99% False Positives: A Qualitative Study of SOC Analysts' Perspectives on Security Alarms

Supplementary Material

BUSHRA ALAHMADI (UNIVERSITY OF OXFORD), LOUISE AXON (UNIVERSITY OF OXFORD), IVAN MARTINOVIC (UNIVERSITY OF OXFORD)

This supplementary document is provided for the USENIX Security'22 submission accepted paper titled: 99% False Positives: A Qualitative Study of SOC Analysts' Perspectives on Security Alarms.
It details the full survey questions used in the study as well as the survey participant information sheet and the written consent form used to obtain the interview participants consent.

1. SURVEY QUESTIONS

1. What is your job title? * Required
2. How many years' experience do you have in your role? * Required
   - 0-3
   - 3-5
   - 5-7
   - 7-10
   - 10-15
   - 15+
   - I prefer not to say
3. How would you rate your level of expertise in network-security monitoring?
   - Very low
   - Low
   - Medium
   - High
   - Very high
4. What is the type of organisation you work in? * Required
   - Government
   - Financial Services
   - Healthcare Providers
   - Higher Education
   - K-12
   - Technology (Non-security focus)
   - Technology (security focus)
   - Manufacturing
   - Media and Entertainment
   - Travel, Hospitality, and Transportation
   - Retail
   - Other
5. If you selected Other, please specify:
6. How would you describe the size of your organisation? * Required
   - Small enterprise
   - Medium enterprise
   - Large enterprise
   - I don't know

- Other

7. If you selected Other, please specify:

8. How many security analysts work in your organization's SOC? * Required

    - 1 - 9
    - 10 - 19
    - 20 - 29
    - 30 - 39
    - 40 - 49
    - 50 - 99
    - 100 - 199
    - 200 +
    - I prefer not to say

9. How many network monitoring devices (e.g., a single IDS, firewall) are you personally responsible for monitoring in the SOC you work in? * Required

    - 1
    - 2 - 4
    - 5 - 6
    - 7 - 8
    - 9 - 10
    - 11 - 12
    - 13- 14
    - 15 - 16
    - 17 - 18
    - 19 - 20
    - 21+
    - I don't know

10. How many network elements does a single monitoring device observe? Optional

11. In which country is the SOC you work in located? * Required

12. Which tasks are you required to carry out in your role? * Required

    - Monitor IDS
    - Monitoring network and systems logs
    - Track and trace intruders
    - Perform forensic evidence collection
    - Produce technical documents
    - Perform artifact analysis
    - Incident handling
    - Perform security policy development
    - Publish advisories or alerts
    - Perform virus handling
    - Provide and answer a hotline
    - Provide training and security awareness
    - Pursue legal investigations
    - Vulnerability handling
    - Security product development
    - Vulnerability scanning
    - Vulnerability assessments
    - Security configuration administration
    - Penetration testing
    - Other

13. If you selected Other, please specify:

14. How many network security alerts does your organization receive on average daily? * Required

    - Less Than 5K

- 5K–10K
- 10K–50K
- 50K–100K
- 100K–150K
- Over 150K
- I don't know
- Other

15. If you selected Other, please specify:

16. How many network security alerts does your organization investigate on average daily? Optional

17. Describe your usual SOC responsibilities: * Required

18. Approximately how many legitimate network security alerts does your organization remediate on average daily? Optional

19. Which of the following does your SOC mostly focus on? You may select more than one if Necessary* Required

    - Threat prevention
    - Threat detection
    - Threat remediation
    - Recovery
    - Other

20. If you selected Other, please specify:

21. What are the main network security threats your organisation faces? * Required

    - Denial of service attacks
    - Abnormal user activity
    - Scanning (reconnaissance e.g., port scans)
    - Unauthorised access attempts
    - Viruses, Worms, Trojans
    - Abnormal network activity
    - Ransomware
    - Advanced Persistent Threats (APTs)
    - Next-generation malware (e.g., Bots)
    - Phishing emails (including spear-phishing)
    - Brute-force attacks
    - Insider threats
    - Web defacement
    - Policy violation (e.g., gaming, streaming)
    - Other

