Security Operations Center

Presenter:
Ahmad Haghighi

Haghighi.ahmad@gmail.com

September 2014

Table of Context

- ❑ Foreword
- ❑ Introduction
- ❑ Build vs. Outsource
- ❑ 5G/SOC
- ❑ Personnel
- ❑ Q&A

FOREWORD

Sl.No	Service	Enterprise Category		
		Small	Medium	Large
1	Infra Security Operations	Yes	Yes	Yes
2	Security Incident and Event Management	Optional	Yes	Yes
3	Database Activity Monitoring	Optional	Yes	Yes
4	Web Application Firewall	Optional	Optional	Yes
5	Network Behaviour Anomaly Detection	Optional	Optional	Yes
6	Vulnerability Management	Optional	Yes	Yes
7	Threat Intelligence	Optional	Yes	Yes
8	Risk Management	Yes	Yes	Yes
9	Anti-Phishing	Optional	Optional	Yes

10	Anti-Malware	Optional	Yes	Yes
11	Data Loss Prevention	Optional	Optional	Yes
12	Virtual Infra Security	Optional	Optional	Yes
13	Network Admission Control	Optional	Optional	Yes
14	Wireless IPS	Optional	Optional	Yes
15	Identity and Access Management	Optional	Optional	Yes
16	Fraud, Forensic Analysis & SIRT	Optional	Optional	Yes
17	Security Matrix Dashboard	Optional	Yes	Yes
18	Application Code Review, SSO, 2FA	Optional	Optional	Yes
19	Physical Security Command Center	Optional	Optional	Yes

Fischbach (Colt Telecom Services)

"We were at the point in the company where security was distributed over many teams -IT, the network guys, some dedicated network engineers, corporate security, and so on,"

"We didn't have a single view into our assets."

Modern & Complicated attack methods

Integrity

Get visibility into your environment

Centralized Management

What is SOC

SOC

A security operations center (SOC) is a centralized unit in an organization that deals with security issues, on an organizational and technical level. An SOC within a building or facility is a central location from where staff supervises the site, using data processing technology. Typically, it is equipped for access monitoring, and controlling of lighting, alarms, and vehicle barriers.

ISOC

An information security operations center (or "SOC") is a location where enterprise information systems are:

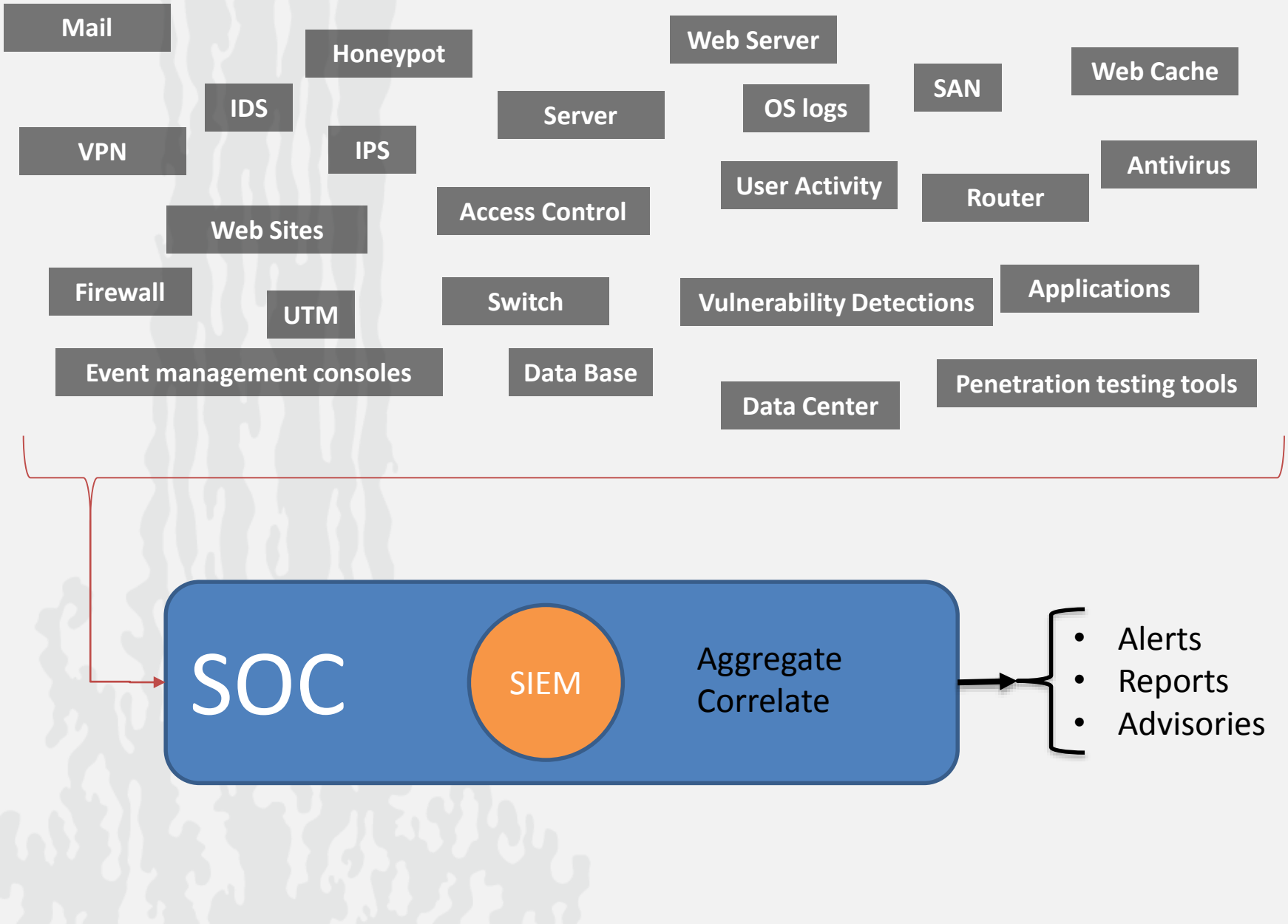
monitored

assessed,

and **defended**.

