OneNeck®

ALERT LOGIC®

Elections, Pandemics and Holidays - Oh My!

Managing, Detecting and Responding to Cyberthreats in the Chaos of 2020

Katie McCullough, OneNeck CISO

Bharath Vasudevan, Alert Logic VP of Product & Technical Marketing

Speakers

Katie McCullough, CISO - OneNeck
Katie McCullough provides direct leadership over Information Security, Governance, Risk and Compliance (GRC). She is responsible for overseeing and driving strategic IT security planning and compliance efforts so the company can deliver custom IT solutions to customers. As the CISO, Katie is accountable for ensuring OneNeck services are built and managed according to the foundational security principles of Confidentiality, Integrity and Availability (CIA). To achieve the CIA triad, she works closely with the OneNeck teams accountable for adhering and improving professional IT services based on key industry best practice frameworks such as ISO, ITIL and the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

Bharath Vasudevan – VP Product Marketing – Alert Logic
Bharath Vasudevan is the Vice President of Product and Technical Marketing at Alert Logic. His team is aligned with R&D and develops positioning, messaging, and competitive differentiation, which ultimately drive pipeline and helps close sales opportunities. Additionally, the team owns field enablement and strategic marketing at the product level, including product launches and supporting campaigns.

The World Around Us is in Chaos.

OneNeck IT SOLUTIONS

ALERT LOGIC

Everyone, no matter how small, is at risk.

OneNeck IT SOLUTIONS

ALERT LOGIC

Say What?!

My remote employee clicked on what?!

OneNeck IT SOLUTIONS

ALERT LOGIC

There are many challenges

Addressing Compliance

Accelerating Cloud Adoption

Detecting and Responding to Threats

Understanding Risk

MSSP vs MDR

MDR defined: Managed detection and response (MDR) delivers 24/7 threat monitoring, detection and lightweight response services to customers leveraging a combination of technologies deployed at the host and network layers, advanced analytics, threat intelligence, and human expertise in incident investigation and response. - Gartner

How is this different from MSSPs or Managed SIEMs?

- MSSPs monitor network security controls
- May send alerts when anomalies are identified
- Do not investigate the anomalies to eliminate false positives
- Do not respond to real threats
- Typically, abnormalities are forwarded to IT personnel who must then determine if it's a real threat

Traditional IT use cases which are not MDR

Manage Firewall	Manage Security Agents	Develop Security Content	Scan for Vulnerabilities	Patch Systems
Manage AV Tool	PEN Testing	Anti-Spam Filter	Research Threats	Threat Intel
Manage IDx	Store Logs	Monitor Logs	Investigate Alerts	Web Content Filtering
Monitor Network	Monitor Changes	24/7 Operations	Incident Response	Security Consultancy

Use cases that *are* MDR focus

Manage Firewall	Manage Security Agents	Develop Security Content	Scan for Vulnerabilities	Patch Systems
Manage AV Tool	PEN Testing	Anti-Spam Filter	Research Threats	Threat Intel
Manage IDx	Store Logs	Monitor Logs	Investigate Alerts	Web Content Filtering
Monitor Network	Monitor Changes	24/7 Operations	Incident Response	Security Consultancy

The must-haves for Managed Detection and Response

OneNeck IT SOLUTIONS
ALERT LOGIC

Reduce the likelihood or impact of a successful attack

Provide 24/7 visibility and cover all assets in an organization

Augment technology with human intelligence to ensure accuracy and value

Provide custom responses that understand cause and reflect business and attack context

Scale to deliver technical analysis and human insights across dynamic environments

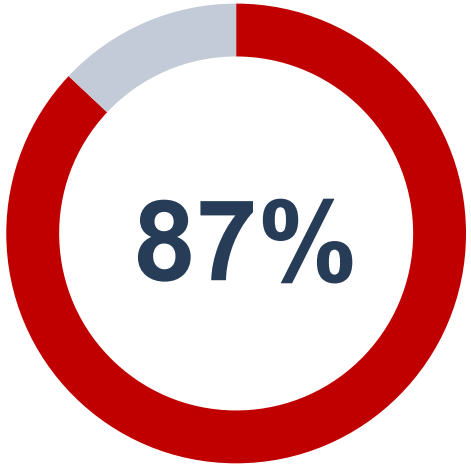
Deliver results and reporting that are credible, accessible and useful