22. If you selected Other, please specify:

23. Which of these network security incidents do your systems detect? * Required

    - Denial of service attacks
    - Abnormal user activity
    - Scanning (reconnaissance e.g., port scans)
    - Unauthorized access attempts
    - Viruses, Worms, Trojans
    - Abnormal network activity
    - Ransomware
    - Advanced Persistent Threats (APTs)
    - Next-generation malware (e.g., Bots)
    - Phishing emails (including spear-phishing)
    - Brute-force attacks
    - Insider threats
    - Web defacement
    - Policy violation (e.g., gaming, streaming)
    - Other

24. If you selected Other, please specify:

25. Which of the following network security incidents do you believe you could do better at addressing if you had the tools? * Required

    - Denial of service attacks
    - Abnormal user activity
    - Scanning (reconnaissance e.g., port scans)
    - Unauthorized access attempts
    - Viruses, Worms, Trojans
    - Abnormal network activity
    - Ransomware
    - Advanced Persistent Threats (APTs)
    - Next-generation malware (e.g., Bots)
    - Phishing emails (including spear-phishing)
    - Brute-force attacks
    - Insider threats
    - Web defacement
    - Policy violation (e.g., gaming, streaming)
    - Other

26. If you selected Other, please specify:

27. Which of the following network monitoring tools do you use? * Required

    - Intrusion Detection System (IDS) - signature-based (e.g Snort, Cisco Secure IDS)
    - Intrusion Detection System (IDS) - anomaly based (e.g., Spade)
    - Intrusion Detection System (IDS) - using machine learning
    - Data collection/ log aggregation (e.g., Splunk)
    - Security visualizations
    - Network monitoring (e.g., Argus, Bro)
    - Text-based data presentation (e.g., Wireshark/tcpdump, Nmap)
    - Information and Event Management (SIEM)
    - Policy management/profiling/posture assessment tool (e.g., Cisco ISE)
    - DNS Enforcer/Intelligent Proxy (e.g., Cisco Umbrella)
    - Other

28. If you selected Other, please specify:

29. If you selected Intrusion Detection System (IDS) - using machine learning or security visualizations in the previous question, please specify the tools used.

30. Which network security data sources do you monitor in your work? For each source you monitor, please indicate whether you monitor the source using a Security Incident and Event Management (SIEM) tool or individually. * Required (Options : Monitor using a SIEM , Monitor individually, Do not monitor , I don't know)

    - Firewall logs
    - Network packet captures
    - Netflow
    - Host logs
    - Server logs
    - IDS logs
    - IPS logs
    - Web proxy logs
    - Website logs
    - Antivirus logs
    - Anomaly detection alerts
    - Domain Name System (DNS) logs
    - Authentication logs

31. Are there any other network security data sources you monitor in your work that were not addressed in the question above? If so, please specify

32. How important are the following features in choosing an ideal network monitoring system? * Required (Options: Very unimportant, Unimportant, Neutral ,Important, Very important, I don't know).

- Cost of required storage
- Cost (money)
- Required processing power
- Number of false positives
- Number of false negatives
- Detection accuracy
- Cross-correlation of logs from different vendor sources (cross-vendor API compatibility)
- Data Visualizations
- Easy to setup/configure/maintain
- Customisable
- Speed in aggregating evidence/triaging events
- Open-source
- Compatibility with existing hardware
- Sophisticated alert management capabilities

33. Do you have any further comments on any of the topics covered on this page?

34. How important are the following data sources in detecting malicious activity on the network? * Required (Options: Very unimportant, Unimportant, Neutral, Important, Very important, I don't know)

    - Network traffic traces
    - Internal network traffic
    - IDS alert logs
    - IPS alert logs
    - Web proxies that log every outbound connection
    - DHCP servers that log dynamic IP address assignments
    - VPN servers that log remote connections to the enterprise network
    - Windows domain controllers that log authentication attempts within the corporate domain
    - Antivirus software that logs the results of malware scans on end hosts.
    - Network firewall
    - Data server logs
    - Anomaly detection logs
    - DNS logs
    - Security vulnerability mailing lists/blog announcements

35. Do you rely on other data sources we have missed? If yes, please specify them below.

36. How important are the following network traffic features in detecting malicious activity on the network? *Required (Options: Very unimportant, Unimportant, Neutral, Important, Very important, I don't know)

    - Source IP
    - Destination IP
    - Source port
    - Destination port
    - Protocol
    - Packet size
    - Byte size
    - Packet content
    - Destination domain URL
    - HTTP status code
    - Web referrer
    - Domain reputation
    - Domain category
    - User-agent string
    - Sent and received bytes
    - DNS response

