



KEAN

WORLD-CLASS EDUCATION



**CAE Tech Talk Forum – Taking a Timely
Opportunity to Evaluate the Security of
your Physical Security Video Solution**

Presented by:

Stan Mierzwa, M.S.; CISSP

November 3, 2021 1:00 PM – 1:50 PM



Thank you!

**A big thank you to Lauren Scott and
the Centers of Academic Excellence in
Cybersecurity (CAE-C) Program
Management Office.**



KEAN

Cybersecurity Center





KEAN

Center for
Cybersecurity

kean.edu/cybersecurity



System Protected

5732C207
7061746

74

85

06

57



1

Speaker
Background

2

Recent Cloud-
Vendor Hacking

3

Cameras
Everywhere!

4

IoT Movement and
Growth

5

Models of Camera
Termination

6

Reviewing Video
Surveillance

7

Conclusion

8

Discussion/
Limitations

9

Questions &
Thank you!

Speaker Background

- Assistant Director and Cybersecurity Lecturer, Center for Cybersecurity, Kean University. CISSP.
- Over 25 years IT experience.
 - Industry: Software developer – UPS.
 - Academic/Non-Profit: Director, IT – large NGO.
 - State Agency: Application Security Lead – State of NY, MTA Police. FBI Infragard.
 - Board Member: CTO – Non-Profit - Vennue.
- International work experience.

Practical “on the ground” international work experience in:			
<u>Europe</u>	<u>Africa</u>		<u>Asia-Pacific</u>
Germany	South Africa	Kenya	Thailand
	Zimbabwe	Morocco	Vietnam
<u>Latin America</u>	Uganda	Egypt	Bangladesh
Guatemala	Malawi	Ghana	India
Mexico	Zambia		




KEAN

Outline

2

Recent Cloud-
Vendor Hacking

Recent Cloud Video Hacking

Bloomberg the Company & Its Products | Bloomberg Terminal Demo Request |  Bloomberg Anywhere Remote Login | Bloomberg Customer Support

Menu Search

Bloomberg

Sign In

Cybersecurity

Hackers Breach Thousands of Security Cameras, Exposing Tesla, Jails, Hospitals

By [William Turton](#)

March 9, 2021, 4:32 PM EST Updated on March 10, 2021, 11:35 AM EST

- ▶ Hacker group says it wanted to show prevalence of surveillance ✓
- ▶ Video footage was captured from Sequoia-backed startup Verkada

Most Read

BUSINESS

Previous Covid Prevents Delta Infection Better Than Pfizer Shot

Recent Cloud Hacking



Source: <https://www.bloomberg.com/news/articles/2021-03-09/hackers-expose-tesla-jails-in-breach-of-150-000-security-cams>

Recent Cloud Hacking



A Tesla facility seen through a Verkada camera. *Tillie Kottmann*

Source: <https://www.bloomberg.com/news/articles/2021-03-09/hackers-expose-tesla-jails-in-breach-of-150-000-security-cams>

Recent Cloud Hacking


The Washington Post
Democracy Dies in Darkness

Tech Help Desk Future of Transportation Innovations Internet Culture Space Tech Policy Video Gaming

Technology

Massive camera hack exposes the growing reach and intimacy of American surveillance


A breach of the camera start-up Verkada 'should be a wake-up call to the dangers of self-surveillance,' one expert said: 'Our desire for some fake sense of security is its own security threat'



11:36:18 AM CST

MOST READ TECHNOLOGY >

facebook facebook facebook
ook facebook facebook fac
facebook facebook facebook
ool facebook facebook fac
fac
ool
fac
ool
fac
ool

