The Practice of Network Security Monitoring

Understanding Incident Detection and Response

by Richard Bejtlich

Errata updated to print 11

Page	Error	Correction	Print corrected
48	In other words, cable R01 would be connected to one of the switches—say **the one connected to location G**— while cable R02 would be connected to **switch** uplink S1.	In other words, cable R01 would be connected to one of the switches—say **switch uplink S1**— while cable R02 would be connected to **the firewall interface facing** uplink S1.	Print 3
166	`WHERE event.timestamp > '2014-02-10 11: 13: 00' AND event.timestamp < '2013-02-10 11:16:00' AND event.signature LIKE 'URL%'`	`WHERE event.timestamp > '2013-02-10 11: 13: 00' AND event.timestamp < '2013-02-10 11:16:00' AND event.signature LIKE 'URL%'`	Print 4

Additional Notes

Page 197

Due to the continuous development of the Security Onion project, the author recommends replacing the deployment and maintenance guidance in Part II with the documentation published at *https://docs.securityonion.net*.