

WORK-FROM-HOME AND COVID-19:

TRAJECTORIES OF ENDPOINT
SECURITY MANAGEMENT IN A
SECURITY OPERATIONS CENTER

*KAILANI R. JONES*¹, *DALTON A. BRUCKER-HAHN*²,
*BRADLEY FIDLER*³, *ALEXANDRU G. BARDAS*¹

¹ UNIVERSITY OF KANSAS, ² SANDIA NATIONAL LABORATORIES, ³ INDEPENDENT RESEARCHER

² PART OF THIS WORK COMPLETED WHILE AT THE UNIVERSITY OF KANSAS

³ PART OF THIS WORK COMPLETED WHILE AT STEVENS INSTITUTE OF TECHNOLOGY

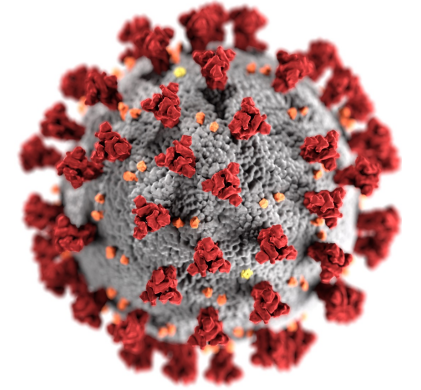
COVID-19 -- Working from Home

Covid-19 Hastens the Work-at-Home Revolution

Parents, children and employers are seeing personal and productive benefits.

By Erica Komisar [1]

Aug. 3, 2020 6:57 pm ET



COVID-19 -- Working from Home

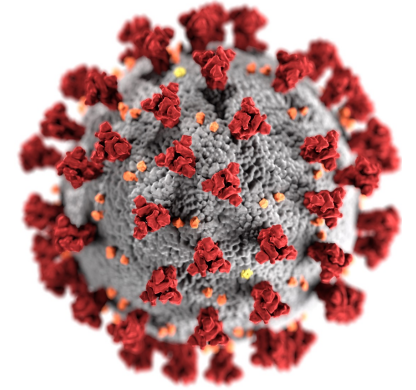
Covid-19 Hastens the Work-at-Home Revolution

Parents, children and employers are seeing personal and productive benefits.

By Erica Komisar [1]
Aug. 3, 2020 6:57 pm ET

Admin Jobs Projected to Stay Remote After COVID-19

By Roy Maurer [2]
July 30, 2020



COVID-19 -- Working from Home

Covid-19 Hastens the Work-at-Home Revolution

Parents, children and employers are seeing personal and productive benefits.

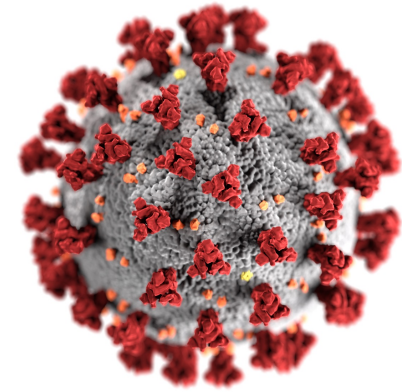
By Erica Komisar [1]
Aug. 3, 2020 6:57 pm ET

Admin Jobs Projected to Stay Remote After COVID-19

By Roy Maurer [2]
July 30, 2020

July 27, 2020 3:52 PM
VOA News [3]

Google Employees to Work from Home Until 2021



COVID-19 -- A Chance to Strike

The Pandemic's Lasting Effects: Are Cyber Attacks One Of Them?



Jesper Zerlang Forbes Councils Member
Forbes Technology Council COUNCIL POST

[4]

Article [Cedric Nabe](#)
Partner [5]

Impact of COVID-19 on Cybersecurity



COVID-19 -- A Chance to Strike

The Pandemic's Lasting Effects: Are Cyber Attacks One Of Them?



Jesper Zerlang Forbes Councils Member
Forbes Technology Council COUNCIL POST

[4]

How COVID-19 has made small businesses more vulnerable to cyberattacks

By Egidijus Navardauskas [6]



Article [Cedric Nabe](#)
Partner [5]

Impact of COVID-19 on Cybersecurity

Cyber Threats Have Increased 81% Since Global Pandemic

McAfee Enterprise and FireEye Highlight At-Risk Industries this Holiday Season [16]

COVID-19 -- A Chance to Strike

The Pandemic's Lasting Effects: Are Cyber Attacks One Of Them?



Jesper Zerlang Forbes Councils Member
Forbes Technology Council COUNCIL POST

[4]

How COVID-19 has made small businesses more vulnerable to cyberattacks

By Egidijus Navardauskas [6]



Article [Cedric Nabe](#)
Partner [5]

Impact of COVID-19 on Cybersecurity

Cyber Threats Have Increased 81% Since Global Pandemic

McAfee Enterprise and FireEye Highlight At-Risk Industries this Holiday Season [16]

The Log4j Vulnerability: Millions of Attempts Made Per Hour to Exploit Software Flaw

Hundreds of millions of devices are at risk, U.S. officials say; hackers could use the bug to steal data, install malware or take control

By [David Uberti](#), [James Rundle](#) and [Catherine Stupp](#)
Updated Dec. 21, 2021 12:15 pm ET | WSJ Pro [7]

COVID-19 -- Effects on Security Operations

CISA Guide to Pandemic Response: Critical Infrastructure
Operations Centers and Control Rooms ^[9]

Is Remote SecOps a Good Long-Term Plan?

By Chris Triolo ^[12]



COVID-19 -- Effects on Security Operations

CISA Guide to Pandemic Response: Critical Infrastructure
Operations Centers and Control Rooms [9]

CISO stress and burnout cause high churn rate

The nature of the CISO role can take a toll, say industry vets, with frustration and stress contributing to high turnover rates and burnout. Learn how to make it work.



By Alissa Irel, Senior Site Editor [11]

Is Remote SecOps a Good Long-Term Plan?

By Chris Triolo [12]



Help Net Security
June 26, 2020

Share



SOC team members battle with burnout, overload and chaos [10]




COVID-19 -- Effects on Security Operations

CISA Guide to Pandemic Response: Critical Infrastructure Operations Centers and Control Rooms [9]

CISO stress and burnout cause high churn rate

The nature of the CISO role can take a toll, say industry vets, with frustration and stress contributing to high turnover rates and burnout. Learn how to make it work.

 By [Alissa Irei](#), Senior Site Editor [11]

Is Remote SecOps a Good Long-Term Plan?

