fishtech

CYDERES

powered by Backstory

THREAT HUNT TOUR

FOUNDED BY EXPERTS

My team and I built the largest cybersecurity provider in North America. But today's cybersecurity challenges are not effectively addressed by those legacy solutions.

Born in the cloud, Fishtech is a digital-era security company leading our clients through next-generation cloud, IT, and security transformation challenges.

- GARY FISH, CEO

FISHTECH GROUP

CYDERES

PROBLEM & OPPORTUNITY

Gartner: "Detection and Response is Key Priority"

1. FRAGMENTED SECURITY SOLUTION MARKET
2. INDUSTRY WIDE SKILLS SHORTAGE
3. SHIFT to DETECTION & RESPONSE
4. SOCs STINK

fishtech

CYDERES

VISION

Our "core purpose" and our BHAG

Deliver real change in the information security industry.

Security-as-a-Service to help solve for the fragmented security solution landscape and the skills shortage.

Provide an exceptional Blue Team as a Service via a Cyber Defense Platform (aka MDR).

fishtech

CYDERES

VALUE PROPOSITION

Human led, machine-driven Security as a Service

CYDERES supplies the people, process, and technology to help organizations manage cybersecurity risks, detect threats, and respond to security incidents in real-time.

Backstory is 10x search for your security data here to ”give good the advantage”.

fishtech

CYDERES

SOLUTIONS

Focus on your business, while we handle your threats

EMDR – Enterprise Managed Detection & Response

Backstory

Detection, investigation, remediation, plus proactive threat hunting

GSOC – Global Security Operations Center

Backstory

Managed Detection *without* response: 24x7 SOC + DIY Response

Cloud – Cloud Governance as a Service

Visibility, Protection, Detection, and Response for your Cloud

S I R T – Security Incident Response Team

Expertise on standby to help with every aspect of a security event

Threat – Red Team as a Service

Attack simulation to improve detection, response and recovery

BK.ES – Backstory as a Service

Backstory

Harness the disruptive power of Backstory without disruption

fishtech

CYDERES

UNDERLYING MAGIC

Faster. Better. Cheaper. Scalable.

1. TECH INDEPENDENT, OPEN SOLUTIONS
2. FIRST MDR 100% BUILT ON Backstory
3. COMPREHENSIVE: CLOUD and ON-PREM
4. LEGENDARY SERVICE at a FAIR PRICE

fishtech

CYDERES CYBER DEFENSE CENTER

CYDERES

HERE IS OUR WHY

Always want to "Start with Why"

ATTACKERS ARE WINNING

IN SPITE OF INCREASING SECURITY INVESTMENTS

PEOPLE ARE BUYING ALERT FACTORIES
(AND THEY'RE NOT LOOKING AT THE ALERTS)

fishtech

CYDERES

SECURITY IS NOT WORKING

Source: Verizon Data Breach Investigations Report

91% of breaches led to data compromise in “days” or less

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

79% of breaches took “weeks” or more to discover

fishtech

CYDERES

THE BOTTOM LINE?

You can't keep them out…

Preventative controls alone
set you up for failure.

Detection and Response is the key.

fishtech

CYDERES

HEY, I'M HERE FOR THREATS…

Bear with me – here's what you came for

ATTACKERS ARE WINNING

IN SPITE OF INCREASING SECURITY INVESTMENTS

BECAUSE PEOPLE ARE BUYING ALERT FACTORIES
AND THEY'RE NOT LOOKING AT THE ALERTS

HERE'S WHAT THAT LOOKS LIKE...

fishtech

CYDERES

START WITH CONTEXT

Because 93% of statistics totally aren't made up

- 1,579: Total number of publicly disclosed breaches
- 71% of US enterprises reported suffering at least one
- 89% experienced data breaches in the past 5 years
- $3.86 million: Average cost of a data breach
- Cost of a data breach is directly related time to detection and containment.

fishtech

Do you have an extra

$3.86 million to spare?

That’s how much the average data breach will cost you.

CYDERES

WHAT'S THE IMPACT?

How do they get there? Some hand waving math:

- Ponemon study: $141 per record

  IBM.com/security/data-breach

"Direct expenses include engaging forensic experts, outsourcing hotline support and providing free credit monitoring subscriptions and discounts for future products and services. Indirect costs include in-house investigations and communication, as well as the extrapolated value of customer loss resulting from turnover or diminished customer acquisition rates."

fishtech

CYDERES

BUT THAT'S NOT REALLY THE THREAT

Meet BEC

Method #1: Business Executive Scam

CEO's email is hacked or impersonated.
The imposter contacts the finance department to request a wire transfer.

Finance department authorizes wire transfer.
Request email will typically indicate transfer must be done quickly and quietly.

Funds are deposited into fraudster's account.
The false wire transfer is delivered to the criminal's fake bank account.

CYDERES

THIS IS THE REAL IMPACT

Real people losing their savings, jobs, companies, lives…

FBI: Global Business Email Compromise Hit $12.5 Billion

- Wire Transfer fraud
- Gift Card Fraud
- Real Estate Transactions
- Payroll Redirection
- Fraudulent Tax Returns
- Romance Schemes

fishtech

CYDERES

BEC EXAMPLE - PAYROLL

One of the easiest approaches to get to the money

From: "Eric Foster" <jnw2346@gmail.com>

Sent: Tuesday, July 19, 2019 9:36 AM

To: [redacted]@fishtech.group>

Subject: [EXTERNAL] -Account Update

CAUTION: This email originated from outside of the Fishtech network. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Hi Johnna,

I recently changed my bank and I would like to update my direct deposit information linked to my wages. Please advise/assist.