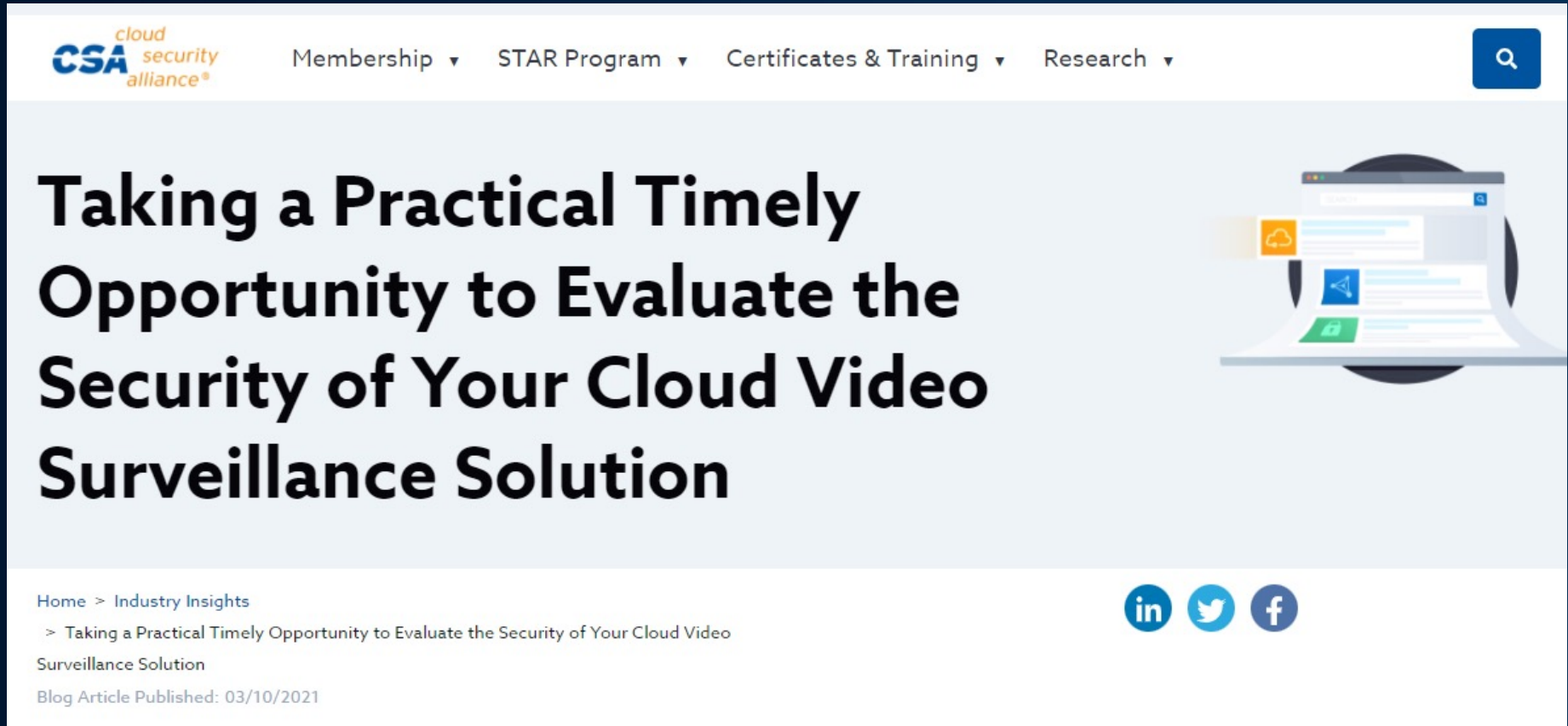


- 1 Facebook is ending use of facial recognition software, deleting data on more than a billion people
- 2 The latest space race is all about improving Internet access. Here's what you should know.
- 3 A QAnon revelation suggests the truth of Q's identity was right there all along
- 4 Breitbart has outsize influence over climate change denial on Facebook, report says
- 5 Recovering locked Facebook accounts is a nightmare. That's on purpose.

Recent Cloud Video Hacking

- Hackers breached Verkada – gaining access to camera feeds.
- Upwards of 150,000 cameras reportedly were compromised.
- Published live feeds (Tesla, Cloudflare, Florida hospital, police station)
- Alleged that the hack was as simple as having gained the account credentials for administrative-level access (super-admin).
- Cameras have built-in maintenance login, permitting super admin access of any camera of any customer.

