Staffing your Intelligent Security Operations

Ideal vs. Reality

There's an ideal way to staff the intelligent security operations center and then there's reality. The two are rarely the same. In today's world, where talent and budget to properly staff a SIOC can be scarce, Micro Focus conducted an assessment of SIOC operations to uncover the most critical roles, the most productive team configurations, and triggers for expanding headcount.

Team of 3

- 8x5 operations with automation and hybrid managed security services for after-hours monitoring

SOC roles

- Manager
- Level 1 analyst (L1)
- Level 2 analyst (L2)
- Security engineer
- Incident handler
- SIEM content author
- Forensic investigator
- Hunt analyst
- Others (security data scientist, vendor liaison, etc.)

Team of 10

- 24x7 in-house operation

SOC roles

- Manager
- L1 analyst
- L2 analyst
- Engineer

Triggers for expanding headcount

- Increase in events per analyst hour (due to addition of technology feeds and other reasons)
- Compliance requirements (GDPR, PCI-DSS, FISMA, HIPAA)
- Expanding coverage (24x7)
- Mergers and acquisitions
- Increase in maturity

For every four L1 analysts, Micro Focus recommends one L2 analyst in a 24x7 SOC

View the full “Intelligent Security Operations: A Staffing Guide” white paper