Secureworks®

Modernizing Threat Detection and Response

Secureworks® Taegis™ XDR

101 - A Conversation Starter

February 1, 2021

The Rapidly Evolving Threat Landscape

- Cyber attacks continue to grow in sophistication

Legacy security tools fail to

meet demands of threat landscape

- Mobile workforces and cloud data requires any time, anywhere protection

Security analysts are overwhelmed by a **mass volume of alerts**

Emerging threats and targeted attacks are **harder to detect**

Many security teams fail to keep pace due to **skills gap** and **understaffing**

Realities of the Modern Threat Landscape

Security analysts are overwhelmed by a mass volume of alerts

70%

70% of security pros investigate 10+ alerts daily (up 25% from previous year)[1]

Emerging threats and targeted attacks are harder to detect

80%

An average of 80% of successful breaches are new or unknown attacks[2]

Many security teams fail to keep pace due to skills gap and understaffing

53%

53% of orgs report a problematic shortage of cybersecurity skills[3]

Reality of Legacy SIEM Limitations

Security analysts are overwhelmed by a mass volume of alerts

Alert Fatigue

SIEMs fail to prioritize advanced threats. As a result, security teams are burdened by chasing meaningless alerts

Emerging threats and targeted attacks are harder to detect

Inadequate Threat Detection

Basic SIEM correlation rules are insufficient to detect unknown threats or targeted attacks

Many security teams fail to keep pace due to skills gap and understaffing

SIEM Complexity

Difficult to deploy and rigorous to maintain, SIEMs require security teams to place major focus on platform management

Security Analytics Meets Demand for SIEM Alternative

"The **complexity and cost of buying** and running SIEM products as well as the emergence of other **security analytics technologies** have driven interest in alternative approaches to collecting and analyzing event data to identify and respond to advanced attacks."[1]

Gartner, 2020

Top 5 Most Challenging Attributes of Legacy SIEMs[2]

Secureworks

Taegis XDR

Delivers **Security Analytics** as a **SIEM Alternative**

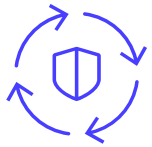
DIFFERENTIATION

Secureworks

XDR Delivers Security Analytics as a SIEM Alternative

Taegis is an open cloud-native platform that combines the power of human intellect with insights from security analytics to unify detection and response across endpoint, network and cloud environments for better security outcomes and simpler security operations.

XDR Positioning Pillars



Advanced Analytics

- Machine Learning
- Data Science
- Advanced Analytics Based Detectors

Accelerated Investigation & Response

- Threat Intelligence Based Detectors
- Mapped to Mitre ATT&CK Framework
- SIEM Investigation & Response Capabilities

Community-Applied Intelligence

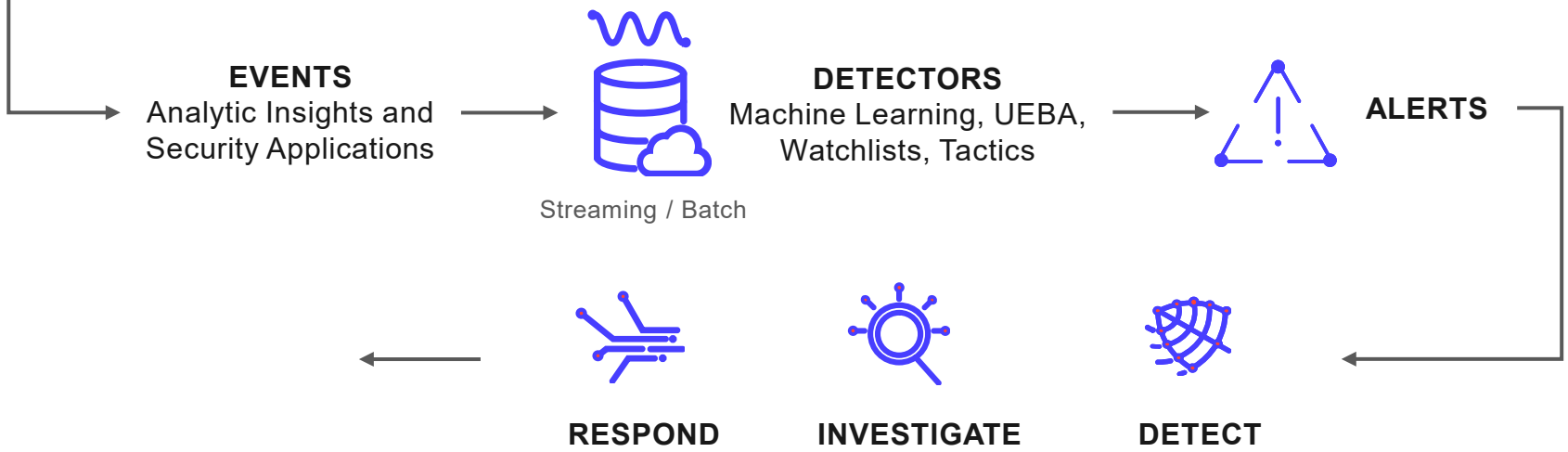
- 300+ Expert Security Analysts
- Ask An Expert
- 4000+ Customers

