TBD
Internet-Draft
Intended status: Informational
Expires: 31 August 2026

M. Parsons
F. Driscoll
UK National Cyber Security Centre

27 February 2026

Security Operations Fundamentals and Guidance
draft-parsons-opsawg-security-operations-00

Abstract

Security operators are responsible for detecting malicious activity, responding to threats and defending their networks and systems from cyber attacks. Security operations are commonly entwined with other operational and management priorities to ensure that both security and operational priorities are considered holistically.

With security operators being a crucial part of operation, management and security of the network, it is valuable to give consideration to them during the design of new protocols. This document builds upon draft-ietf-opsawg-rfc5706bis, describing the fundamentals of security operations to provide a foundation for considerations for protocol design and guidance. This document also describes how security operations considerations can be most usefully included in other IETF documents.

About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-parsons-opsawg-security-operations/.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Copyright Notice

Table of Contents

1. Introduction

Security operations are a crucial part of both the security and management of a network, enterprise or system. Security operators work to not only prevent cyber attacks but also to identify, limit the impact of and recover from attacks that bypass preventative security controls, through monitoring and responding to threats as part of day-to-day operation.

The approach, tools and day-to-day work of security operators is deeply tied together with the protocols that run over their networks and are used by attackers and defenders. As such, it is valuable to provide security operators with guidance to address any changes that may affect ability to detect and respond to threats when deploying a new protocol. This document describes how one might consider how the range of functions of a security operator may be impacted and, where possible, suggests how to document these and provide guidance on deployment or operation. This early guidance is particularly valuable as retrofitting mechanisms can be difficult and any impact may risk both the operational efficiency and security of the network.

Security operations are commonly run from a Security Operations Centre (SOC); a centralised team or function that includes both cyber security analysts and operational engineers protect and defend the network.

Those who work in security operations may have many different roles or job titles including, but not limited to, cyber security analyst, incident responder, security engineer and security operations manager. In this document the term security operator is used to cover all roles in security operations.

Security operators improve the security of the network through a broad range of functions. These range from pre-emptive threat intelligence and knowledge building, through continuous network management and monitoring for suspicious activity, responding to incidents and defending the network during an attack, and recovery of the system to a secure state following an incident.

One organisational model is for operational and security responsibilities to be managed by separate teams with distinct objectives: security teams focusing on identifying and mitigating cyber security threats, and operational teams prioritising availability, performance, and the overall efficiency of network services. This model can have advantages, for example in enabling separation of duties. However, complete separation can also lead to conflicting priorities and outcomes. For example, security or compliance requirements could delay the deployment of new services, while operational and efficiency requirements could inadvertently introduce weaknesses that increase security risks.

The term SecOps [SECOPS], is commonly used to define an approach to combine operational and security teams, tools and processes to ensure both the protection and reliable operation of networks. As cyber security threats continue to increase in both frequency and scale, a more integrated and coordinated approach is often necessary. When security processes are siloed from operational processes, it can be challenging to adapt to emerging threats in a timely manner, and overall security may be reduced. Embedding security practices directly into operation and management, rather than as a bolt-on, is often vital for security, hence security operations becoming an integral part of the operation and management of many environments and enterprises. This approach considers the system as a whole in order to achieve both security and operational goals.

As such, security operations should be considered during the design of new protocols. This document outlines the key fundamentals of security operations to supplement the guidance provided in [I-D.ietf-opsawg-rfc5706bis] to support protocol designers.

2. Responsibilities of Security Operators

Security operators have key responsibilities to ensure the security of their network, which can be broken down into the categories below. During the design of new protocols, it may be useful to take these responsibilities into account to reduce or highlight any potential adverse impact. Different organisations will consider different functions and roles as part of their security operations team, so these categories will not apply to all organisations.

2.1. Threat Intelligence

Threat Intelligence (TI) is a term used to refer to the knowledge of cyber attackers' activities. This may include an understanding of a threat actor's motivations, in-depth technical descriptions, and indicators of an attacker's activities. Security operators can both produce their own Threat Intelligence and consume it from other sources to stay ahead of new attacker techniques. Building Threat Intelligence includes the collection, analysis and dissemination of information about possible cyber security threats. Security operators are responsible for developing their understanding of threat actor capabilities, tools and techniques in order to plan ahead to mitigate and respond to potential threats. They also ensure Threat Intelligence information is deployed across their network to support detection of malicious activity. Effective deployment of Threat Intelligence contributes not only to the security of the networks under the operators' responsibility but also strengthens the broader security community by enabling shared awareness of evolving threats.

