From : Your Boss <bill.tench@techmaster.milxc>

To : You <terry.page@techmaster.milxc>

Subject: Incident management

Hey Terry,

I hope this email finds you well.

The SOC escalated me a SIEM alert that has been triggered few hours ago concerning our customer CandyRiver SAS – a customer specialized in the candy e-commerce. It seems their NIDS detected something bad enough to be escalated to the team.

This is not a false positive obviously. We have been able to reach out the CISO of the customer that provides valuable information to better understand the situation. The meeting notes have been attached to this email.

I'd like you to setup an incident response team to tackle this issue. This customer is strategic and we need to be professional and provide them the assistance they deserve. A detailed incident report is expected as usual.

You'll find more details about the alert below:
- Rule name: Suspicious HTTP POST request
- Severity: P1 (Critical)
- Initial source: Suricata
- Server source: dmz-web (10.87.1.2)
- Remote IP: 100.120.0.4
- Raw log:
10/20/2024 [**] [1:283:3] Suspicious HTTP POST request [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 100.120.0.4 -> 10.87.1.2

Good luck to manage this case and keep me posted.

Regards,

Bill Tench
CSIRT Manager