SANDFLY SECURITY

AGENTLESS THREAT HUNTING

Insider’s History of Intrusion Detection Technology

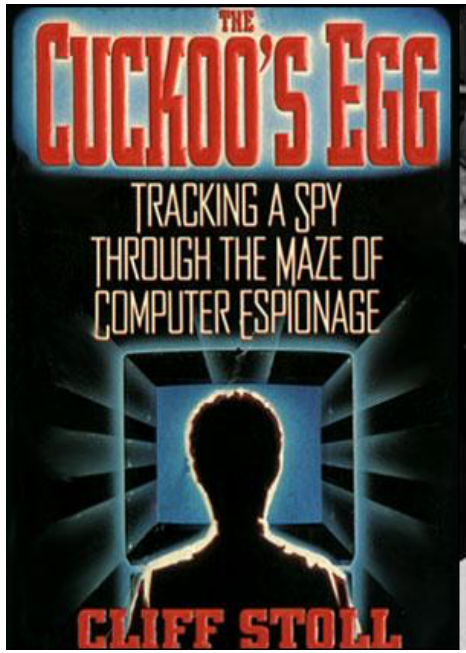
Craig H. Rowland - Founder

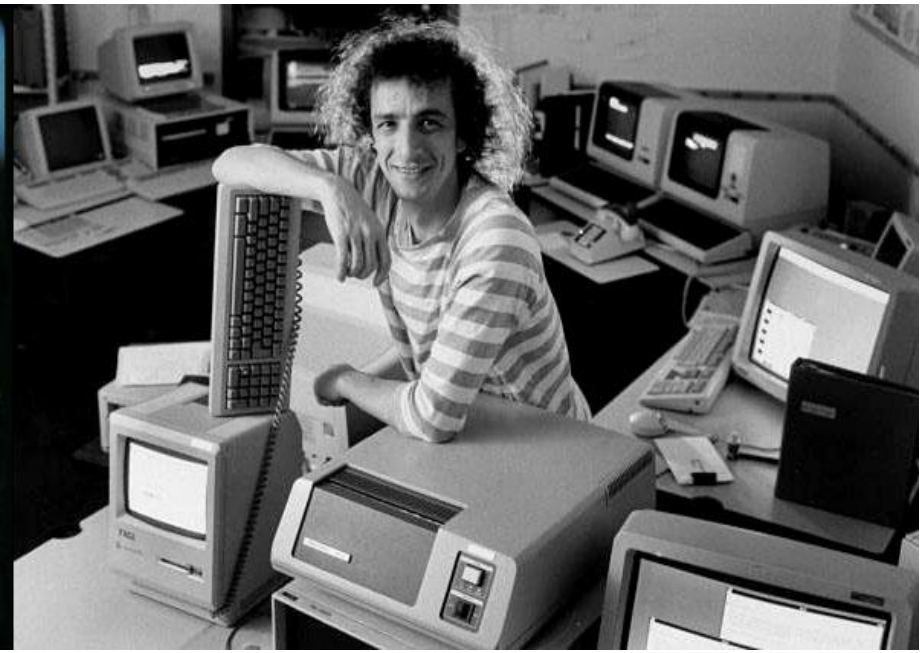
@CraigHRowland @SandflySecurity

www.sandflysecurity.com


MOLNICK
MOLNICK

Early IDS.


THE
CUCKOO'S EGG
TRACKING A SPY
THROUGH THE MAZE OF
COMPUTER ESPIONAGE
CLIFF STOLL



UC DAVIS
UNIVERSITY OF CALIFORNIA

NSM and ASIM

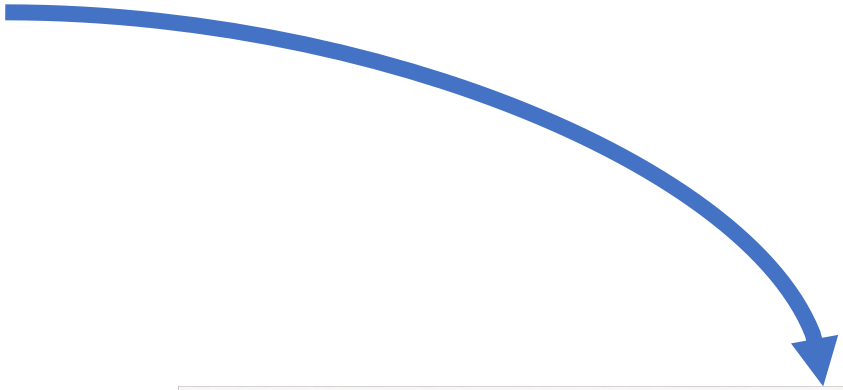
Network analytics.
Not real-time.
Manual process.

