

Whoami

Bao

IT安全威胁情报团队

张三丰的疯言疯语作者



七步曲

**Determine the
Intelligence Requirements**

Analyze Internal Information

Enrich the Information

Validate the Information

Store the Information

Share the Information

**Productize the
Information**

分析步骤

#01 Determine the Intelligence Requirements

明确情报的需求

回答why

商业价值

User-Agent

#02 Analyze Internal Information

分析内部信息

IR/malware/其他

钻石模型
killchain

log

#03 Enrich the Information

丰富信息

情报渠道

Whois/IP/
domain

ctr@huawei.com

分析步骤

The screenshot displays the THREATCONNECT interface. A central table provides analysis results for six exhibits across three criteria. The interface also shows navigation elements like 'Home', 'INDICATORS', and 'WORKFLOW'.

	Hard spy who passed classified info	Was performing job honestly	Was storing intellectual property for next job
Exhibit A	Neutral	Consistent	Inconsistent
Exhibit B	Inconsistent	Inconsistent	Consistent
Exhibit C (!)	Very Consistent	Inconsistent	Consistent
Exhibit D	Very Consistent	Very Consistent	Very Consistent
Exhibit E	Inconsistent	Neutral	Neutral
Exhibit F	Inconsistent	N/A	N/A

Below the table, the interface shows search results for 'Email' with identifiers like 'E20160716B: PRIME AIR TRAV' and 'E20160716A: RICHARD HOWELL TOTAL UK'. It also includes a 'Common Community' section with a count of 534 and a table with columns for likes, comments, and date added.

#07 Productize the Information
生成信息

ACH

指导行动

总结报告

张三丰的
疯言疯语

THANKS

Cyber Threat Report
ctr@huawei.com