Software with Security at Its Core

SECURITY RELEVANT DATA SOURCES AND INTEGRATIONS

Ingest, Normalization, and Storage

Endpoint Agent Telemetry | Intrusion Detection Systems | Firewalls and Proxies | Cloud Security and Data APIs | On-prem Data Collection and Forwarding



INTELLIGENCE SOURCES

- **Secureworks®** Community-Applied Intelligence
- **Secureworks®** Incident Response Findings
- **Secureworks®** CTU® Threat Intelligence
- Third-party Intelligence

Secureworks®

XDR Delivers Security Analytics as a SIEM Alternative

New SIEM Capabilities Enhance Investigation and Response for Security Teams

01

Log Collection & Retention

- Reliably ingest and retain logs from a variety of data sources

02

Search & Reporting

- Easily ask questions of the data and share the results in several different ways

03

Custom Alerting

- Enables customers to customize the platform to make it relevant to their environment

New SIEM Capabilities Empower Security Analysts

- Gain more ability to actively investigate and proactively hunt
- Easily share insights for rapid communication and decision making

Customer Quote

It’s picked up threats we wouldn’t have seen. Taegis **XDR isn’t just the next generation of SIEM, it’s an evolution.**

DAVID LEVINE
VP CORPORATE & INFORMATION SECURITY, CSO
RICOH, Inc.

10

Taegis XDR

Replace Legacy SIEMs with Improved Efficiency & Efficacy

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

Replace Your Legacy SIEM with Taegis XDR

Your SIEM Challenges	XDR Offers	How This Impacts You
Alert Fatigue What if you could significantly reduce the number of meaningless alerts and increase accuracy?	**Advanced Analytics Detectors** that come with large training data sets leveraging Secureworks Community-Applied Intelligence to improve accuracy and eliminate meaningless noise	**Trust Your Alerts** Gain confidence in the criticality of an alert and prioritize investigations
Advanced Threat Detection What if you could detect advanced threats your SIEM wouldn't notice?	**Threat Intelligence Detectors** that integrates behavioral analytics based on knowledge of adversary TTPs from 1000s of IR engagement	**Detect Advanced Threats** Recognize adversaries by their behavior, be alerted to unknown threats often missed by legacy SIEMs

Replace Your Legacy SIEM with Taegis XDR

Your SIEM Challenges

Security Expertise
What if you could get an expert opinion to provide added context to respond to a threat?

Time & Labor Intensive
What if you could dedicate time and resources to investigations versus managing infrastructure?

XDR Offers

“Ask an Expert” chat feature,
provides real-time collaboration from within the user interface.

Cloud-based, Software as a Service
that is easy to manage because updates, backups, and tuning are covered.

How This Impacts You

Streamline & Collaborate
Give your security teams access to a senior intrusion analyst to help with an investigation or recommend a response

Take the Right Action
Save on time and resources when you put more focus on security rather than mundane platform management tasks.

Taegis XDR

Case Studies

Case Study

Secureworks helps Ricoh Group cut through the noise to quickly find threats with less effort

Challenge

Separate Threats From Noise

- Difficulty detecting advanced threats with current tools and resources
- Drowning in security alert noise / false-positives
- Decreased focus on issues that matter

The Solution

Taegis XDR

- Aggregate data from across the entire enterprise
- Use advanced AI to interpret that data and detect legitimate threats

Benefits

Identify Malicious Behavior

Recognize adversaries by their behavior, even if they're using little to no malware enabling you to detect unknown threats

Alert Enrichment

Gain confidence in the criticality of an alert to get the context you need to prioritize investigations and response

Eliminate Meaningless Alerts

Stop chasing false positives and focus limited resources on defending against real threats

Read the Full Case Study

“Taegis XDR combines Secureworks Taegis analytics with additional advanced tools previously unavailable to us. **It’s picked up threats we wouldn’t have seen.** Taegis XDR isn’t just the next generation of SIEM, it’s an evolution.”

David Levine

VP Corporate & Information Security,
CISO Ricoh USA, Inc.

Case Study

MinterEllison partners with Secureworks to holistically monitor, detect and prevent threats

Challenge

Secure Business Transformation

- Support business transformation, market demands while keeping security a priority
- Detect advanced threats related to mobile workforce and cloud data
- Reduce volume of meaningless alerts

The Solution

Taegis XDR

- Gain a full understanding of the threat scenario across your endpoints, network, and cloud data
- Machine learning helps eliminate meaningless alerts and detect previously unknown threats.

