

ALERT LOGIC®



SECURING MODERN INFRASTRUCTURES

A BS-Free Guide To Cybersecurity Awareness In Next-Generation Architectures

**This content is rated IT
and is intended for real professionals only.**

Viewer discretion is advised.



TR

TRUTH



RE

REALITY



IT

INFORMATION TECHNOLOGY



ML

MILD LANGUAGE

Many forays into cybersecurity begin with someone we do not recognize:

Someone in a
hooded
sweatshirt plans
to ruin your day.

Are you secure?



Secure | https://delivery.panerabread.com/

```
{
  "accounts": [
    {
      "username": "[REDACTED]",
      "name": "[REDACTED]",
      "cardNumber": "*****"
    },
    {
      "username": "[REDACTED]@hotmail.com",
      "name": "[REDACTED]",
      "cardNumber": "*****"
    },
    {
      "username": "[REDACTED]@msn.com",
      "name": "F B",
      "cardNumber": "*****7921"
    },
    {
      "username": "[REDACTED]@yahoo.com",
      "name": "C",
      "cardNumber": "*****710"
    },
    {
      "username": "[REDACTED]",
      "cardNumber": "*****61"
    },
    {
      "username": "[REDACTED]@aol.com",
      "name": "[REDACTED]",
      "cardNumber": "*****"
    },
    {
      "username": "[REDACTED]@yahoo.com",
      "name": "[REDACTED]",
      "cardNumber": "*****"
    },
    {
      "username": "k",
      "name": "[REDACTED]",
      "cardNumber": "*****4412"
    },
    {
      "username": "[REDACTED]1",
      "name": "[REDACTED]",
      "cardNumber": "*****8386"
    },
    {
      "username": "[REDACTED]@aol.com",
      "name": "[REDACTED]",
      "cardNumber": "*****"
    },
    {
      "username": "[REDACTED]@optonline.net",
      "name": "[REDACTED]",
      "cardNumber": "*****"
    },
    {
      "username": "[REDACTED]@hotmail.com",
      "name": "[REDACTED]",
      "cardNumber": "*****"
    },
    {
      "username": "[REDACTED]",
      "name": "[REDACTED]",
      "cardNumber": "*****6"
    },
    {
      "username": "[REDACTED]",
      "name": "[REDACTED]",
      "cardNumber": "*****70"
    },
    {
      "username": "[REDACTED]@hotmail.com",
      "name": "[REDACTED]",
      "cardNumber": "*****4220"
    },
    {
      "username": "[REDACTED]",
      "cardNumber": "*****9123"
    },
    {
      "username": "art",
      "name": "[REDACTED]",
      "cardNumber": "*****8139"
    },
    {
      "username": "[REDACTED]",
      "name": "[REDACTED]",
      "cardNumber": "*****0102"
    },
    {
      "username": "[REDACTED]@msn.com",
      "name": "[REDACTED]",
      "cardNumber": "*****6851"
    },
    {
      "username": "k",
      "name": "[REDACTED]",
      "cardNumber": "*****2654"
    }
  ]
}
```



02 Panerabread.com Leaks Millions of Customer Records

APR 18

Panerabread.com, the Web site for the American chain of bakery-cafe fast casual restaurants by the same name, leaked millions of customer records — including names, email and physical addresses, birthdays and the last four digits of the customer's credit card number — for at least eight months before it was yanked offline earlier today, KrebsOnSecurity has learned.

From: Mike Gustavison <Mike.Gustavison@panerabread.com>
Date: Wed, Aug 9, 2017 at 11:02 AM
To: Dylan Houlihan <[dylan@\[REDACTED\]](mailto:dylan@[REDACTED])>

Yes sir...

Thank you for the information we are working on a resolution.