Led to a Focus on this Topic - CSA



The screenshot shows the top portion of a web page. At the top left is the CSA logo, which includes the text "cloud security alliance" in orange and blue. To the right of the logo is a navigation menu with four items: "Membership", "STAR Program", "Certificates & Training", and "Research", each followed by a downward-pointing triangle. In the top right corner, there is a blue square search button with a white magnifying glass icon. Below the navigation is a large light blue banner area. On the left side of this banner, the main title of the article is written in large, bold, black font: "Taking a Practical Timely Opportunity to Evaluate the Security of Your Cloud Video Surveillance Solution". On the right side of the banner, there is a stylized illustration of a laptop computer. The laptop screen displays a webpage with various icons, including a cloud, a shield, and a document. Below the banner, there is a white footer area. On the left side of the footer, there is a breadcrumb trail: "Home > Industry Insights > Taking a Practical Timely Opportunity to Evaluate the Security of Your Cloud Video Surveillance Solution". Below the breadcrumb trail, it says "Blog Article Published: 03/10/2021". On the right side of the footer, there are three circular social media icons for LinkedIn, Twitter, and Facebook.

cloud security alliance®

Membership ▾ STAR Program ▾ Certificates & Training ▾ Research ▾

Taking a Practical Timely Opportunity to Evaluate the Security of Your Cloud Video Surveillance Solution

Home > Industry Insights
> Taking a Practical Timely Opportunity to Evaluate the Security of Your Cloud Video Surveillance Solution
Blog Article Published: 03/10/2021

in tw f

<https://cloudsecurityalliance.org/blog/2021/03/10/taking-a-practical-timely-opportunity-to-evaluate-the-security-of-your-cloud-video-surveillance-solution/>



KEAN

Outline

3

Cameras
Everywhere!

Cameras Everywhere!



Cameras Everywhere!



Cameras Everywhere!



Cameras Everywhere!



Photo: Rachel Cericola



KEAN

Outline

4

IoT Movement and
Growth

IoT Movement Has Momentum!

- Growth of IP-based video surveillance systems considered one of the fastest increasing elements in this evolution.
- Report from Allied Market Research – video surveillance industry annual growth expected to reach \$144.8 billion by 2027 – increase of 14.6% (Compound Annual Growth Rate) between 2020 to 2027.



KEAN

Outline

5

Models of Camera
Termination

Models and Varieties of Camera Termination Options

- Varying makes and models of cameras.
- Cameras terminating in:
 - Housed or on premise or IaaS.
 - Appliances, as in the case of home systems.
 - Cloud-based shared systems.
 - Hosted paid providers (think TV advertisements).
- With all the growth and model options – latest hacking in 2021 is a wake up call to review.
 - Assess surveillance governance.
 - Assess security protocols to prevent exploitation.
 - Give this topic attention.

Popular Enterprise Video Surveillance

GenetecTM

AVIGILONTM

PELCO[®]
a Motorola Solutions Company

 **milestone**

VERINT

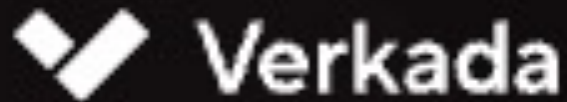
tyco

 **OnSSI**

 **Qognify**

HIKVISION[®]

Example - Cloud-Based Video Surveillance (VSaaS)

The logo for Verkada, featuring a white checkmark icon on a dark background followed by the word "Verkada" in white text.The logo for Nest, consisting of the word "nest" in a lowercase, rounded, grey font.The logo for Rhombus Systems, featuring a blue diamond shape containing a white lowercase "r." followed by the words "rhombus" and "systems" in a lowercase, sans-serif font.The logo for Eagle Eye Networks, featuring a stylized blue eagle head icon to the left of the words "EAGLE EYE" and "NETWORKS" in a blue, uppercase, sans-serif font.The logo for Arlo, featuring the word "arlo" in a lowercase, dark blue font, followed by a green stylized bird icon.



KEAN

Outline

6

Reviewing Video
Surveillance

Key Areas to Review - 1

- Endpoint surveillance camera devices
 - It may be possible that a variety of vendor cameras are installed in the environment.
 - If firmware exists, determine if updates are needed and apply them.
 - Many IP-based cameras now permit direct login, for configuration settings.
 - Ensure secure – default passwords changed.
 - Enable MFA.
 - Setup alerts with login activity.
 - HTTPS camera connectivity.
 - Review encryption settings – attempt to prohibit traffic sniffing.

