CROWDSTRIKE

NEXT-GEN SIEM AND THE MODERN SOC

Philip Scheidl, Sales Engineer

Survival of the Fastest:

The imperative of a speed advantage for stopping breaches

Avg. eCrime Breakout Time

62 min

Fastest eCrime Breakout Time

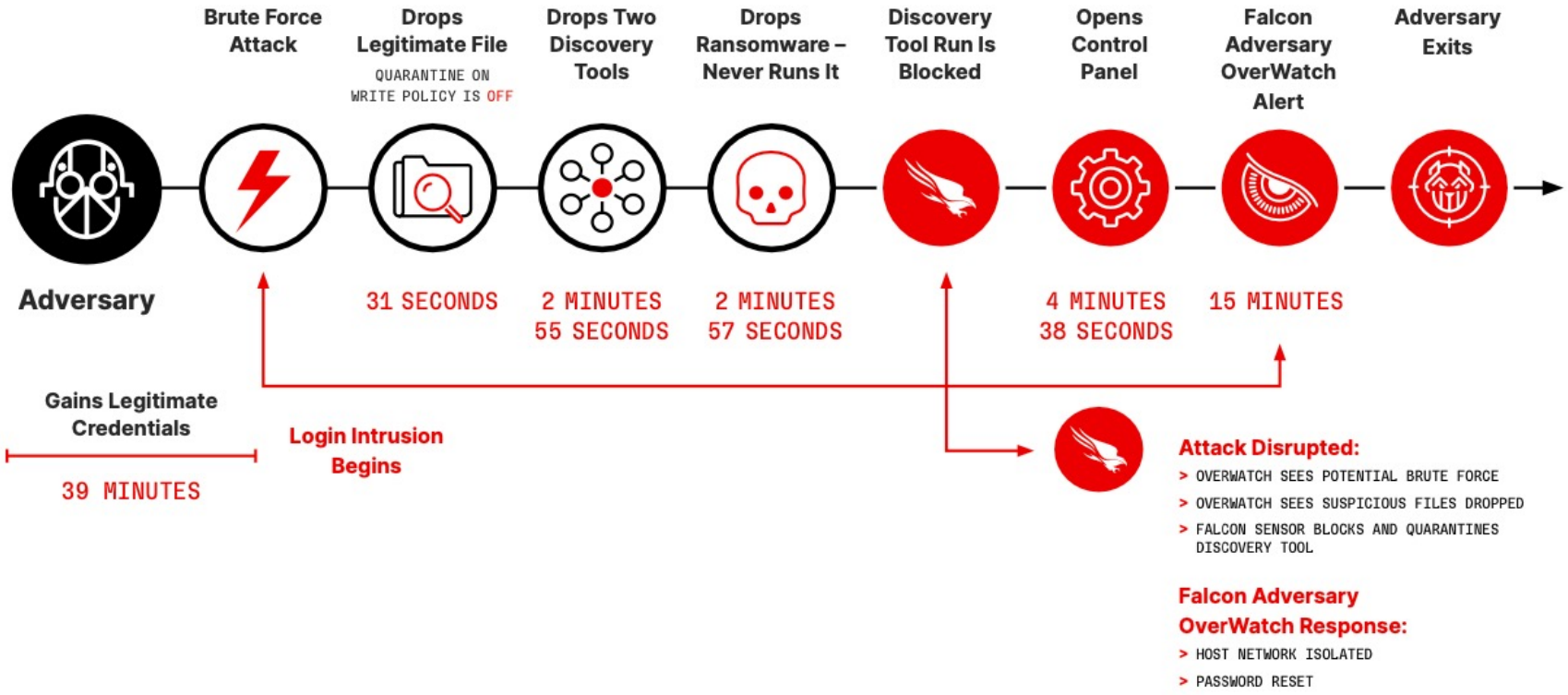
2 m 7s

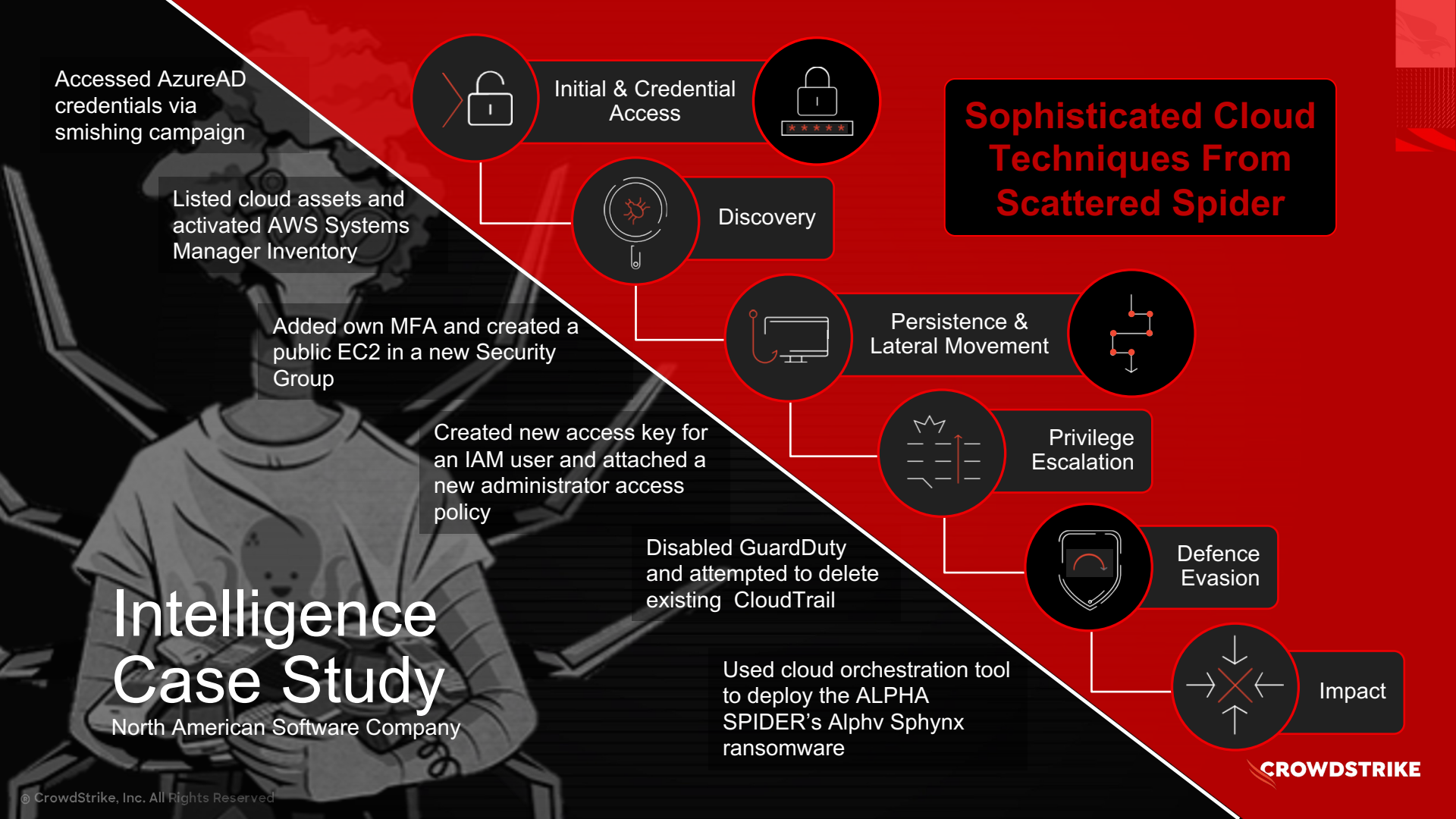
Drop in Breakout Times vs. 2022

↓26%

CROWDSTRIKE

Anatomy of a real attack

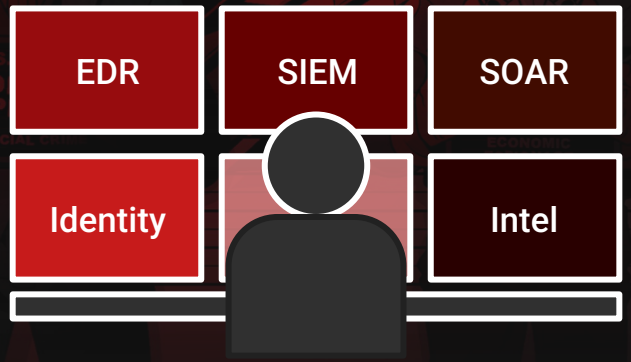




Today's SOCs struggle to keep up with adversaries

Siloed data and tools

Poor SIEM performance



Low-fidelity alerts and intel

Manual triage and investigations

"With our previous SIEM, SOC analysts would initiate queries on Friday and come back on Monday for results. Sometimes, their queries timed out altogether. Not to mention logs getting stuck in the ingestion pipeline, failing to make their way into the SIEM. It was a nightmare for our SOC analysts." — *Kevin Nejad, CEO, Vijilan*