DIDS

Host analytics.
Had signatures.
Real-time automated.

Commercial Network IDS.


AF INFORMATION WARFARE CENTER




WheelGroup™
corporation
Trusted Professionals ◆ Secure Connections

Employment Tip

Don’t launch network attacks against the people about to hire you just because the CFO thinks it would be funny.

NetRanger IDS Strengths

Network monitoring.

Real-time.

Signature based.

Could block attackers.

Some network analytics.

NetRanger IDS Weaknesses

Bandwidth limits.

Packet fragmentation limits.

Vulnerable to spoofed attacks.

Temptation to watch too much.

NetRanger IDS Realities

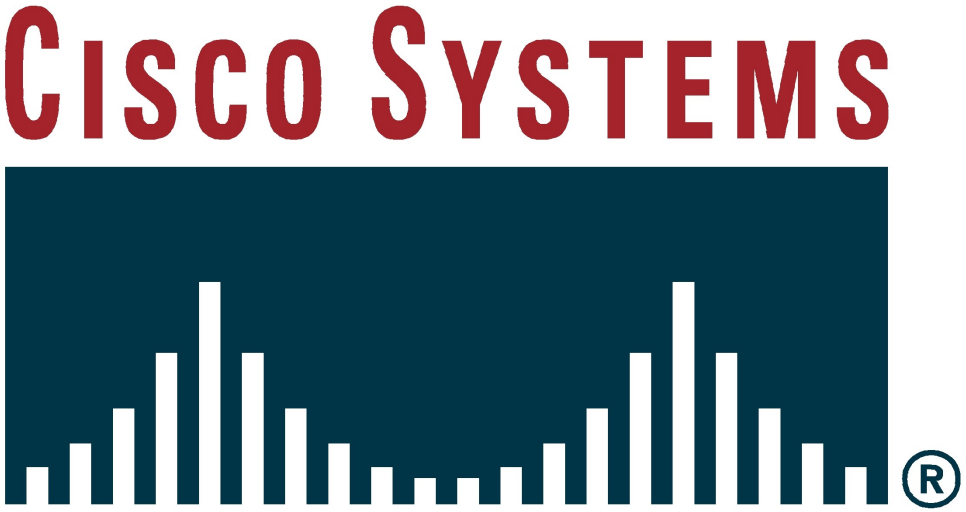
Hardware was not fast enough as bandwidth increased.

TCP reassembly could cause resource starvation attacks.

Automated attacks created alarm deluge.

If you’re being attacked,
you’re making a difference.


WheelGroup
TM
corporation
Trusted Professionals ◆ Secure Connections


CISCO SYSTEMS
®

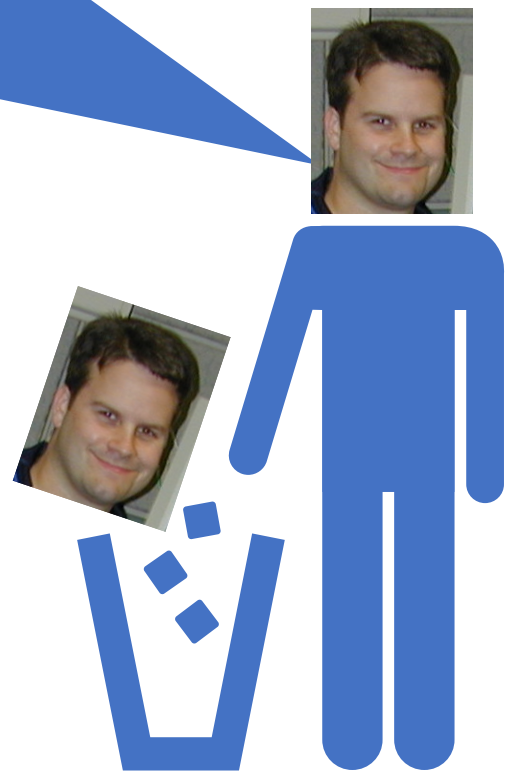
Perfect is the enemy of the good.

False Alarms.

I’m going to start a HIDS company.

Forget you 1999 Google. I have a dream!

Actually, I'll make an agentless investigator.