Mike

From: Dylan Houlihan [mailto:[dylan@\[REDACTED\]](mailto:dylan@[REDACTED])]
Sent: Monday, August 07, 2017 9:47 PM

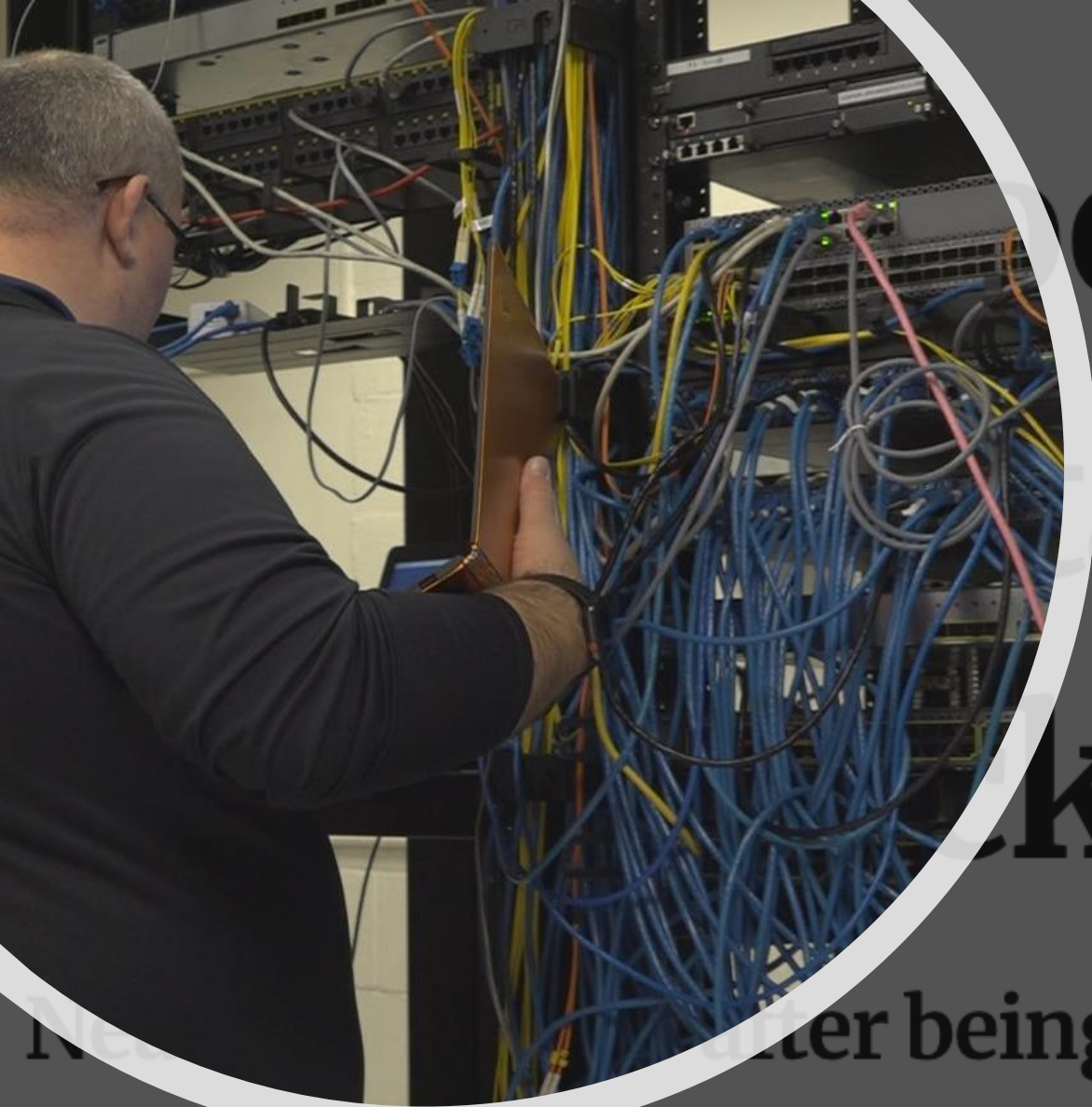
...



Hooded sweatshirt person
influences us to invest in
cybersecurity.

"I think they should fear me more. Panera does. Ask them."

-Brian Krebs, probably.