By Chris Triolo [12]

 Help Net Security
June 26, 2020

Share    

SOC team members battle with burnout, overload and chaos [10]



Cybersecurity ops may never be the same after COVID-19, but that's not all bad [8]

[Amos Stern](#) April 6, 2021

COVID-19 -- Effects on Security Operations

CISA Guide to Pandemic Response: Critical Infrastructure
Operations Centers and Control Rooms [9]

Is Remote SecOps a Good Long-Term Plan?

CISO stress

The nature of the CISO role
stress contributing to high

By [Alissa Irel](#), Senior Site Editor

What impacts does COVID-19 have upon Security
Operations Centers (SOCs)?

- Immediate effect
- Long-term consequences



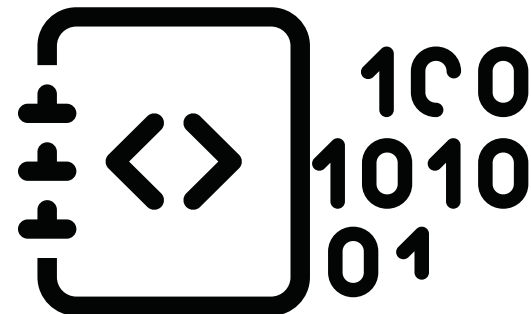
Cybersec
same after COVID-19, but that's not all
bad [8]

[Amos Stern](#) April 6, 2021



First-Hand Experience

- Fieldworker deployed over **34 months** (June '19 to May '22)
 - **1000+ hours in a SOC**
 - 352 field notes from discussions and observations
- Active before, during, and emerging from COVID-19 pandemic
 - Observed first-hand the fundamental shift to endpoint management

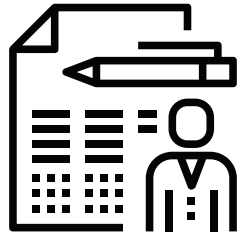
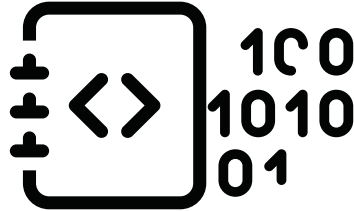


Ethnography

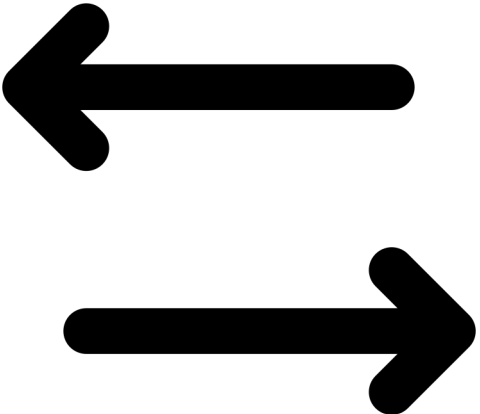


Participant
Observation

Grounded Theory
Method Analysis

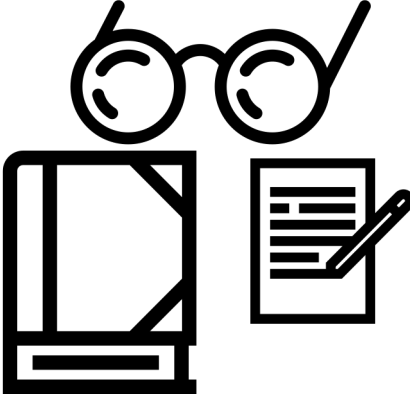


Quan+Qualitative
Interviews



Historical Analysis

Deep Literature
Study



Google Books
Ngram Viewer



Analysis of Historical
Trends and Context



*Additional methodological procedure
details available in the paper (see Fig. 1)*

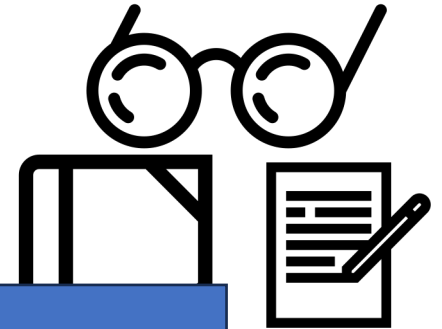
Ethnography



Participant
Observation

Historical Analysis

Deep Literature
Study



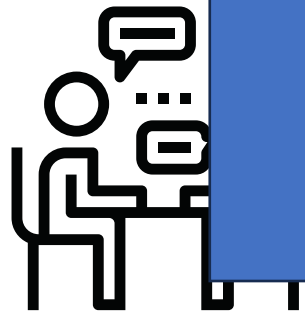
Grounded
Method A

**Our analysis indicates that COVID-19's WFH shift
represents a critical evolution point in SOCs.**

Network Perimeter --> Endpoint Devices



Historical
Context

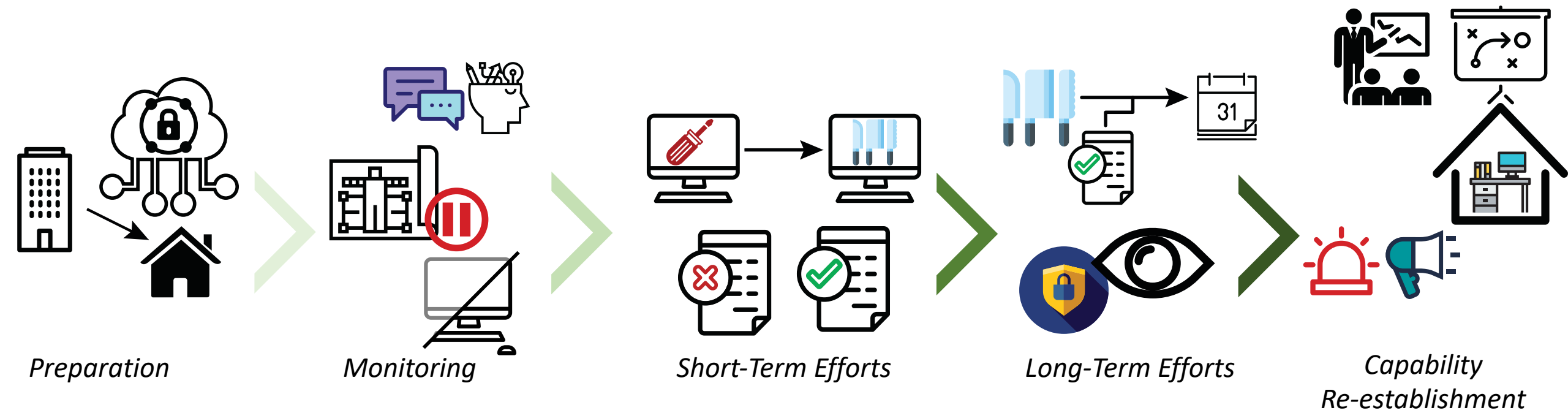


Interviews

*Additional methodological procedure
details available in the paper (see Fig. 1)*

