Secureworks®

New Threats and the New Methods to Stop Them!

Robert Shaw

Sr. CyberSecurity Specialist

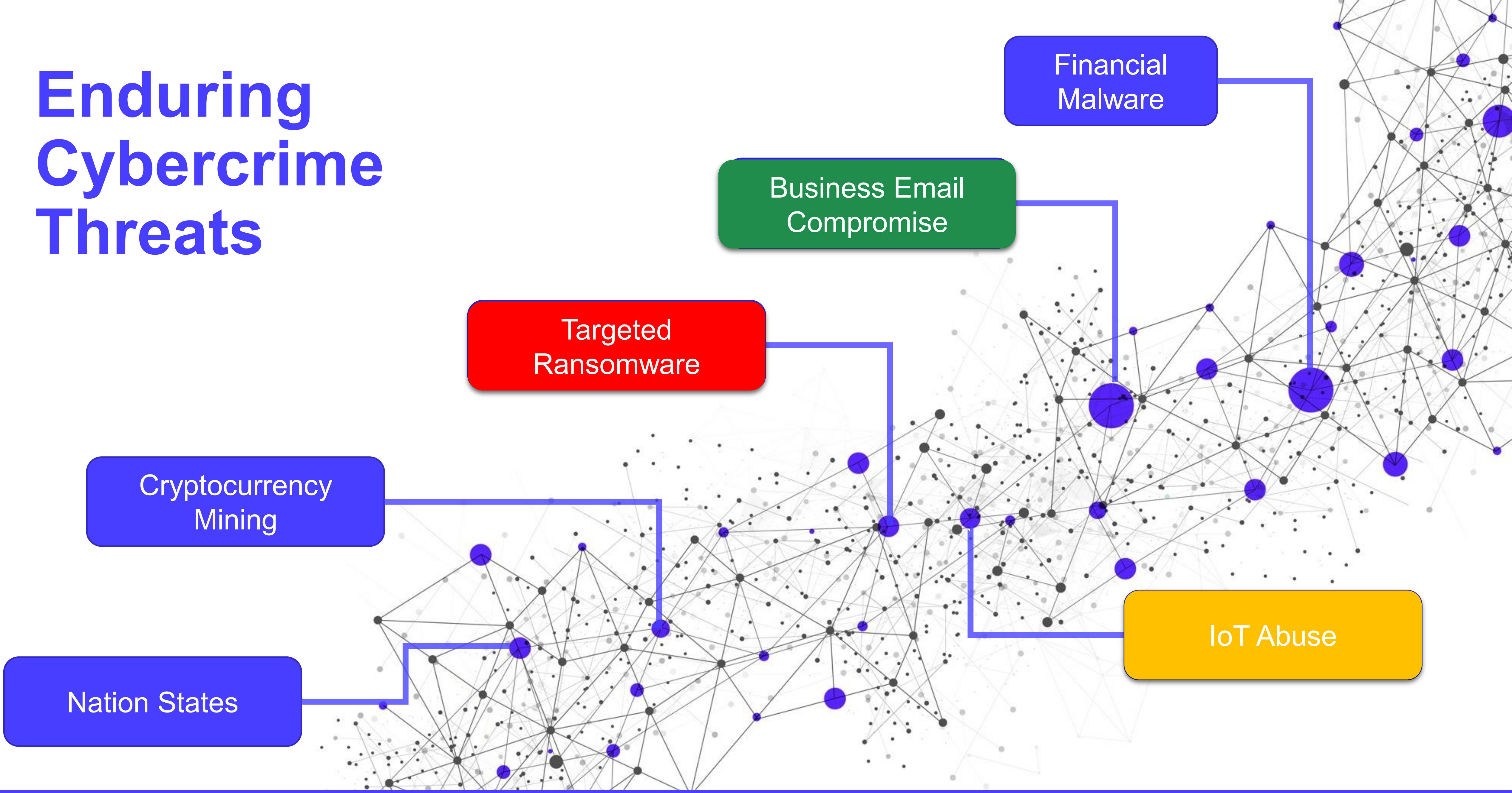
October 11, 2019

Secureworks®

Today’s Discussion

- The Latest on Ransomware
- What can you do to Protect yourselves?