Dale Layne Superintendent Jerome School District

- So far, "they haven't been able to give specific answers about what information has been affected," Layne said, but it's very similar to other cases they've seen across the nation. "We're trying to find out how (the cybercriminals) got in."
- "It sounds like they — whoever they are — do try to go after municipalities like schools and hospitals," he said, because they don't tend to have a large IT staff.

After being hit by a massive ransomware cyberattack, the Jerome School District is still working to recover

B2B Impact: Who are you offering services to?

If you open your customer to a breach, will they renew your contracted services?



So what?

- One threat in 2018 was leveraged by multiple attackers against multiple entities with one thing in common: centralized contact with its customer base
- The attack was via 3rd party contact center services and each attacked entity leveraged different solutions
- Millions of customers impacted: Each impacted entity moved away from the 3rd party provider
- 6 months between POC announcement and attack

And so...it begins...

You Need Security? Let's Go Shopping!

- Network Detection Security & Awareness





You Need Security? Let's Go Shopping!

- Network Detection Security & Awareness
- Log Management & User/Entity Based Analytics

You Need Security? Let's Go Shopping!

- Network Detection Security & Awareness
- Log Management & User/Entity Based Analytics
- Endpoint Detection/Reverse Proxy Technology



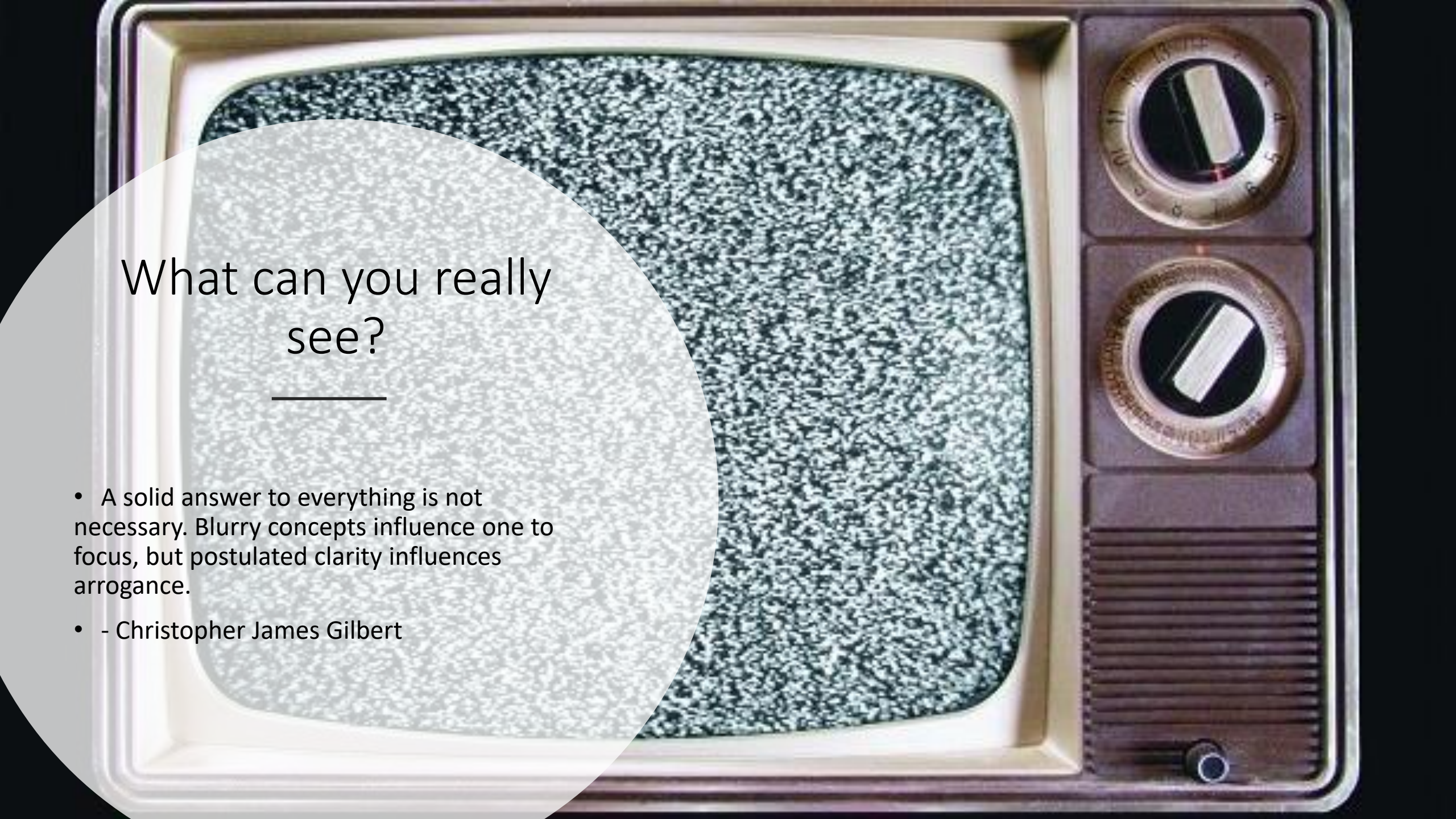


Did you want SIEM with that?

You only know what you know.

Reports that say that something hasn't happened are always interesting to me, because as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don't know we don't know. And if one looks throughout the history of our country and other free countries, it is the latter category that tend to be the difficult ones.





What can you really see?

- A solid answer to everything is not necessary. Blurry concepts influence one to focus, but postulated clarity influences arrogance.
- - Christopher James Gilbert

The Blind Men

- Development
- Security
 - (InfoSec | Cyber Security)
- Operations
- Audit
 - (Internal | External)
- Compliance
- General Public



Building a Security Operations Center—The Components

DESIRED CAPABILITIES

Protect web apps
Identify network threats
Uncover incidents of compromise in logs
Discover advanced multi-vector attacks
Find vulnerabilities
Threat intel and security content
24x7 monitoring and analysis
Availability and performance monitoring

REQUIRED TECHNOLOGY

Web application firewall (WAF)
Intrusion detection/ protection
Log management
Threat analytics platform
Vulnerability management
Databases, information management, malware
Analysis tools
Middleware, APIs, and monitoring tools