Continuously be refreshed with research on new threats and vulnerabilities

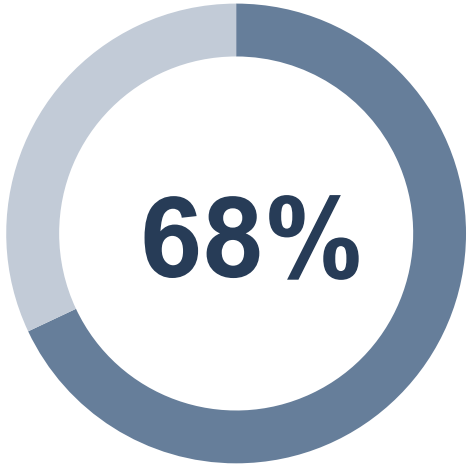
There is a huge upside to getting it right

Breaches happen quickly and usually go undiscovered for months

Of environments are not static



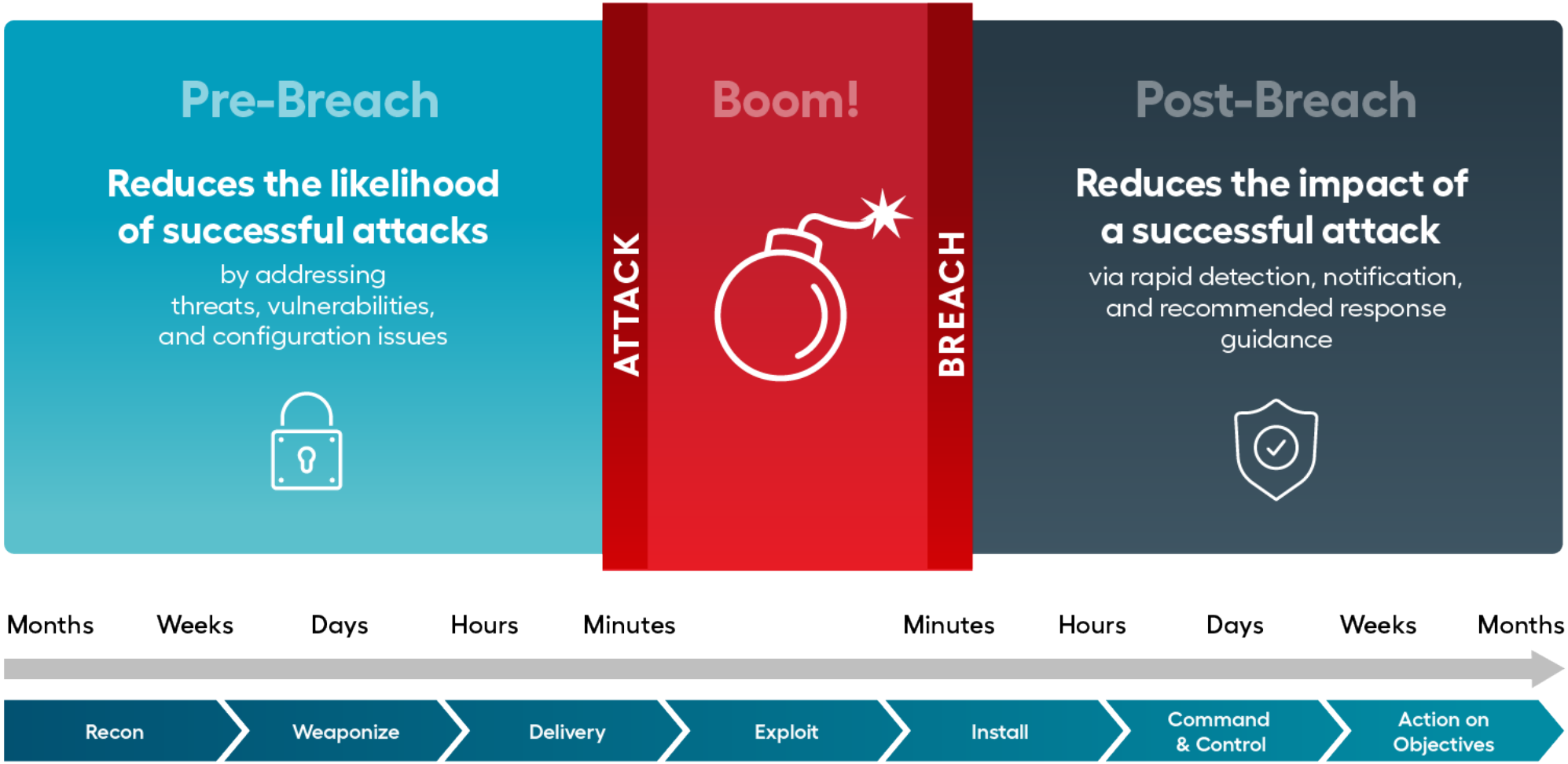
Most attacks and data theft succeed in minutes or less