Alternative names

- Security defense center (SDC)
- Security intelligence center
- Cyber security center
- Threat defense center
- security intelligence and operations center (SIOC)
- Infrastructure Protection Centre (IPC)


Mail
Honeypot
Web Server
Web Cache
IDS
SAN
Server
OS logs
VPN
IPS
Antivirus
User Activity
Router
Access Control
Web Sites
Firewall
Applications
Switch
Vulnerability Detections
UTM
Event management consoles
Data Base
Penetration testing tools
Data Center
SOC
SIEM
Aggregate
Correlate
Alerts
Reports
Advisories

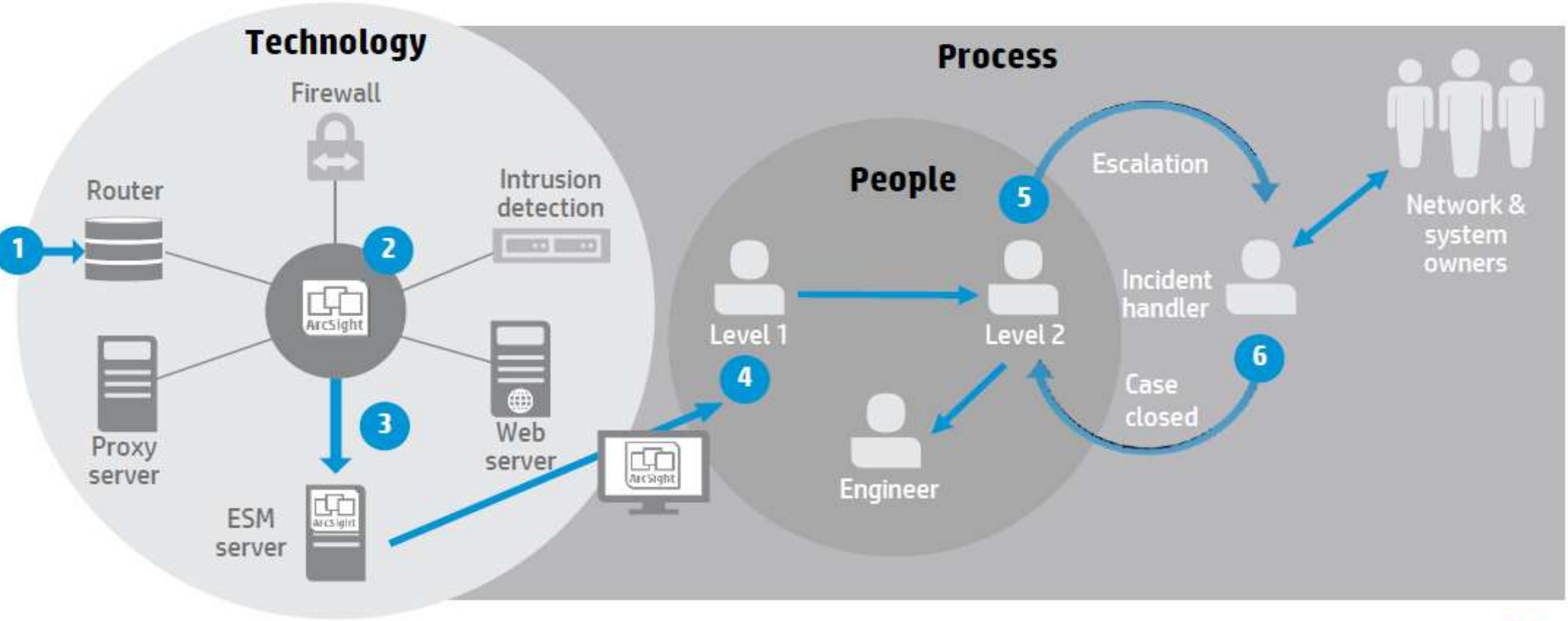
Use Cases

Use Case	Primary Data Sources	Alert Criteria	Action
Botnet activity	Firewall, IDS, Proxy, Mail, Threat Intelligence	Connection to or from known malicious host or domain	Display in analyst active channel
Virus outbreak	Antivirus	3 viruses detected with same name in 10 minutes	Page desktop team / display in dashboard
Successful attack / malicious code	IDS/IPS, Vulnerability	Targeted asset exhibits vulnerability, relevance=10	Page server team / display in active channel / display in dashboard
SQL injection	Web Server, DAM, IDS/IPS	5 injection attempts within specified time frame	Display in analyst active channel
Phishing	Threat Intelligence, Firewall, IDS, Proxy, Mail	Connection to or from known malicious host or domain	Display in analyst active channel
Unauthorized remote access	VPN, Applications	Successful VPN authentication from a non domain member	Display in analyst active channel / Page network team
New vulnerability on DMZ host	Vulnerability	New vulnerability identified on publicly accessible host	Email daily report to vulnerability team
Suspicious activity	Firewall, IDS, Mail, Proxy, VPN	Escalating watch lists (recon, exploit, brute force, etc.)	Email daily suspicious user activity report to level 1
Statistical anomaly	IDS, Firewall, Proxy, Mail, VPN, Web Server	Moving average variation of X magnitude in specified time frame	Display alerts in situational awareness dashboard
New pattern of activity	IDS, Firewall, Proxy, Mail, VPN, Web Server	Previously unseen pattern detected	Display in analyst active channel

SOC

- Technology
- People
- Process & Procedure
- Environment

People, process, technology



Do we need a SOC?