Key Areas to Review - 2

- Communication network.
 - For enterprise designs, use of network segmentation at a minimum.
 - Integrate with internal firewalls.
 - Perform a risk analysis to minimize connection hemorrhage into the segment.
 - Assess physical connection to cameras, in an effort to prevent MITM attacks.
 - Review firewall configuration and ports open to all endpoint surveillance cameras and server administrative applications.

Key Areas to Review - 3

- Backend surveillance security manager server (on premise, hybrid, or in the cloud).
 - Ensure the OS is patched.
 - Security manager software at the latest version?
 - Limit administrative access – MFA and PAM for a login defense layer.
 - Consider the paradigm of Zero Trust Security to define boundaries.
 - Configure logging and alerting of anomaly events providing a “heads up” for security analysts to respond to potential breaches.
 - Remind staff of ethical responsibility of having access to video recordings. Chain of Custody.

Key Areas to Review - 4

- PaaS or VSaaS security management solutions.
 - Stay on top of vulnerability announcements – requiring updates or configuration changes (think Ring doorbell!).
 - Query provider on strategy for notifications of breaches.
 - Review the administrative access password practices and policies used by the vendor.
 - Who has access to stored or recorded video?
 - Evaluate the cloud vendor using such assessment tools as the Cloud Security Alliance bank of tools – Cloud Control Matrix (CCM).

Key Areas to Review - 5

- Third-party vendor access.
 - There is the possibility that the physical security equipment operation and maintenance is outsourced.
 - Think supply chain! Follow the trail of access!
 - Review all access levels – de-provisioning in order?
 - Review policies of third-party vendors and bring into your enterprise risk management practices for routine checks.



KEAN

Outline

7

Conclusion

In Conclusion

- Software and hardware physical security solutions are created by humans, and vulnerabilities will emerge.
- The video surveillance industry is rapidly expanding – IoT.
- Keep security in mind when provisioning or installing video surveillance solutions.
- If not already established – consider merging physical security technology with the Information Technology security team.



KEAN

Outline

8

Discussion/
Limitations

9

Thank you!

Limitations

- Outlined a high-level introduction and awareness to physical security video surveillance technology.
- cursory set of factors considered, many other that may be unique to your environment may exist.

In Review - Do's and Don'ts



Setup MFA and logging on camera devices.



Do nothing – this issue is not going away.



Review open ports used with VMS.



Put your complete trust in the cloud vendor.



Enforce PAM or MFA for backend access.



Don't avoid assessing or querying the vendor.



Review cloud-vendor policies for access.



Go at it alone.



De-provision third-party accounts not in use – assess!



Consider management oversight in IT.

References

- Turton, W. (2021). Hackers Breach Thousands of Security Cameras Exposing Tesla, Jails, Hospitals. Bloomberg. As Retrieved from: <https://www.bloomberg.com/news/articles/2021-03-09/hackers-expose-tesla-jails-in-breach-of-150-000-security-cams>
- Allied Market Research. (2020). Future of Video Surveillance Market Sales to Grow \$144.85 Bn, Globally, by 2027 at 14.6% CAGR. Retrieved from: <https://www.globenewswire.com/news-release/2020/07...>
- Harwell, D. (2021). Massive camera hack exposes the growing reach and intimacy of American Surveillance. The Washington Post. As retrieved from: <https://www.washingtonpost.com/technology/2021/03/10/verkada-hack-surveillance-risk/>
- MalwarebytesLabs. (2021). 150,000 Verkada security cameras hacked – to make a point. Retrieved from: <https://blog.malwarebytes.com/iot/2021/03/150000-verkada-security-cameras-hacked-to-make-a-point/>
- Mierzwa, S. & Perez, E. (2021). Taking a Practical Timely Opportunity to Evaluate the Security of Your Cloud Video Surveillance Solution. Retrieved from: <https://cloudsecurityalliance.org/blog/2021/03/10/taking-a-practical-timely-opportunity-to-evaluate-the-security-of-your-cloud-video-surveillance-solution/>



Thank you!!



KEAN

WORLD-CLASS EDUCATION