SOC COVID-19 Response

- Five distinct phases
 - Varying activities, responses, and strategies



SOC COVID-19 Response

- Preparation

“[Virtual] communication went through the roof” (P1)

“Hallway conversations don’t exist anymore, so we have to be more direct.” (P5)



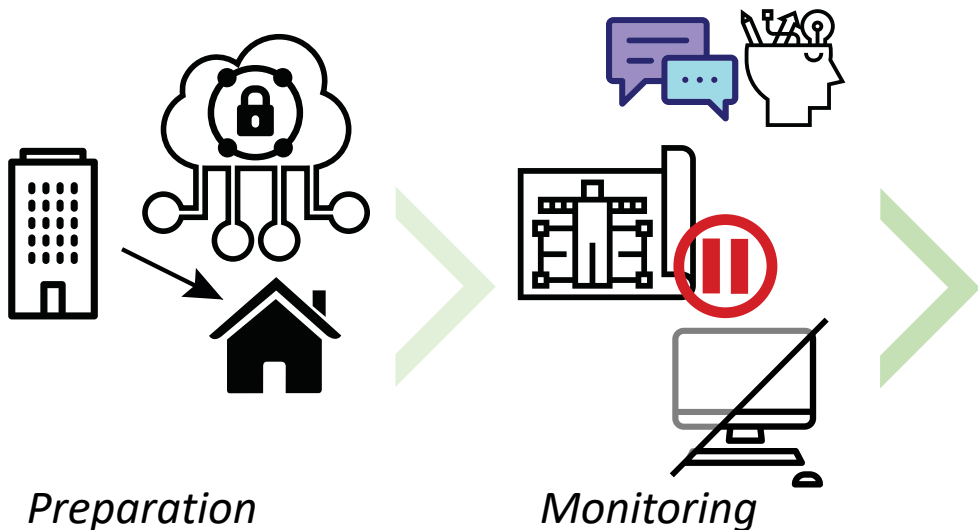
Preparation

SOC COVID-19 Response

- Monitoring

“It doesn’t do any good to provide security on campus when there isn’t anyone there anymore.” (P2)

“we just don’t have visibility on what endpoints are doing” (P2,P3,P5)

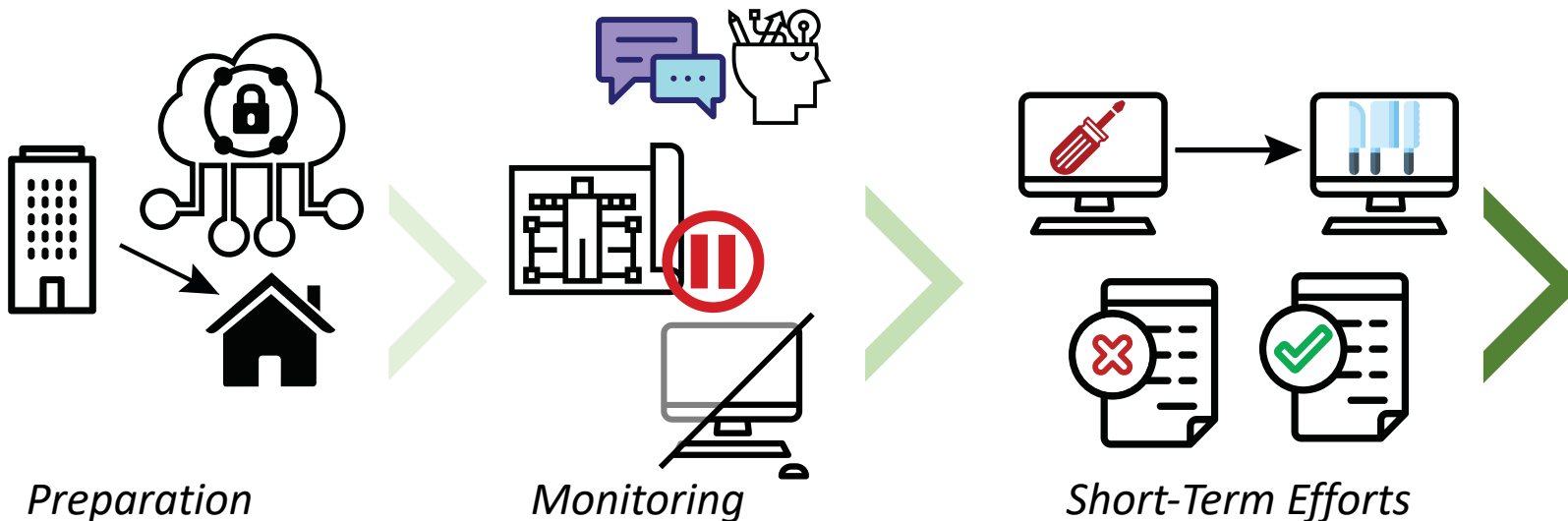


SOC COVID-19 Response

- Short-Term

“...are there any other COVID-19 emails you could forward to me? I’m working up a memo”.
(P5)

“FYI the Zoom changes went through last night. Password required on all Zoom meetings after the change (this can’t be shut off) and caller ID masking is enabled for dial in users” (P5)