CROWDSTRIKE

Evolution of Threat Detection & Response

PREVENTION & PROTECTION & COMPLIANCE

Point Products for each Domain

EDR
AV
FW

CSPM
Cloud
FW

PAM
MFA

SSPM
CASB

FW
IDS
ZTNA

SIEM

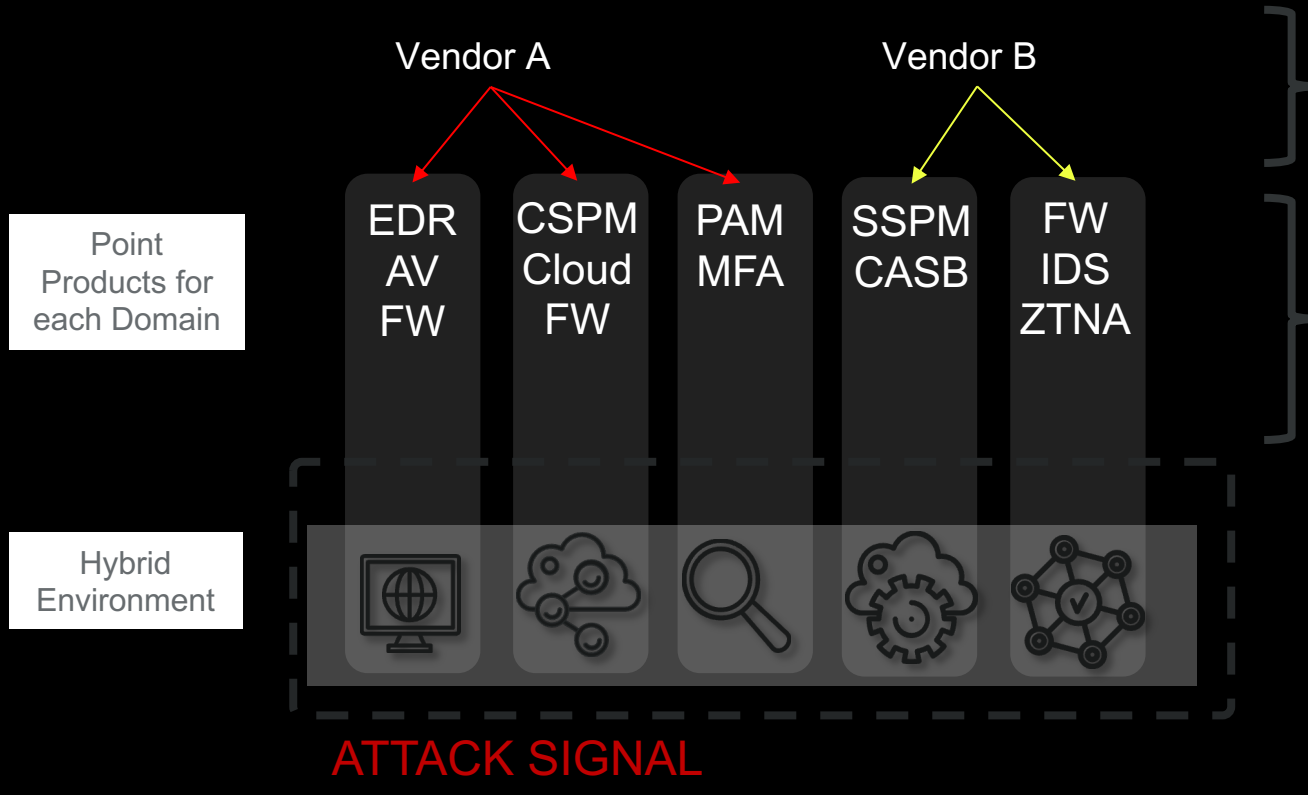
Custom defined & developed use-cases

Hybrid Environment

ATTACK SIGNAL

CROWDSTRIKE

Evolution of Threat Detection & Response



eXtended Detection & Response (XDR) products

Integrated for products of the same vendor

SIEM

Custom defined & developed use-cases

CROWDSTRIKE

So, what is XDR?

"Extended detection and response, or XDR, is an **open cybersecurity architecture** that integrates security tools and unifies security operations across all security layers—users, endpoints, email, applications, networks, cloud workloads and data. With XDR, security solutions that aren't necessarily designed to work together can interoperate seamlessly on threat prevention, detection, investigation and response.." – **IBM, 2023**

"Extended Detection and Response (XDR) is a security **solution that unifies multiple security technologies** into a single platform, providing greater visibility and control over threats." – **Gartner**, **2021**

"Extended detection and response (XDR) **collects threat data** from previously siloed security tools across an organization's technology stack for easier and faster investigation, threat hunting, and response. An **XDR platform** can collect security telemetry from endpoints, cloud workloads, network email, and more. – **CrowdStrike, 2023**

"The **evolution of EDR**, which optimizes threat detection, investigation, response, and hunting in real time. XDR unifies security-relevant endpoint detections with telemetry from security and business tools such as network analysis and visibility (NAV), email security, identity and access management, cloud security, and more. It is a cloud-native platform built on big data infrastructure to provide security teams with flexibility, scalability, and opportunities for automation." – **Forrester, 2021**

CROWDSTRIKE

What can we conclude?

