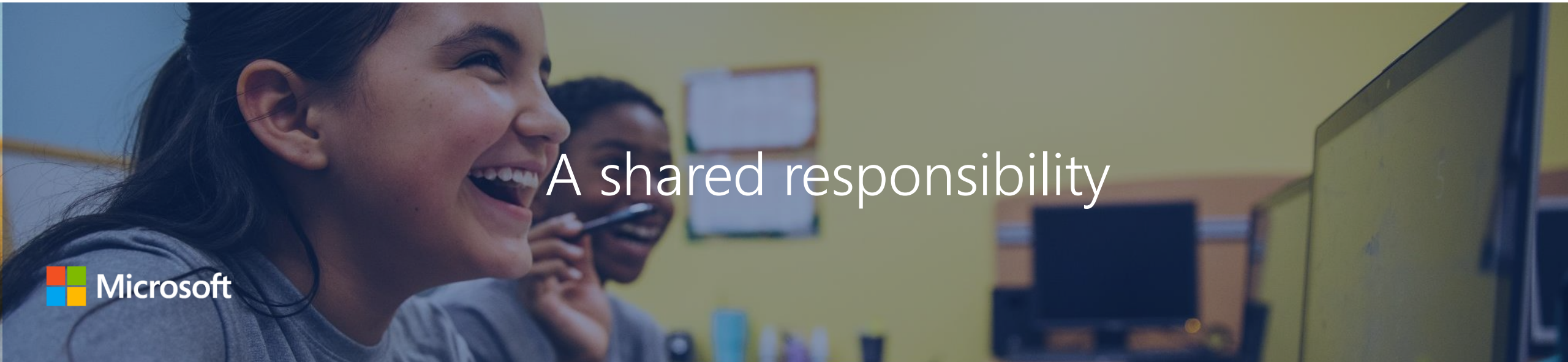
Microsoft's commitment to Digital Peace

Microsoft

"Cyberspace, unlike the traditional planes of warfare like land, sea and air, is typically privately owned. Cyberspace in fact consists of concrete elements in the real world, such as data centers, undersea cables, and laptops and mobile devices…. While the tech sector has the first and highest responsibility to protect this technology and the people who rely upon it, this is an issue that requires that governments, companies and civil society come together."

Brad Smith, Microsoft President



What can the industry do

Microsoft follows coordinated vulnerability disclosure

- ISO/IEC 29147:2018 on Vulnerability Disclosure
- The CERT Guide to Coordinated Vulnerability Disclosure

WE WANT TO AWARD GOOD RESERACH

- Submissions that contain steps to reproduce your proof of concept cope along with detailed analysis are eligible for higher awards as they help us quickly assess the risk

WE ARE LOOKING FOR NEW VULNERABILITIES

- Your contributions help us address vulnerabilities we may have missed in the development process. If you are the first external researcher to identify a vulnerability we already know about and are working to fix you may still be eligible for an award.

AVOID HARM TO CUSTOMER DATA, PRIVACY AND SERVICE AVAILABILITY

- Some security research may occur on production services that our customers use and depend on. Do you best to avoid research that violates customer privacy, destroys data, or interrupts series. Fi you discover customer data while researching, or are unclear if it is safe to proceed please stop immediately and contact us.

THE RULES

- The Microsoft Bug Bounty Programs are subject to the legal terms and conditions outlined here, and our bounty Safe Harbor policy.


Microsoft
Cybersecurity Tech Accord

Protect all of our users and customers everywhere.

Oppose cyberattacks on innocent citizens and enterprises.

Increase cybersecurity capabilities everywhere.

Help each other respond to cyberattacks.