- **Expensive (Infrastructure, Personnel, Training, …)**
- **TCO – TBO ROI**
- **Current equipment is not enough?**
- **Do We need a SOC?**

Nick Bradley (senior operations manager for IBM):

"Think worse-case scenario -what type of data would be accessed if you were breached, and would you have the resources to recover, or could you recover?“

"If the answer is terrifying and keeping you up at night, then the answer is yes, you need a security operations center."

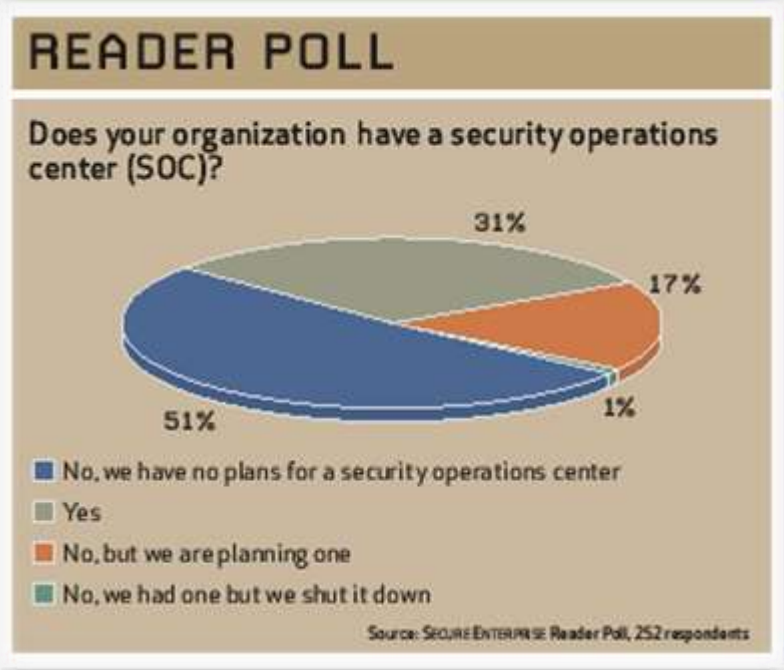
Survey of Secure Enterprise readers (2005)

72 percent of respondents with fewer than 5,000 employees had no plans to build a SOC

Among the 28 percent who have a SOC or plan to build one

53 percent will collocate in the NOC

The rest plan to house the SOC in a separate location, either a building (25 percent) or a room (22 percent).



Build-in vs. Outsource

MSSP

Advantages

Challenges (Limitations)

Hybrid

Some Providers:

- Microsoft (3 SOC)
- IBM
- Dell SecureWorks (7 SOC)
- HP (ArcSight) ->BMW
- Verizon
- Symantec

Possible Shopping Lists

Hosts:

- Firewalls
- IDS/IPS
- Data Loss Prevention
- Behavior Based Detection
- Anti-Spyware
- Rogue Host Detection
- Policy Auditor
- Devise Control (USBs, etc.)
- Asset Management
- Baseline Monitoring (FDCC)
- Application White listing
- Patch Management
- Remote Forensics
- Etc.

Possible Shopping Lists

Network:

- Log Aggregation and SIM
- Flow Monitoring
- Full Packet Capture
- Next Generation Firewalls – shift from blocking IPs and Ports to controlling applications
- Web Application Firewall
- Web Proxy
- Content Monitoring (Network Based DLP)
- New IDSs – Code Behavior/ Reputation
- Continuous Vulnerability Scanning
- Honeypot

Possible Shopping Lists

Other:

- SOC -- provide Incident Response, Forensics Capabilities, Threat Monitoring, Intelligence Gathering
- Continuous Monitoring
- Better User Training and Awareness – First line of defense: Informed Users!
- Contingency Planning
- Red Team/Blue Team (inc. Third Party Penetration Testing & Web/Application Testing)
- Encryption
- 2 Factor Authentication
- Identify, classify, and tag what you need to protect, what are your crown jewels, what will affect your organizational viability.
- MORE FUNDING & RESOURCES!!!

SOC generations (5G)