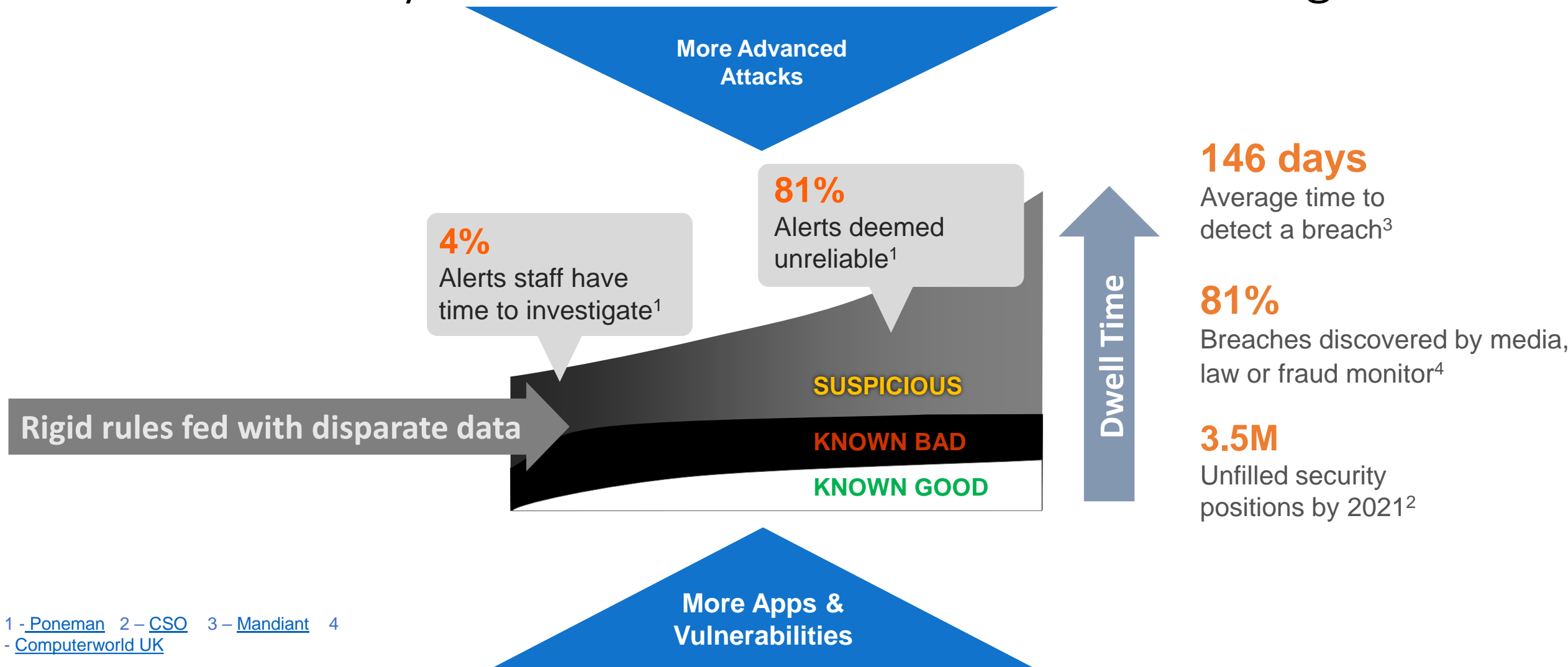
SECURITY CONTENT

Whitelists, blacklists
Signatures, rules
Log parsers and correlation rules
Taxonomy, correlation rules
CVE coverage
Emerging threats, zero days, malware
Incident information
Availability and performance metrics

HUMAN EXPERTISE

