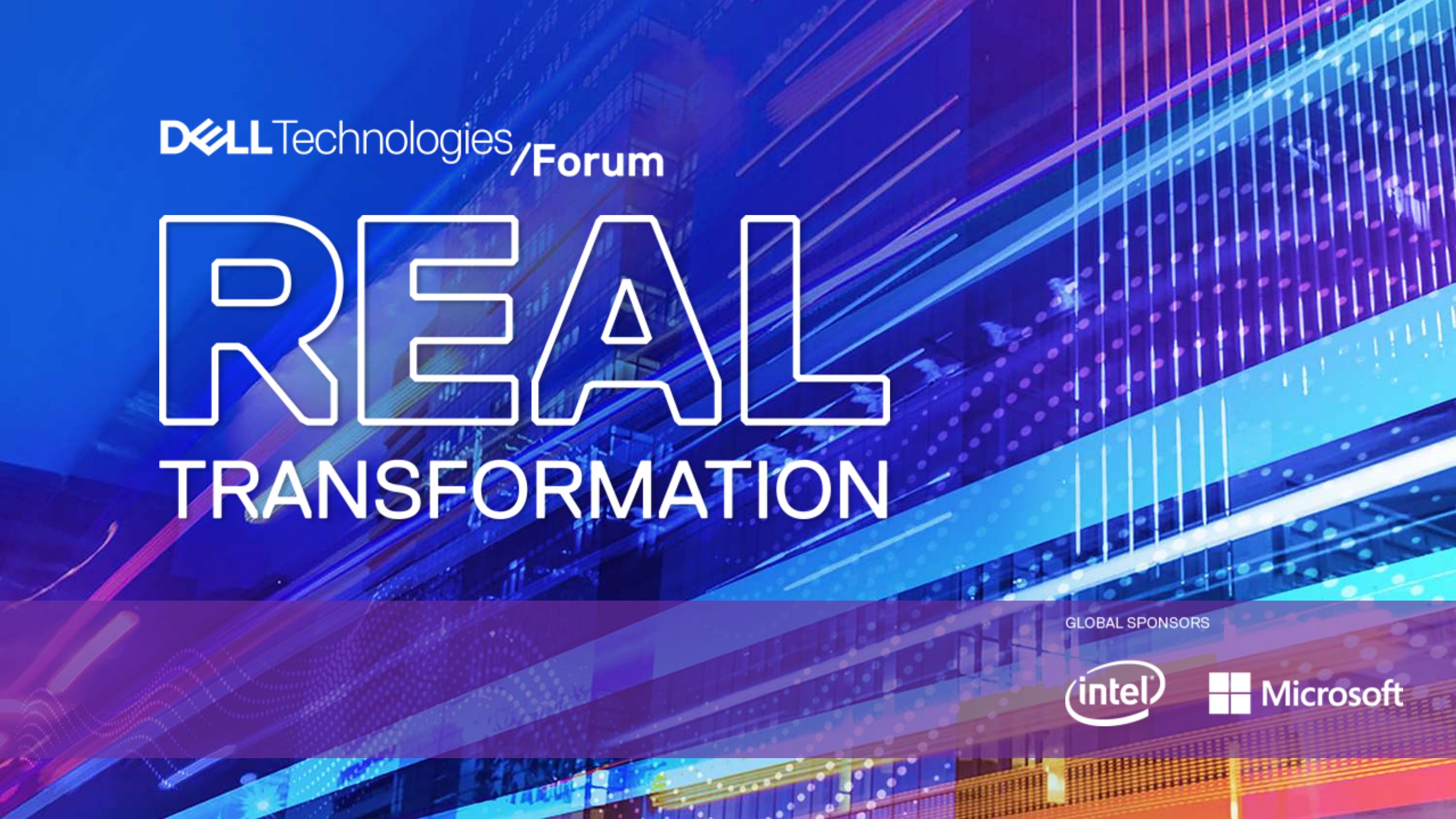

DELL Technologies /Forum
REAL
TRANSFORMATION
GLOBAL SPONSORS
intel
Microsoft

Red Cloak™ Threat Detection & Response

Andre von Ameln

19 September 2019

Secureworks®

Agenda

01 “Detection & Response” – Where Do You Stand Today?