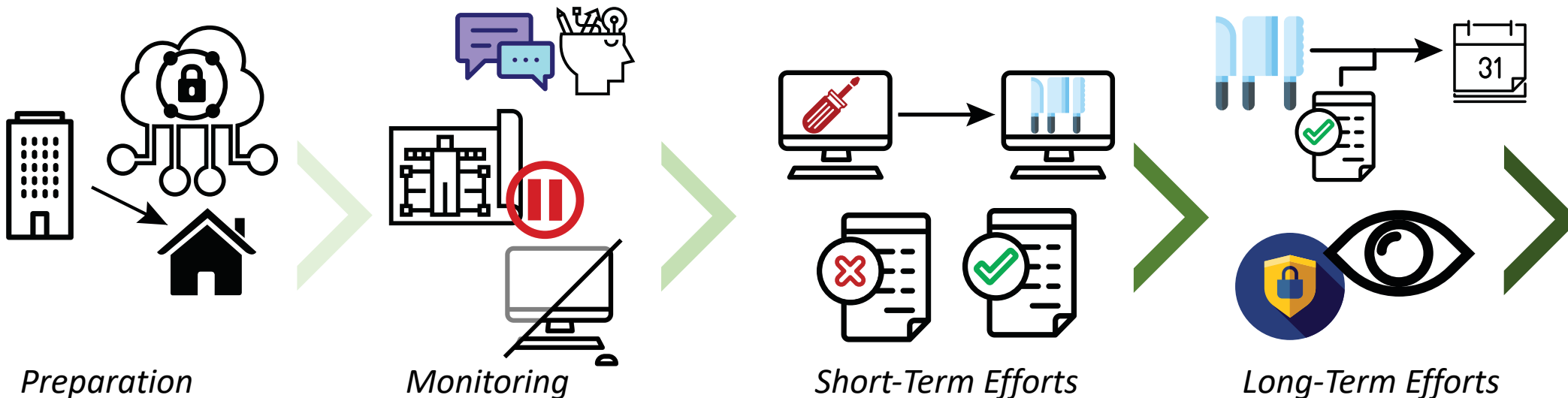


SOC COVID-19 Response

- Long-Term

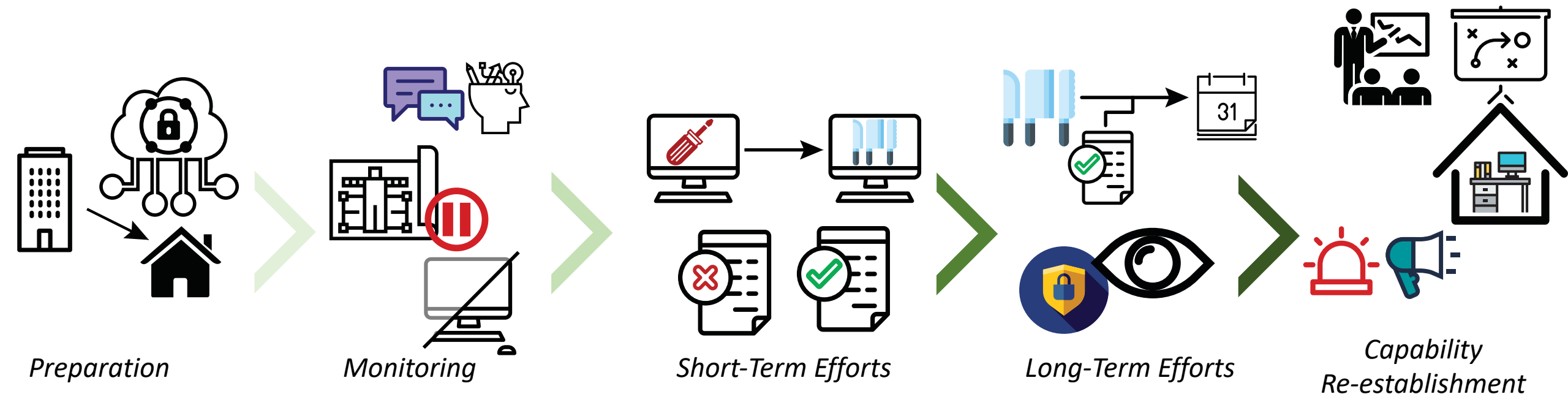
“User behavior [analytics] is a political issue ... the current language is ‘we only monitor devices’ yet it’s typically a 1-to-1 ratio”(P2)

“Daily checks of botnet activity... Periodic check of SaaS platforms... In regards to potential data exfiltration.” (P4)



SOC COVID-19 Response

- Re-Establishment
 - Permanent support for WFH capabilities
 - Long-term strategy



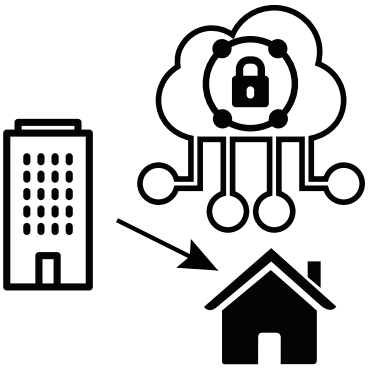
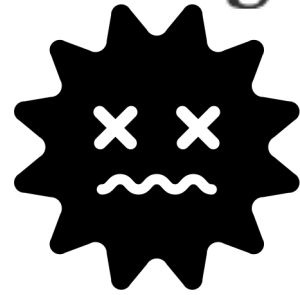
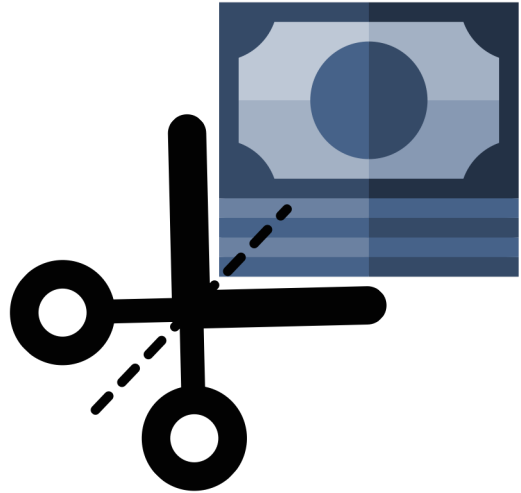
SOC COVID-19 Response

The Log4j Vulnerability

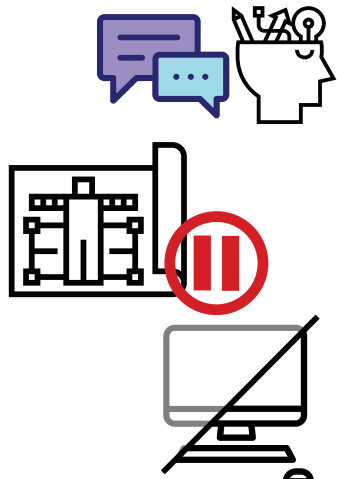
Russia-Ukraine war: What happened today
(March 15)

