From: Company CEO

To: IT Staff

Subject: Incident Reports

As you catch bad guys actively connecting to our systems, I'd like to know about it. Fill out a report and send it to me. You can use this incident report form our previous admins used or you can come up with your own format if you'd like. If using your own format be sure to provide the same information as the current form (but you can add anything else you think helps).

At a bare minimum you have to include the source IP address of the incident, the target of the incident, what the attackers are using to maintain access, and what you did to address the incident. I am only interested in active connections that you find; you do not need to report anything that does not have an active connection with an external IP.

Thanks,

Company CEO