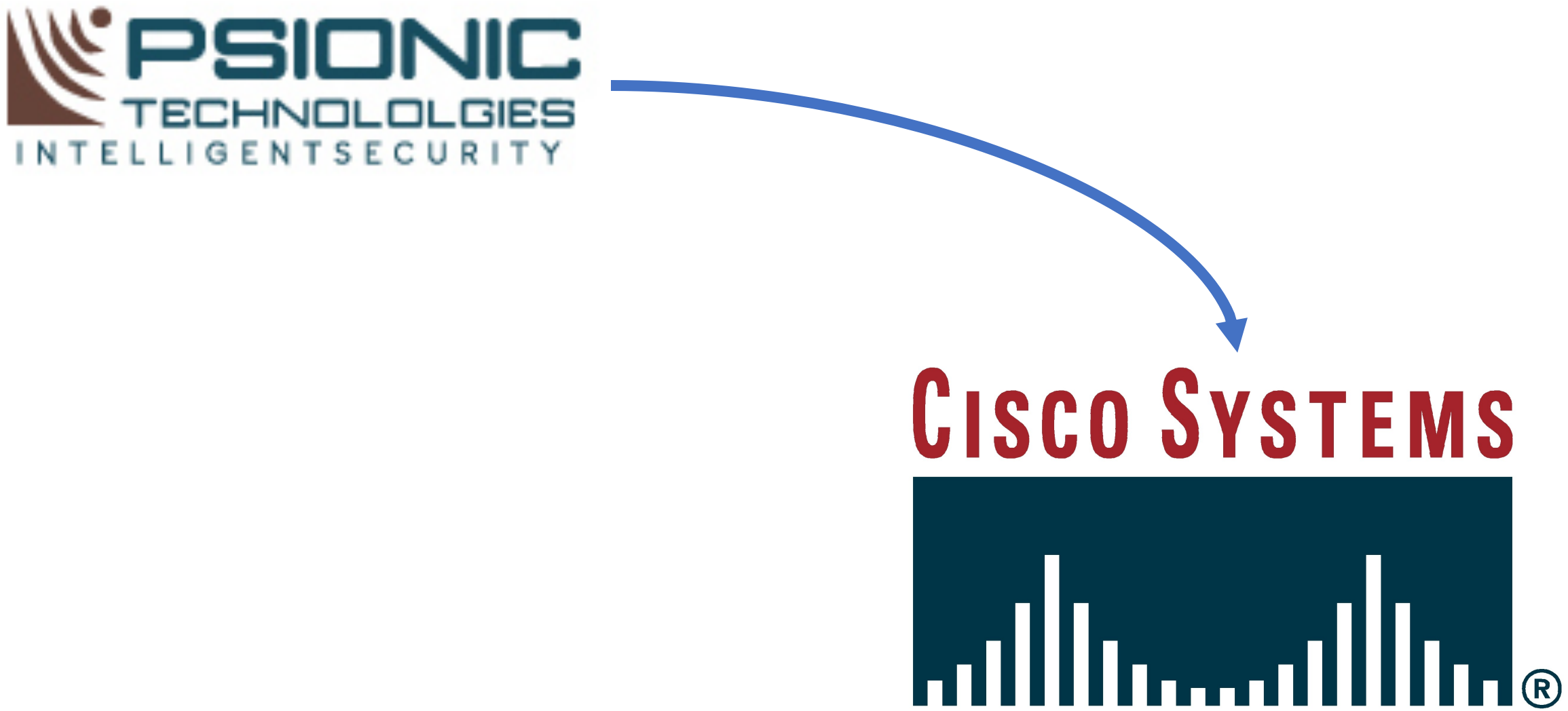


Psionic ClearResponse

Agentless IDS alert investigator.

Eliminated 95-99% of false alarms.

First automated host investigation system.


PSIONIC
TECHNOLOGIES
INTELLIGENTSECURITY
CISCO SYSTEMS

CISCO SYSTEMS

The Rise of IPS.


i-opener
Tell a Friend
Mail
Web Guide
Shopping
News
i-opener
Weather
Sports
Finance
Entertainment
Help
Contrast

“I have a PhD in Electrical Engineering and MBA from Stanford. I’m telling you that it *can’t be done*.”

- Analyst from big name Silicon Valley VC firm on why TippingPoint wouldn’t work.


TippingPoint
6100N
TippingPoint
NCP
TippingPoint
BLANK
1A 2A 3A 4A 5A
6A 7A 8A 9A 10A
11A 11B
1B 2B 3B 4B 5B
6B 7B 8B 9B 10B
LINK ACT
LINK ACT
CompactFlash®
ZPHA
CONSOLE
MGMT

Done.