Two-thirds go undiscovered for months or more

Focus on both pre- and post-breach is critical

OneNeck IT SOLUTIONS
ALERT LOGIC



Managed Detection & Response

Alert Logic MDR: a unique set of capabilities

OneNeck IT SOLUTIONS
ALERT LOGIC

Alert Logic's Platform Fabric Coverage

Hybrid protection, both on-premises and in multi-cloud environments

Including network and endpoint telemetry

Threat Intelligence, Vulnerability Research & Analytics

Global team of security researchers, data scientists, and security engineers

Over 30 Petabytes of threat data across hundreds of thousands of systems, collected and continuously analyzed

Leveraging machine learning to achieve scale and proactively inform customers of their exposure to new and emerging threats

Industry Experts

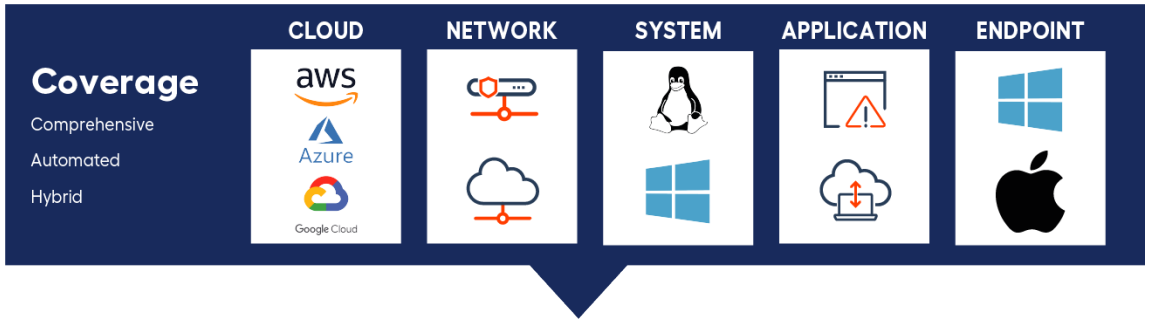
150+ trained SOC analysts

Proprietary internal training program

- Organically grow entry level analysts to security experts
- Enabling scalability to support rapid growth

Twice the industry average for security analyst retention

Alert Logic's coverage



Visibility and protection across hybrid, on-premises and cloud environments.