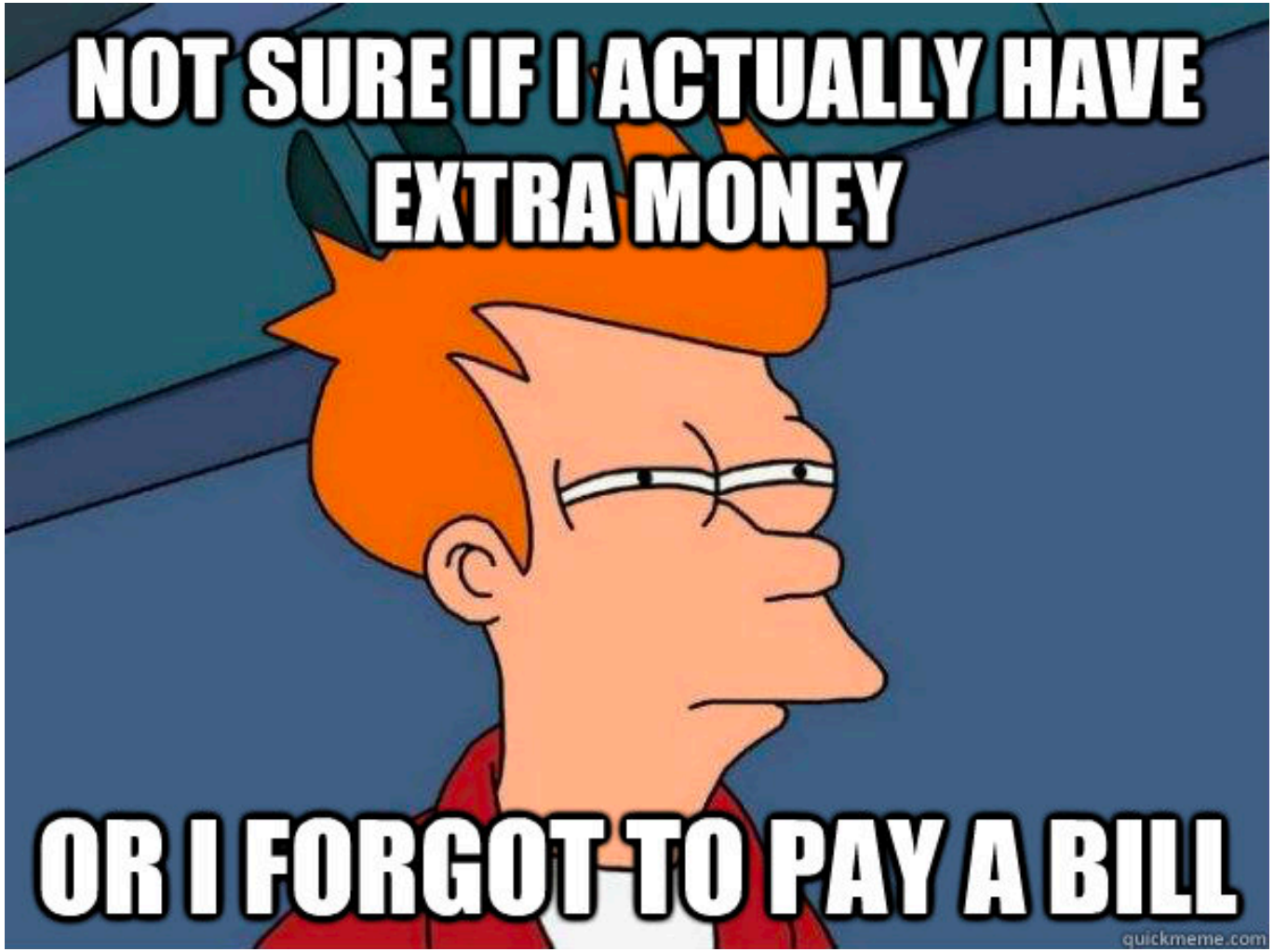
Thanks.
Eric Foster

fishtech

CYDERES

IT ALL STARTED WITH…

A system administrator failing to pay a bill



fishtech

CYDERES

HERE ARE THE INITIAL IOC's

Why BEC? Because that's where the money is…

Envelope and Header Summary

Received Time: 12 Jun 201[redacted] 10:47:09 (GMT -05:00)
Subject: <URGENT ACTION NEEDED> [redacted] DOCUMENT TO ALL EMPLOYEES (From CEO)
Envelope Sender: Kimberly.[redacted]@dhs.[redacted].gov

Sending Host Summary

Reverse DNS Hostname: mail-dm2on.outbound.protection.outlook.com (verified)
IP Address: 23.103.201.135 (MSFT)

fishtech

CYDERES

Message Document.pdf (215 KB)

From: , Kimberly L [mailto:Kimberly. @dhs. .gov]
Sent: Monday, June 12, 201 10:55 AM
Subject: <URGENT ACTION NEEDED> DOCUMENT TO ALL EMPLOYEES (From CEO) 06/12/201

A message from , Chief Executive Officer :

Dear Team,

I have some important documents to share with you which requires all staffs prompt attention.

Please read through secure attached document.

It's of high importance all staffs read through on what improves the welfare of our company.

CYDERES

Document.pdf (1 page)

Search

SECURE ONLINE DOCUMENT

CLICK HERE TO ACCESS
VIA MICROSOFT PDF READER

fishtech

Not Secure espinozalawoffices.com/falop/index.php

You are about to extract a File from **Microsoft PDF Reader**

File Details:

- File Name: **Shared Document.pdf**
- File Size: **42KB**
- File Type: **PDF**

Microsoft® Office

Download File

Not Secure | espinozalawoffices.com/falop/index.php

Your email provider is recognised by Microsoft server. Login below to access file.....

You are about to extract a File from **Microsoft PDF Rea**

File Details:

- File Name: **Shared Document.pdf**
- File Size: **42KB**
- File Type: **PDF**

Download File

Login with your valid details:

Send File To: My Email

Email Id: Enter valid password

Password: Enter valid password

Extract File Now

CYDERES

تم الاختراق ولكل شي نهاية
اذا كانت حرية اقولكم لاضابط لها..... فلتتسع صدوركم لحرية افعالنا

BBM:D3426186

الحلم السيئ

Bad Dream

fishtech

CYDERES

LET'S TALK TIMELINE

TTP's: Tactics, Techniques, Procedures

1. Protections down 36 hours before
2. Web gateway: logging outage at 10:30
3. First emails came in at 10:47
4. First infections by BYOD regardless
5. First reports came from end users
6. First actions by defenders: 11:30

fishtech

FW: ***IMPORTANT MESSAGE **** Organizational Exclusive Communications From CEO (06/1...

FILE MESSAGE

Mon 6/12/201 12:23 PM

, Jim

FW: ***IMPORTANT MESSAGE ** Organizational Exclusive Communications From CEO (06/12/201)**

To

Message Document.pdf (215 KB)

Dear Employees,

I have some important documents to share with you which requires all staffs prompt attention.

Please read through secure attached document.

It's of high importance all staffs read through on what improves the welfare of our company.

CYDERES

HERE'S WHERE IT GETS FUN

TTP's: Tactics, Techniques, Procedures

- Originating IP was 23.105.131[.]169
  - of course, an anonymous VPN endpoint
- Continuous ADFS access 10:26 – 19:29
- What's tied into AD SSO?
- First change at 11:57
- 21 changes by 13:30

workday.

ishtech

CYDERES

NOW? NOW IS WHEN WE PANIC

fishtech

CYDERES

Richard Bejtlich ✓
@taosecurity

Following

If you suspect an intrusion, resist the temptation to flail around by changing passwords, running AV, manually reviewing file systems, etc. Instead, review whatever logs or data you have. If you have no data, instrument the network first, and then look for adversary activity.

8:07 AM - 7 Nov 2018

90 Retweets **219** Likes

15 90 219

Tweet your reply

Richard Bejtlich ✓ @taosecurity · Nov 7

This Tweet was inspired by the terrible “security advice” I see on public forums.

fishtech

CYDERES

Dr. Anton Chuvakin @anton_chuvakin · Nov 7

Replying to @taosecurity

I think your advice is solid, but "hop into a time machine, go to 2017 and deploy NSM, EDR, log analysis before the intrusion" may enrage some people too....

2 3 8

Richard Bejtlich @taosecurity · Nov 7

If they are responsible for data that has value to the owners, then it is the constituents who should be enraged with an organziation that would treat their data in such a negligent manner.

2 1 10

fishtech

CYDERES

SERIOUSLY THOUGH

Instrument all the things ahead of time

- START WITH NTA: very high ROI
- MAKE SURE YOU HAVE LOGS
  (and are keeping the logs)
- MFA A MUST; EDR IS KEY
- DNS + PROXY
- DECEPTION IS AWESOME

fishtech

CYDERES

THINGS YOU MIGHT MISS

Learn from the mistakes of others…

- Look at email forwarding rules
- Look at SSO connected systems
- Follow the money
- Watch for secondary infections / outbreaks
- Almost certainly have pwned all the emails

fishtech

CYDERES

THINGS TO DO RIGHT NOW

Stand on the shoulders of giants…

HAVE A WRITTEN RESPONSE PLAN

- SANS Incident Handler's Handbook
- NIST 800-61 - Incident Handling Guide
- CMU CSIRT (training and plan)

