BlueHat CFP Instructions

We have done our best to make the submission process as simple as possible. This year, you can submit your proposal via our new CFP submission portal: **https://aka.ms/bhcfp/**

CFP Timeline

Please submit your proposals by **August 18th, 2017**. Notification of acceptance will be sent out 1-2 weeks later. Here are the important dates to remember:

- **CFP Open**: June 1st, 2017
- **CFP Close:** August 18th, 2017
- **Speaker Notifications:** August 31st, 2017

CFP Themes

Some possible themes we are interested in seeing abstracts on are:

- Virtualization & Cloud-based research, exploits, and defense
- How customers are getting owned (case studies, threat intelligence, and research)
- New Exploit techniques
- Emerging Threats & Trends
- Anti-exploitation techniques
- Identity & Authentication research, exploits and defense
- Infrastructure & IoT Security research, exploits and defense
- Industry & Government Roles in Cybersecurity

A limited number of presentation spaces are available and all submissions will be reviewed by the Content Advisory Board on a rolling basis until all talk slots are filled. Presentations should target 30-minute or 60-minute format with no more than three speakers specified. Some presentations will be selected to present to Microsoft executives in a smaller format in addition to the large format at the event.

How to Submit Your Paper

Step 1: Go to **https://aka.ms/bhcfp/**

Step 2: Login to the submission portal.

NOTE: If you are a Microsoft employee, click “Microsoft Login”. If you are an external guest, click “Create Account” or “Login”.

Step 3: Click “Create New Submission”. The new submission page will prompt you to enter the following:

1. **Talk Title*** – this is the talk title that will be posted on the website schedule.
2. **Abstract*** – provide us with an abstract about what you will be presenting at the conference (2000 characters maximum). This is the abstract that will be posted on the website schedule, so please make sure that it is in complete sentences and that it is written in the third person.
3. **Authors*** – list all the individuals who have contributed to this proposal. Provide us with each author's name, email address, and the company/organization name. You will need to identify no more than THREE presenters in the section below.
4. **Subject Areas*** - select the topics that best represent the content of your proposal.
5. **Files** – upload your presentation slides or supportive files (optional).
6. **Time*** - your presentation should target 30-minute or 60-minute format, including approximately 10-15 minutes for Q&A at the end of the presentation.
7. **Live Streaming and Recording* -** all BlueHat presentations will be live-streamed and recorded.
8. **Call to Action*** – the heart of the BlueHat conference is the practical and innovative content. It would be extremely beneficial to our attendees if the speakers can offer a couple actionable takeaways. Hence, we ask all BlueHat speakers to provide strong calls to action in their presentations.
9. **Presenter(s)*** – provide us with each presenter's name, email, organization, and biography. Talks with more than 3 presenters will not be accepted.
10. **Experience Level*** – identify the knowledge level of your targeted attendee (Beginner, Intermediate, Advanced, Any).
11. **Additional requirements** - list any technical requirements that you have for your presentation over and above the standard projector, screen and wireless Internet.

The authors can always login to update the submission before we close the CFP on August 18th, 2017.

If you have any questions regarding the submission process, please don't hesitate to contact us at bluehat@microsoft.com.

Tips and Guidelines

The heart of the BlueHat conference is the practical and innovative content. Based on our experience with the past BlueHat events, it would be extremely beneficial to our attendees if the speakers provide a couple actionable takeaways in their presentations. Also, this is the abstract that will be posted on the website schedule, so please make sure it is in complete sentences and written in the third person.

We definitely do not expect every presentation to have technical deep-dives but a sales or marketing pitch is something you should avoid when preparing your talk.

Here are some good examples:

Attackers Hunt Sysadmins. It's time to fight back

Lee Holmes |Microsoft

What do the NSA, APT groups, and run-of-the-mill attackers have in common? They. Hunt. Sysadmins. After all, what's a better way to compromise an entire infrastructure than to target the folks with complete and unconstrained access to it? It's time to fight back. In this talk, we introduce PowerShell Just Enough Administration, a powerful platform capability that lets you add role-based access controls to your existing PowerShell-based remote management infrastructure.

Windows Management Instrumentation - The Omnipresent Attack and Defense Platform

Matt Graeber | Veris Group

A resourceful attacker seeking to maximize his or her compromise/effort ratio will naturally target any omnipresent technology present in a homogeneous environment. Windows Management Instrumentation (WMI) is one such technology that is present and listening on every Windows operating system dating back to Windows 95. WMI is a powerful remote administration technology used to get/set system information, execute commands, and perform actions in response to events. While it is a well-known and heavily used technology by diehard Microsoft sysadmins, attackers (i.e. diehard unintended sysadmins) find such built-in technology enticing, especially those who wish to maintain a minimal footprint in their target environment. In reality, targeted and criminal actors are making heavy use of WMI in the wild and defenders need to be informed of its capabilities both from an offensive and defensive perspective. This talk aims to inform the audience of the basics of WMI, in the wild attacks, theoretical attack scenarios, and how defenders can leverage the WMI eventing system against an attacker.

Call to Action:

- Attackers are actively using WMI
- Set and audit namespace ACLs accordingly
- Fight WMI with WMI

Network Defense- Isolation Enforcement

Scott Longheyer | Microsoft

Some things are meant to be shared, some are not. From dedicated to software-defined networks, we discuss modern solutions to enforce network isolation in extremely dynamic, often exposed, single or multi-tenant hosting environments. The tools are getting better, let's wield them. Network certifications are not required to attend.

Call to Action:

- Differentiate based on asset purpose
- frontend vs backend vs corporate
- Apply policy to block/detect traffic that is not explicitly allowed.
- Network-level isolation between the control network and corporate network is an absolute requirement.
- Allow remote access only to legitimate users and services; leverage Endpoint ACL's
- Keep each host on only one network.
- Jump-box, Web, or DB servers are rarely the best gatekeepers (or routers).

Secure Development for Snake People: New Ideas for the Next Generation

Leigh Honeywell and Ari Rubinstein | Slack

Startups hear the word “process" and freak out - shipping code every day isn't optional. What if you could build a secure development process that accelerated development, instead of slowing it down? At Slack, we have - allowing our small team to distribute security work to developers, and building up their security skills from intern to senior engineer. We'll talk through the tools and processes we built - a flexible, open source framework including a lightweight self-service assessment tool, a checklist generator, and most importantly a chat-based process. Together, these encourage security thinking in the tools developers already spend their time in - allowing us to effortlessly document people's thought processes around risk. By empowering developers to think about security themselves and incorporate secure practices into their own teams and workflows, we've defeated the fear of the checkbox and replaced it with new tooling and process that teams actually want to work with.

If you are not sure about your abstract, reach out to us at bluehat@microsoft.com and we will be more than happy to work with you on your proposal.