Enduring Cybercrime Threats



Financial Malware

Business Email Compromise

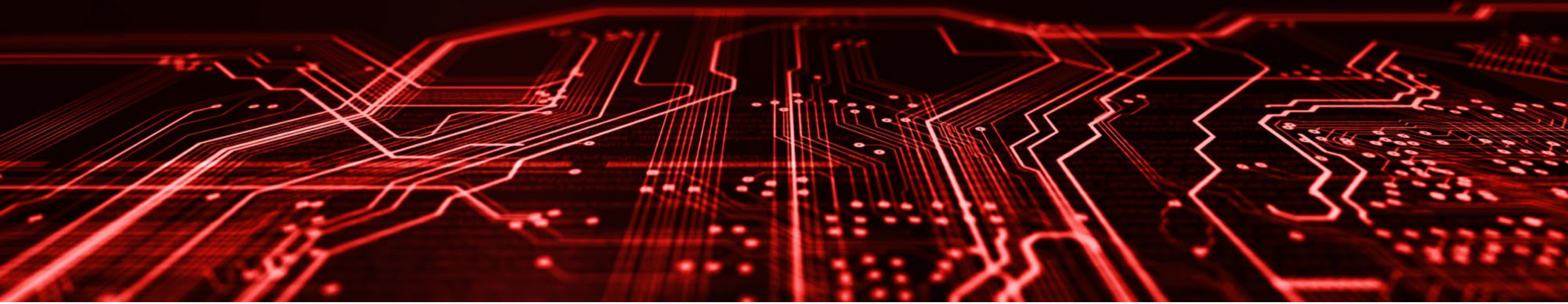
Targeted Ransomware

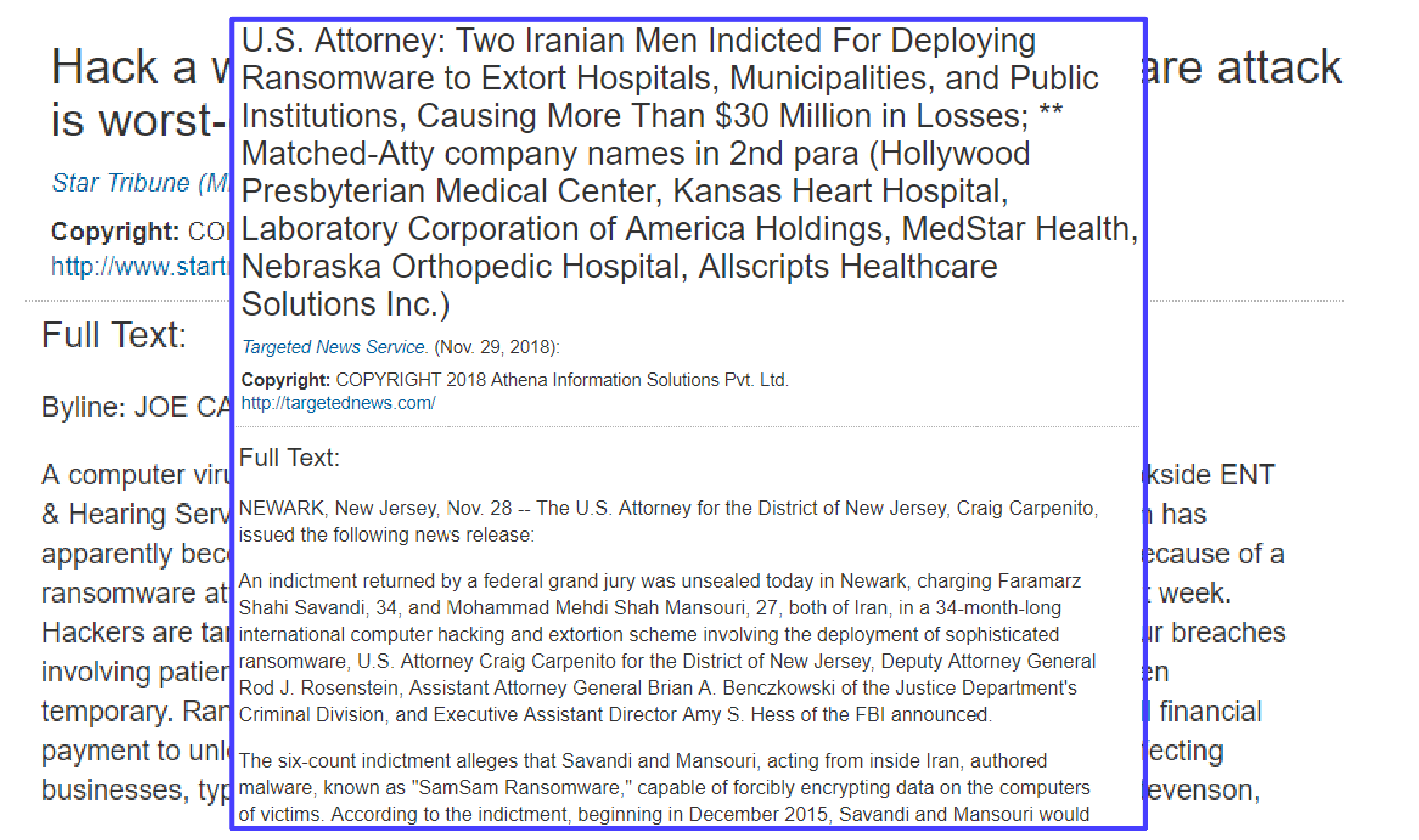
Cryptocurrency Mining

Nation States

IoT Abuse

What’s New with Ransomware?





Hack a w ... are attack is worst-

Star Tribune (M

Copyright: CO

http://www.start

Full Text:

Byline: JOE CA

A computer viru ... kside ENT & Hearing Serv ... n has apparently bec ... ecause of a ransomware at ... week. Hackers are ta ... r breaches involving patie ... en temporary. Ran ... financial payment to unl ... fecting businesses, typ ... evenson,

U.S. Attorney: Two Iranian Men Indicted For Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing More Than $30 Million in Losses; ** Matched-Atty company names in 2nd para (Hollywood Presbyterian Medical Center, Kansas Heart Hospital, Laboratory Corporation of America Holdings, MedStar Health, Nebraska Orthopedic Hospital, Allscripts Healthcare Solutions Inc.)

Targeted News Service. (Nov. 29, 2018):

Copyright: COPYRIGHT 2018 Athena Information Solutions Pvt. Ltd.
http://targetednews.com/