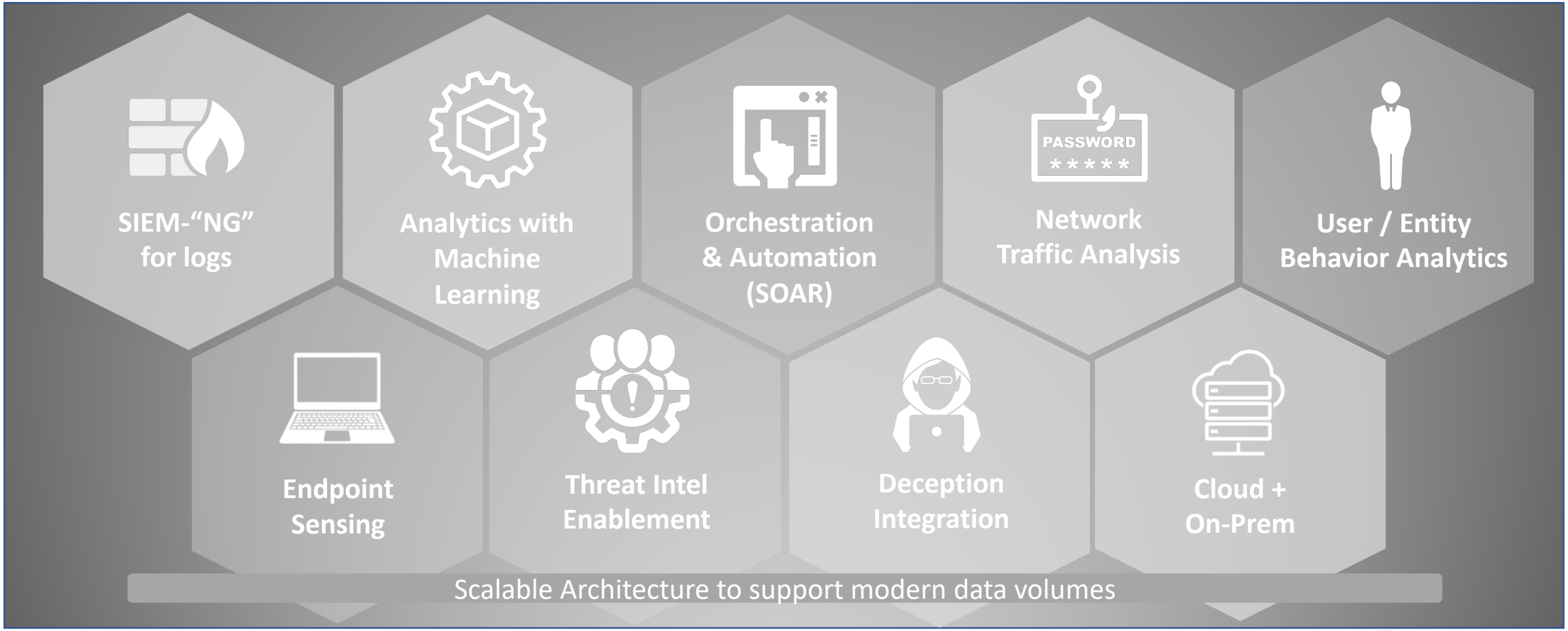
… and a checklist

https://www.sans.org/score/

fishtech

CYDERES

Cyber Defense Platform



fishtech

CYDERES

Additional Resources

Free/Open Source/ Surprisingly Low Cost Solutions

fishtech

CYDERES

A FEW DISCLAIMERS

When standing on the shoulders of giants…

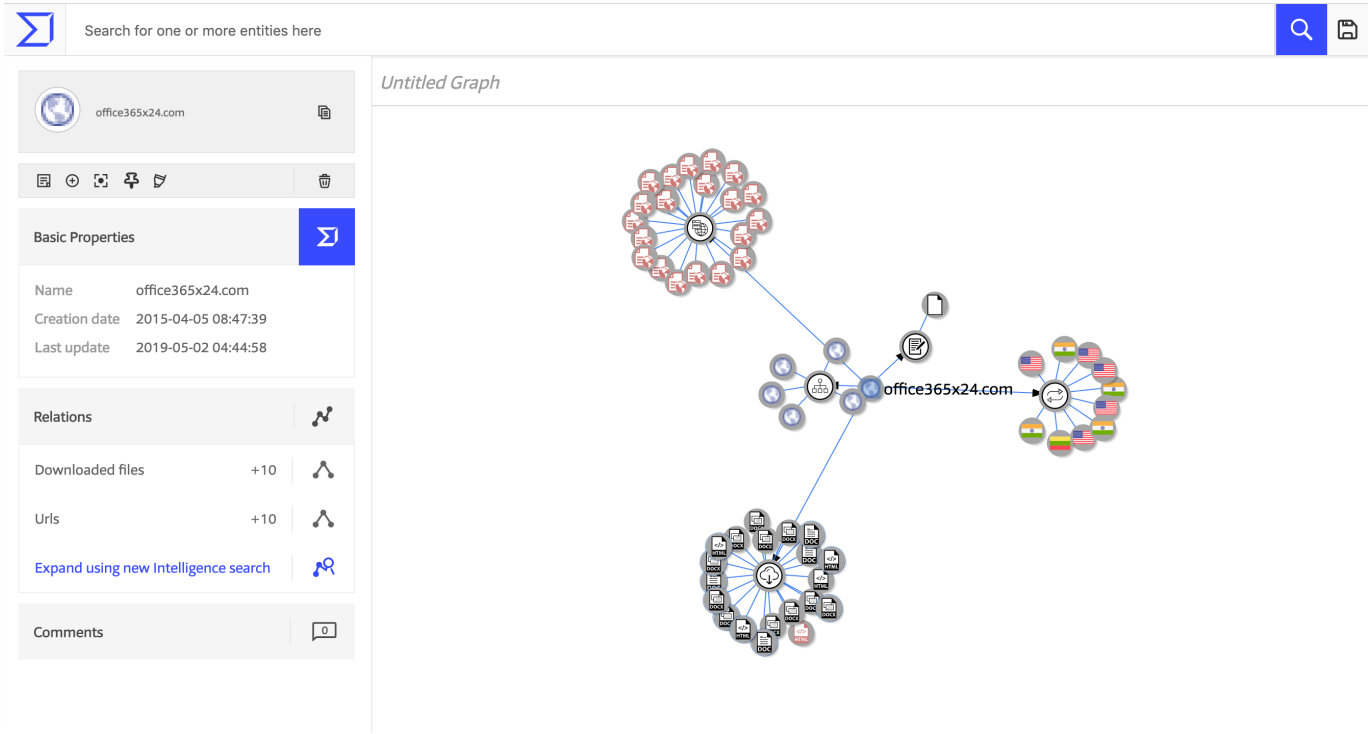
- Free / low cost not always bad
- Free / low cost not always actually low cost
- Consider the ROI vs. total cost
- This is what works for us (CYDERES)
- Your mileage may vary

fishtech

CYDERES

VIRUS TOTAL

- https://www.virustotal.com
- All the malwares, all the time
- Starts around $10k/year
- You'll get a link for a run of Enterprise Edition



CYDERES

SWIFT FILTER

- https://github.com/SwiftOnSecurity/SwiftFilter
- Requires tuning but SOOOOO worth it
- Also see:
  http://DecentSecurity.com
  http://GotPhish.com