WAF rules expert
Network security expert
Log analyst expert
Correlation rules expert
Scanning expert
Expert knowledge of criminal underground
Security analysts
Network ops experts, system admins

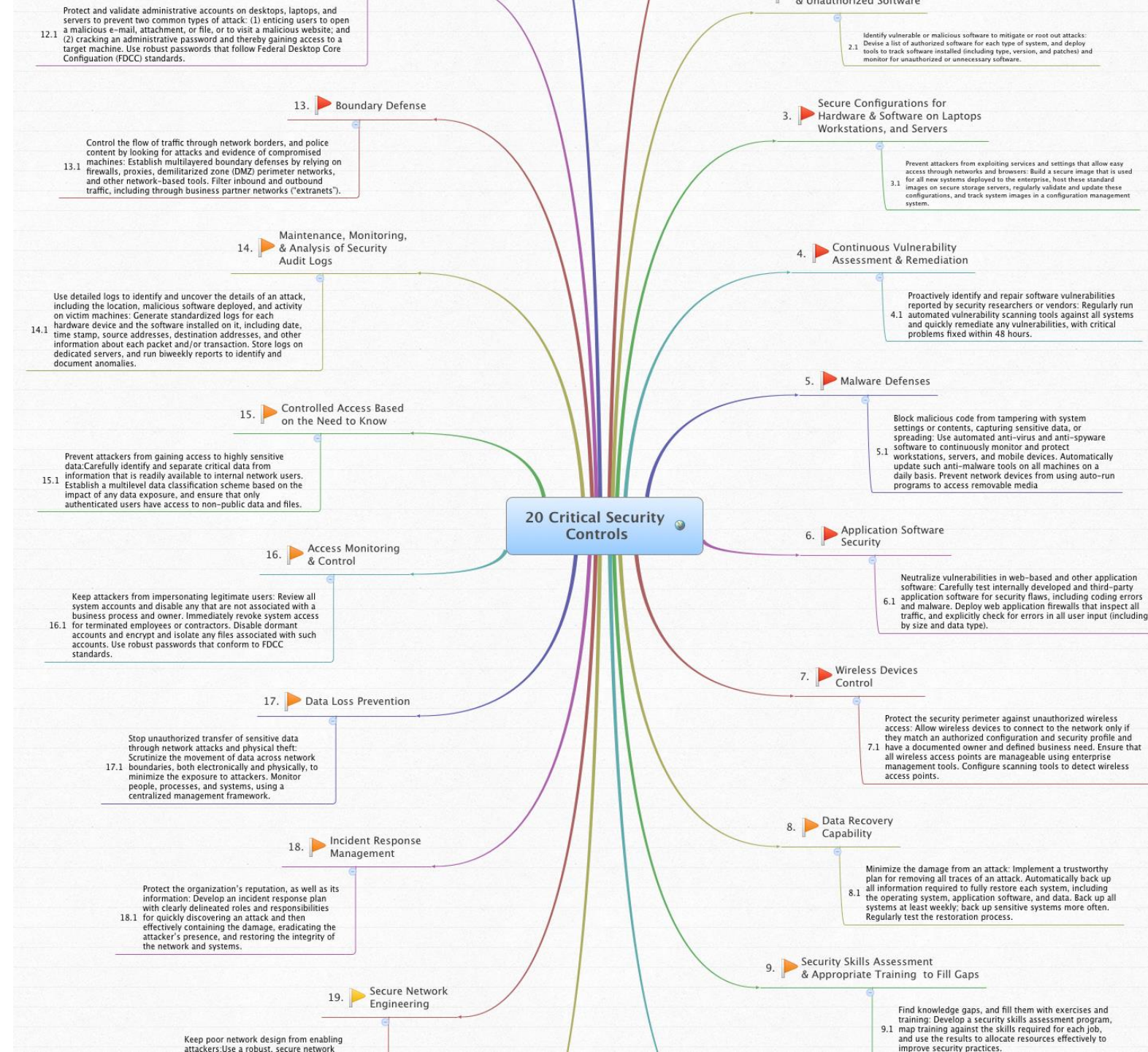
Most tool-only detection efforts fail due to alert fatigue

