Security Tool Alignment to Cyber Kill Chain[1]

Coleman Kane
Coleman.Kane@ge.com

August 22, 2014

Attack Landscape

Extranet The networked world outside your network with which your users require access. Generally not under your control.

Intranet The networked world inside your perimeter, which is under your control

Host A node within a network, consisting of servers, PCs, routers, etc.

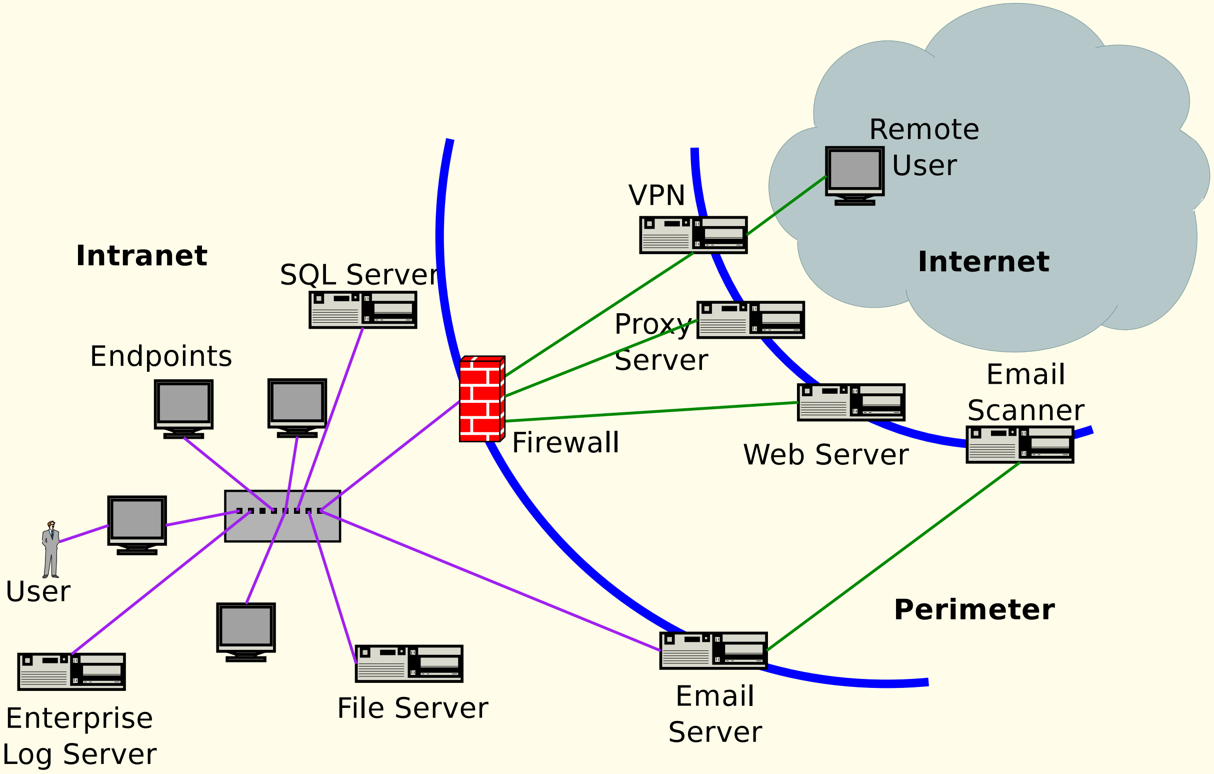
Perimeter The network devices and systems which are connected to at least one extranet as well as an intranet. Generally these act as monitors, gateways, and service providers

Endpoint A type of *host* which is the connection between a user and your *intranet*

Network Architecture

- Web servers providing content to customers, installed at perimeter
- Extranet not "layer 3"-routable by non-Perimeter Intranet devices
- HTTP proxy server installed at Perimeter to provide users with Extranet connectivity
- Endpoints installed in Intranet
- Remote users may connect to a VPN system, installed at the Perimeter, which connects their endpoint to the Intranet network
- Perimeter devices are "layer 3"-routable by all Intranet hosts, and vice-versa

Visual


Remote User
VPN
Internet
Intranet
SQL Server
Endpoints
Proxy Server
Email Scanner
Firewall
Web Server
User
Perimeter
Enterprise Log Server
File Server
Email Server

Cyber Kill Chain[1] Alignment (1-4)

Alignment against phases 1-4, where attacker attempts to gain access

Reconnaissance	Weaponization	Delivery	Exploit
VPN Server logs		Perimeter Proxy	Perimeter Proxy
Mailserver logs		Mailserver Logs	Host Anti-Virus
Webserver logs	E-mail Scanning	E-mail Scanning	E-mail Scanning

Metrics:

- **Best Coverage = 3**: Reconaissance, Delivery, & Exploit phases
- **Worst Coverage = 1**: Weaponization phase

Cyber Kill Chain[1] Alignment (5-7)

Alignment against phases 5-7, where attacker has gained some level of access

Installation	Command & Control	Actions on Objectives
		Endpoint Remote Desktop Logs
	Perimeter Proxy	Perimeter VPN Logs
	Host Firewall	Host Firewall
	Intranet Firewall	Intranet Firewall
Host Anti-Virus		Host Anti-Virus

Metrics:

- **Best Coverage = 5**: Actions on Objectives phase
- **Worst Coverage = 1**: Installation phase

Cyber Kill Chain[1] Alignment (conclusion)

- Measure coverage points of failure/redundancy
- Identify per-tool coverage breadth
  - **Broadest**: E-mail scanner (3), Perimeter Proxy (3), Host Anti-Virus (3)
- Not uncommon to have more coverage for higher phases, as risk increases so does investment

References

[1] Lockheed Martin Corporation. Cyber kill chain®.
http://www.lockheedmartin.com/us/what-we-do/information-technology/cyber-security/cyber-kill-chain.html. Cyber Kill Chain is a registered trademark of Lockheed Martin Corporation.