CYDERES

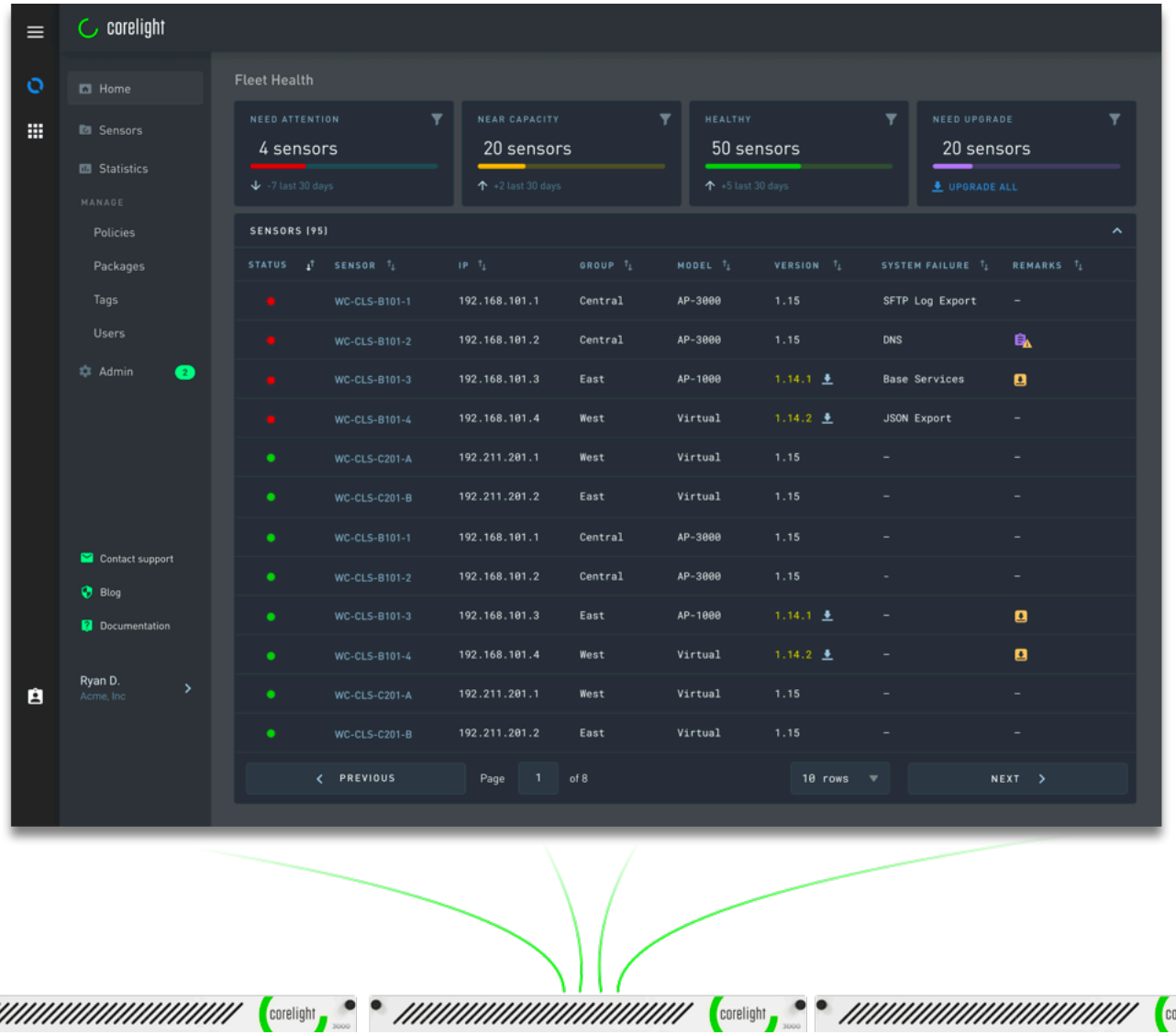
U2F tokens

- https://www.yubico.com
- Starts at $45 per key
- Will virtually eliminate phishing overnight
- Different scale if you're huge, but still strong ROI

CYDERES

CORELIGHT (NTA)

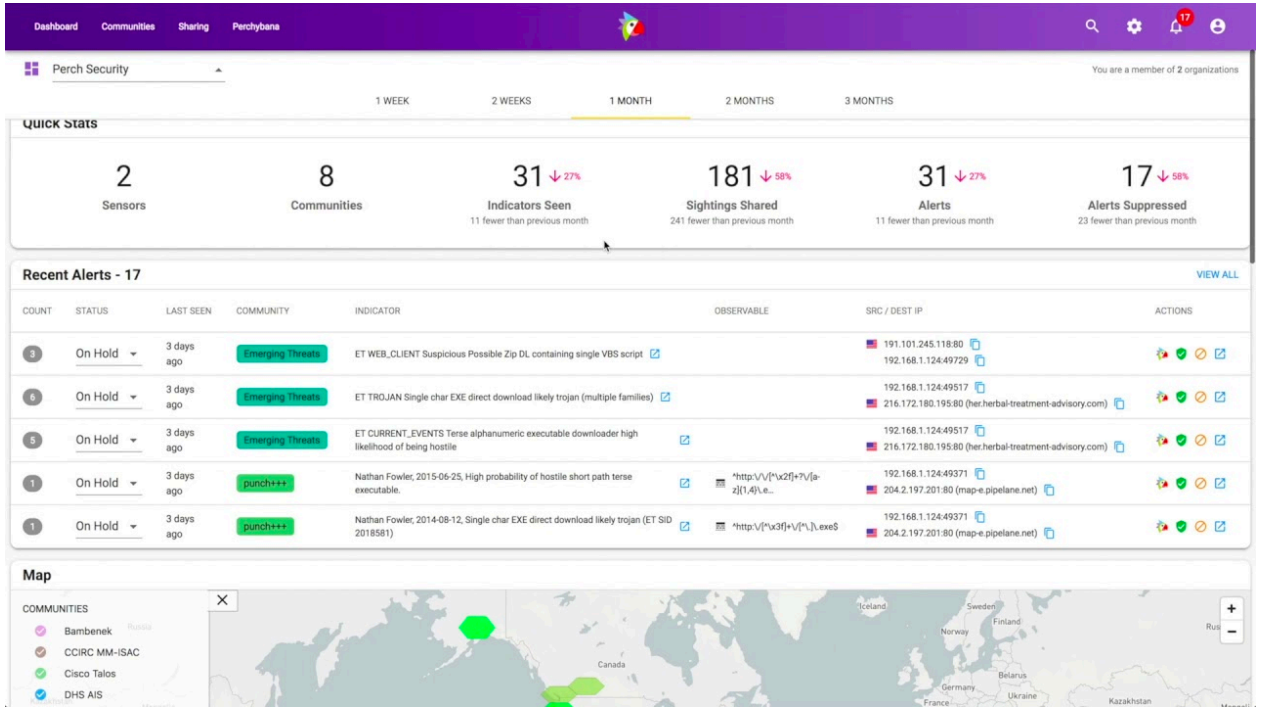
- https://www.corelight.com/
- Network traffic analysis
- Zeek on steroids
- Virtual / physical / cloud
- $10k/year for 2gbs



CYDERES

PERCH SECURITY (NTA)

- https://perchsecurity.com/
- Co-managed Threat Detection
- ISAC/ISAO friendly
- Licensed by IP address
- Add-ons for SOC, SIEM
- Starts at $6,400 / year



CYDERES

Bambanek Feed

- https://osint.bambenekconsulting.com/feeds/
- Start with the “high confidence”
- Starts at $2,500 /yr

ALL FAMILIES	C2 IP Feed	C2 Domain Feed
HIGH-CONFIDENCE FAMILIES ONLY	High-Confidence C2 IP Feed	High-Confidence C2 Domain Feed