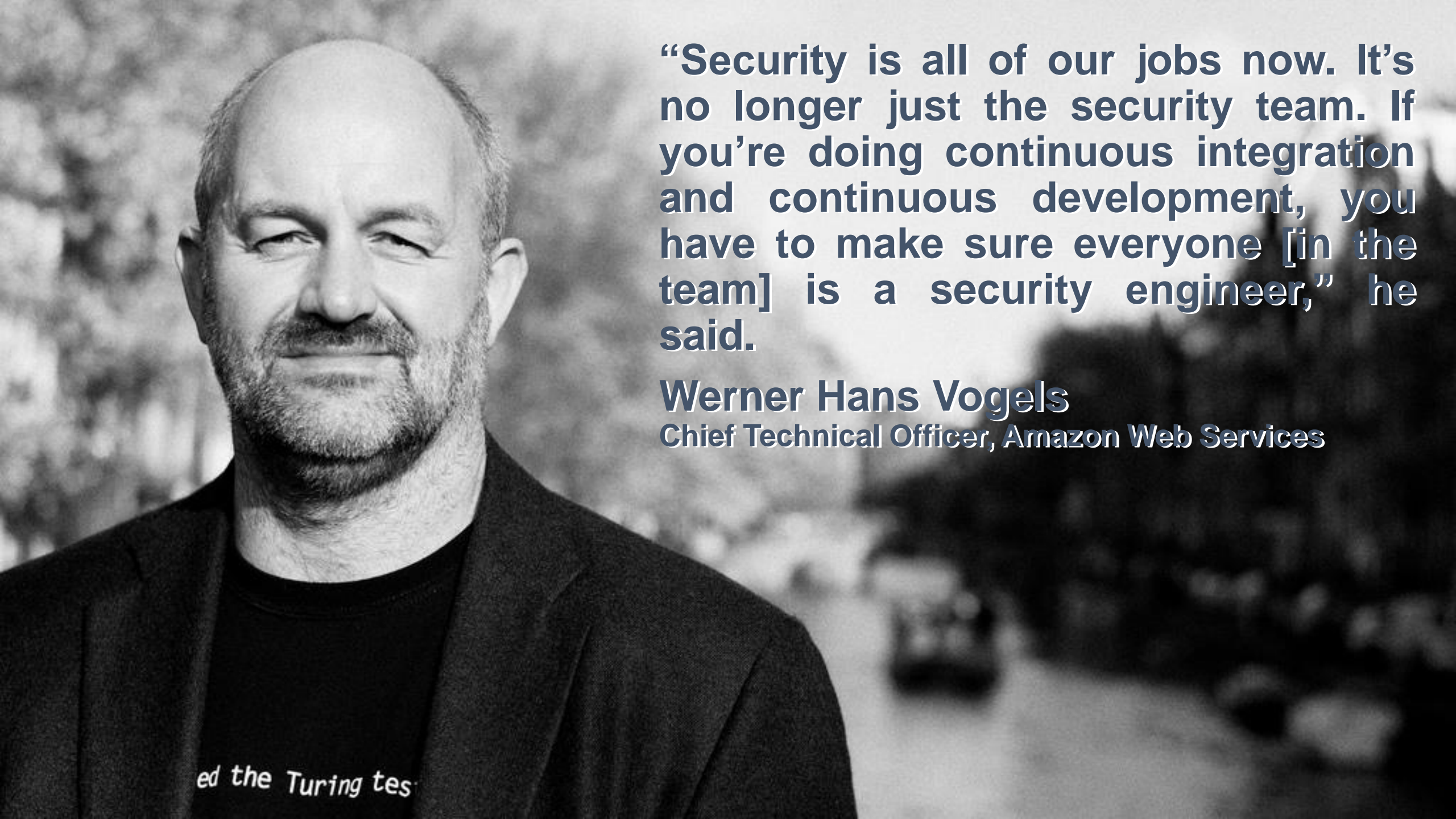


"Implementing SIEM solutions continues to be fraught with difficulties, with failed and stalled deployments common as well as solutions not meeting goals a year or more afterward." Gartner

Why does it matter?

Nobody can do all of this on their own.



