Environmental Context

Table of Contents

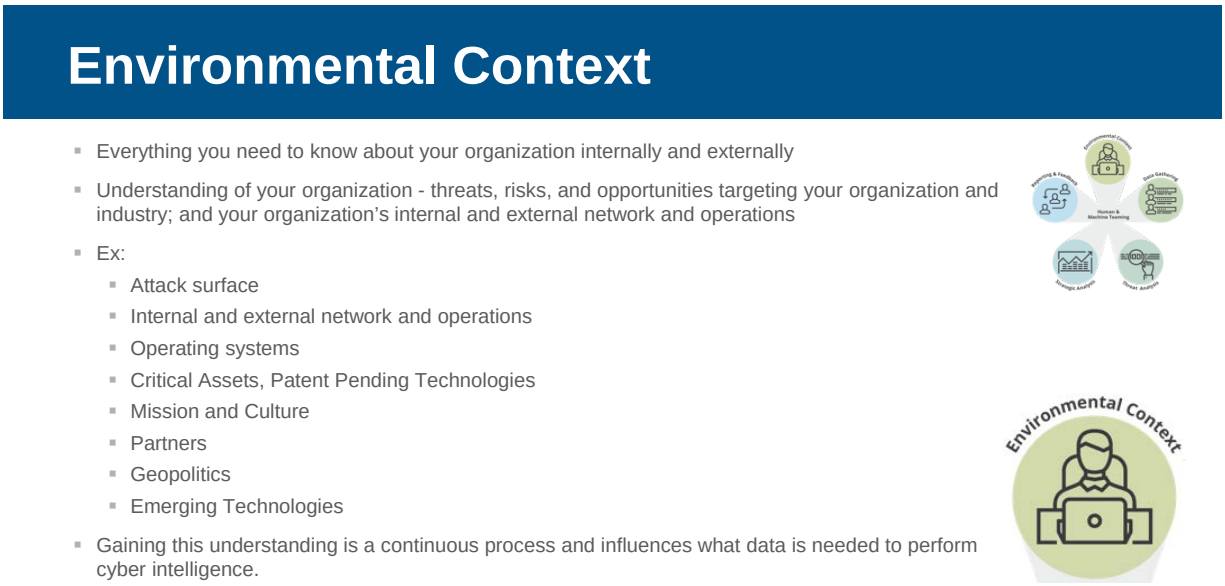
Environmental Context

Environmental Context

22

**022 Let's talk about environmental context.

Environmental Context



**023 What environmental context means is having a deep understanding of your organization, including your organization's entire attack surface; threats, risks, opportunities targeting your organization and industry, and your organization's internal and external network and operations. Gaining this understanding is a continuous process and influences what data is needed to perform cyber intelligence.

More specifically, a cyber intelligence analyst would want to know the entire attack surface, which includes internal and external network and operations, servers, operating systems, endpoints. Your organization's mission and culture. Processes, policies, business partners, suppliers, geopolitics,

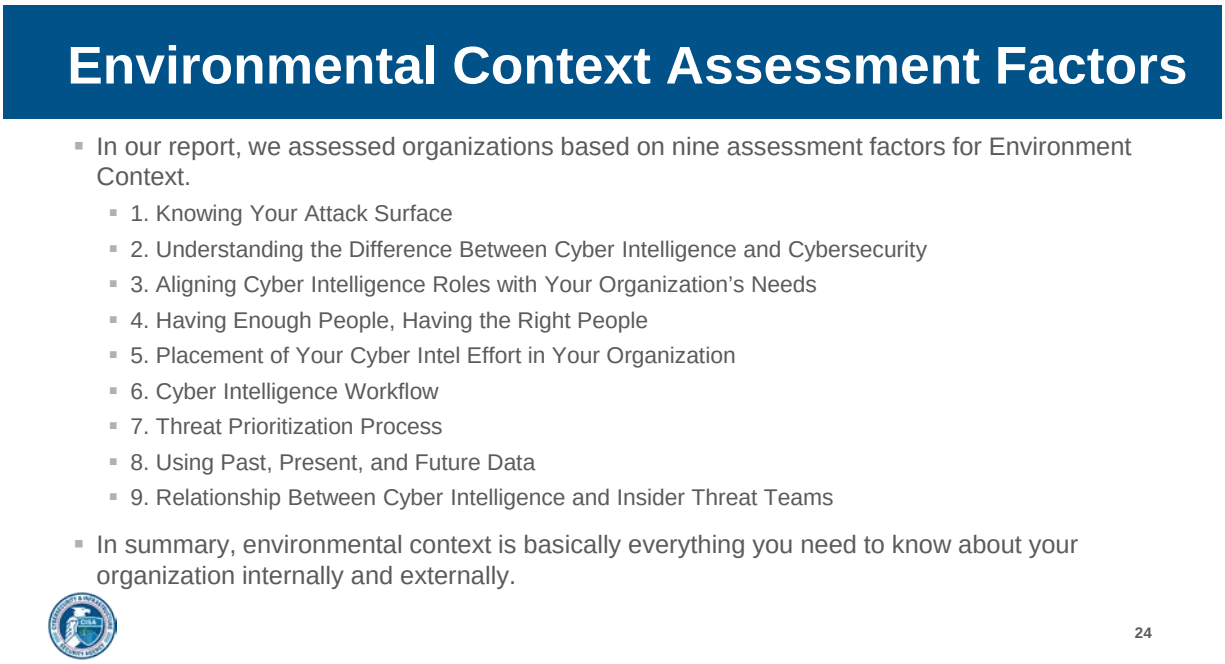
emerging technologies, and position in industry relative to competitors.

In other words, some questions you might want to ask are, "What is my network, how big is it? Do I have subnets? Where are my hosts? How many hosts do I have, how many servers, where are they located? What kind of cloud infrastructure do I have? What is in the cloud? Do I have a complete and accurate inventory of everything, hardware and software, and what OS is used, mobile systems? What about company policies?"

"What are my suppliers and third-party business operators, and what do you know about your building security? Where are your buildings located? Are some in foreign countries, and what is located in near, around those buildings?"

Other things to consider, the culture of your organization, your business. What are you trying to sell? What is your IP? And who would want your IP in your critical assets? Who has access to those assets now and in the past? Who are your major competitors, and what new inventions is your organization working on?

Environmental Context Assessment Factors



**024 In our report, we assessed organizations based on nine assessment factors for environment context. These involve knowing your attack surface, having a cyber intelligence effort positioned in the organization to be able to know the attack surface, and having the people to do the work.

We actually assessed organizations based on nine assessment factors. So again, knowing your attack surface, one. Understanding the difference between cyber intelligence and cybersecurity was two. The third is aligning cyber intelligence roles with your organization. Four, does your organization have enough people, and does it have the right people? The fifth is are you placing your cyber intelligence effort in the right place in your organization so it's

able to understand the entire attack surface? The sixth was does your organization have a cyber intelligence workflow to be able to do cyber intelligence. The seventh is a threat prioritization process. Is your organization able to effectively prioritize threats that that are targeting itself and its industry? Is your organization, eight, able to use past, present and future data effectively in order to make assessments about threats? And the ninth assessment factor was the relationship between cyber intelligence and insider threat teams.

So in summary, environmental context is basically everything you need to know about your organization internally and externally.

Notices

Notices