Benefits

Trust Alerts

Trusting alerts with state-of-the-art data science methodologies to increase detection fidelity

Secure Business Growth

Supporting real-time business transformation through holistic cyber security measures

Reduce Risk With Less Effort

Stop chasing false positives and focus limited resources on defending against real threats

Securing Business Growth with MinterEllison (Video-1:40)

"We generate around 2 billion events each month. With Secureworks, we are able to crunch down that number to **20-30 high fidelity alerts** — and that makes my team's job much easier."

Sunil Saale

Head of Cyber and Information Security Minter Ellison

A Software Company with Security At Its Core

Delivering the Latest in Analytics & Threat Intelligence for Better Security Results

Elevate your security posture and ease the burden on your security teams with the combined value of **Taegis VDR & XDR**

VDR

Eliminate the manual effort required to significantly reduce enterprise vulnerability risk.

- Asset: Web and Machine Discovery
- Scanning and Identification
- Vulnerability Prioritization
- Remediation Planning

XDR

Detect, investigate and respond to advanced threats across the entire ecosystem to drive better security outcomes

- Advanced Analytics
- Accelerated Investigation and Response
- Community-Applied Intelligence

Secureworks®

Cost of Complacency is High

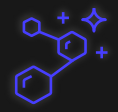
Detection and Response Speed is Critical