March 15, 2022 · 5:04 PM ET

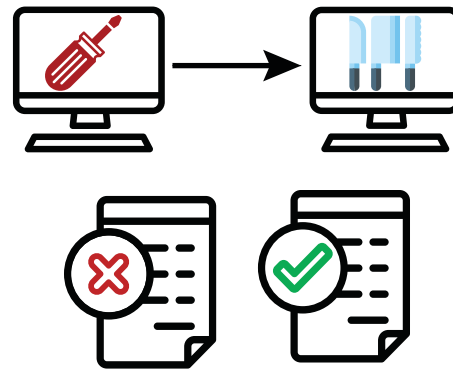
By NPR Staff [17]



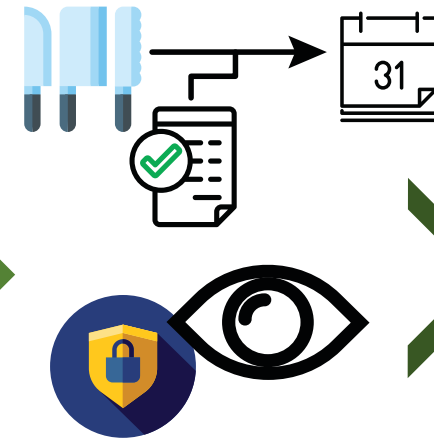
Preparation



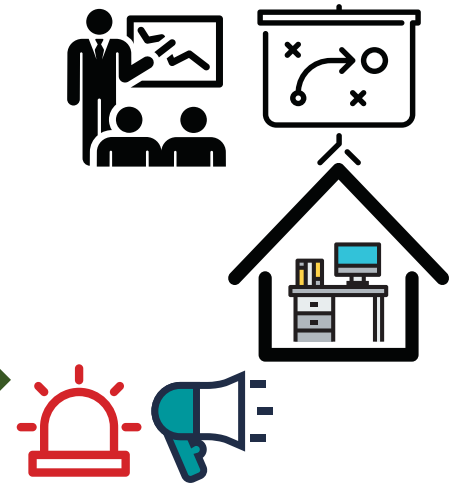
Monitoring



Short-Term Efforts



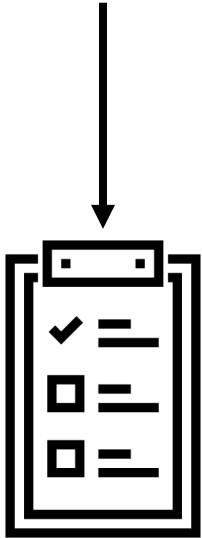
Long-Term Efforts



*Capability
Re-establishment*

Historical Analysis -- Deriving Common Terms

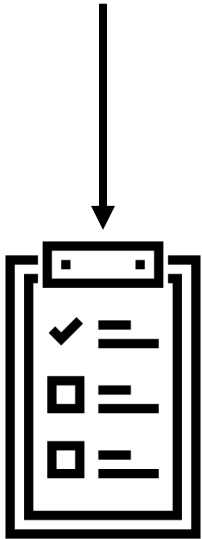
“endpoint management”



A). Keyword List

Historical Analysis -- Deriving Common Terms

“endpoint management”



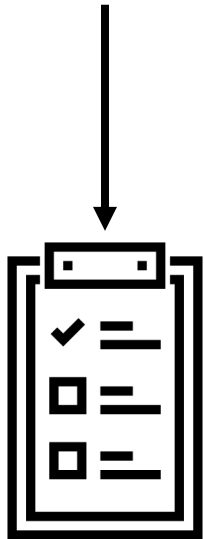
A). Keyword List



B). Search Historical Repositories for relevancy

Historical Analysis -- Deriving Common Terms

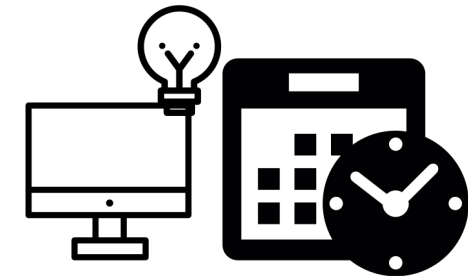
“endpoint management”