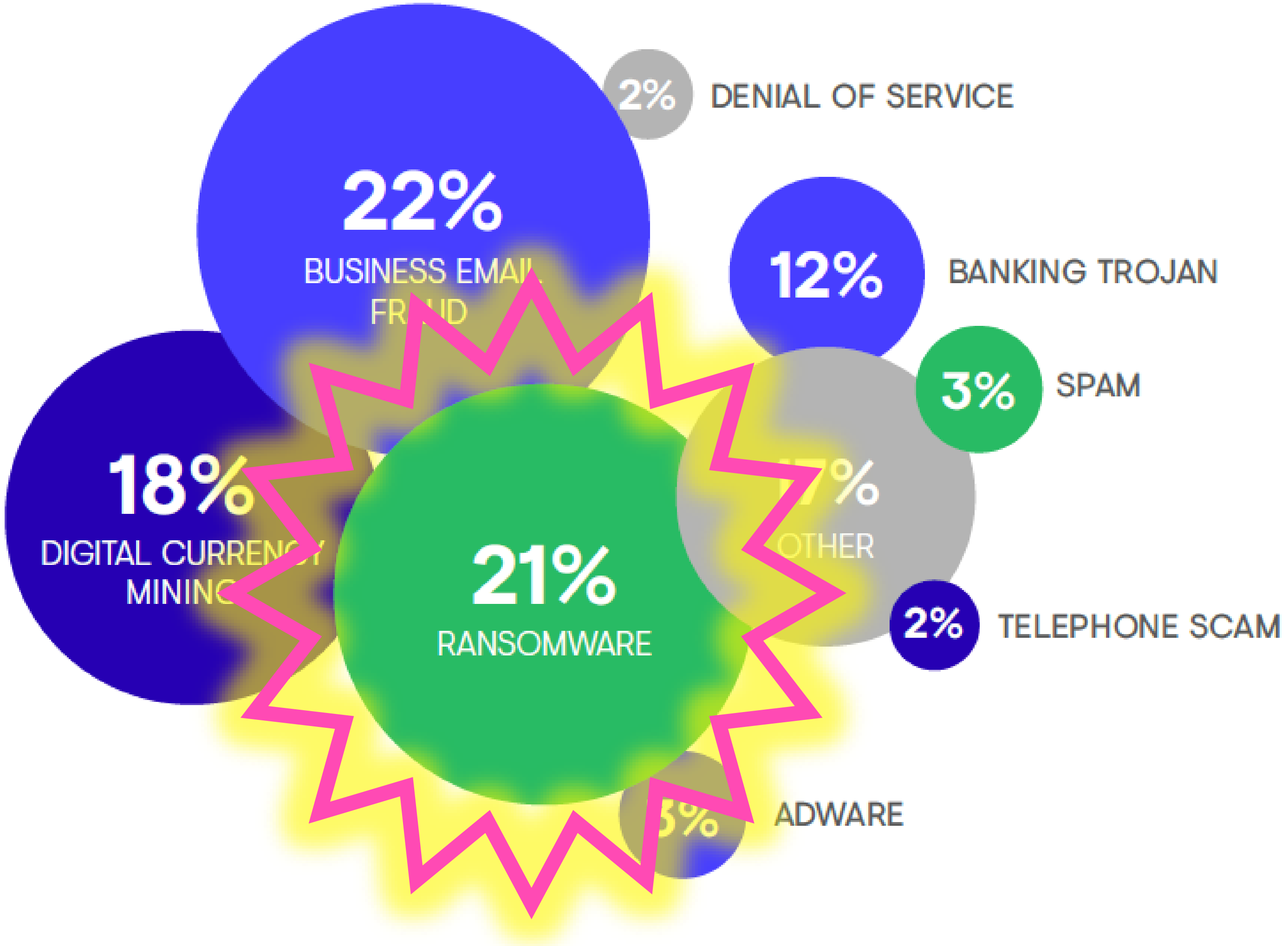
Full Text:

NEWARK, New Jersey, Nov. 28 -- The U.S. Attorney for the District of New Jersey, Craig Carpenito, issued the following news release:

An indictment returned by a federal grand jury was unsealed today in Newark, charging Faramarz Shahi Savandi, 34, and Mohammad Mehdi Shah Mansouri, 27, both of Iran, in a 34-month-long international computer hacking and extortion scheme involving the deployment of sophisticated ransomware, U.S. Attorney Craig Carpenito for the District of New Jersey, Deputy Attorney General Rod J. Rosenstein, Assistant Attorney General Brian A. Benczkowski of the Justice Department's Criminal Division, and Executive Assistant Director Amy S. Hess of the FBI announced.

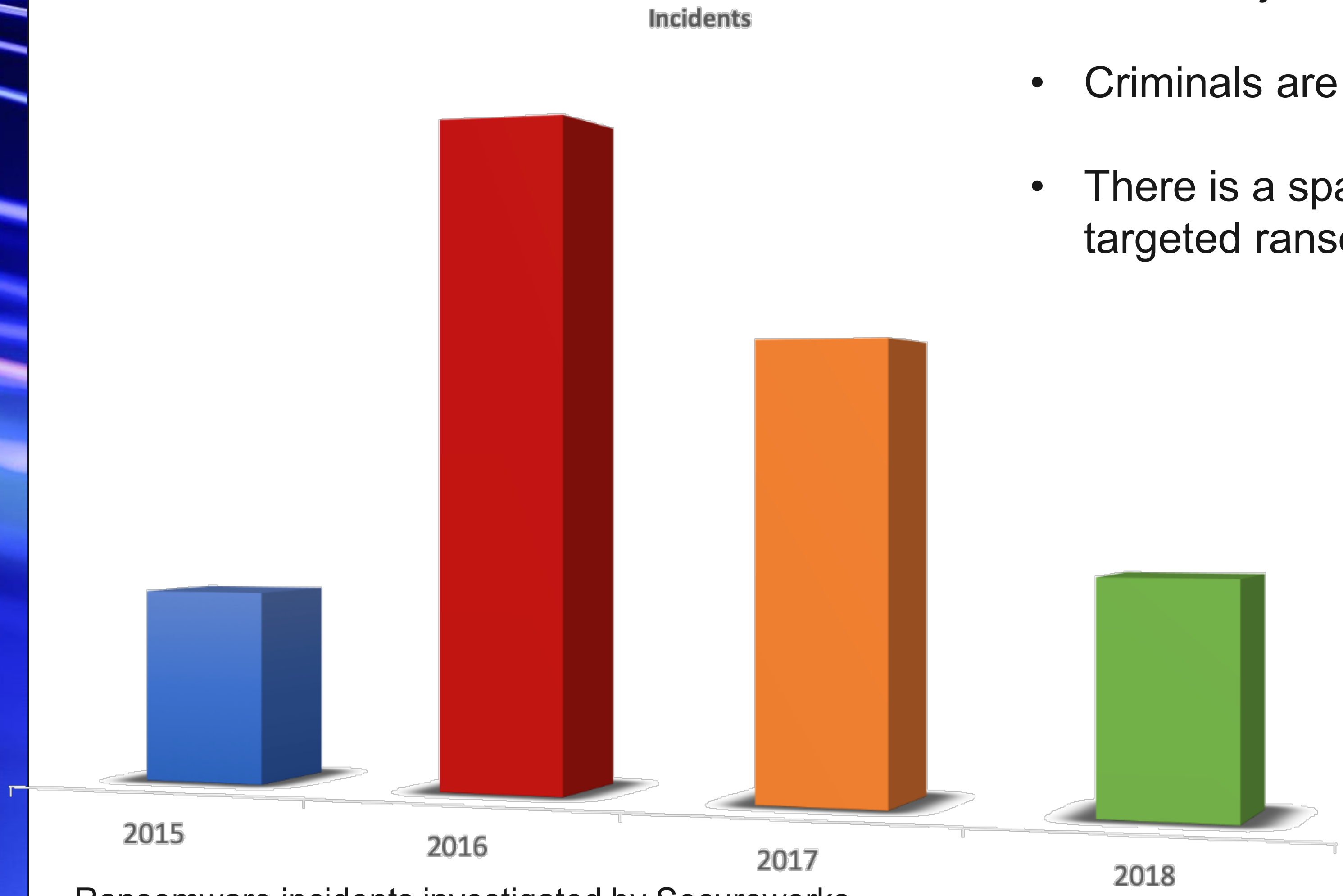
The six-count indictment alleges that Savandi and Mansouri, acting from inside Iran, authored malware, known as "SamSam Ransomware," capable of forcibly encrypting data on the computers of victims. According to the indictment, beginning in December 2015, Savandi and Mansouri would

