Security Operations Fundamentals and Guidance

draft-parsons-opsawg-security-operations

Michael Parsons, Florence Driscoll

Goals

- Informational draft to increase understanding of security operations at IETF to support protocol designers.
- Complement operational considerations highlighted in 5706bis
- Improving security by helping protocol designers consider security operators and their effort to mitigate cyber threats.

Definitions/Jargon

- Security operators are responsible for detecting malicious activity, responding to threats and defending their networks and systems from cyber attacks.

- 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 who protect and defend the network.

Definitions/Jargon

- The term 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.

What security operators do

- Build and use Threat Intelligence
- Conduct security monitoring
- Respond to cyber incidents

What security operators need/use

- Understanding of assets
- Sight of Indicators of Compromise (IoCs)
- Digital forensic and logging information
- Tooling

Security operation considerations

- Availability of Indicators of Compromise (IoCs)
- Attacker capabilities
- Traffic management
- Impacts on logging
- Impacts on tooling
- …

Next steps?

- Comments?
- Questions?
- Feedback?
- Next steps?