aws · Azure · Google Cloud · vmware

IBM Cloud · docker · kubernetes · Amazon ECS · Amazon EKS

okta · Azure Active Directory · Auth0

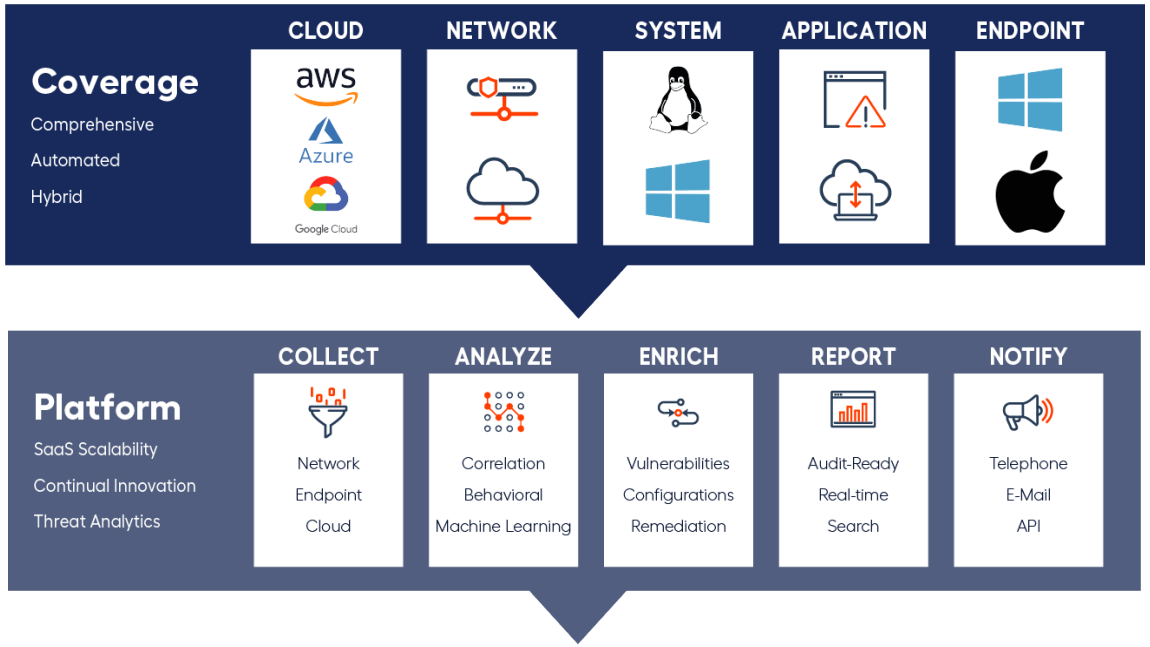
G Suite · Office 365 · salesforce

f5 · cisco · JUNIPER NETWORKS · paloalto networks · Check Point SOFTWARE TECHNOLOGIES LTD

SOPHOS · Symantec · McAfee · Carbon Black. · DARKTRACE

And many more ....

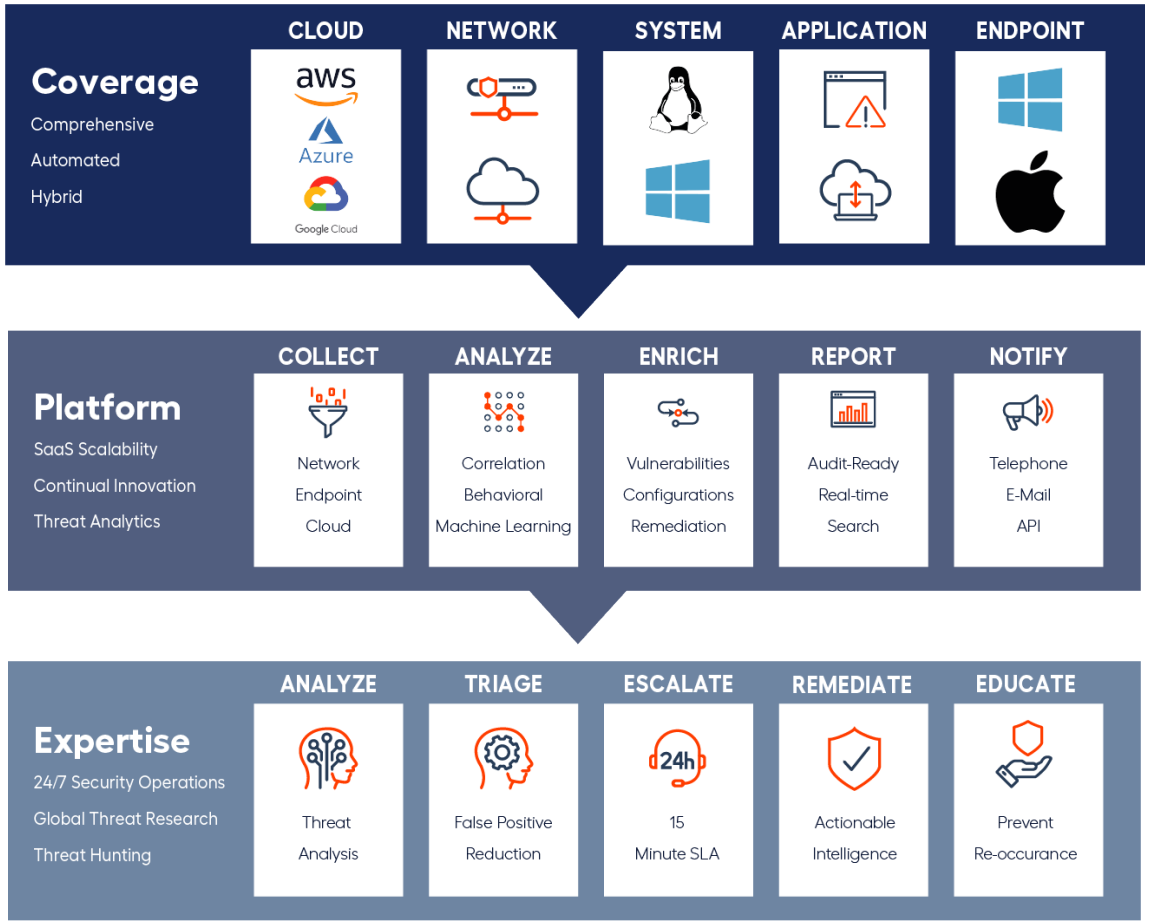
Scalable SaaS platform



Collection, storage, analytics & reporting at massive scale across assets, logs, events, network telemetry, endpoint, user and file access.