2018 SWX Emergency IR Engagements



Is ransomware use declining?

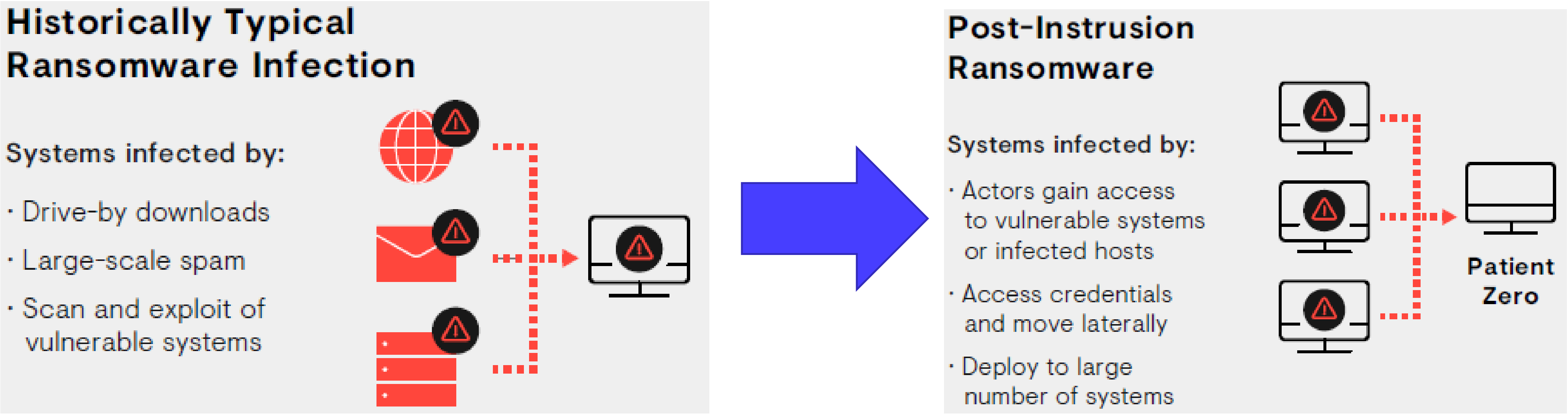
Statistically, yes, but…



Ransomware incidents investigated by Secureworks

- Still a major threat to unprepared organisations
- Criminals are business oriented
- There is a spate of recent attacks using targeted ransomware.

Ransomware Landscape Shift -1



Historically Typical Ransomware Infection

Systems infected by:

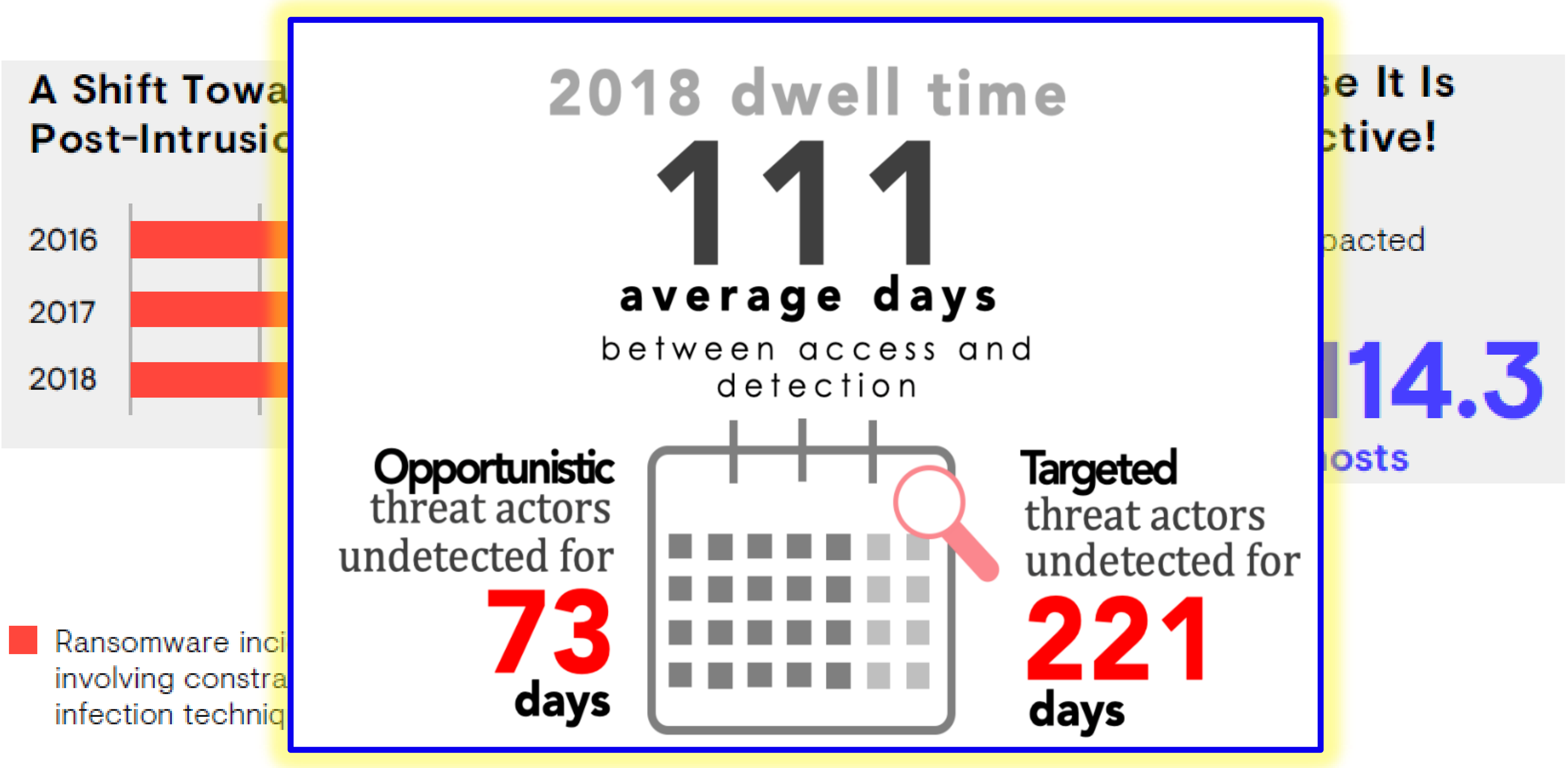
- Drive-by downloads
- Large-scale spam
- Scan and exploit of vulnerable systems

Post-Instrusion Ransomware

Systems infected by:

- Actors gain access to vulnerable systems or infected hosts
- Access credentials and move laterally
- Deploy to large number of systems

Ransomware Landscape Shift -2



2018 dwell time

111

average days

between access and detection

Opportunistic threat actors undetected for 73 days

Targeted threat actors undetected for 221 days

Local Gov’t/Healthcare Payouts

2018-2019

Organisation	Source	Year	Amount paid
Hancock Health	The Canadian Press	2018	$55,000
West Haven, Conn.	AP	2018	$2000
Delaware Guidance Services for Children	AP	2019	“thousands”
Lake City, Florida	New Scientist	2019	$530,000
Riviera Beach, Florida	Washington Post	2019	$600,000

What if you pay the ransom?

That’s not the end of your problems

- We worked with an organization that paid $7.2 Million in BitCoin.
  - They were emailed a decrypt tool
- They had thousands of hosts that needed decrypting
  - The tool was not multi-threaded, had bugs, lower quality than the ransomware
  - They had no way to distribute the tool, to execute it centrally and report back
  - What about the hosts that didn’t boot up anymore?
- Is the threat actor still in the environment?
  - Did they do anything else while they were in, did they steal anything?
  - Is the network clean and trustworthy?

The Good News

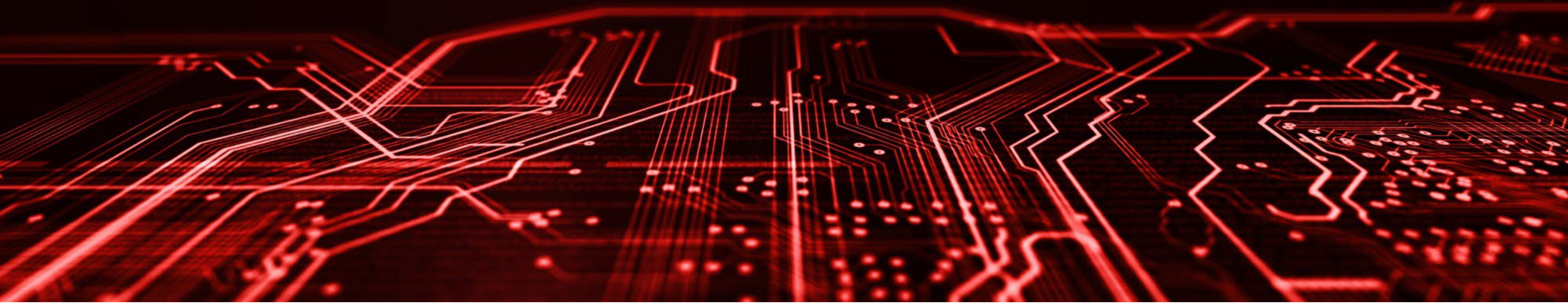
Kind of

🤷‍♂️

- In several targeted ransomware incidents where files were encrypted and the victim organization crippled
  - Threat Actors were in the network for weeks before dropping ransomware
  - Threat Actors used standard tools and techniques in that time