02 Our Approach

03 Red Cloak Threat Detection & Response

04 MDR Powered by Red Cloak

05 How It Works / Optional Demo

76%

Of organizations are finding detection and response either **much more or more difficult** today than two years ago.

Source: ESG Master Survey Results, *The Threat Detection and Response Landscape*, April 2019

Top reasons why respondents say it's getting more difficult...

34%

Say amplified **threat volume**

The remaining 66% say:

- increasing workload
- enlarged attack surface
- manual processes
- too many tools
- lack of staff

This is forcing a few changes…

82%

Think improving detection and response is a high priority

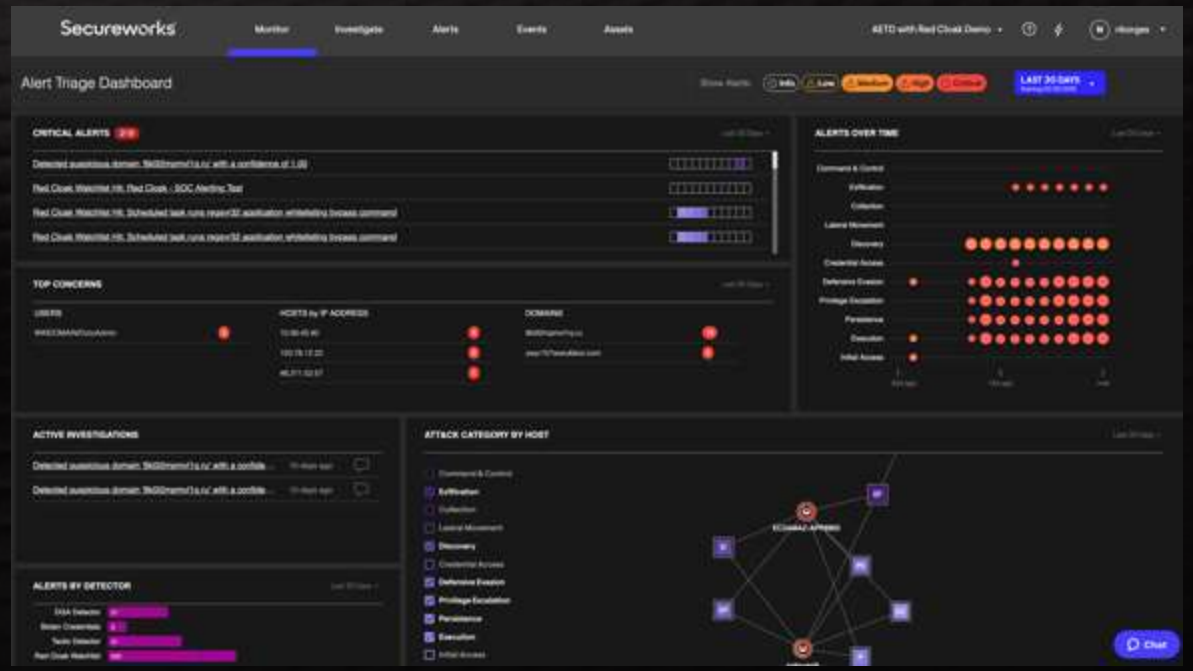
89%

Are increasing detection and response spending over the next 12-18 months

Our Approach: Software-Driven Security

We have taken our 20 years of security operations experience, threat intelligence and the most significant technological advancements in the last 5 years to reimagine how security should be done.

Red Cloak™ Threat Detection & Response



A Security Analytics Application for security analysts to:

- Detect
- Investigate
- Respond

Designed and built by Security experts with experience solving complex data challenges

What Does it Do?

Correlates security-relevant data from endpoint, network, cloud, and business systems

Detects both known and unknown threats to protect your environment from a wide range of threats