The definitions may vary, but there are a **few consistencies** across them:

- XDR is a combination/cooperation of multiple tools or systems
- The goal of XDR is to improve threat detection, to provide visibility
- Some Response component, ideally automated, is part of XDR

That leads to some conclusions of what XDR is and needs to provide:

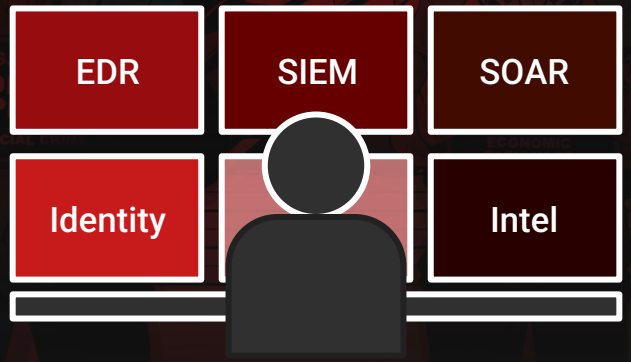
- XDR needs to be seen more like a **concept/architecture.** It brings together **telemetry & threat data/signal from different sources** to monitor and analyse activity and detect attacks in an automated way
- **Data sources are expanding**. In addition to primary data sources like **network** and **endpoint**, **Identity** and **SaaS** must be included as sources for analysis
- It must offer native **automated respond capabilities**
- It must be open and support ease of **integration into the existing security stack**

CROWDSTRIKE

Today's SOCs struggle to keep up with adversaries

Siloed data and tools

Poor SIEM performance



Low-fidelity alerts and intel

Manual triage and investigations

"With our previous SIEM, SOC analysts would initiate queries on Friday and come back on Monday for results. Sometimes, their queries timed out altogether. Not to mention logs getting stuck in the ingestion pipeline, failing to make their way into the SIEM. It was a nightmare for our SOC analysts." — *Kevin Nejad, CEO, Vijilan*

CROWDSTRIKE

CROWDSTRIKE

Modernize the SOC with AI-Native Next-Gen SIEM

Stop breaches

Reduce response time with blazing-fast search and workflow automation

Cut costs by unifying SecOps on one AI-native SOC platform

CROWDSTRIKE

Ask any question to accelerate investigations

and get fast, actionable answers to stop threats quickly

CROWDSTRIKE

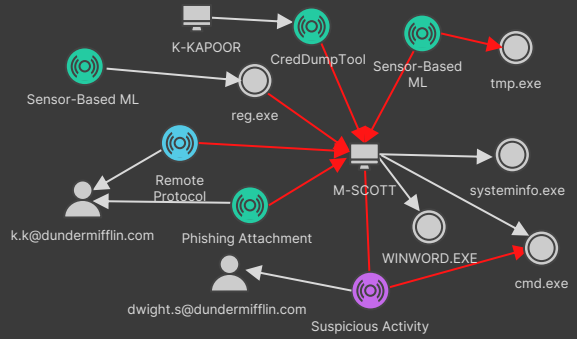
Imagine if you could...

Get a complete picture of threats across any source

Centralize alerts and intelligence

Critical	Remote Services: Remote Desktop Protocol	Network
High	Honeytoken Account Activity	Identity
Medium	Multifactor Authentication Request Generation	Identity
Critical	Phishing: Spear-Phishing Attachment	Email
High	cmd.exe on SE-ICR-WIN10-DT$ by dwight.s	Endpoint
Medium	svchost.exe on SE-ICR-WIN10-DT$ by dwight.s	Endpoint

Simple, visual investigations



Collaboration and auditing

Apply response action: Add to restricted group

Applying this response action adds dwight.s@dundermifflin.com to a designated Zscaler internet access group.

This change may take up to 10 minutes to apply. More about XDR response actions.

MS: Added to restricted group based on activity.

Cancel | Apply response action

to simplify investigations

CROWDSTRIKE

Imagine if you could...

Reduce MTTR and boost analyst productivity

Automate complex workflows with 125+ workflow actions and 55+ triggers

Drive any endpoint response action

Respond across your ecosystem with 61,000+ customer-defined unique playbooks[1]

Schedule or run playbooks on demand

with native SOAR capabilities integrated across your platform

[1] Based on analysis of CrowdStrike Falcon deployments

CROWDSTRIKE

Thank you