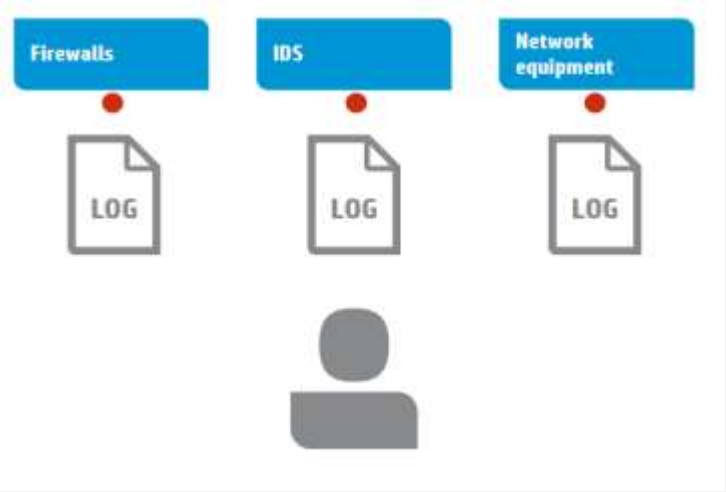
1st Generation SOC: 1975-1995

Birth of the Internet: businesses not connected, or via slow connections

Nuisance programs and minimally impacting malicious code era

Information security tools appear

Military and governments start to build SOCs and CERTs

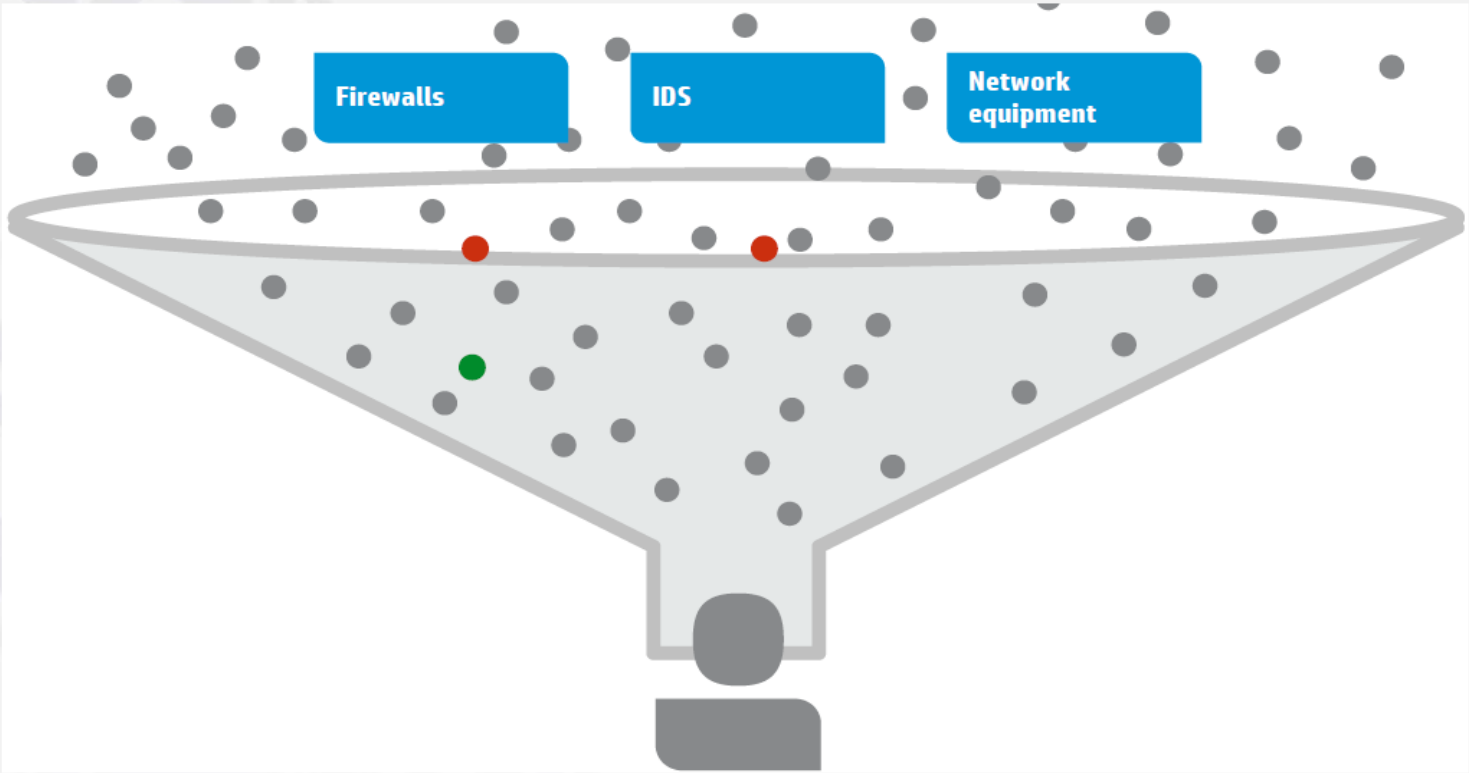


2nd Generation SOC: 1996 2001