- **Cloud-delivered for massive scale**
- **Over 30 petabytes of threat data**
- **100s of thousands of systems**
- **Deep analytics and machine learning**
- **Proactive awareness of new risk**

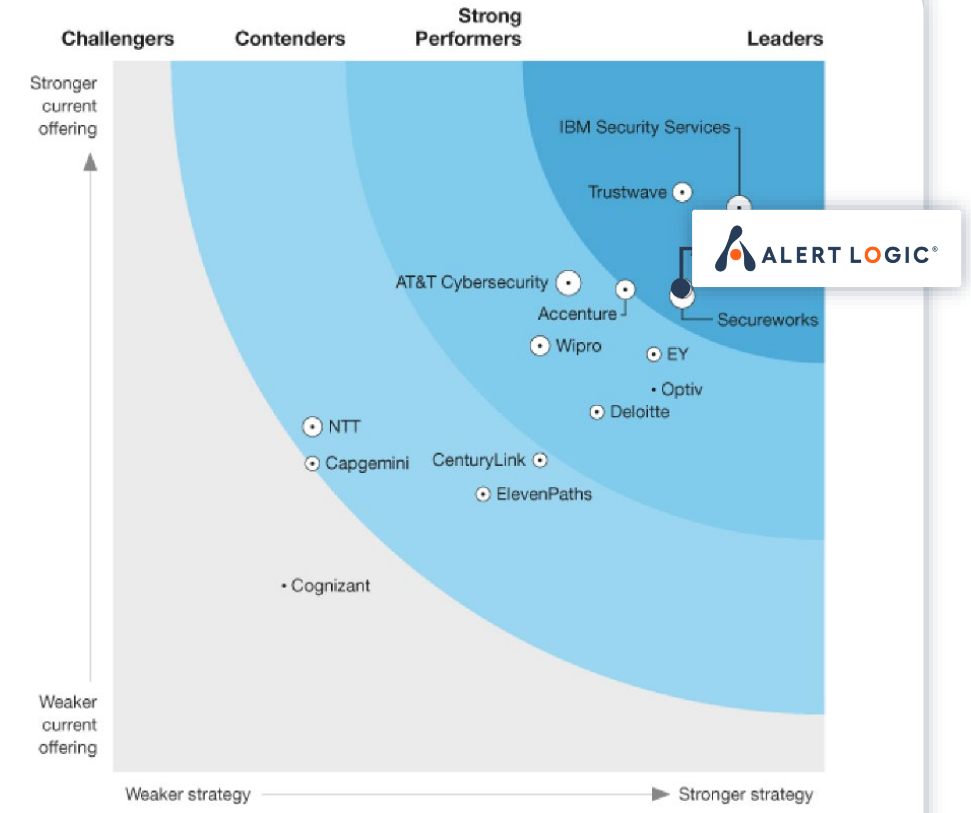
Alert Logic's expertise



A global team of security researchers, data scientists, and engineers that support more than 150 trained analysts to stalk, identify, and provide rapid response to threats.

- **24/7 monitoring in the SOC**
- **Investigate Indicators of Compromise**
- **Search adjacent data**
- **Validate the incident**
- **Deliver response recommendations**