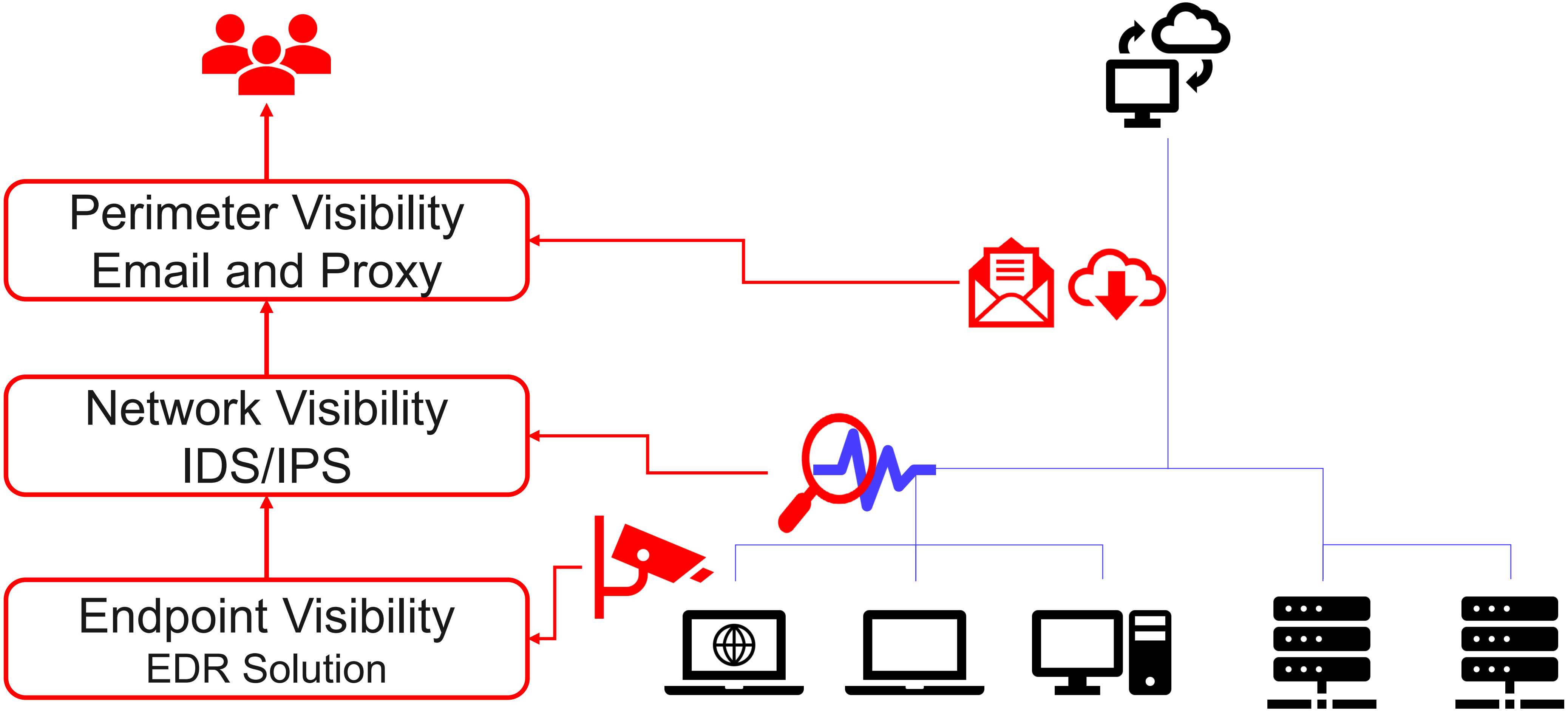
- They could have been stopped, if
  - You have visibility into the environment
  - You apply Threat Intelligence to that visibility
  - You respond immediately and effectively to evict the Threat Actor
  - You prevent them from re-entering the environment