Malware outbreaks & intrusion detection

MSSPs begin to offer SOC as a service to customers

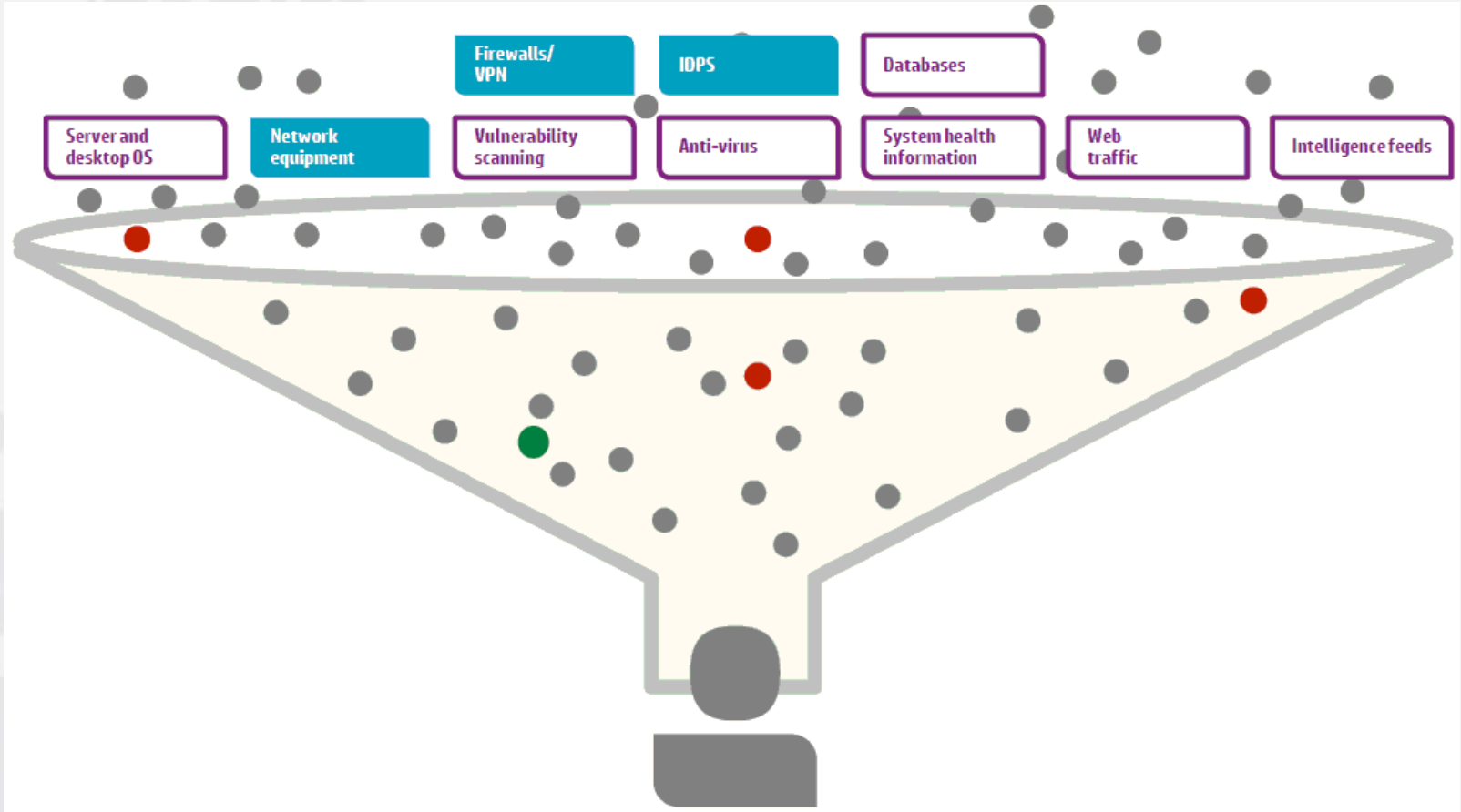
SIEM concepts are introduced



3rd Generation SOC: 2002 2005

Botnets, cybercrime, intrusion prevention, and compliance

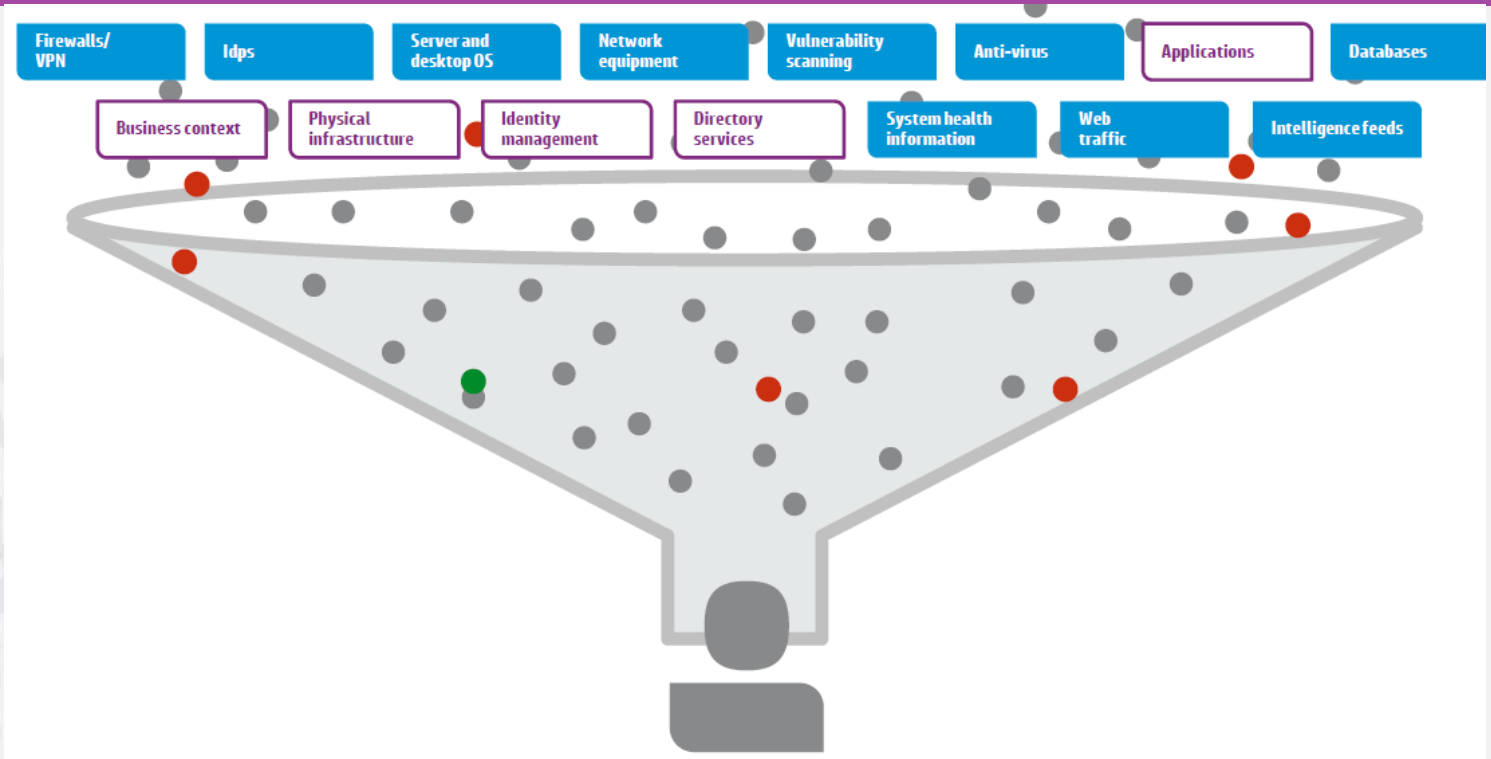
Largest companies in specific industries create SOCs internally