2.2. Security Monitoring

Security operators are responsible for monitoring all parts of the environment that they are protecting and managing including any infrastructure, network traffic, endpoints, data flows and log sources. The objective of this monitoring is to establish a baseline of normal activity and identify deviations that may indicate malicious activity. It is essential that this monitoring is continuous as advanced actors frequently "dwell" in the network to evade immediate detection and conduct malicious activity at known operational downtimes to reduce the likelihood of being observed by security operators. In addition to reactive monitoring, security operators perform proactive "threat hunting". Rather than awaiting alerts generated by security tooling, threat hunting involves targeted analysis of the network and investigation to identify previously unknown indicators of malicious activity. Based on the Threat Intelligence responsibility, security operators are responsible for developing their capability to detect attackers, through developing and using tooling, which will involve engineering and operational experts to ensure this capability is maintained and improved.

2.3. Incident Response

Security operators are responsible for responding to cyber security incidents should the network be targeted by a cyber attack. Such attacks can have significant impact, so a vital part of a security operator’s role is to design, implement and update an incident response plan. Through effective security monitoring, security operators discover potential suspicious activity, and it is their responsibility to investigate this and determine whether the activity is malicious. In the event of confirming such an attack on the network, the security operators will follow their plan to conduct rapid response to defend against the attack, reduce its impact and return the network to a secure and operational state. Following the resolution of an incident, security operators also conduct post incident analysis to understand the impact, for example if any data breaches occurred, and may perform a root-cause analysis to prevent similar attacks in future.

Security operators have a range of tools and techniques that they commonly deploy and rely upon to be able to fulfil these responsibilities, which should be considered during protocol design.

3. Artefact Requirements

This section outlines some of the fundamental artefacts that are used by security operators to ensure security and operation of the network.

With increasingly complex cyber threats, and to support both operational and security objectives, it is vital that security operators have multiple opportunities to detect malicious activity at different parts of the network and to account for different points of failure. Thus, network defence techniques often use multiple layers of defence with several different mitigations at each layer - a concept referred to as "defence-in-depth". This approach can apply to considering security at different parts of the network, for example detecting activity at the network edge and on endpoints, and security operators also apply network level controls to separate traffic to support their security monitoring responsibilities. Security operators rely upon artefacts from a variety of sources to achieve their goals.

3.1. Asset Management

Defence and management of an environment relies on knowing what hardware and software assets have access to, or are installed on, a network or system. An accurate inventory is necessary to manage the security of an organisation’s assets, to ensure that unauthorised devices are not present on the system and to understand how an organisation may be impacted by a cyber incident.

The term "Shadow IT" is often used to refer to assets that are not accounted for. This can include devices which are not officially onboarded or are misconfigured, but also includes services, tools and accounts with access to the system. Shadow IT may introduce threats to the security of the system as protections and controls put in place may be ineffective.

A good asset management approach will use tools to scan the environment for new, modified or removed assets on a regular or continuous basis. It should maintain an authoritative and accurate source of information, which should be made accessible to security operators. It could use a variety of data sources including procurement records, mobile device management and logging platforms. Security operators are most likely to use asset management systems to identify devices or software that should not be on the system, as well as to identify legitimate assets that need to be protected as part of a cyber incident.

3.2. Indictors of Compromise

The identification of Indicators of Compromise (IoCs) is relied upon by security operators to identify and defend against malicious activity on the network and endpoints that they are responsible for. As outlined in [RFC9424], IoCs are observable artefacts relating to a cyber threat actor or their activities, such as their tactics, techniques, procedures (TTPs), or tooling and attack infrastructure. Examples of IoCs include hash values of known malicious files or executables, IP addresses or domain names associated with malicious traffic or software and tooling used by attackers. These artefacts could be network based, such as information about Command and Control (C2) infrastructure embedded in network protocols, endpoint based, such as suspicious files or software, or behaviour based such as irregular account or access activity.

These artefacts can be observed on the network or at hosts and endpoints, including infrastructure, services and applications. They help security operators to proactively block malicious activity, whether that be blocking traffic or preventing code execution at a point in the network. IoCs support Incident Response as they are

crucial in determining whether an attack has taken place. Similarly, they can be used to link discovered suspicious activity to a known attackers, which enables further investigation and mitigations to be put in place. Having IoCs deployed to various security control points across a system supports a defence-in-depth approach which should be used by security operators.

Security operators not only discover, use and deploy IoCs in the systems that they are responsible for, but also consume and share IoCs with the wider security community to increase wider understanding of emerging cyber threats.

3.3. Digital Forensics and Logging

Alongside deployment of IoCs to detect and reduce the effects of compromise, security operators require digital forensics from the network, endpoints, hosts and applicationsto enable effective incident response or threat hunting. For example, details of authentication or authorization events, network traffic or endpoint-detection events can be found in logs.

