelihood to outsource forensics than Cyber companies (experts) and Government
  • (more on Retail on next slides)

• Education – I suspect this is simply a cost issue

• Insurance, Utilities, Technology, Media, Manufacturing – I am surprised how many keep it insourced
Digression on Retail

- **Retail** shows less likelihood to outsource forensics than **Cyber** companies (experts) and **Government**
  - Most likely a low sample size issue with not having a representative population
- What those respondents outsource?
- Turns out, not much (next slide)
- Most commonly outsourced is “Security Monitoring and Detection”
Retail Respondents – little outsourcing

Security monitoring and detection
Threat research
Remediation
Incident response
Compliance support
Security architecture and engineering
Security administration
Security roadmap and planning
eDiscovery and legal evidence collection
Digital Forensics

Sort: sum(out+both), out, both, in
Security Monitoring and Detection
n=264

- Government, Tech, Cyber, Education, Telecom, Retail not likely to outsource security monitoring
- I considered doing (out+both) / (in+both) – might be a better comparison

<table>
<thead>
<tr>
<th>Industry</th>
<th>In-House</th>
<th>Outside Services (MSSP, Cloud)</th>
<th>Both</th>
<th>(Out+Both) / Sum(all)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government</td>
<td>23</td>
<td>0</td>
<td>6</td>
<td>0.2069</td>
</tr>
<tr>
<td>Technology</td>
<td>25</td>
<td>3</td>
<td>5</td>
<td>0.24242</td>
</tr>
<tr>
<td>Cyber security</td>
<td>31</td>
<td>4</td>
<td>7</td>
<td>0.2619</td>
</tr>
<tr>
<td>Education</td>
<td>8</td>
<td>0</td>
<td>3</td>
<td>0.27273</td>
</tr>
<tr>
<td>Telecommunications/ISP</td>
<td>11</td>
<td>2</td>
<td>3</td>
<td>0.3125</td>
</tr>
<tr>
<td>Retail</td>
<td>7</td>
<td>2</td>
<td>2</td>
<td>0.36364</td>
</tr>
<tr>
<td>Utilities</td>
<td>8</td>
<td>1</td>
<td>5</td>
<td>0.42857</td>
</tr>
<tr>
<td>Insurance</td>
<td>10</td>
<td>1</td>
<td>7</td>
<td>0.44444</td>
</tr>
<tr>
<td>Banking and finance</td>
<td>22</td>
<td>5</td>
<td>13</td>
<td>0.45</td>
</tr>
<tr>
<td>Healthcare</td>
<td>8</td>
<td>2</td>
<td>5</td>
<td>0.46667</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>11</td>
<td>3</td>
<td>7</td>
<td>0.47619</td>
</tr>
<tr>
<td>Media</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0.5</td>
</tr>
<tr>
<td>Transportation</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>0.66667</td>
</tr>
<tr>
<td>Hospitality</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Nonprofit/Association</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Thoughts on Security Monitoring and Detection

• Anecdotally, people tell me their companies outsource Tier 1 Network Security Monitoring (NSM)
  • Usually with tepid satisfaction, still done because of 24x7 requirements and staffing issues
• Personally, I think it is a great opportunity for efficiency if the org can define clear escalation use cases (from Service Provider) and have the same data in-house for tier 2+ analysis
  • Usually achievable only in mature SOCs
eDiscovery and Evidence Collection n=236

- Telecoms and Transportation likely to outsource in some way
- Retail, Edu, Cyber, Government unlikely to outsource
Thoughts on eDiscovery

- If you already have a legal team to do this, don’t fight to bring it into the SOC
  - If you don’t, this is something you should prepare to do for the organization
- Skillset and application is slightly different, technology (particularly if you have host agents already installed) is largely the same
  - I’ve used agent based forensic tools to conduct eDiscovery at scale
Additions and Improvements

• Please take time to share (tweet maybe) your thoughts about questions you’d like to include for next year
• I’m also interested in hearing about your SOC architecture, if you are permitted to share
Summary

• SOC survey with ~300 respondents
• Looking forward to future insight
• Interested in anecdotes and case studies regarding your SOC

• Twitter: @CCrowMontance