37. Do you rely on other network features we have missed? If yes, please specify them below.

38. How important are the following Indicators of Compromise in detecting malicious activity on the network? *Required (Options: Very unimportant, Unimportant, Neutral, Important ,Very important, I don't know)

    - Unusual outbound network traffic (sudden spike in traffic)

- Anomalies in privileged user account activity
- Geographical irregularities
- Log-in red flags
- Swells in database read volume
- HTML response sizes
- Large numbers of requests for the same file
- Mismatched port-application traffic
- Suspicious registry or system file changes
- DNS request anomalies
- Unexpected patching of system
- Mobile device profile changes
- Bundles of data in the wrong places
- Web traffic with inhuman behavior
- Signs of DDoS activity
- Users' complaint of slow system

39. Do you rely on other Indicators of Compromise we have missed? If yes, please specify them below

40. How much do you rely on your experience in analyzing and aggregating data sources to detect malicious activity as apposed to relying on security monitoring system alerts? * Required

    - 1% - 10% of the time
    - 11% - 30% of the time
    - 31% -50% of the time
    - 51% - 70% of the time
    - 71% - 80% of the time
    - 81% - 100% of the time
    - I don't know

41. In what ways (if any) does your experience aid in network security monitoring tasks?

42. How do you choose the security alerts you process?

    - Affected subnet/business sector criticality
    - Random sampling
    - Based on problems faced recently
    - Based on awareness of normal network activity
    - New announced vulnerabilities in security blogs
    - Alert severity rating
    - Classifying malicious executables to a malware family
    - Other

43. If you selected Other, please specify:

44. Do you have any further comments on any of the topics covered on this page?

45. Network Monitoring Tools: Please indicate your level of agreement with the following assertions. * Required (Options: Strongly disagree, Disagree, Neutral, Agree, Strongly agree)

    - The monitoring tools I use frequently produce false positive results (they detect a security event when there was not actually a security event)
    - The monitoring tools I use frequently produce false negative results (they fail to detect a security event that occurs)
    - I sometimes rely on my experience and intuition to detect attacks rather than monitoring system alerts
    - I rely on my custom scripts to aggregate the data I need to analyze an incident
    - To detect malicious activity on the network I deploy custom created scripts

46. Intrusion Detection Systems: Please indicate your level of agreement with the following assertions. *Required (Options: Strongly disagree, Disagree, Neutral, Agree, Strongly agree)

    - I believe that current IDS are inadequate in detecting attacks
    - Current IDS solutions are incapable of coping with the high data rates
    - Current IDS solutions lack in effective and speedy threat detection and response
    - Current IDS solutions are built on the assumption that threats are observed as they enter the network in specific perimeter points at the Internet edge
    - The number of alerts generated by most IDS are overwhelming

- To reduce the number of false positives, I limit the IDS signature set to focus on important attacks
- I pick IDS alerts of interest based on problems we have been having lately

47. Data Presentation Tools: Please indicate your level of agreement with the following assertions. *Required (Options: Strongly disagree, Disagree, Neutral, Agree, Strongly agree)

    - Data presentation tools, such as visualizations, are important in my work
    - Data presentation tools such as visualizations can help me to detect incidents that are missed by the automated systems, or that do not fit the automated attack detection profile
    - Visualizations are useful for finding interesting patterns in raw network packet data
    - Visual distractions sometimes mean I miss important information that is conveyed visually

48. Do you have any further comments on any of the topics covered on this page?

49. The "Human in the Loop": Please indicate your level of agreement with the following assertions. * Required (Options: Strongly disagree, Disagree, Neutral, Agree, Strongly agree)

    - For my monitoring work, it is important that I maintain a continuous awareness of the network security state
    - It is important to have a "human in the loop" for the detection and preliminary analysis of potential security events - this process cannot be carried out by automated systems alone
    - Human analysts monitoring the network are capable of detecting network anomalies that are missed by automated systems
    - The monitoring setup I use enables me to detect network anomalies that are missed by automated systems
    - I am often required to make decisions on the accuracy of the alerts produced by automated systems
    - Maintaining awareness of the network security state is important in enabling me to make decisions on the accuracy of alerts produced by automated monitoring systems