4th Generation SOC: 2006 today

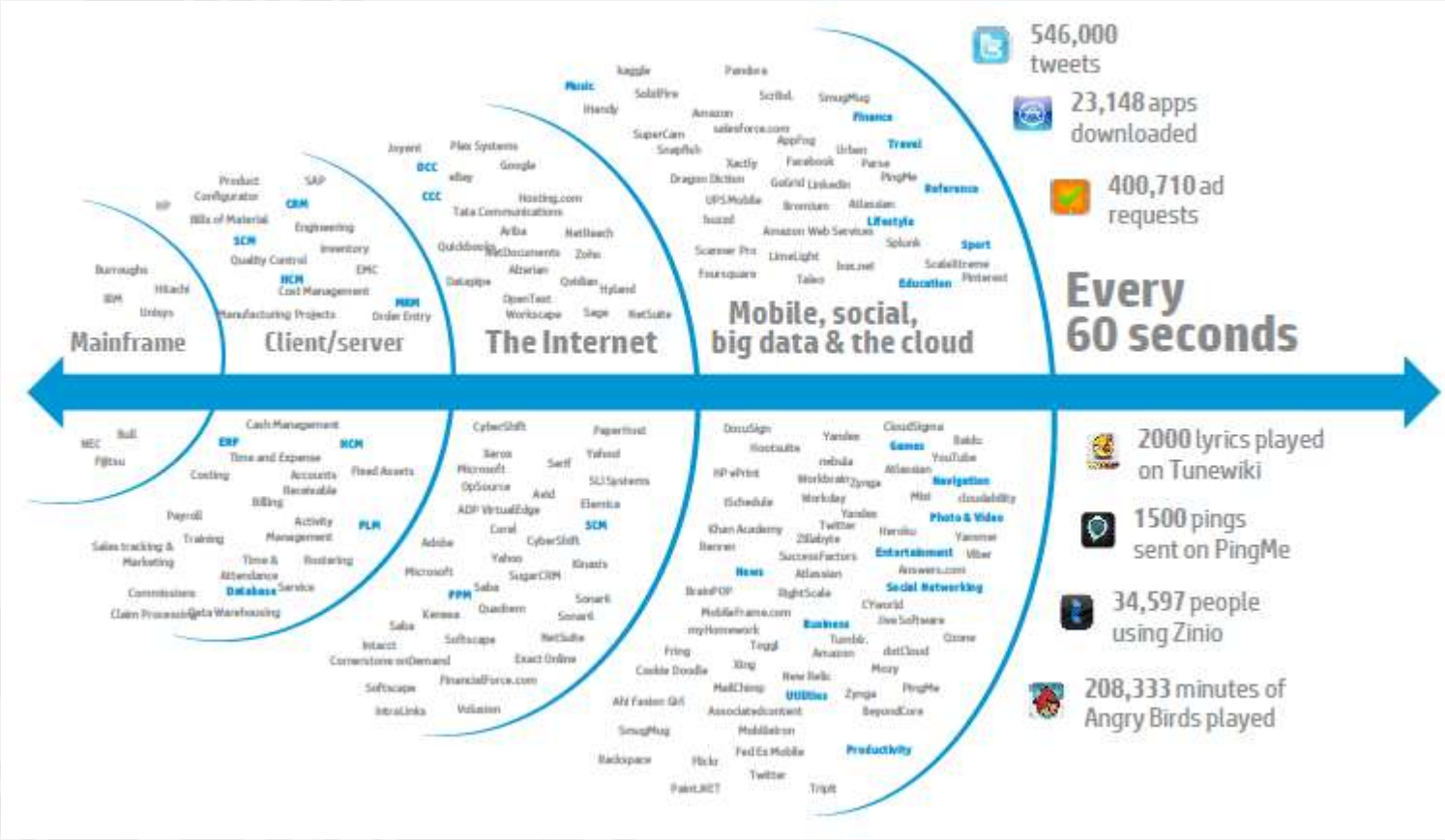
Hacktivism, intellectual property theft, advanced persistent threat(APT)

Wide adoption of continuous security monitoring as breaches fill headlines



5th Generation SOC: 2013 ?

Subtle threat detection, hunt teams, counter-intel, anti-fragile, Advanced analytics, big data



Security Operations Maturity Model (CMMI Based)

SOMM Level	Name	Description
Level 0	Incomplete	Operational elements do not exist
Level 1	Performed	Minimum compliance requirements to provide security monitoring are met
Level 2	Managed	Business goals are met and operational tasks are repeatable
Level 3	Defined	Operations are well-defined, subjectively evaluated, and flexible
Level 4	Measured	Operations are quantitatively evaluated, reviewed consistently, and proactively improved
Level 5	Optimizing	Operational improvement program has been implemented to track any deficiencies and ensure all lessons learned continual drive improvement

People (Personnel)

People Skills

- 724
- Forensics knowledge
- Proficiency in coding, scripting and protocols
- Managing threat intelligence
- Breach management
- Penetration testing
- Data analysts
- Minimum two years of experience in NID monitoring and incident response.
- Familiarity with network security methodologies, tactics, techniques and procedures.
- Experience with IPS/IDS, SIEMs and other CND security tools.
- Ability to read and write Snort IDS signatures.
- Experience reviewing and analyzing network packet captures.
- Experience performing security/vulnerability reviews of network environments.
- Possess a comprehensive understanding of the TCP/IP protocol, security architecture, and remote access security techniques/products.
- Experience with enterprise anti-virus solutions, virus outbreak management, and the ability to differentiate virus activity from directed attack patterns.