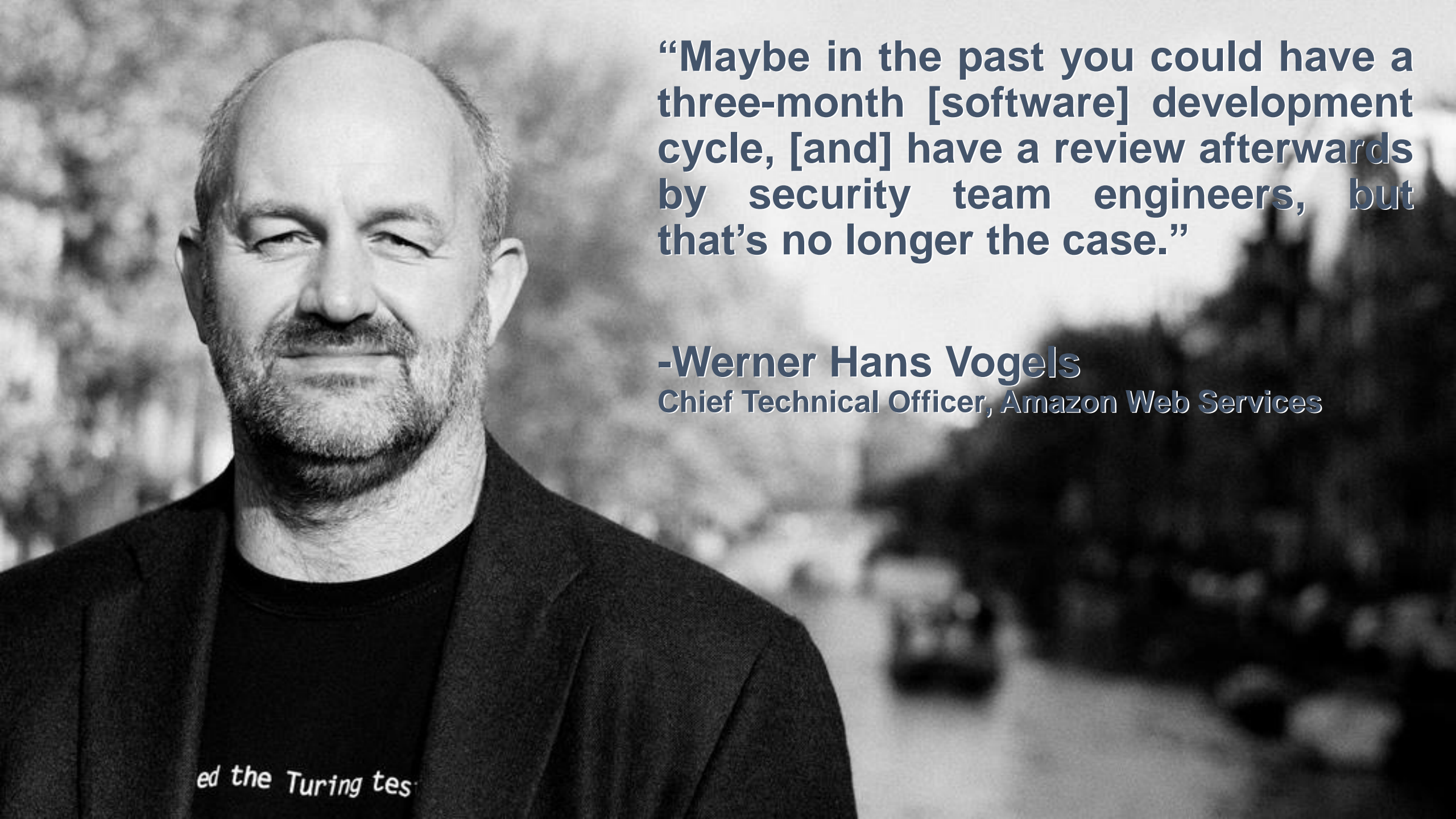


“Security is all of our jobs now. It’s no longer just the security team. If you’re doing continuous integration and continuous development, you have to make sure everyone [in the team] is a security engineer,” he said.

Werner Hans Vogels

Chief Technical Officer, Amazon Web Services

ed the Turing tes



“Maybe in the past you could have a three-month [software] development cycle, [and] have a review afterwards by security team engineers, but that’s no longer the case.”

-Werner Hans Vogels

Chief Technical Officer, Amazon Web Services

ed the Turing tes

A blurred background image showing several people sitting around a table in a meeting room, with large windows in the background. The image is dark and out of focus, serving as a backdrop for the text.

Broad Use Cases For A Common Goal

Be Impervious to attack.

Not
prevention,
but,

Not capable of being harmed

SINCE 1828

JOIN MWU | GAMES | BROWSE THESAURUS | WORD OF THE DAY | VIDEO | WORDS AT PL

impervious

DICTIONARY | **THESAURUS**

impervious



adjective | im·per·vi·ous | \(\)im-ˈpər-vē-əs\
Popularity: Top 20% of words | Updated on: 3 Dec 2017

⚡ **TRENDING NOW:** [noel](#) [ballistic](#) [net neutrality](#) [surrogacy](#) [gentrification](#), [gentrify](#) [SEE ALL](#)

Examples: IMPERVIOUS in a Sentence ▼

Editor's Note: Did You Know? ▼

Definition of IMPERVIOUS

- a : not allowing entrance or passage : **IMPENETRABLE** • a coat *impervious* to rain

b : not capable of being damaged or harmed • a carpet *impervious* to rough treatment
- : not capable of being affected or disturbed • *impervious* to criticism

—imperviously *adverb*

—imperviousness *noun*

As a result of the cyberattack, "we've learned a few things," Layne said. "We're doing a better job with preparing."

How can we be impervious to attack?

Engineer for both failure and the response to failure.



THE "IT DOESN'T APPLY TO ME" FALLACY

Embrace Chaos

Avoid the fallacies of complacency

"Why is there a fear of chaos when it's inevitable?"

AWS
re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



How can we be impervious to attack?

1

Engineer for both
failure and the
response to failure

2

Include everyone in
the effort to be
secure

3

Assume nothing,
question everything

We can show you how.

Our experienced and talented team of highly certified security operations center engineers and solution architects work together to help your company use the resources you have to their *fullest potential* and keep them **secure**.



Thank you.