A). Keyword List

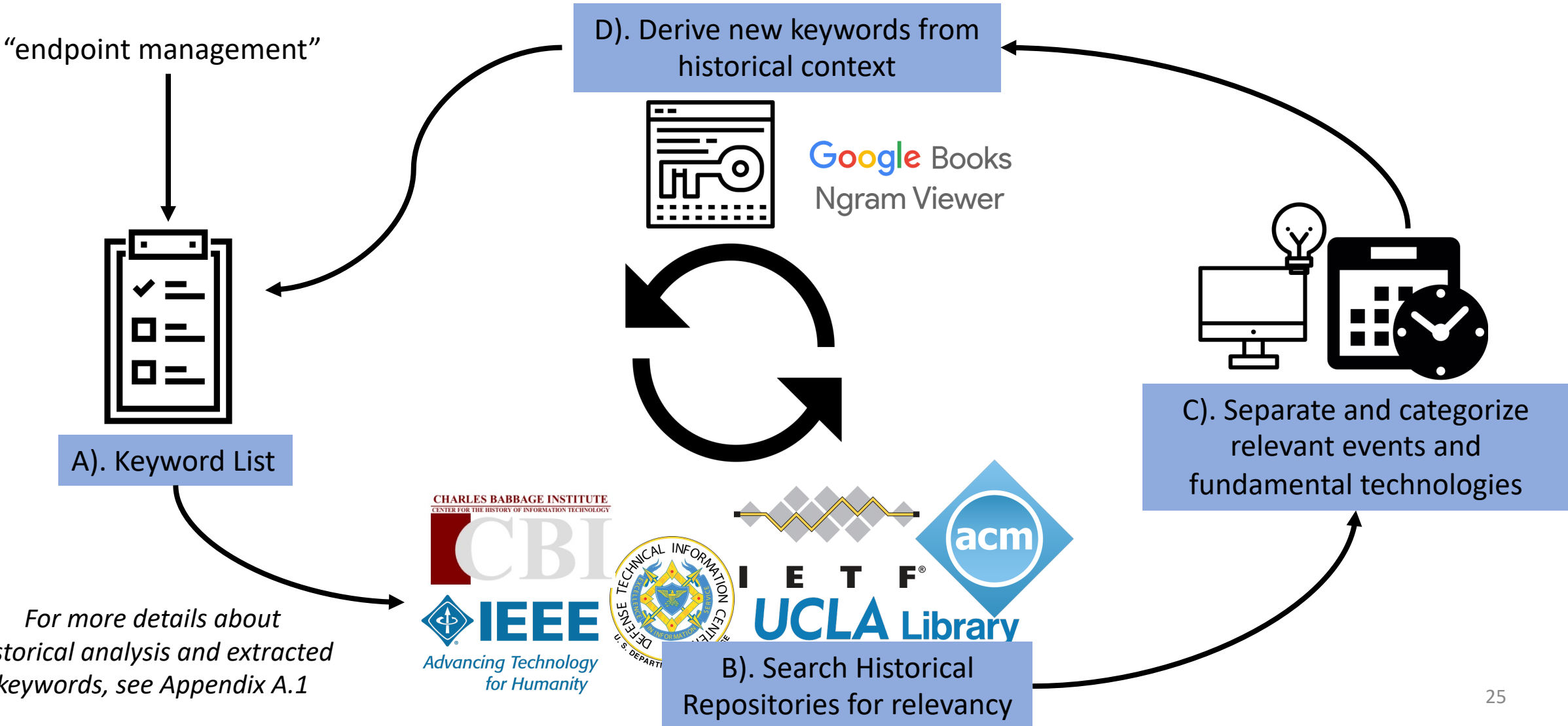


B). Search Historical Repositories for relevancy



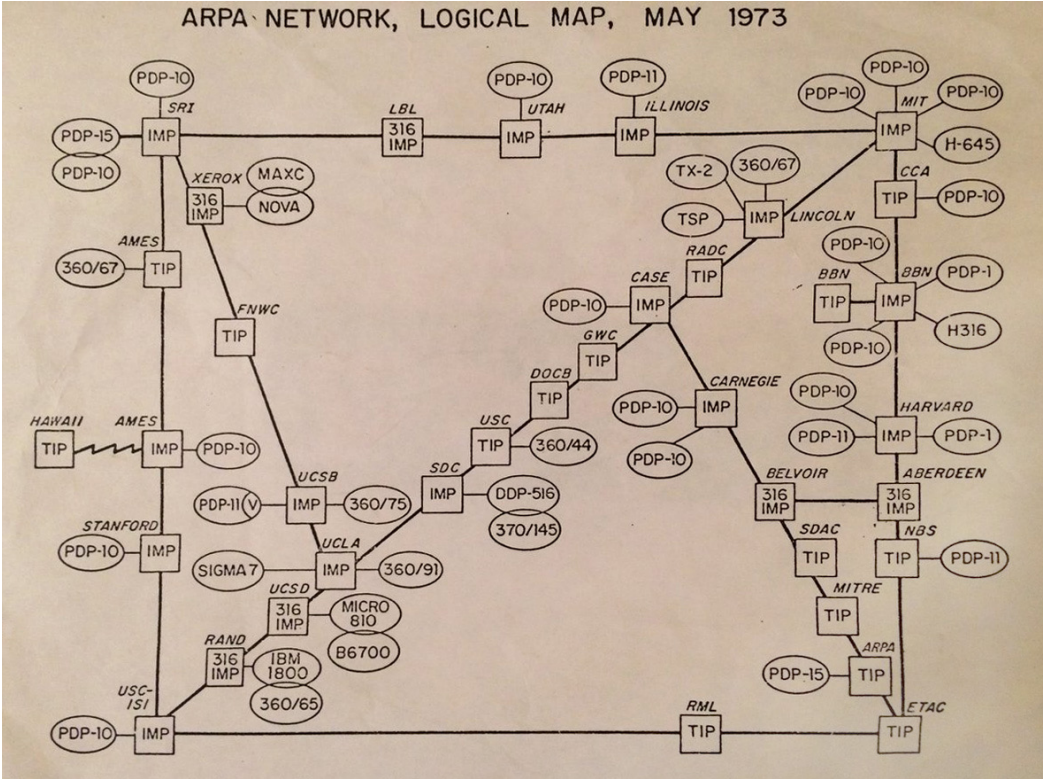
C). Separate and categorize relevant events and fundamental technologies

Historical Analysis -- Deriving Common Terms



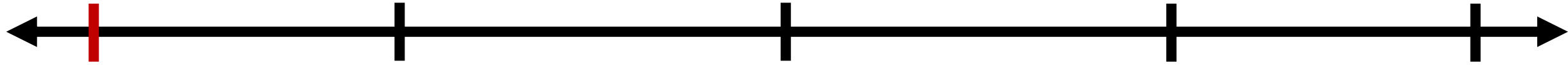
For more details about historical analysis and extracted keywords, see Appendix A.1

Mapping Historical Trends -- 1972 to 1979



- Local interaction with network
- Physical access control measures

1972-1979



Early Operational Arpanet

For research works of each time period and relevant keywords, see Table 5 in Appendix

Mapping Historical Trends -- 1980 to 1986



192.168.0.1



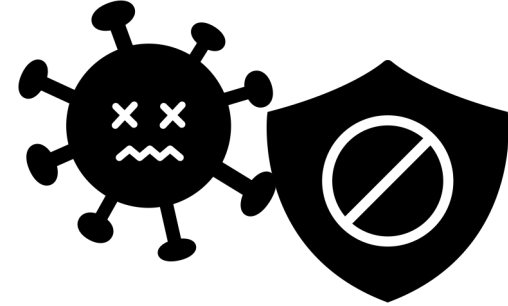
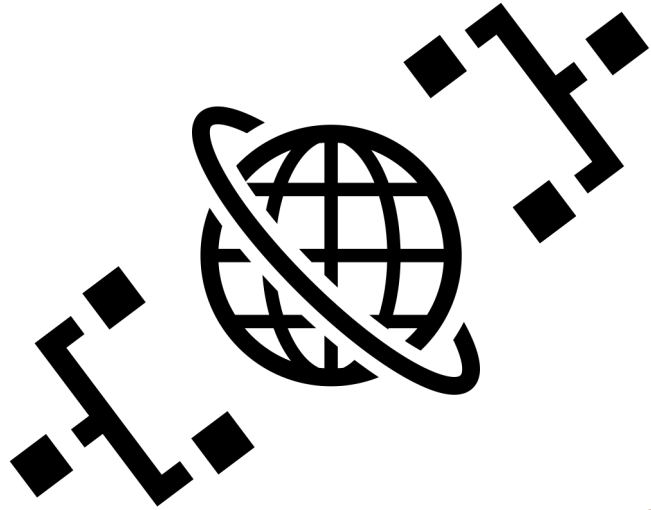
- Transition from terminal rooms to PCs
- Modems packaged with PCs
- Implementation of the Domain Name System