Startup Tip

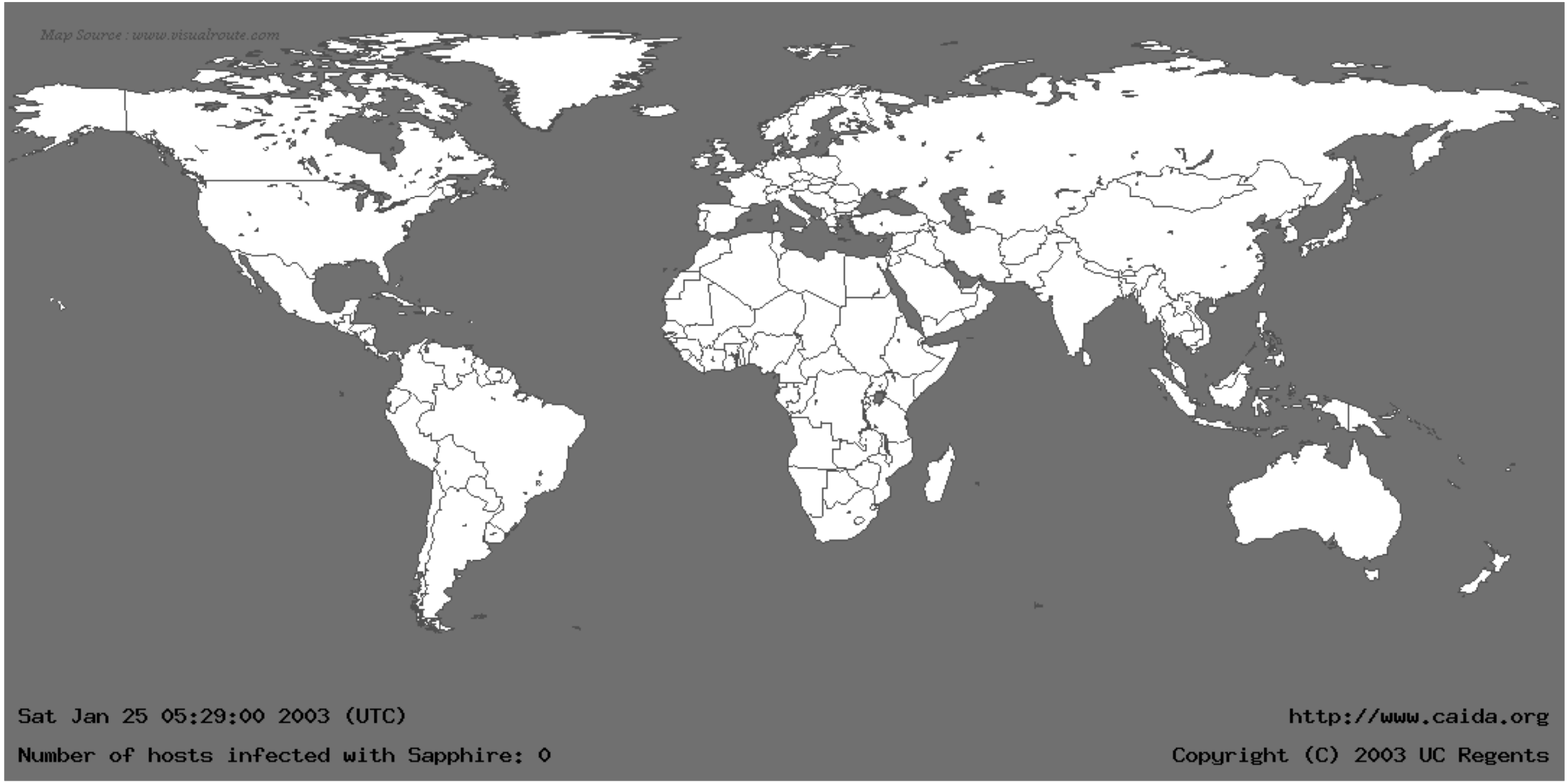
Customers only tell you about the product they want today, not the one they actually need in the future.