Enriches data with relevant user and asset context to speed sense-making

Maps security alerts to MITRE ATT&CK framework

Supports collaborative investigations

Automates containment and prevention actions

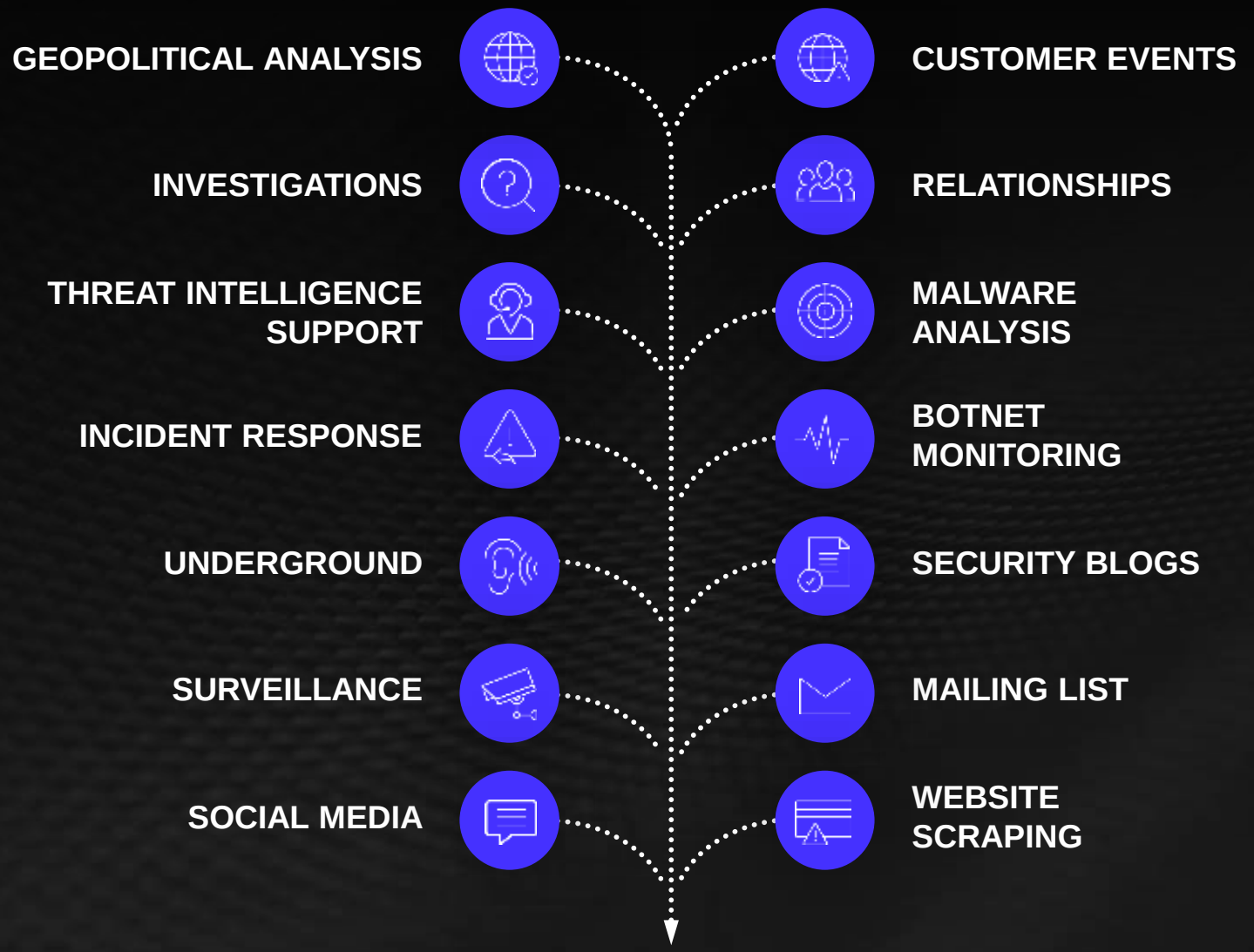
Includes Secureworks' market-leading threat intelligence and Red Cloak endpoint agent

Red Cloak™ Threat Detection & Response

DIFFERENTIATION

Threat Intelligence

From the Secureworks Counter Threat Unit™ research team



Network Effect

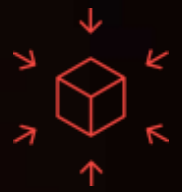
- ✓ Over **20** years of attack and threat actor data
- ✓ Over **70** researchers in our Counter Threat Unit™
- ✓ Over **135** threat groups actively monitored
- ✓ Over **1,000** IR engagements performed last year
- ✓ Over **52,000** unique threat indicators updated daily
- ✓ **Thousands** of customers across the globe

Tactic Graphs™

Domain Generation Algorithm (DGA)

Stolen Credentials

Rare Program And Rare IP



Punycode

Detectors

Command & Control

Brute Force Success

Login Anomalies

Network Countermeasures

Endpoint Watchlists

Internal Use - Confidential

Classification: //Secureworks/Confidential - Limited External Distribution:

Red Cloak™
Threat Detection
& Response

Benefits for Your Team

01 Detect Advanced Threats

02 Trust Your Alerts

03 Streamline & Collaborate

04 Automate the Right Action

73% of organizations have been impacted by the cybersecurity skills shortage

Your team uses our software

We'll do it for you

Red Cloak™
Threat Detection
& Response

Managed Detection and Response

POWERED BY Red Cloak™

[1] Source: ESG Research Publication, *The Life and Times of Cybersecurity Professionals*, April 2019

Managed Detection and Response

POWERED BY Red Cloak™

- ✓ 24x7 Software-Driven Service
- ✓ Access to Red Cloak TDR
- ✓ Collaborative Investigations
- ✓ Proactive Threat Hunting
- ✓ Incident Response

A 24x7 Threat Detection and Response Unit that Helps You

Scale Your Security Operations & Expertise

Managed Detection and Response

POWERED BY Red Cloak™

ENDPOINT | NETWORK | CLOUD | BUSINESS SYSTEMS

Detect

DETECTORS

Detection use cases in Red Cloak TDR leveraging threat intelligence and advanced analytics (machine learning, deep learning, UEBA, statistical analysis)

Investigate

INVESTIGATION

Analyst recommendations provided within the TDR application

VALIDATION

Analyst investigates leveraging additional context and enrichment

Respond

IMMEDIATE ACTIONS

Software-driven actions performed by our analysts to contain the threat.

INCIDENT RESPONSE

Performed by our industry recognized global IR team

Applied Intelligence

Secureworks® Network Effect, Incident Response Findings, Secureworks® CTU® Threat Intelligence

Proactive Threat Hunting

Threat hunting across our customers by our advanced team of global threat hunters

24x7 Analyst Access

Via in-app Chat, Email, and Phone

Solution Features

Managed Detection and Response Powered by Red Cloak	
24x7 Service	✓
Access to Red Cloak TDR	✓
Support for AWS, O365, & Azure Event Sources	✓
Threat Triage & Prioritization	✓
Investigation & Validation	✓
Security Expert Assistance	✓
Secureworks Executed Containment	✓
Remote Incident Response Hours	✓
Proactive Threat Hunting	✓
Threat Engagement Manager	✓
Collaborative Investigation Interface	✓
Live Chat Support	✓
Agent & Sensor Support	
Red Cloak Agent	✓
Crowdstrike Support	✓
Threat Intelligence & Analytics	
CTU Countermeasures (Cisco and Palo Alto)	✓
Red Cloak TDR Analytics	✓
Applied Threat Intelligence	✓

Available as Add-Ons	
iSensor	✓

- MDR is priced by # of Endpoints
- Subscription based

FORRESTER®

“Unfortunately, many providers without a strong background in incident response have launched MDR services, which will result in disaster when a high-profile incident occurs. Stay away from the pretenders with no bona fides”

JEFF POLLARD, APRIL 26 2018
FORRESTER RESEARCH, INC.

Forrester Research Inc., Now Tech: Managed Detection And Response (MDR) Services, Q2 2018, Jeff Pollard

Secureworks®

"In 2018, Secureworks conducted more than a thousand incident response engagements that totaled more than 40,000 professional incident response hours. More than 120 terabytes of investigative data were collected. Secureworks analyzes this data to help organizations plan for, detect, respond to, and recover from cybersecurity incidents."

The Secureworks Incident Response Insights Report 2019

Industry Recognition

Placed in the “Full Scale Forensics” category in Forrester’s latest MDR report

Forrester Research Inc., Now Tech: Managed Detection And Response (MDR) Services, Q2 2018, Jeff Pollard