Using a range of log sources is vital, as each log source will give a different view of attacker activity to build a full picture and enable effective defensive mitigations. For example, authentication logs provide details when adversaries attempt to gain unauthorised access to systems, DNS logs can provide the first indications of a compromise device, and anti-malware software logs help to identify specific attacker capabilities.

Understanding and interpreting log sources is not always straightforward, so security operators typically use log analytic techniques to index, enrich and query log data and thus take effective action.

Security operators, through their Threat Intelligence insight play a role in threat modelling which enables effective identification of valuable log sources. Security operators are responsible for ensuring that logging processes and data are secured effectively.

4. Tooling Requirements

Changes to protocols may require changes to tooling in order to continue to be effective for security operations, and this should be highlighted when writing drafts. To assess this, the following section outlines the common tooling used and relied upon by security operators and which could be considered in protocol development. This is non-exhaustive, so other operational tools and techniques may also be worth considering.

Endpoint Detection and Response (EDR) tools are deployed to endpoints, or end-user devices such as workstations, laptops or phones attached to the network that security operators are responsible for. EDR tooling can also be deployed to workloads in cloud environments. EDR tooling monitors events and provides security operators visibility of any malicious activity where they are deployed. EDR tooling also allows security operators to not only monitor and identify threats, but also respond to them, for example by isolating potentially compromised devices from the network in order to prevent a cyber threat actor’s next stages of attack. A challenge that security operators face when using EDR tooling is the increase in cyber threat actors deploying "living off the land" techniques, so that their activity does not appear malicious and thus is not identified by EDR tooling.

Network Detection and Response (NDR) tools are designed to detect threats by analysing network data and traffic flows to identify suspicious patterns. As a complement to EDR, NDR tooling is often relied upon to detect threats that may be hard to detect at the endpoint, for example an attacker moving laterally through the network towards more sensitive data or suspicious behaviour such as unauthorized credential use or data exfiltration. Security operators often use NDR tooling to establish a baseline of the network’s normal behaviour patterns and deviations from this trigger alerts. As with EDR, NDR tooling can offer the ability to respond to threats in addition to monitoring for them, for example by blocking malicious traffic.

Security Information and Event Management (SIEM) tooling is used by security operators to collect and analyse data from across the network in order to build a comprehensive view of the network activity, which is key to identify and respond to malicious activity. Note that, in comparison to EDR and NDR, SIEM tools collect and analyse events, rather than monitor the network directly. SIEM analysis would not be possible manually, so security operators rely on tooling to combine and analyse a range of data, including log data, network events and threat intelligence feeds in order to identify suspected suspicious events that require further investigation. SIEM tooling will send security operators automatic alerts based on predefined security rules to reduce the impact of compromise. These rules require effective management, as false positive may lead to "alert fatigue", where too frequent alerts may be ignored, raising the risk of real compromises being missed.

Security Orchestration, Automation, and Response (SOAR) tooling offers security operators the ability to automate routine security and operational tasks to improve efficiency of response. Based on threat related data that is collected, SOAR tools are used to

automate responses without human intervention, based on predefined "playbooks". These playbooks are designed by security operators with both incident response and operational priorities in mind. This automation is vital to security operators who experience an overwhelming volume of threats and would otherwise be unable to defend their networks. This automated action provided by SOAR tools complements the data analytic and insight provided by SIEM tools to respond to threats identified.

Security operators rely upon Protocol Dissectors to parse and interpret individual network protocols. Dissecting protocols across network layers allows security operators to understand, analyse and filter traffic on their system in order to detect and defend against attacks. Dissectors support the identification of suspicious behaviour and malicious traffic that would otherwise be hidden within regular network traffic. These tools also support forensic investigation after an attack to understand how an attacker gained access and prevent this in future.

5. Additional Benefits of Security Operations

Whilst the core responsibilities of security operators are outlined above, they may be well placed to support other important security functions.

5.1. Vulnerability management

Security operators are well positioned to proactively find vulnerabilities in the systems and infrastructure that they are responsible for. As part of their investigations security operators may conduct vulnerability scanning and security assessments and thus be able to triage and report priority issues to system owners who are responsible for patch management. This helps to mitigate security issues found before they can be exploited by cyber threat actors. This patching and remediation is an example where the joining of security and operational teams has particular value as patch management may involve prioritisation based on impact, risk and deployment considerations. When designing new protocols, consideration should be given to enabling efficient patching, for example supporting cheap and fast connection handoffs and reconnections.

5.2. Threat Modelling and Architecture Review

With their unique position, security operators are well placed to support wider security teams in developing the required security posture for their network. Blending insight from Threat Intelligence with a deep understanding of the operational aspects of the network, security operators can work with design teams to ensure their priorities are supported. This perspective of current cyber threats and operational experience can also be considered in protocol development.