1980-1986

The ARPA Internet

For research works of each time period and relevant keywords, see Table 5 in Appendix

Mapping Historical Trends -- 1986 to 1990



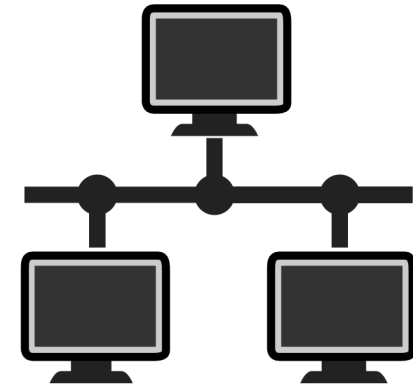
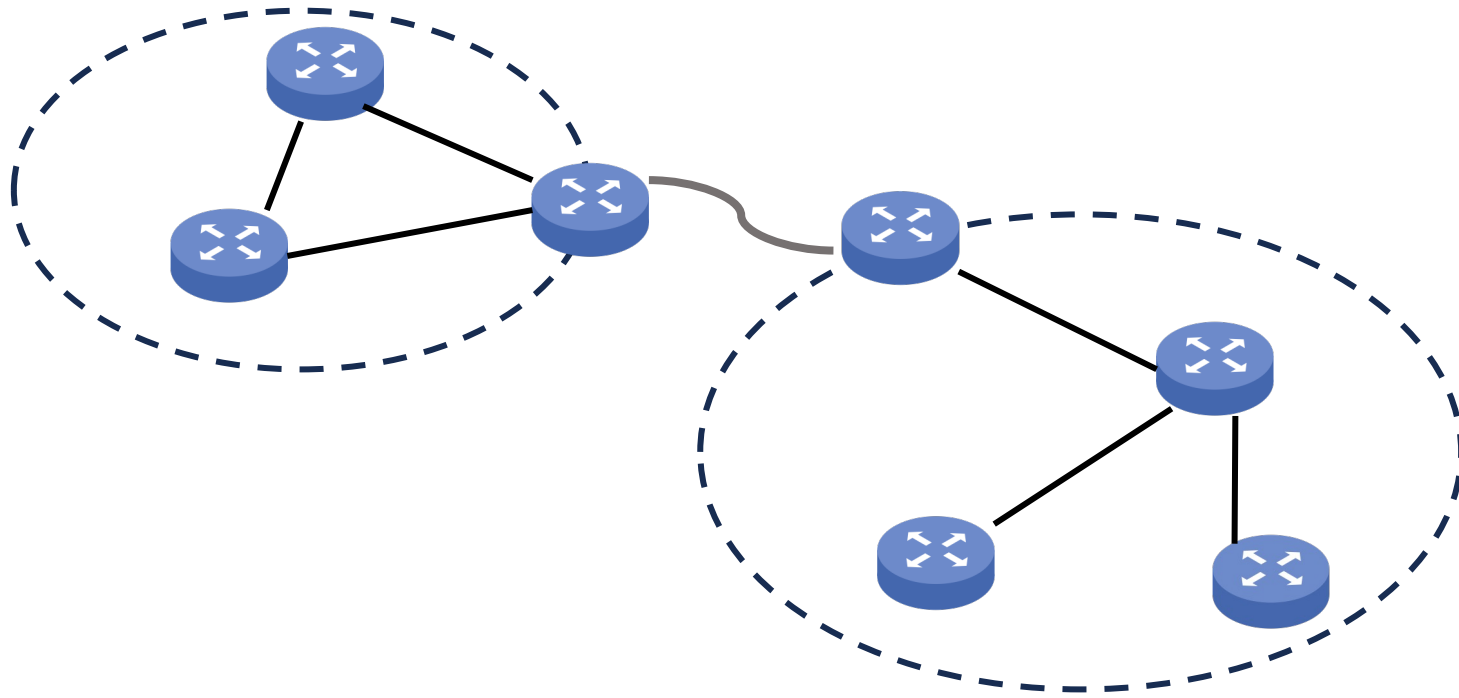
- Private network attachment and heterogenous protocols
- Acceptable Use Policies emerge
- Anti-virus and disk management software appear

1986-1990

NSFNET
Pre-Privatization

For research works of each time period and relevant keywords, see Table 5 in Appendix

Mapping Historical Trends -- 1991 to 1999



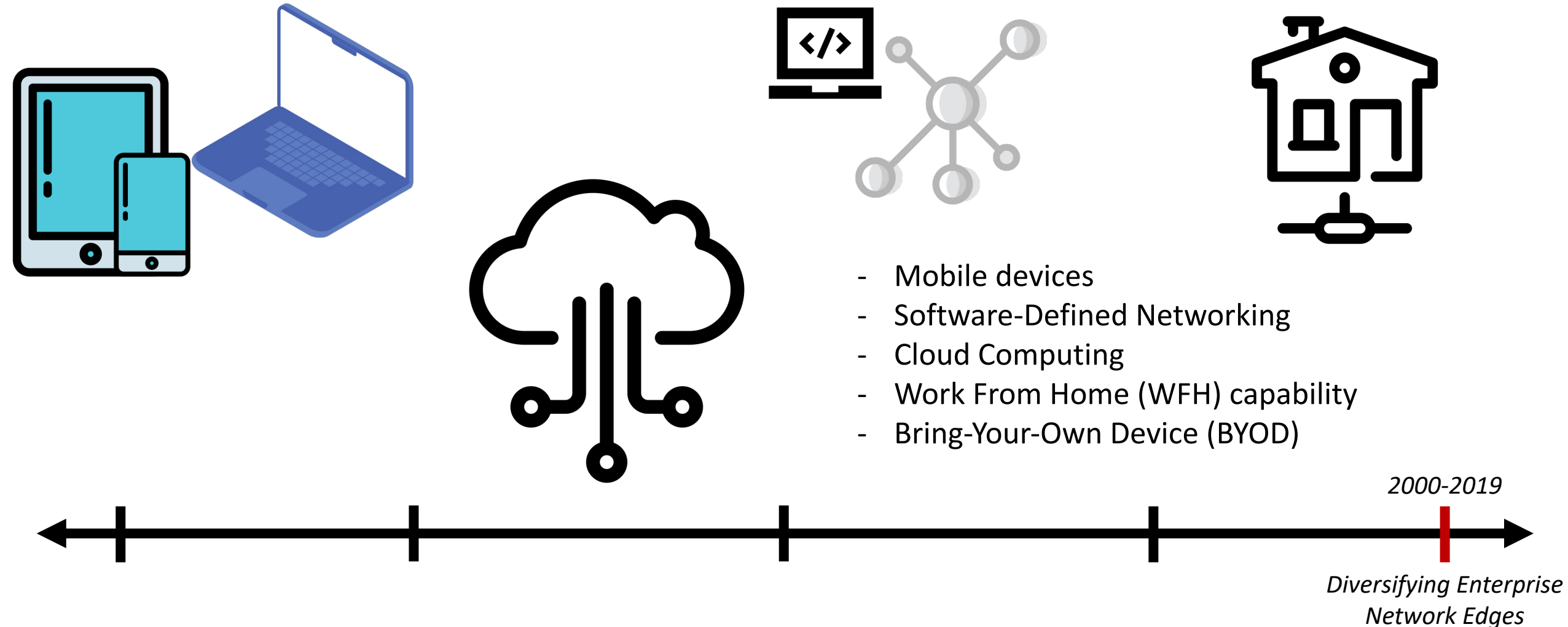
- Border Gateway Protocol introduction
- Acceptable Use Policies become ubiquitous
- Local Area Network server use increases