Red Cloak™

Secureworks®

Industry Recognition

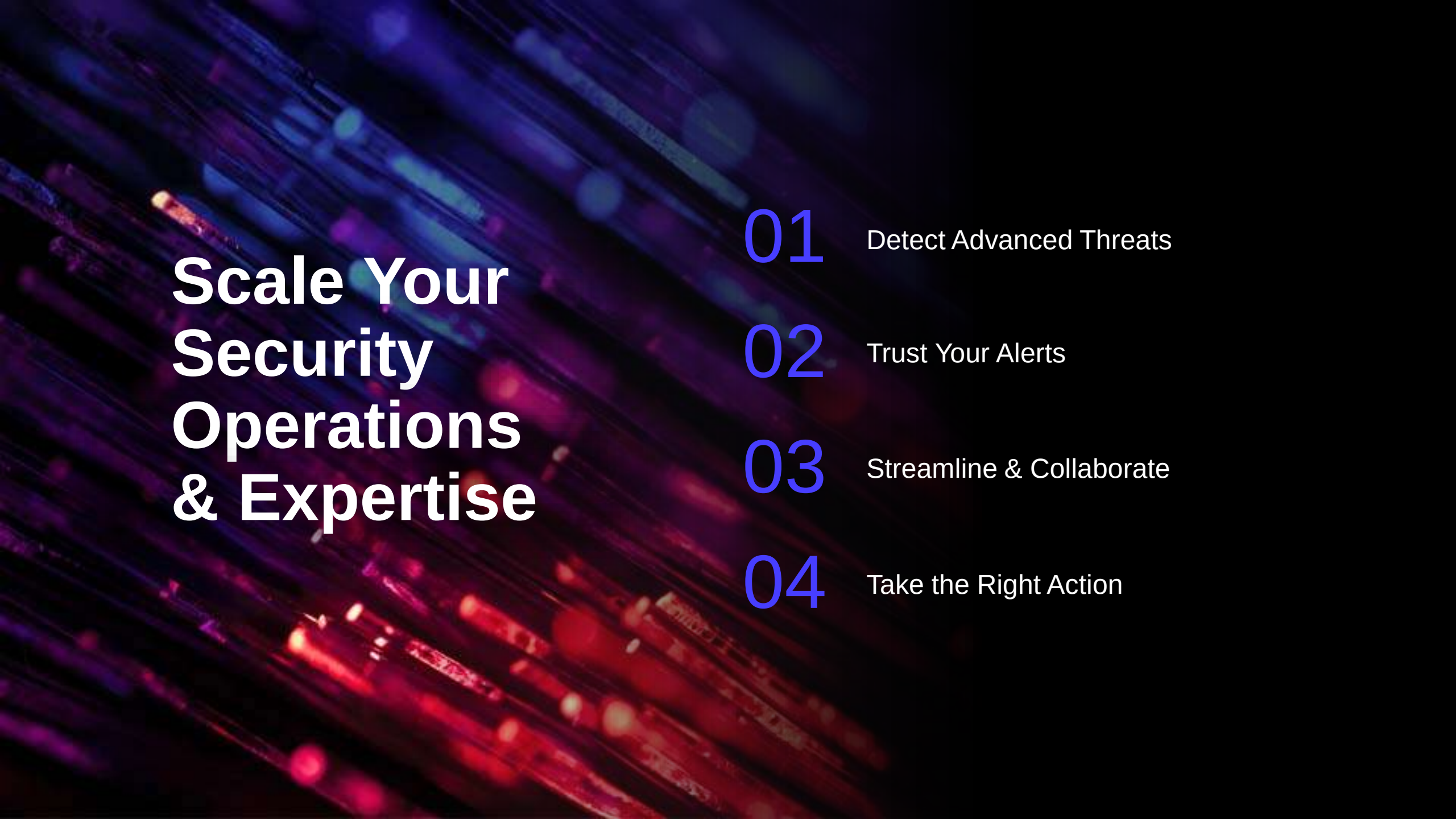
Mentioned as a **Representative MDR Provider** in Gartner's Market Guide for MDR Services

Gartner Inc., Market Guide for Managed Detection and Response Services, Toby Bussa, Kelly M. Kavanagh, Sid Deshpande, Craig Lawson, Pete Shoard, Jul 2019

Mentioned as a **Sample Vendor** in Gartner's Hype Cycle for Endpoint Security

Gartner Inc., Hype Cycle for Endpoint Security, 2019, Dionisio Zumerle, John Girard, Jul 2019

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.


Scale Your Security Operations & Expertise
01
Detect Advanced Threats
02
Trust Your Alerts
03
Streamline & Collaborate
04
Take the Right Action

Questions?

Andre von Ameln

Mobile: +49 162 8834460

Email: aameln@secureworks.com

Secureworks®


DELL Technologies
DELL
DELL EMC
Pivotal
RSA
Secureworks
virtustream
vmware