People Skills

- Working knowledge of network architecture.
- Strong research background, utilizing an analytical approach.
- Candidate must be able to react quickly, decisively, and deliberately in high stress situations.
- Strong verbal/written communication and interpersonal skills are required to document and communicate findings, escalate critical incidents, and interact with customers.
- Highly motivated individual with the ability to self-start, prioritize, multi-task and work in a team setting.
- Ability and willingness to work shifts ranging within 7:00 AM EST 11:00 PM EST.

MOST-WANTED SKILLS

Here are guidelines for desired skill sets in your security operations center.

	Windows	Unix	Script writing	C/Java//Perl programming	App development	Pen testing	Packet analysis	Forensic	Networking
Level 1 Analyst	L	L							L
Level 2 Analyst	M	L	L	L					M
Level 3 Analyst	H	M	M	M	L	M	M	L	H
Level 4 Analyst	H	H	H	M	L	H	H	M	H

Knowledge level key: L=low, M=medium, H=high

Principle Duties and Responsibilities:

- Monitor and analyze network traffic and IDS alerts.
- Investigate intrusion attempts and perform in-depth analysis of exploits.
- Provide network intrusion detection expertise to support timely and effective decision making of when to declare an incident.
- Conduct proactive threat research.
- Review security events that are populated in a Security Information and Event Management (SIEM) system.
- Analyze a variety of network and host-based security appliance logs (Firewalls, NIDS, HIDS, Sys Logs, etc.) to determine the correct remediation actions and escalation paths for each incident.
- Independently follow procedures to contain, analyze, and eradicate malicious activity.
- Document all activities during an incident and providing leadership with status updates during the life cycle of the incident.
- Create a final incident report detailing the events of the incident
- Provide information regarding intrusion events, security incidents, and other threat indications and warning information to US government agencies! (NASA)
- Assist with the development of processes and procedures to improve incident response times, analysis of incidents, and overall SOC functions.

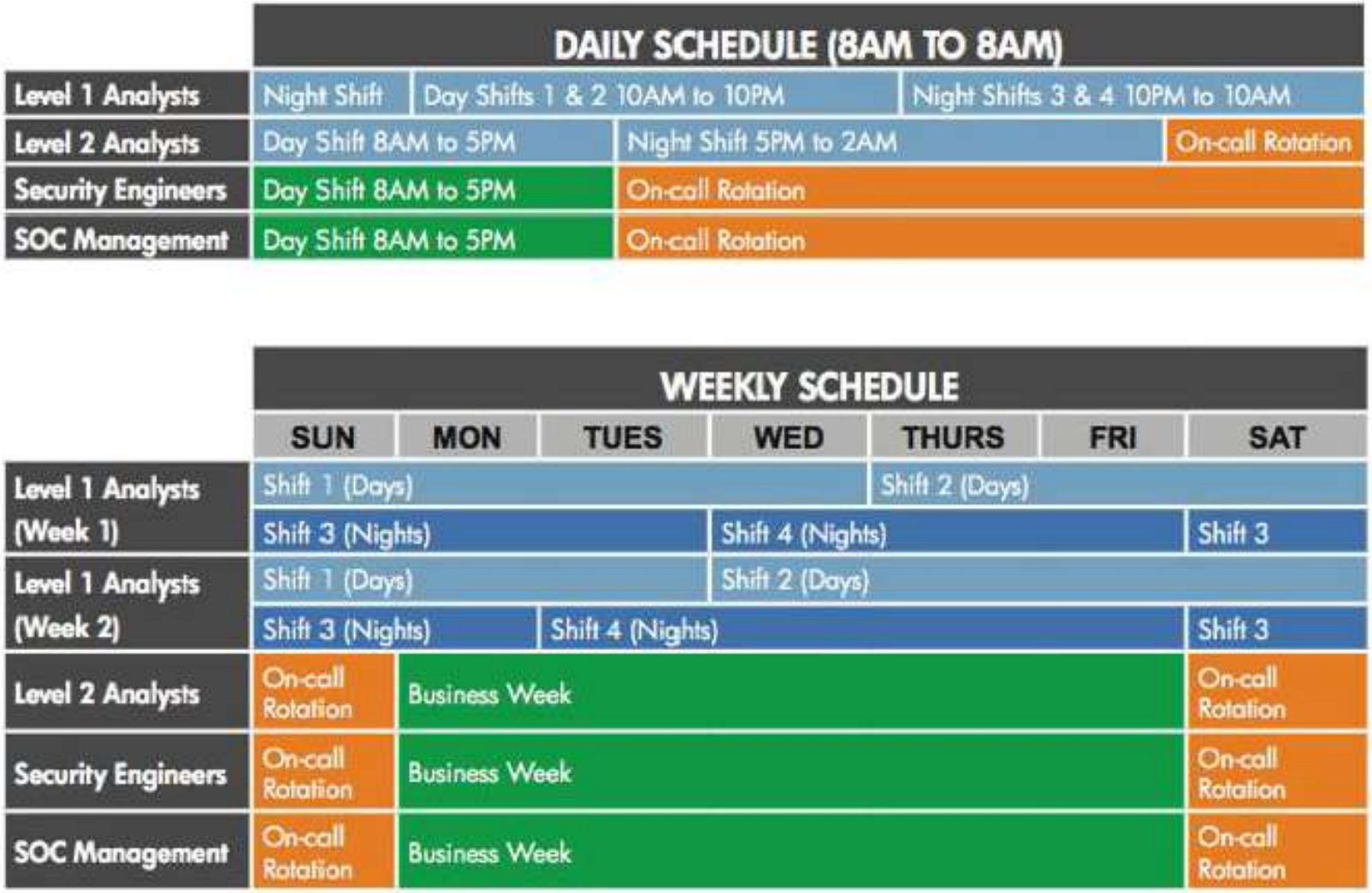
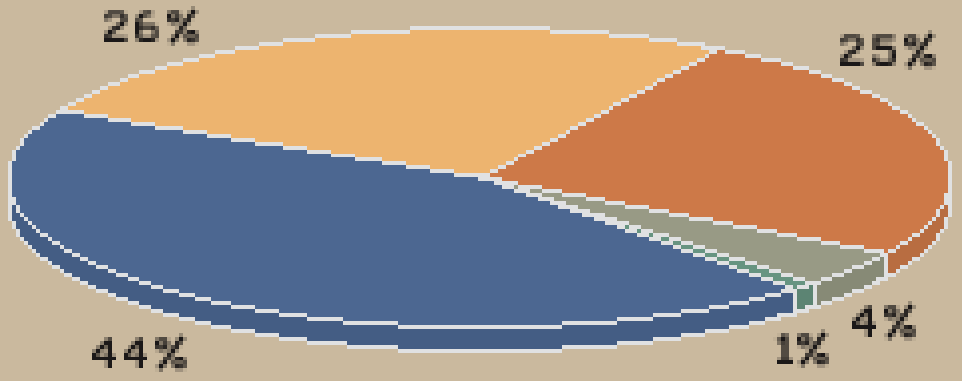