CYDERES

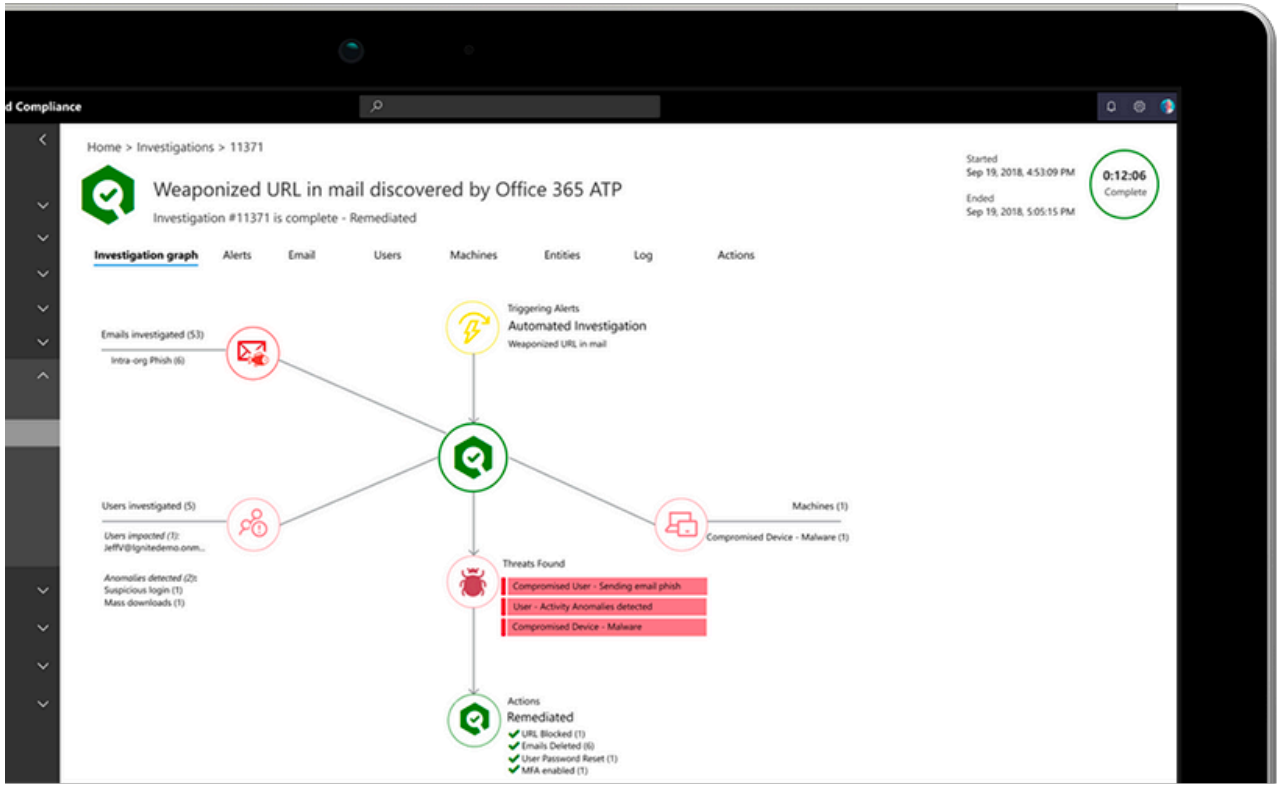
JOIN AN ISAC / ISAO

- https://www.nationalisacs.org
- https://www.isao.org/
- Information Sharing and threat feeds
- Starts at $2k / year depending on revenue

CYDERES

MICROSOFT EOP / ATP

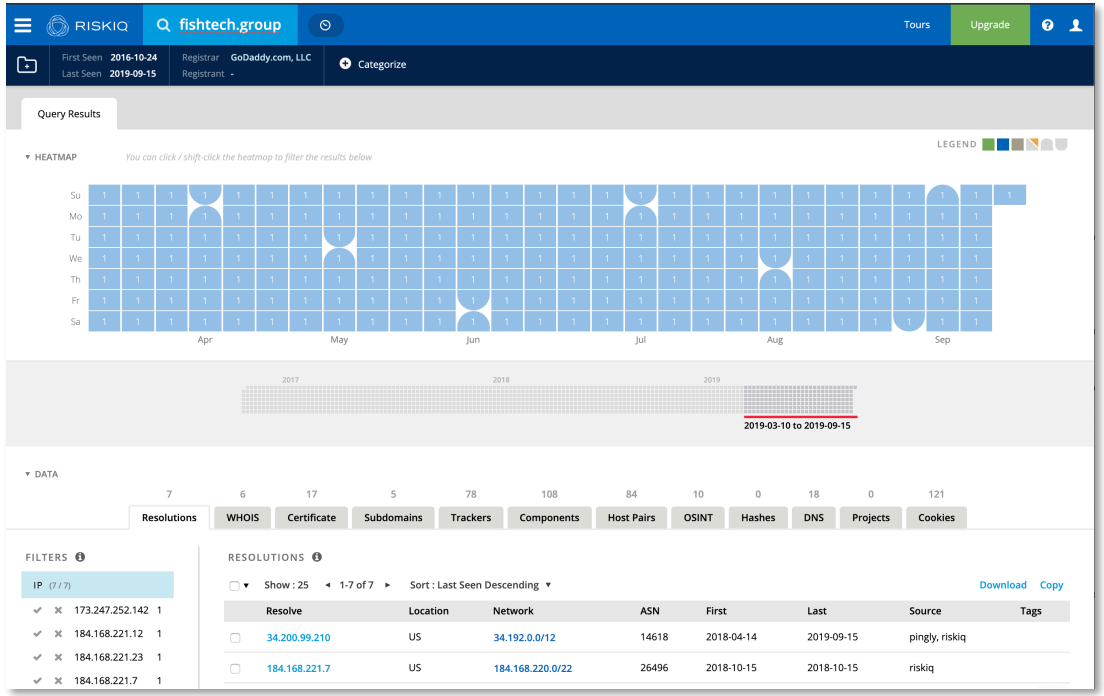
- https://products.office.com/en-US/exchange/exchange-email-security-spam-protection
- EOP = $1 a month
- ATP = $2 a month
- Can deploy just for HVT (via groups)



CYDERES

RiskIQ Community (PassiveTotal)

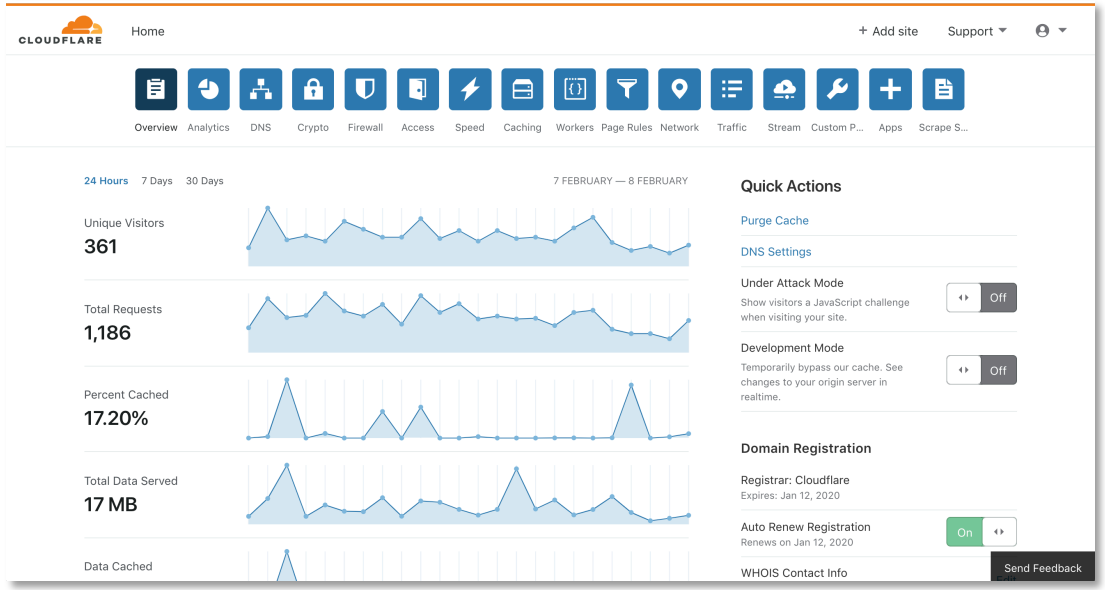
- https://community.riskiq.com
- Discover your Digital Footprint
- Uncover Rogue IT
- Bonus code:
  THW-CYDERES-MA
  for additional queries