Cyber Security Is a Journey, Not a Destination



Visibility into the environment

Layers of visibility



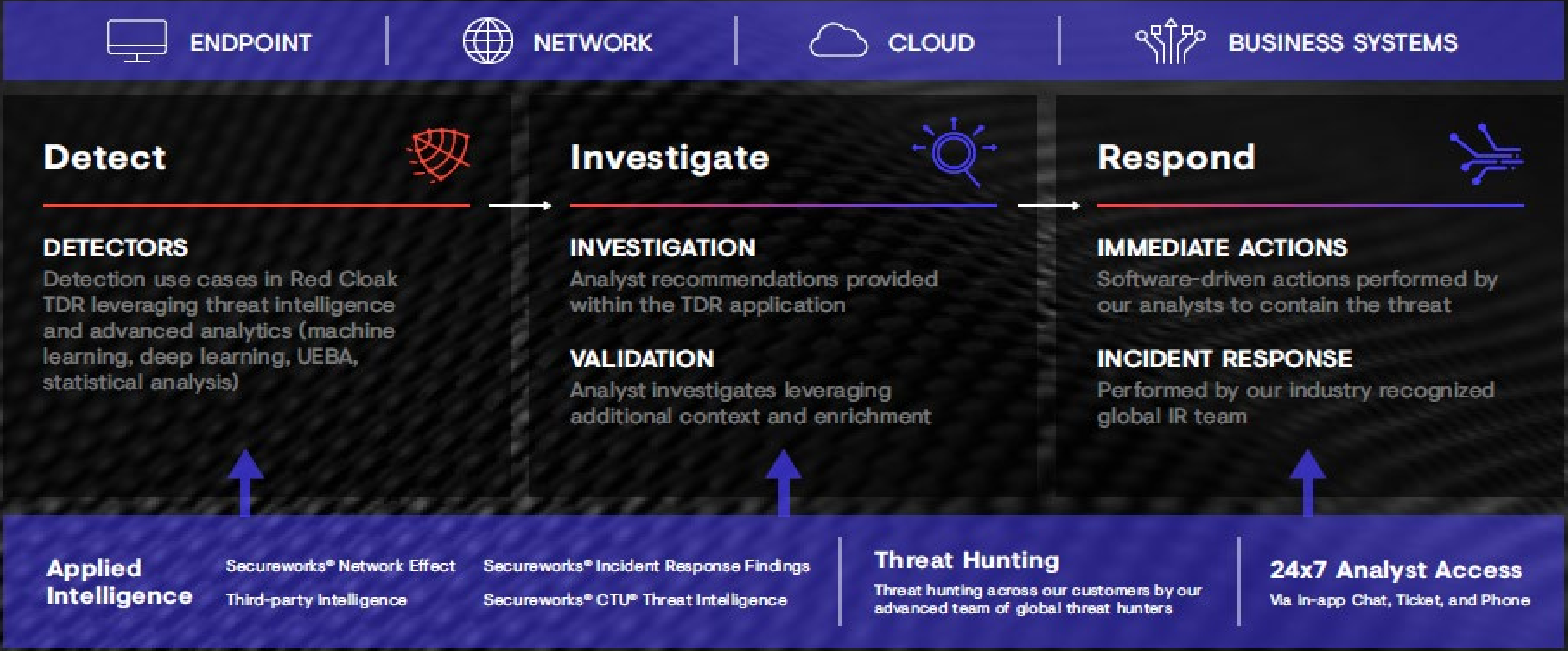
Perimeter Visibility
Email and Proxy

Network Visibility
IDS/IPS

Endpoint Visibility
EDR Solution

Our Approach to MDR

Secureworks combines security analytics software with our expertise and threat intelligence to help your security team detect, investigate and respond to threats faster than ever before.



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

Third-party Intelligence

Secureworks® Incident Response Findings

Secureworks® CTU® Threat Intelligence

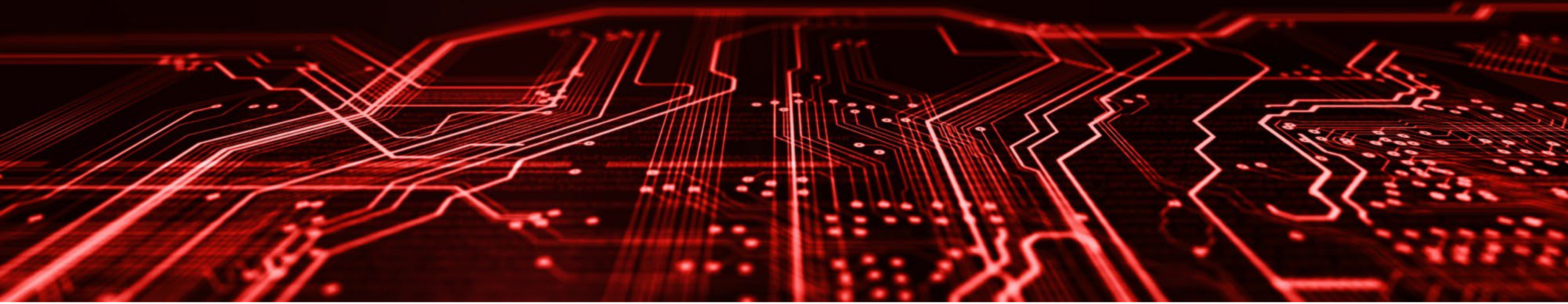
Threat Hunting

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

24x7 Analyst Access

Via in-app Chat, Ticket, and Phone

Advanced Anomaly Detection



Building Threat Detectors with Advanced Analytics and Threat Intelligence

Tactic Graphs

Evaluate series of events from multiple data sources for series of tactics associated with known threat actor patterns (Business Email Compromise, Ransomware, etc.)

Domain Generation Algorithm

Performs **supervised deep-learning** on automatically generated labels to distinguish known DGAs from benign DNS requests

Command & Control Detector

Identify potentially compromised endpoints by looking for rare DNS requests for domains that have recently been registered

Rare Program to IP

Builds a model of all outbound connections from processes to IPs. Identifies potential threats by raising the most rare combos to the top.

Top Recommendations From 2019 IR Insights Report

Implement Multifactor Authentication (MFA)

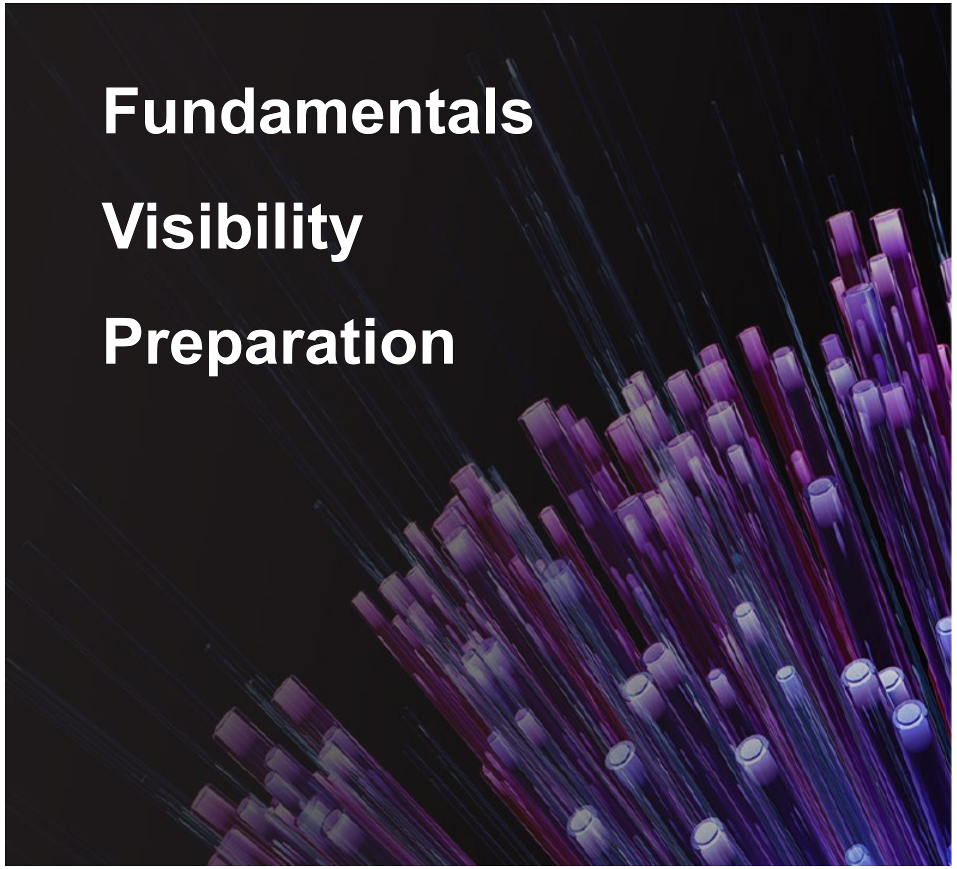
Increase Visibility and Enhance (Specific) Logging