Recognized industry leader and visionary



FORRESTER® | "Leader" 2020

Gartner® | "Visionary" 2019

Trusted by over 4000 customers

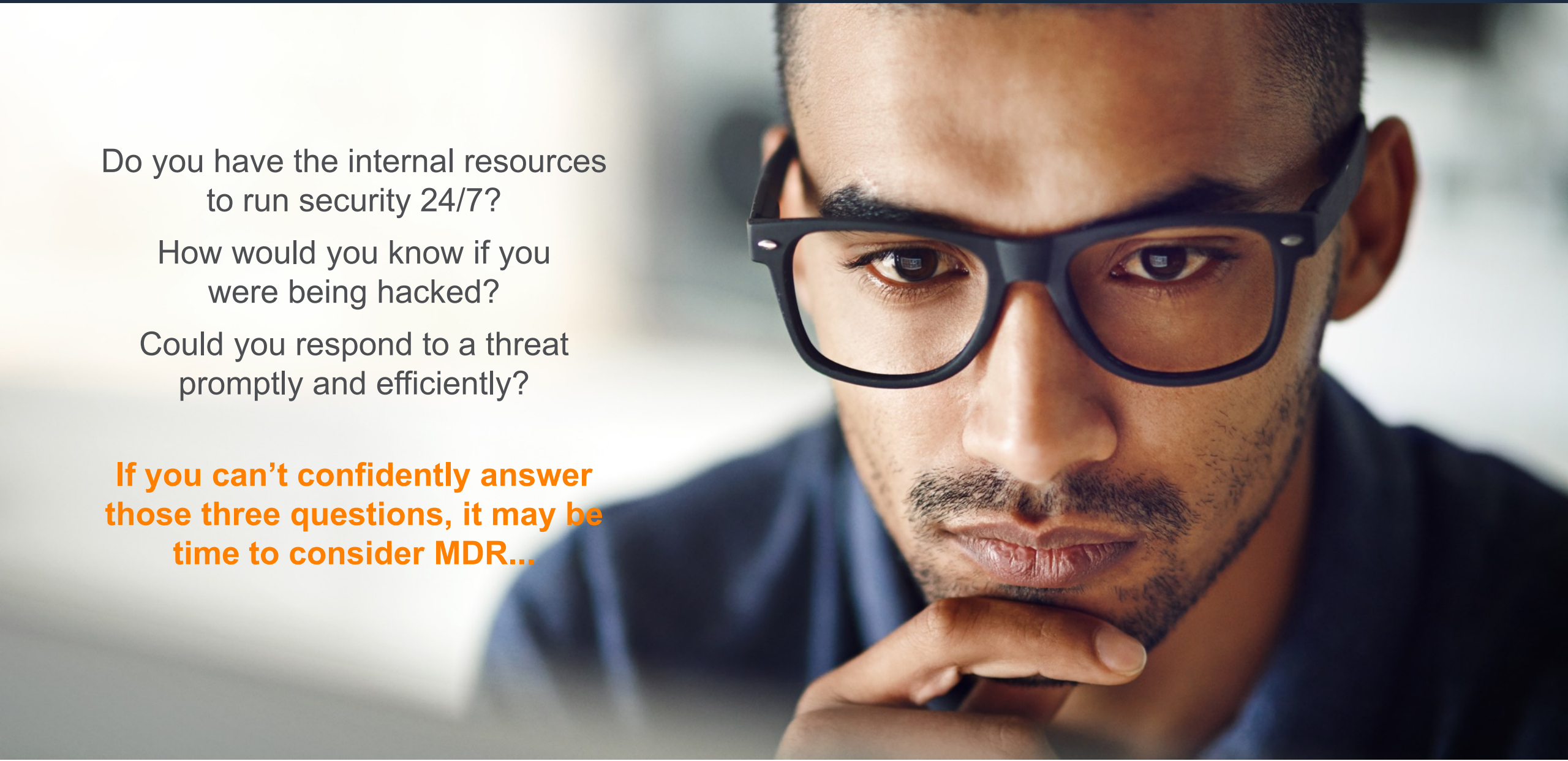
OneNeck IT SOLUTIONS
ALERT LOGIC

> Because we have one place to go now, where we can quickly look up the details of the threat or potential threat, it saves us a lot of time. **Alert Logic gives us peace of mind.**

> Knowing that Alert Logic's SOC is constantly monitoring the security of our systems **gives me peace of mind** that I will receive a notification within minutes of anything suspicious happening. I could never employ enough people to provide this kind of service, and I can't put a price on that.

> **The biggest benefit in working with Alert Logic is peace of mind.** They know that the information their customers provide using the Travel Tripper reservation engine is secured.

Final Considerations – Ask Yourself...



Do you have the internal resources to run security 24/7?

How would you know if you were being hacked?

Could you respond to a threat promptly and efficiently?

If you can't confidently answer those three questions, it may be time to consider MDR...

Thank You!

For additional information or to learn more, reach out to us at: info@oneneck.com