6. Security Operation Considerations

The previous sections outline what security operations is, and the artefacts and tooling that it relies upon. During the design and development of protocols, it is valuable to consider how security operators could be impacted by changes and mitigate such impact if possible. If they cannot be mitigated, then clearly documenting such considerations will aid security operators if and when the new protocol is deployed.

New protocols may have implications for the types, locations or availability of IoCs and it is important for security operators to understand these implications in order to continue to effectively monitor for malicious activity.

Similarly, consideration should be given to how a new protocol or a change to a protocol may impact attackers' capabilities, such as Command and Control (C2) communications, network traversal or facilitation of exfiltration of data from the network. Where there are new or different opportunities for performing such malicious activity or where current defence techniques are prevented, it is important that this is captured to inform security operations and mitigated where possible to ensure their Threat Intelligence function can be fulfilled.

One indicator of malicious activity that security operators use is to consider traffic levels and traffic patterns in order to identify suspicious activity or to defend against malicious distributed denial-of-service (DDoS) attacks. Mitigations should be included or threats documented if new protocols could be used to create DDoS attacks, for example amplification attacks in DNS or NTP. [RFC4732] provides further considerations for protocol designers with regards to denial-of-service.

As outlined above, security operations rely on a variety of log sources enable effective incident response or threat hunting. If a new protocol changes the properties or topology of the network, this

may impact the requirement for digital forensics. The mitigation for this may be to design new ways, schema or formats to providing such logging information when designing a new protocol. [I-D.ietf-quic-qlog-main-schema] is an example of structured logging for network protocols.

Impact on tooling should be considered. Updating and augmenting existing tools is expected when the network is upgraded or new functionality is deployed, but having to completely rebuild such tooling will greatly reduce the effectiveness of security operators. A mitigation for this may be to consider designing flexibility for future versions and extensions into protocols so that code can be easily written to handle, identify and differentiate between protocol versions.

In general, where protocols are being updated or replaced, consideration should be given to the current techniques employed by security operators who use the deployed protocol. This should include the techniques, tooling and corresponding infrastructure used to provide security and effective operation of the network. Where possible, these practices should remain consistent, or mitigations or documentation included to ensure security operations are not adversely affected.

7. Operational Considerations

This document focuses primarily on operational considerations in addition to [I-D.ietf-opsawg-rfc5706bis] .

8. Security Considerations

This document supports improving security by helping protocol designers consider security operators and their effort to mitigate cyber threats. It focused on the operational aspects, rather than the security of the protocols.

Security operators have access to sensitive data, which is critical to protect for the security and privacy of the network. It is important that such data is suitably secured and that appropriate controls are in place to enforce this, for example ensuring security operations data is segregated from the rest of the network, security operations tools and actions audited, and logs and forensic data securely stored and access controlled. Additional legal and governance requirements are often raised on security operators to ensure that such access is only being used for the intended purpose and thus benefiting the security of the system.

9. IANA Considerations

This document has no IANA actions.

10. Informative References

[I-D.ietf-opsawg-rfc5706bis]
Claise, B., Clarke, J., Farrel, A., Barguil, S., Pignataro, C., and R. Chen, "Guidelines for Considering Operations and Management in IETF Specifications", Work in Progress, Internet-Draft, draft-ietf-opsawg-rfc5706bis-02, 19 February 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-opsawg-rfc5706bis-02>.

[I-D.ietf-quic-qlog-main-schema]
Marx, R., Niccolini, L., Seemann, M., and L. Pardue, "qlog: Structured Logging for Network Protocols", Work in Progress, Internet-Draft, draft-ietf-quic-qlog-main-schema-13, 20 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-quic-qlog-main-schema-13>.

[RFC4732] Handley, M., Ed., Rescorla, E., Ed., and IAB, "Internet Denial-of-Service Considerations", RFC 4732, DOI 10.17487/RFC4732, December 2006, <https://www.rfc-editor.org/rfc/rfc4732>.

[RFC9424] Paine, K., Whitehouse, O., Sellwood, J., and A. Shaw, "Indicators of Compromise (IoCs) and Their Role in Attack Defence", RFC 9424, DOI 10.17487/RFC9424, August 2023, <https://www.rfc-editor.org/rfc/rfc9424>.

[SECOPS] "NICCS Glossary", February 2026, <https://niccs.cisa.gov/resources/glossary>.

Acknowledgments

Authors' Addresses

Michael Parsons
UK National Cyber Security Centre
Email: michael.p1@ncsc.gov.uk

Florence Driscoll
UK National Cyber Security Centre
Email: florence.d@ncsc.gov.uk