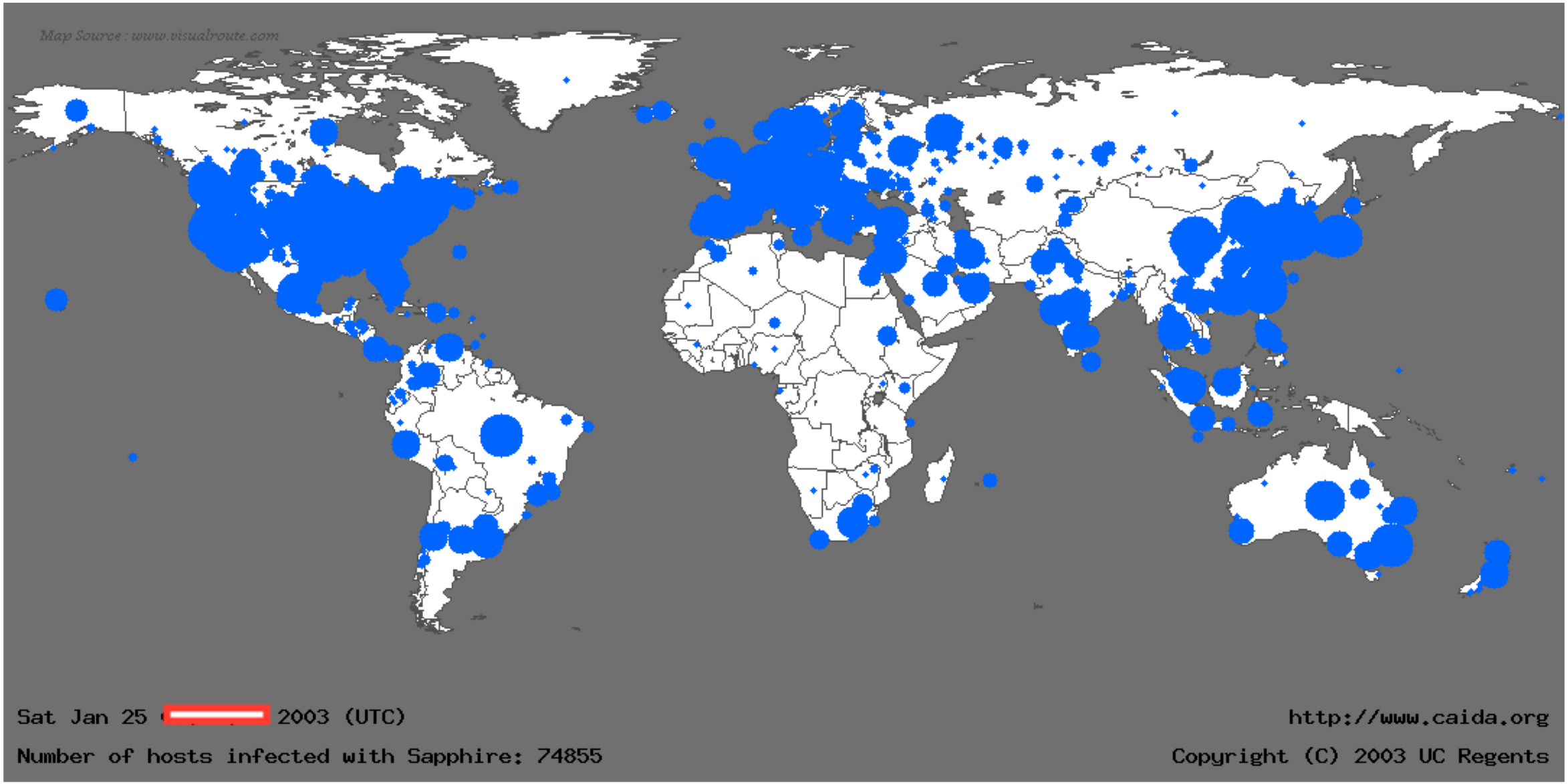
“We will never install that fuc*ing thing on our network.”

Sincerely,
Goldman Sachs

“Yes, you will.”

Love,
Slammer Worm


Map Source : www.visualroute.com
Sat Jan 25 05:29:00 2003 (UTC)
Number of hosts infected with Sapphire: 0
http://www.caida.org
Copyright (C) 2003 UC Regents


Map Source : www.visualroute.com
Sat Jan 25 [redacted] 2003 (UTC)
Number of hosts infected with Sapphire: 74855
http://www.caida.org
Copyright (C) 2003 UC Regents

NETWORKWORLD
FROM IDG

Slammer's aftermath: Product hype

By Paul F. Roberts

IDG News Service | JAN 27, 2003 12:00 AM PT

Is it hype if it works? No.

What now?

Network Analytics

Good for spotting suspicious network activity.

Can give high-level information on encrypted communications.

Can watch too much.

Network IDS/IPS

Good for stopping known malicious traffic.

Bad for encrypted traffic.

Can watch too much.

Host Analytics

Good for spotting out of ordinary host activity.

Can watch too much.

Host IDS/IPS

Good for monitoring inside encryption.

Good for spotting known malicious host activity.

Can watch too much.

Leverage the 1000:1 Rule.

Network Analytics

Network IDS/IPS

Host Analytics

Host IDS/IPS

SANDFLY SECURITY

AGENTLESS THREAT HUNTING

@CraigHRowland @SandflySecurity

www.sandflysecurity.com