CYDERES

Cloudflare

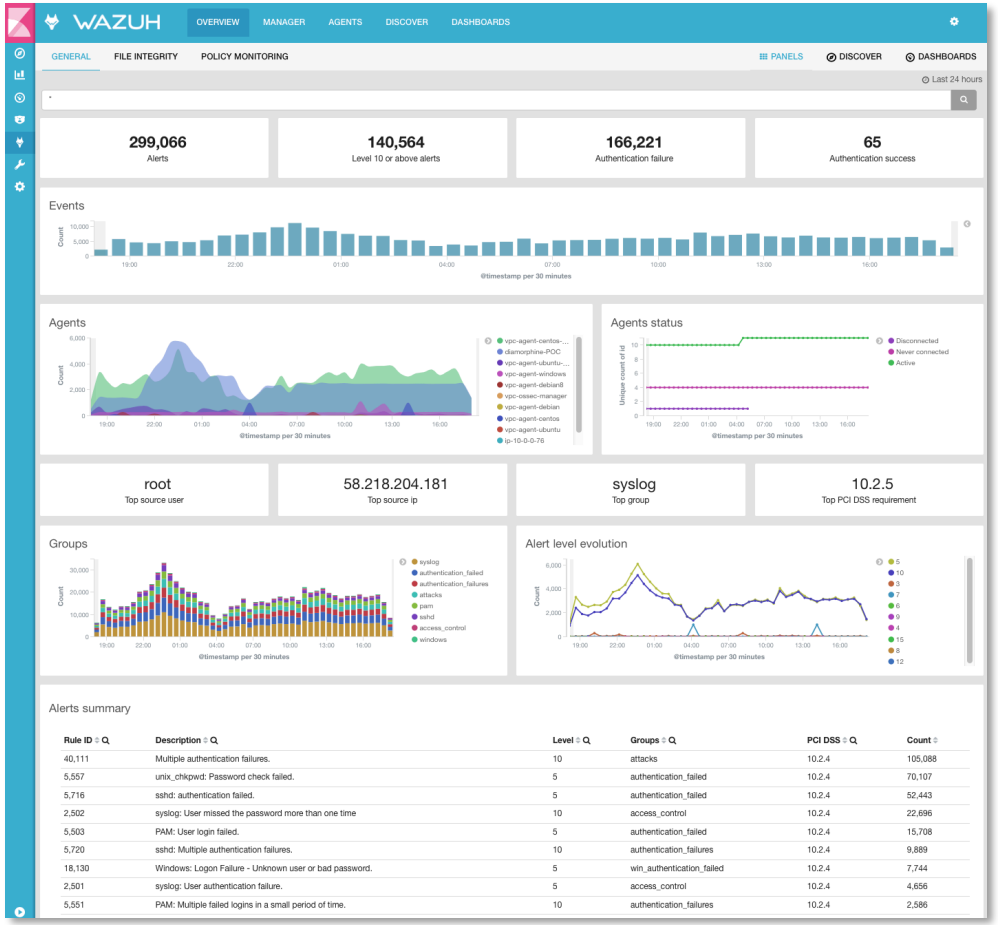
- https://www.cloudflare.com/plans/business/
- DDOS Protection
- Web Application Firewall
- Content Delivery Network
- Significant value for free
- Pro $20/mo
- Business $200/mo for support



CYDERES

Wazuh / OSSec

- https://wazuh.com/
- https://www.ossec.net/
- Open Source hidS SECurity
- Host-based Intrusion Detection System
- File Integrity Monitoring
- Also like for some use cases: https://osquery.io/



CYDERES

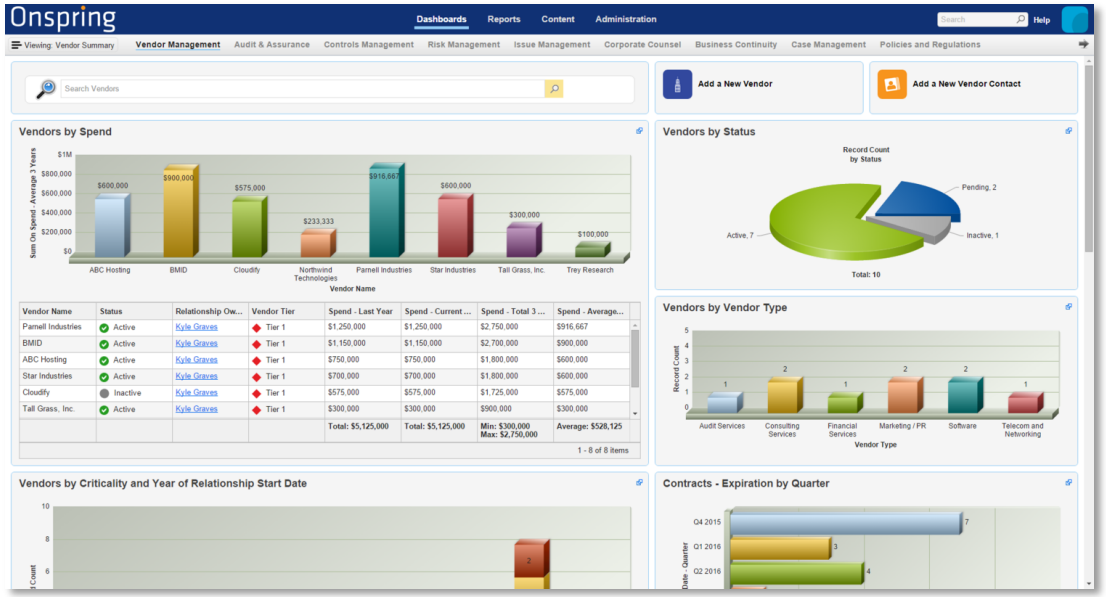
Thinkst Canary

- https://canary.tools/
- Deception honeypots
- Many flavors:
  - Physical
  - Virtual Machine
  - Cloud-based
- Free tokens at https://canarytokens.org
- Starts at $5k / year

CYDERES

Onspring

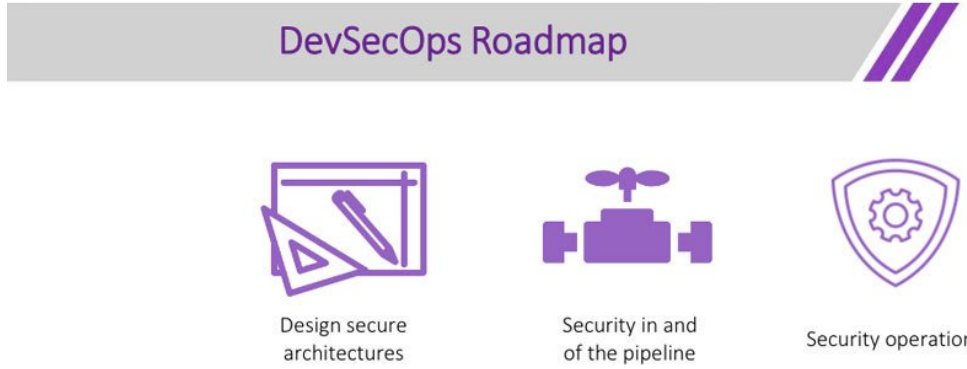
- https://onspring.com/
- Inventory your assets in a CMDB
- GRC > Excel
- Classify them based on risk profile
- Starts at $175/user/month



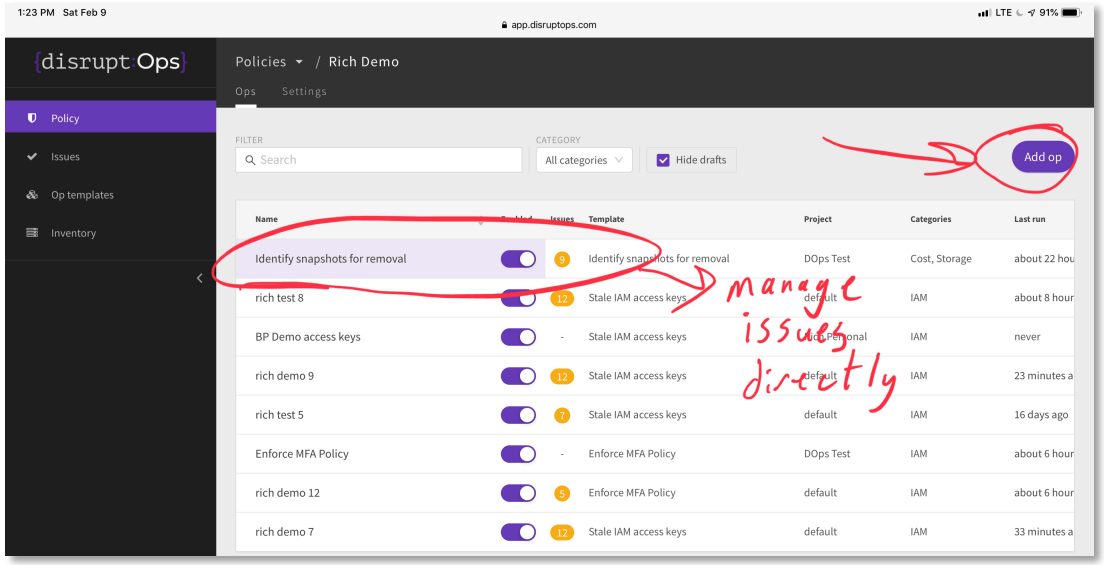
CYDERES

DisruptOps

- https://disruptops.com/
- Guardrails for your AWS environment
- Discover and remediate:
  - Unused IAM users/roles
  - Stale access keys
  - Network access from suspicious locations
- Starts at $1 per resource