50. Data Fusion: Please indicate your level of agreement with the following assertions. * Required (Options: Strongly disagree, Disagree, Neutral, Agree, Strongly agree)

    - In monitoring , I am required to watch multiple monitors depicting different data at one time
    - I am required to watch multiple dashboards on the same monitor depicting different data at one time
    - I am required to simultaneously monitor information from multiple monitoring sources (eg. network traffic, IDS logs, firewall logs, etc)
    - Monitoring the status of the network involves interacting with an IDS and other monitoring tools in addition to the following external information resources for vulnerability
    - I am required to simultaneously monitor the state of multiple network elements (e.g., individual machines, database server, web server etc.)
    - I am required to monitor the network, while carrying out other tasks simultaneously (e.g., responding to emails, carrying out incident response)
    - SIEMs require collecting and storing billions of logs every day, we have limited resources and are not able to keep these logs for long periods of time
    - Aggregation of billions of log alerts a day presented in heterogeneous data structures makes analysis a challenge
    - Devices may generate logs that are either incomplete or inconsistent (e.g., different time-stamps) making analysis an even bigger challenge
    - The tools I use are effective at supporting data fusion and correlation across incidents and data sources

51. Network Configurations: Please indicate your level of agreement with the following assertions. *Required (Options: Strongly disagree, Disagree, Neutral, Agree, Strongly agree)

    - Keeping up with changing configurations in the network is difficult, but necessary to provide the context needed to analyze and diagnose an alert
    - Keeping track and knowing the network environment is important to detect attacks
    - I track network configurations using personal memory
    - I track network configurations by keeping an updated database of network devices and configuration changes

52. Do you have any further comments on any of the topics covered on this page?

53. Do you have any further comments you would like to make about aspects of network security monitoring in SOCs that have not been covered in this survey?

Security Operations Centre Monitoring Tools Study
University of Oxford. Robert Hooke Building, Parks Road, Oxford, OX1 3PR.
Louise Axon and Bushra Alahmadi, {firstname}.{lastname}@cs.ox.ac.uk

Participant Information Sheet

1. **Study title** Security Operations Centre Monitoring Tools Study

   CUREC ethics reference: R48822/RE001

2. **Background and aims of the study**

   The study has three aims:

   1. To capture requirements for improving security monitoring tools by gathering information on the strengths and weaknesses of existing tools.
   2. To identify thought processes of analysts in security monitoring, and data features to be included in security tool development
   3. To compare working practice and security tool use across the Security Operations Centres of different organisation types.

   We will gather information for the above three parts through questions on SOC working practice, security tool use, attack indicators, and security monitoring and detection techniques applied by security analysts in Security Operations Centres (SOCs) in organisations.

   The researchers are Louise Axon and Bushra Alahmadi, who are doctoral students in the Centre for Doctoral Training in Cybersecurity. The research is being conducted under the supervision of Professor Sadie Creese, Professor Michael Goldsmith and Professor Ivan Martinovic.

   Contact details:
   Louise Axon/ Bushra Alahmadi
   Robert Hooke Building
   Parks Road
   Oxford
   OX1 3PR

   Email: louise.axon@cs.ox.ac.uk / bushra.alahmadi@cs.ox.ac.uk

3. **Why have I been invited to take part?**
   You have been invited to take part because of your experience working as a security analyst.

4. **Do I have to take part?**
   You can ask questions about the study before deciding whether to participate. You can choose whether you participate and, if you agree to participate, you may withdraw yourself and your data from the study without penalty at any time, and without giving a reason, by advising the researchers of this decision.

5. **What will happen in the study?**
   If you are happy to take part in the study, you will be asked to sign a consent form. The research will be conducted in form of face-to-face interview. One of the researchers will come to your premises, Interviews will take approximately 40 minutes to complete and will comprise a set of open and closed questions. Interviews will be audio-recorded.

6. **Are there any potential risks in taking part?**

There are no known risks or disadvantages of taking part and no specific preparatory requirements, as we strive to protect your confidentiality, unless you explicitly agree that the type or nature of your company can be mentioned in publications arising from the research.