1991-1999

*Connected, Private
Enterprise Networks*

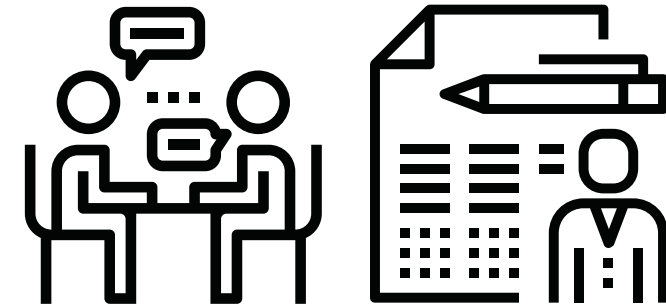
*For research works of each time period and relevant
keywords, see Table 5 in Appendix*

Mapping Historical Trends -- 2000 to 2019



For research works of each time period and relevant keywords, see Table 5 in Appendix

Validation Methods

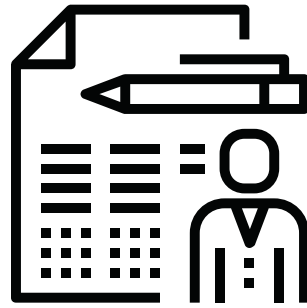
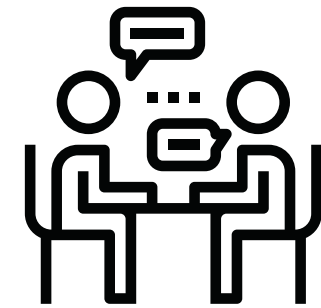


- Qualitative validation of themes from 352 field notes
 - Semi-structured interviews, 30 minutes
 - 12 participants across two rounds of interviews
- Quantitative validation of themes from 352 field notes
 - **7 new SOCs** (separate from participant observation)
 - Targeted leading roles in a SOC (e.g. - Chief Information Security Officers)

For more details about validation efforts and questions asked, see Appendix A.3 and accompanying Appendix Tables



Validation Methods



- Qualitative validation of themes from 252 field notes

Largest determining factor for decreased adoption of endpoint management:

details about reports and questions in Appendix A.3 and Appendix Tables

- Qu

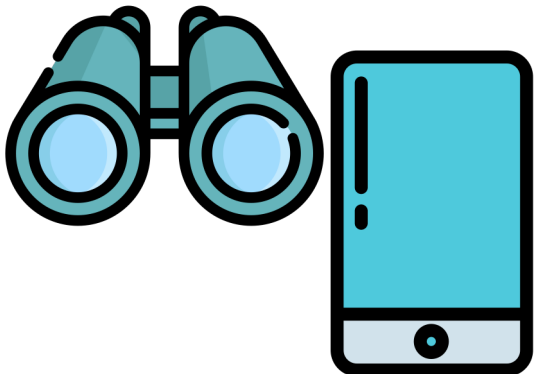
A mostly local, centralized workforce

FORTUNE
500



Recommendations and Action Items

- Focus on device coverage and visibility
- Document policies/procedures with respect to end-user privacy
- Investment in training



Conclusions

- Endpoint management concerns began long before COVID-19 and a shift to WFH activities
- Endpoint management challenges intensified due to dramatic increase in WFH activity
- Human concerns, such as employee stress and burnout, grew during COVID-19's WFH shift

Questions?

kkj.research@gmail.com

dabruck@sandia.gov

brfid@icloud.com

alexbardas@ku.edu



References

1. <https://www.wsj.com/articles/covid-19-hastens-the-work-at-home-revolution-11596495435>
2. <https://www.shrm.org/resourcesandtools/hr-topics/talent-acquisition/pages/admin-jobs-projected-stay-remote-covid19.aspx>
3. https://www.voanews.com/a/silicon-valley-technology_google-employees-work-home-until-2021/6193521.html
4. <https://www.forbes.com/sites/forbestechcouncil/2022/07/20/the-pandemics-lasting-effects-are-cyber-attacks-one-of-them/?sh=5db90e9d2b76>
5. <https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html>
6. <https://www.securitymagazine.com/articles/98427-how-covid-19-has-made-small-businesses-more-vulnerable-to-cyberattacks>
7. <https://www.wsj.com/articles/what-is-the-log4j-vulnerability-11639446180>
8. <https://www.scmagazine.com/news/cybersecurity-ops-may-never-be-the-same-after-covid-19-but-thats-not-all-bad>
9. <https://www.securitymagazine.com/articles/92236-cisa-guide-to-pandemic-response-critical-infrastructure-operations-centers-and-control-rooms>
10. <https://www.helpnetsecurity.com/2020/06/26/soc-team-burnout/>
11. <https://www.techtarget.com/searchsecurity/feature/CISO-position-burnout-causes-high-churn-rate>
12. <https://www.securitymagazine.com/articles/92413-is-remote-secops-a-good-long-term-plan>
13. <https://en.wikipedia.org/wiki/ARPANET>
14. <https://twitter.com/microcenter/status/1433461995773247490>
15. <https://www.computerhistory.org/timeline/1982/>
16. <https://www.businesswire.com/news/home/20211108005775/en/Cyber-Threats-Have-Increased-81-Since-Global-Pandemic>
17. <https://www.npr.org/2022/03/15/1086671754/russia-ukraine-war-what-happened-today-march-15>