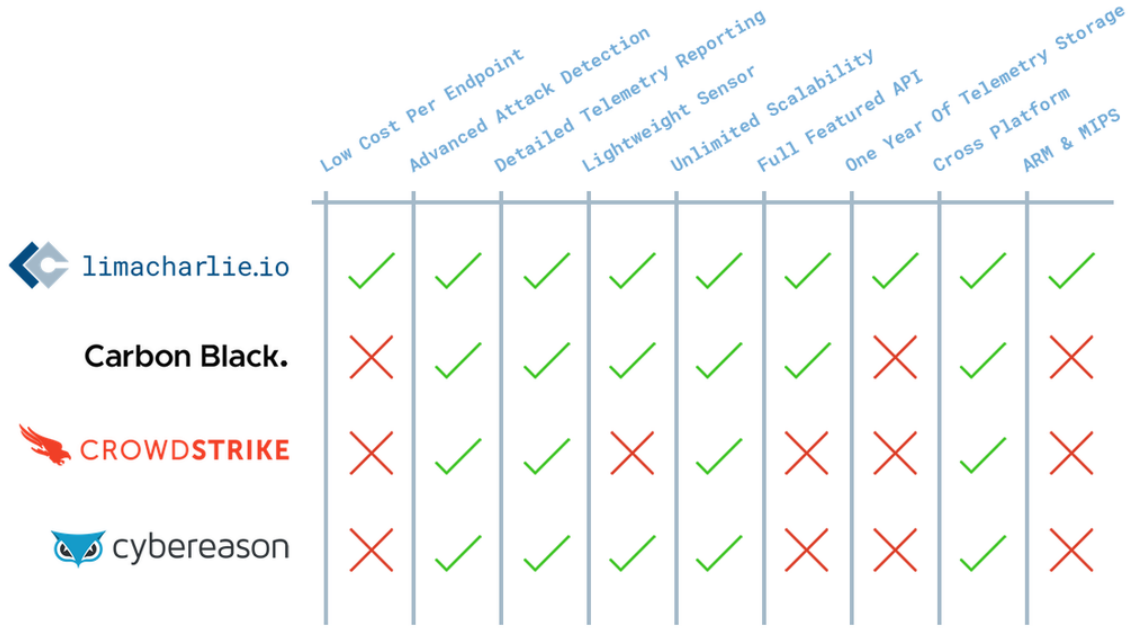
{disrupt:Ops}

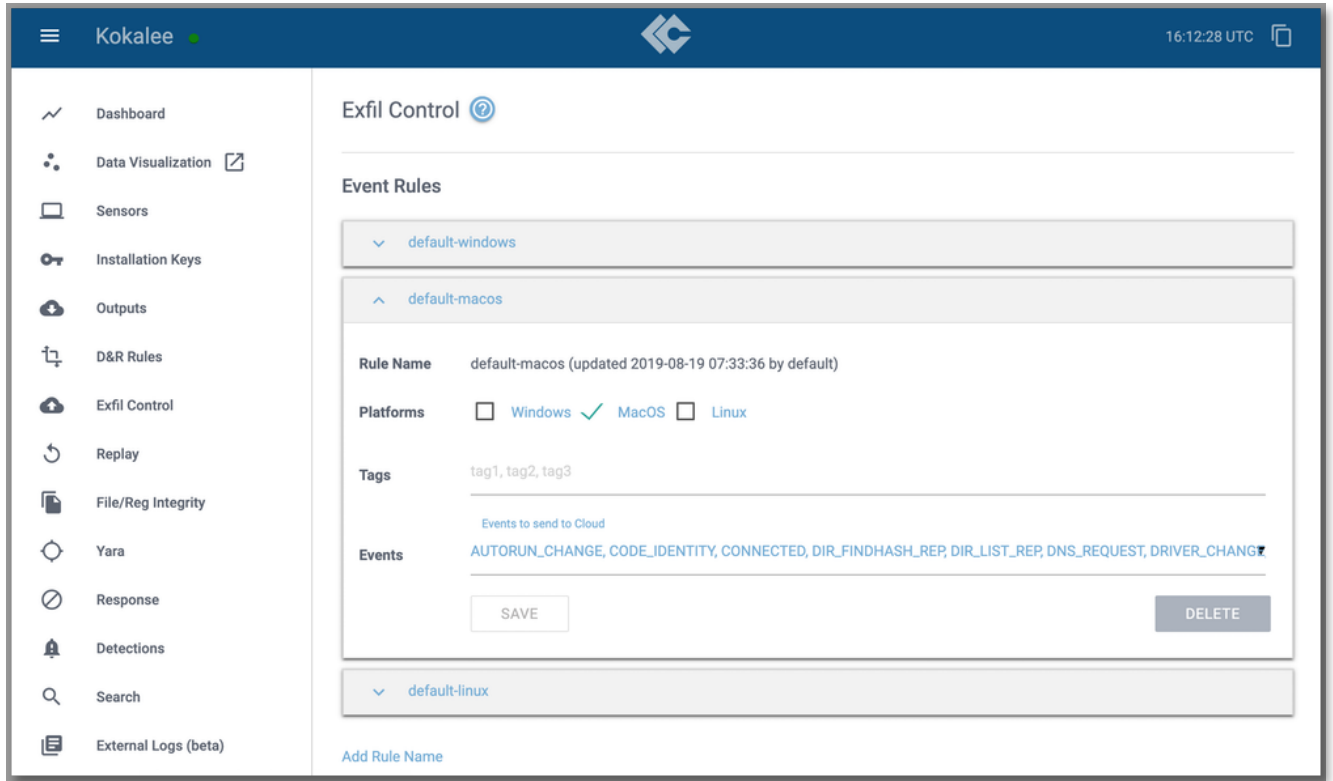


CYDERES

LimaCharlie

- https://www.limacharlie.io/
- Endpoint Detection and Response
- MacOS, all Linux & Windows
- 50¢/endpoint/month





CYDERES

ASSORTED BLUE TEAM RESOURCES

- https://urlscan.io
- MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing https://www.misp-project.org/
- https://github.com/securitywithoutborders/hardentools
- https://github.com/nsacyber/Windows-Secure-Host-Baseline
- https://github.com/davehull/Kansa - powershell IR