digital COOPERATION

GCSC

PARIS 11 · 12 CALL FOR TRUST AND SECURITY IN CYBERSPACE

WHOIS

GLOBAL CYBER ALLIANCE

Cybersecurity Tech Accord: Key Initiatives

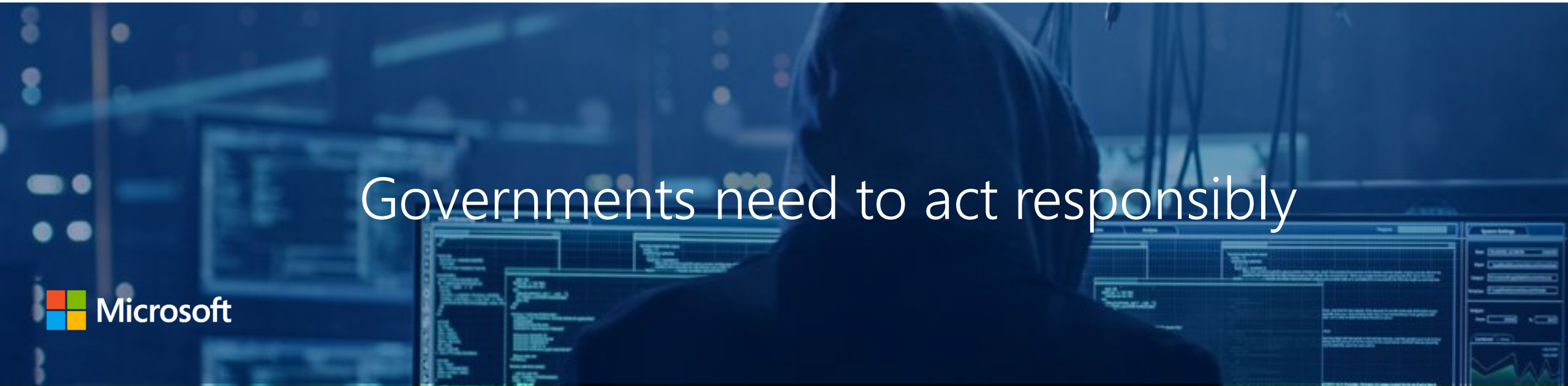
MANRS

GFCE Global Forum on Cyber Expertise

Microsoft

Microsoft

"States should have a clear principle-based policy for handling product and service vulnerabilities that reflects a strong mandate to report them to vendors rather than to stockpile, buy, sell, or exploit them.



Governments need to act responsibly

Microsoft

Governments role in disclosing vulnerabilities

Microsoft

- Increase legal certainty for security researchers;
- Raise awareness of the importance of disclosure for vendors and agencies;
- Expand funding for defensive vulnerability discovery and research;
- Develop and make public the criteria used in determining whether to disclose a vulnerability;
- Mandate that all government-held vulnerabilities, go through an evaluation process leading to a decision to disclose or retain it;
- Presume disclosure as the starting point;
- Define the process of making a disclosure decision and ensure that stakeholders involved include national security and law enforcement, but also economic, consumer, and diplomatic interests;
- Prohibit use of contractors or other third parties as a means of circumventing the disclosure process;
- Ensure any decision to retain a vulnerability is subject to a six-month review;
- Establish oversight through an independent body within the government with an annual public report on the body's activities;
- Ensure that any retained vulnerabilities are secure from theft (or loss).


Microsoft
Annex

What are we talking about?

Microsoft

A weakness in a product that could allow an attacker to compromise the integrity, availability, or confidentiality of that product.

SECURITY VULNERABILITY

A software program or sample code that (when executed against a vulnerable system) uses a security vulnerability to cause unintended or unanticipated behavior.

EXPLOIT

Takes advantage of a security vulnerability on the same day that the vulnerability becomes generally known.

There are zero days between the time the vulnerability is discovered and the first attack.

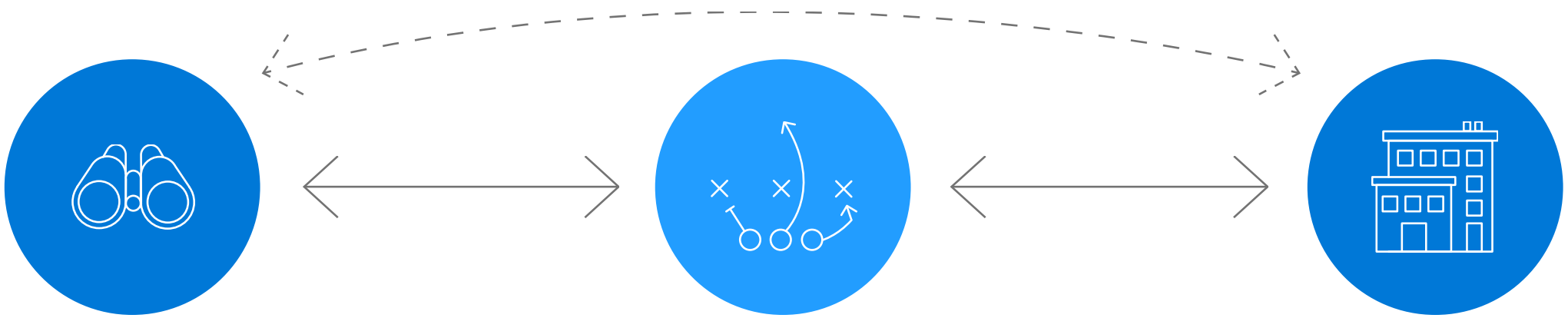
ZERO DAY EXPLOIT

COORDINATED VULNERABILITY DISCLOSURE (CVD)

CVD is about minimizing risk – for customers, businesses, and critical infrastructures.

Coordinated vulnerability disclosure (CVD): roles and principles

Microsoft



FINDERS

A security researcher finds and discloses newly discovered vulnerabilities directly to:

- **the vendors of the affected product or service; or,**
- **a coordinator.**

(If active exploit, then maybe publicly with coordination on mitigations.)

COORDINATORS

Often a CERT/CSIRT or a bug bounty provider. Cooperatively works with finders and vendors to privately disclose newly disclosed vulnerabilities directly to the vendor of the affected product or service. Acts as intermediary between finders and vendors.

VENDORS

Has a way to receive vulnerability reports. Coordinates with finders throughout the vulnerability investigation and provides the finder with updates on case progress. Diagnose and offer fully tested patches, workarounds, or other corrective measures.

Why are we talking about CVD now?

Microsoft

INCREASING GOVERNMENT CONCERN ABOUT CYBERSECURITY

- Increasing dependence, understanding of potential risk.
- Vulnerabilities are a major cause of security incidents.

INTERNET OF THINGS (IOT)

- Major IT vendors have been working on CVD for more than a decade.
- IoT vendors are new “technology providers” but haven’t started putting CVD processes in place.