Figure 1: Sample 24x7x365 SOC shift schedule

READER POLL

How well is your SOC staffed?

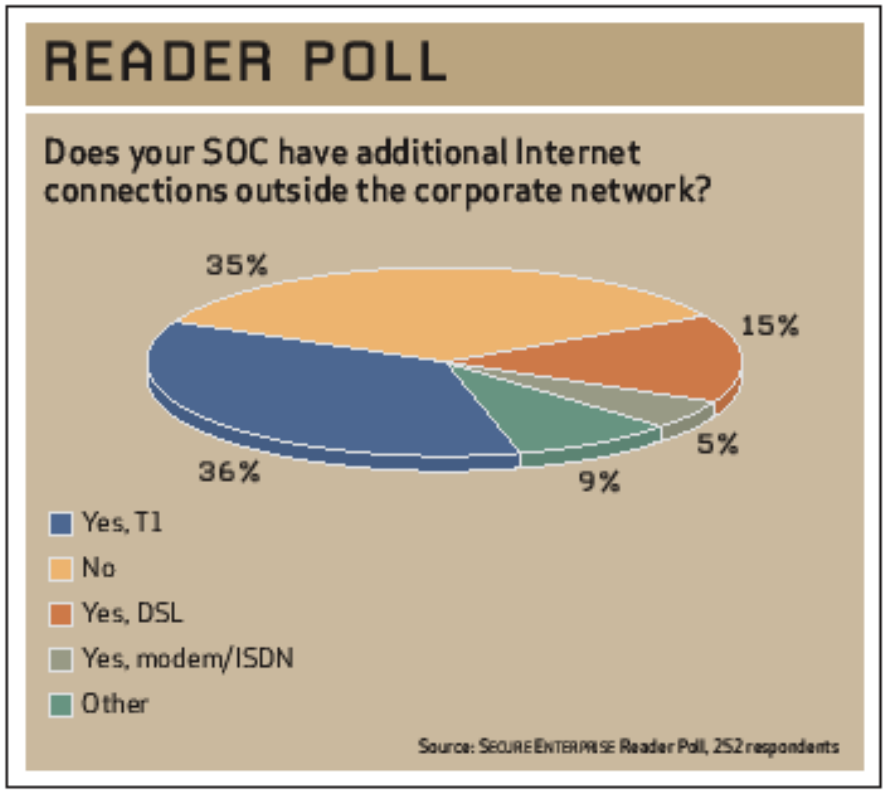


- 7 day a week, 24 hours a day
- During normal business hours only
- During normal business hours with on-call paging
- Outsourced
- Other

Source: SECURE ENTERPRISE Reader Poll, 252 respondents

Some Points:

- SOC Security
- Environment (Location, Temperature, Humidity, Ergonomics, Lighting)
- Collect as much as you can, even if you don't have the capacity to analyze it in real time. Because if you store it, it may become useful to you later on
- A network connection to the Internet separate from your corporate network.
- Dedicated phone lines
- A fax line
- Documentation
- A secure wireless network
- Electrical Power (UPS)
- Clear Responsibilities (Duties, Time shifting, …)
- Easy of Use



Resources:

- Building a successful SOC (HP whitepaper)
- 5G/SOC: The NOW of security operations (HP whitepaper)
- 5G/SOC: Inside the world's most advanced SOCs (HP WP)
- How mature is your SOC? (HP WP)
- SECURITY OPERATION CENTER (Reply communication valley)
- arming_your_security_operations_center_with_the_right_technology_and_services (WIPRO.com)
- Building Security Operation Center (HP presentation)
- Building, Maturing & Rocking a Security Operations Center (Brandie Anderson)
- intelligence-driven-security-ops-center (RSA Technical Brief)
- Anatomy of a Security Operations Center (By John Wang, NASA SOC)
- Best Practices for Building a Security Operations Center (Diana Kelley and Ron Moritz)
- Creating an Effective Security Operations Function (RSA Whitepaper)
- Wikipedia.com
- Build Your Own Security Operations Center (Jay Milne)
- Do You Need A Security Operations Center? (Robert Lemos)
- Best Practices for SOC Design (David G Aggleton)
- …


Thank You!
☺