CYDERES

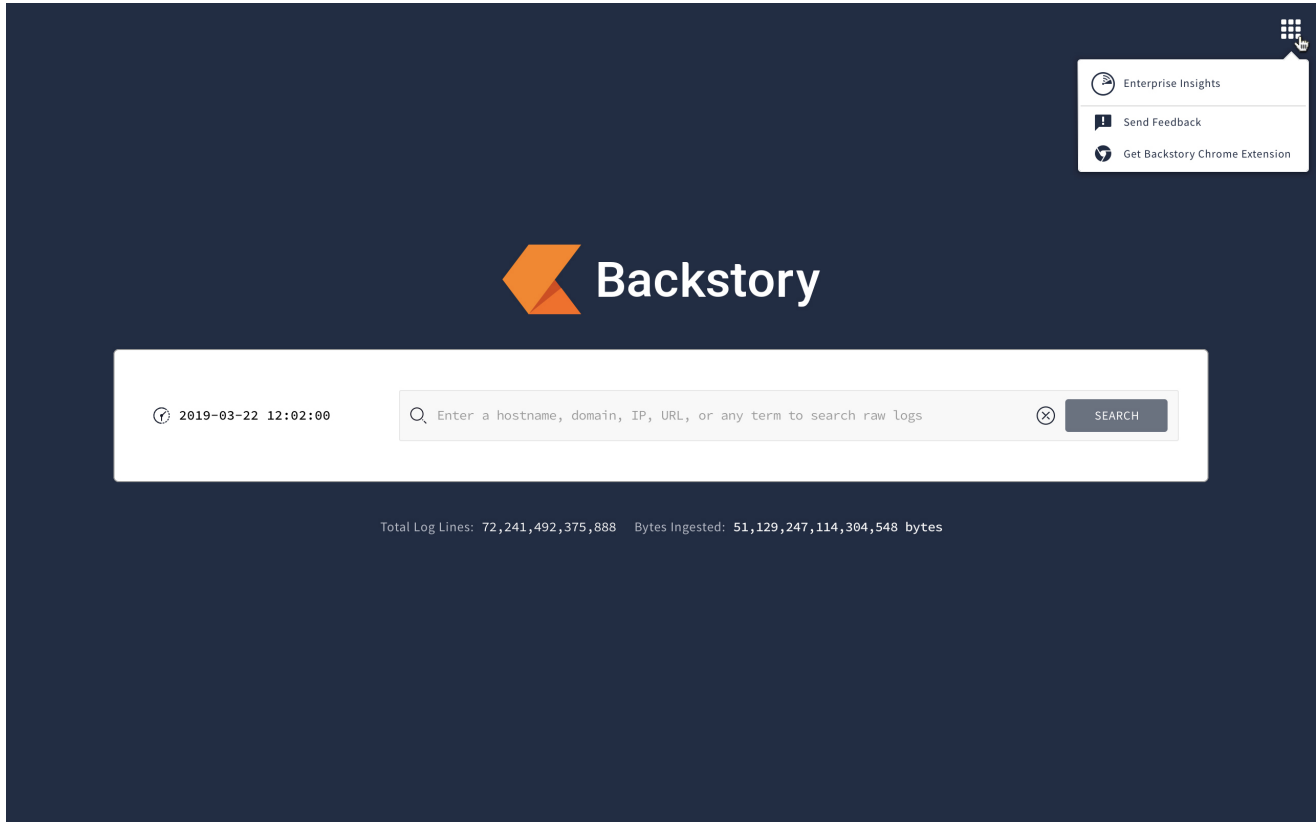
ASSORTED DEV/OPS RESOURCES

- Prowler - AWS hardening - https://github.com/toniblyx/prowler
- https://playbook.cloud/ - secure Ansible as a service - $20/mo

CYDERES

Google Backstory

- https://chronicle.security
- Security telemetry platform
- Unlimited ingest
- 1-year hot retention
- Sub-200ms search times
- Starts at $45/employee

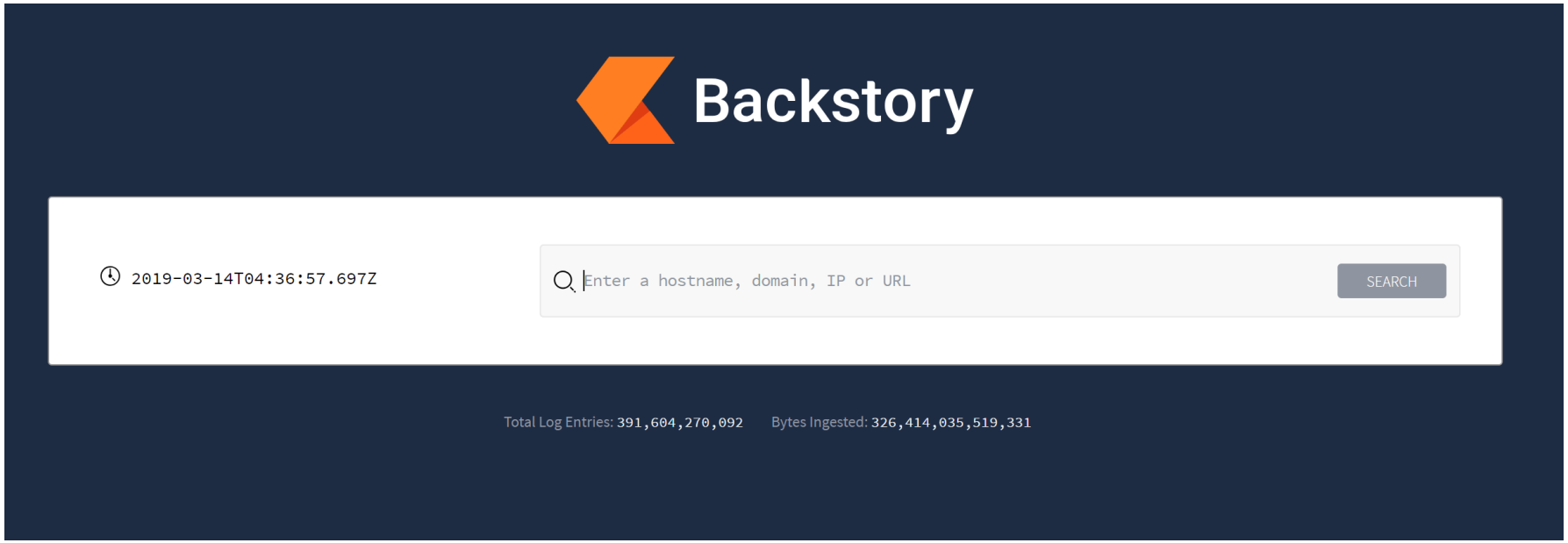


CYDERES

BACKSTORY KILLS SIEM

Powerful security analytics: instant, easy, and cost-effective.

Backstory = 10x your security data



fishtech

CYDERES

YOUR SIEM STINKS.

And here's why

- SIEM was built for a world of smaller data volumes (Arcsight: 2000; Splunk, LogRythm: 2003)
- SIEMs are expensive and complex
- SIEMs require too much effort to produce useful insight

fishtech

CYDERES

BACKSTORY KILLS SIEM… DEAD

And here's why

- Store a minimum of a full YEAR of security logs AND high volume telemetry
- Search all that data with sub-second queries
- Backstory automatically correlates threat intelligence and signals based on techniques and tools developed within Google to protect itself
- It does that across its entire data set simultaneously

fishtech

CYDERES

10x YOUR SIEM… SERIOUSLY

This is a REALLY big deal

- Backstory is a specialized security analytics system, built on the core infrastructure that powers Google.
- Backstory inherits massive storage and parallel-compute capabilities: the world's best storage and search architecture.
- Backstory can trivially spawn 5,000 servers to perform a computation in parallel, with zero customer administration.
- "Effectively unlimited compute and unlimited storage"

fishtech

CYDERES

BUT HERE'S WHERE IT GETS INSANE

The "what" is awesome. The "how much" is the killer.

- Unlike ALL existing SIEM products *and* cloud provider platforms, Backstory is licensed at a fixed price based on number of employees
- No charges for data ingested or stored.
- A single, low, fixed annual price.

fishtech

CYDERES

Let's Hunt Some Threats

fishtech

CYDERES

One More Thing…

fishtech

IF YOU HAVE ?'s or NEED HELP

Hey, I just met you and this is crazy
But here's my number, so call me maybe

CYDERES

QUESTIONS?

- eric.foster@fishtech.group
- 816.695.1432
- linkedin.com/in/ericfoster
- @performify and @cyderes