Secureworks®

What Does XDR 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

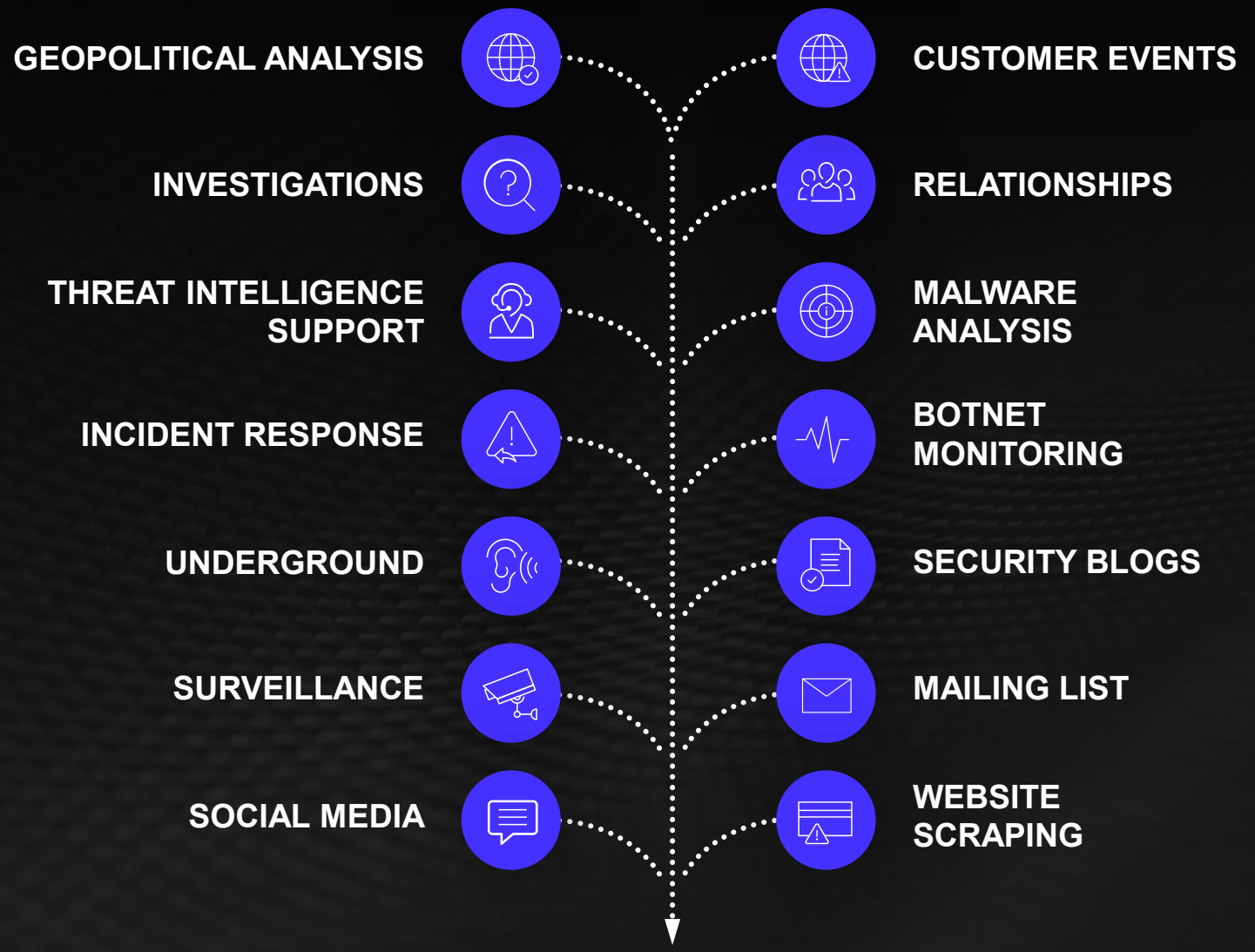
Supports collaborative investigations

Automates containment and prevention actions

Includes Taegis market-leading threat intelligence and endpoint agent

Threat Intelligence

From the Secureworks Counter Threat Unit™ research team



Our Approach: Software-Driven Security

We have taken our 20+ years of security operations experience, threat intelligence, and technological advancements to reimagine how security should be done.

Secureworks®

The XDR Difference

20+

Years of Attack & Threat Data

1400

IR Engagements Performed in the last year

300+

Expert Security Analysts, Researchers & Responders

52,000

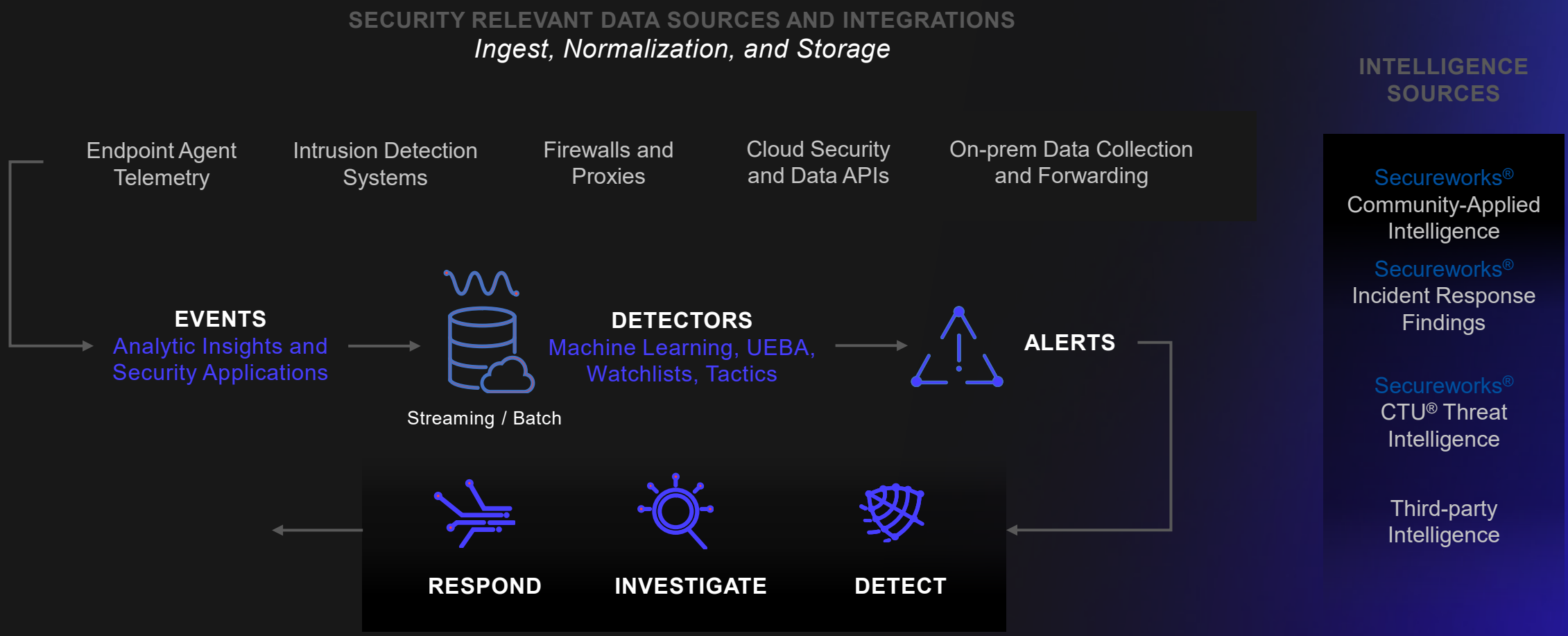
Database of 52k unique threat indicators managed & updated daily

Modernize your Threat Detection & Response with Security Analytics

Security Analytics combines big data capabilities with threat intelligence to help detect, analyze and mitigate threats before they cause any damage.[1]

- Alert Enrichment
- Holistic Visibility
- Behavioral Analytics
- Threat Intelligence

Software with Security at Its Core



Secureworks®