7. What happens to the research data provided?

All participants in this study will remain anonymous. Only the researchers will have access to the personal data provided. The data will be stored in a password-protected file on the researcher's computer, and will be destroyed at the end of the project. Audio recordings will be destroyed and/or deleted once the project has been submitted for publication/examined. The typed version of your interview will be made anonymous by removing any identifying information including your name. Anonymised direct quotations from your interview may be used in the reports (only with your prior consent) or publications from the study, so your name will not be attached to them. All your personal data will be confidential and will be kept separately from your interview responses.

8. Will the research be published?

The results of this study may be published in conference proceedings, peer-reviewed journals and online in University archives. The results of the study will also contribute towards the DPhil theses of the two researchers, which will be published online. No personal data from this study will be published in any of the above; all study participants will remain anonymous and the data collected will be stored in a password-protected file on the researchers' computers, accessible only by the researchers.
The University of Oxford is committed to the dissemination of its research for the benefit of society and the economy and, in support of this commitment, has established an online archive of research materials. This archive includes digital copies of student theses successfully submitted as part of a University of Oxford postgraduate degree programme. Holding the archive online gives easy access for researchers to the full text of freely available theses, thereby increasing the likely impact and use of that research.
If you agree to participate in this project, the research will be written up as a thesis. On successful submission of the thesis, it will be deposited both in print and online in the University archives, to facilitate its use in future research. The thesis will be published with open access, meaning it will be available to every internet user.

9. Who has reviewed this project?

This project has been reviewed by, and received ethics clearance through, the University of Oxford Central University Research Ethics Committee.
This research is funded by the Engineering and Physical Sciences Research Council (EPSRC). The results of the study may be published in academic conferences or journals, and will be published in the researcher's thesis.

10. Who do I contact if I have a concern about the study or I wish to complain?

If you have a concern about any aspect of this project, please speak to the researchers, Louise Axon and Bushra Alahmadi (louise.axon@cs.ox.ac.uk, bushra.alahmadi@cs.ox.ac.uk) or their supervisors, Professor Sadie Creese (sadie.creese@cs.ox.ac.uk), Professor Michael Goldsmith (michael.goldsmith@cs.ox.ac.uk), and Professor Ivan Martinovic (ivan.martinovic@cs.ox.ac.uk) who will do their best to answer your query. The researcher should acknowledge your concern within 10 working days and give you an indication of how he/she intends to deal with it. If you remain unhappy or wish to make a formal complaint, please contact the chair of the Research Ethics Committee at the University of Oxford (using the contact details below) who will seek to resolve the matter in a reasonably expeditious manner:

Chair, **Social Sciences & Humanities Inter-Divisional Research Ethics Committee**; Email: ethics@socsci.ox.ac.uk; Address: Research Services, University of Oxford, Wellington Square, Oxford OX1 2JD

Security Operations Centre Monitoring Tools Study: Written Consent Form
University of Oxford. Robert Hooke Building, Parks Road, Oxford, OX1 3PR.
Louise Axon and Bushra Alahmadi, {firstname}.{lastname}@cs.ox.ac.uk

UNIVERSITY OF
OXFORD

Written Consent Form

STUDY TITLE Security Operations Centre Monitoring Tools Study

RESEARCHER DETAILS: Louise Axon and Bushra Alahmadi, Doctoral Students. Address: Robert Hooke Building, Parks Road, Oxford, OX1 3PR. Email: bushra.alahmadi@cs.ox.ac.uk or louise.axon@cs.ox.ac.uk

PURPOSE OF STUDY: To capture requirements for developing network security monitoring tools by gathering information on the strengths and weaknesses of existing tools; and to identify existing best practice in network security monitoring methods and tool use.

participant initials
each box

1. I have read the information sheet, have asked questions and received satisfactory answers □

2. I understand that this project has been reviewed by, and received ethics clearance through, the University of Oxford Central University Research Ethics Committee □

3. I understand that my participation is voluntary and that I am free to withdraw myself and my data at any time, without giving any reason, and without any adverse consequences or academic penalty □

4. I understand who will have access to personal data provided □

5. I understand that all anonymised research data will be stored securely for a minimum of three years □

6. I understand that the results of the research will be published in a thesis, and may be published in academic conference proceedings or journals □

7. I understand how to raise concerns or make a complaint □

8. I consent to being audio recorded □

9. I understand how audio recordings will be used in research outputs □

10. I agree to take part in the above study □

Name of Participant: ______________________________

Signature: ______________________________ Date: ______________

Name of researcher: ______________________________

Signature: ______________________________ Date: ______________