Implement Endpoint Detection Capabilities

Improve and Test Incident Response Preparedness

Educated Users on Security Vigilance and Policies

Choose a Framework For Governance



Fundamentals

Visibility

Preparation

REPORTS

Secureworks State of Cybercrime Report 2018

The Deep, Dark Truth Behind the Underground Hacker Economy

- Download the 2018 State of Cybercrime report

  www.secureworks.com/resources/rp-2018-state-of-cybercrime

- Visit secureworks.com

- Call me if you have any questions:

Robert Shaw
CyberSecurity Specialist
West Region Public Sector
CyberSecurity SLED | West Coast
949-246-7223 cell
rshaw@secureworks.com

Thank you!

Questions that Need Answers

- What internal discussions do I need to have to improve my understanding of our true corporate risk and accurately convey this to the C-Suite?
- Does my risk dictate I need more advanced tools?
- Do I have the right logs / data / plan / process to detect and respond to an attack today?
- What people / process / technology changes will I make to reduce my time to detect and respond in 2020?

Organizations Know Security is a Priority

But going it alone is not easy

Lack of Visibility

More attack surfaces. Hackers evade controls.

Too Much Complexity

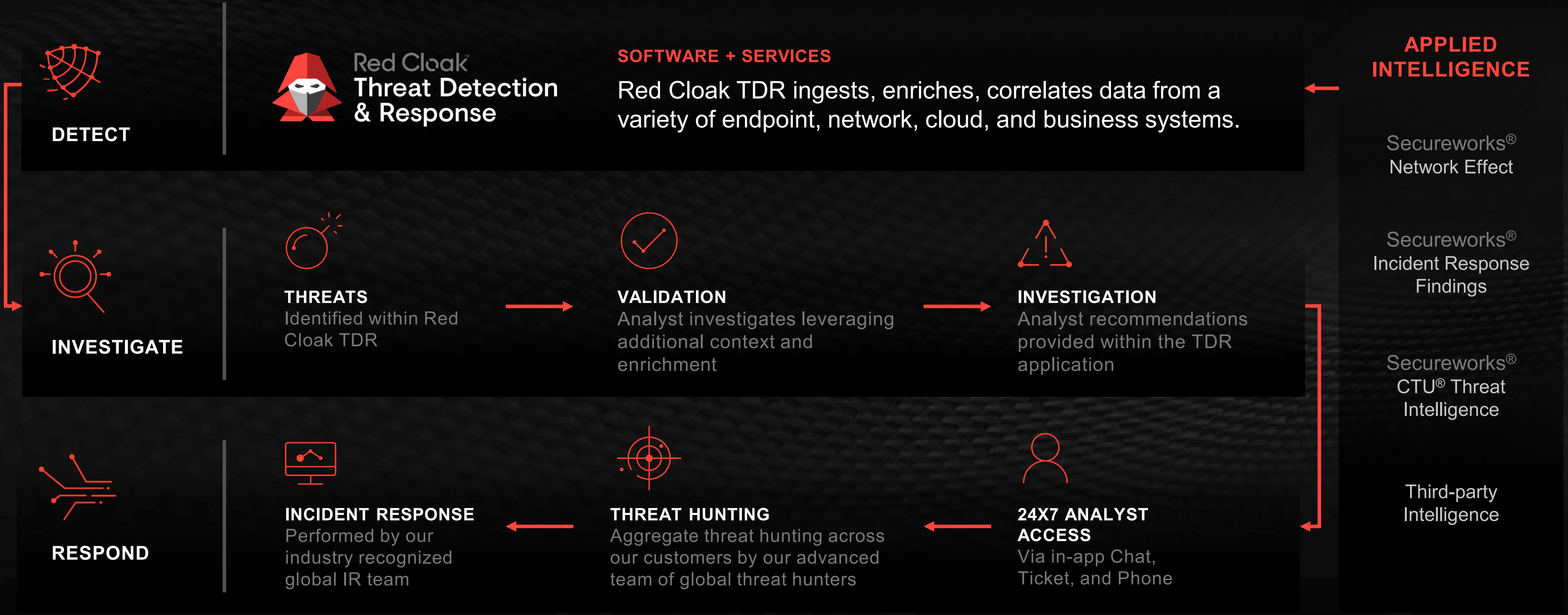
Thousands of signals. Which one matters?

Competing Priorities

Not enough context to know which action to take.

MDR

A security analytics platform combined with managed security services from the industry leader in security operations – integrated into one solution.



DETECT

Red Cloak™ Threat Detection & Response

SOFTWARE + SERVICES

Red Cloak TDR ingests, enriches, correlates data from a variety of endpoint, network, cloud, and business systems.

INVESTIGATE

THREATS
Identified within Red Cloak TDR

VALIDATION
Analyst investigates leveraging additional context and enrichment

INVESTIGATION
Analyst recommendations provided within the TDR application

RESPOND

INCIDENT RESPONSE
Performed by our industry recognized global IR team

THREAT HUNTING
Aggregate threat hunting across our customers by our advanced team of global threat hunters

24X7 ANALYST ACCESS
Via in-app Chat, Ticket, and Phone

APPLIED INTELLIGENCE

Secureworks® Network Effect

Secureworks® Incident Response Findings

Secureworks® CTU® Threat Intelligence

Third-party Intelligence