FORTINET

Building a Cybersecurity Strategy

Tim Wostradowski PSE

Birthday Paradox

How many people need to be in a room before the probability that two of them sharing the same Birthday (Day) is greater than 50%?

$$p(23) \approx 1 - \left(\frac{364}{365}\right)^{\binom{23}{2}} = 1 - \left(\frac{364}{365}\right)^{253} \approx 0.500477.$$

23

The human brain tends to be bad at doing permutations

In cybersecurity, it’s called a Birthday attack. In short, collisions are bad, so salt your passwords.

Who’s Tim?

- I’ve been in technology for close to 20 years
- I’m an engineer at heart
- I’m probably too honest to be in sales
  - But here I am
- I’m motivated by challenge
- I have a reasonable tolerance for risk
  - But I prefer to reduce it where possible
- I love the outdoors

The rules

That apply to both

=

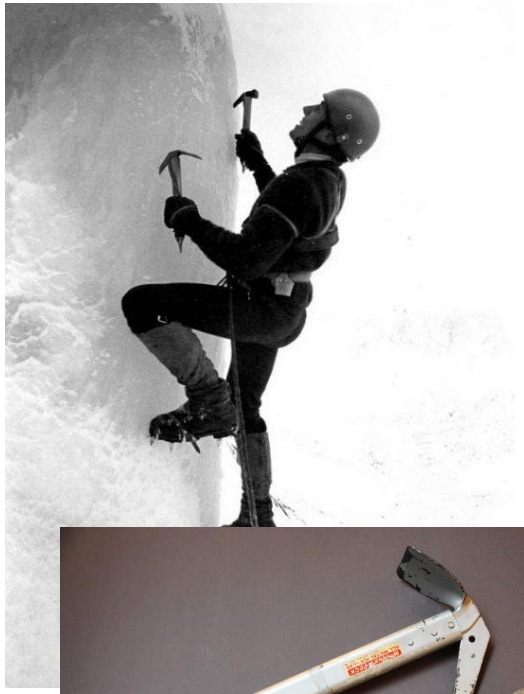
- Rule 1 – Don’t Fall
- Rule 2 – But really… Don’t Fall
- Rule 3 – Proper process ensures that you have a reasonable margin of safety
- Rule 4 – Your planning should prepare you for the worst case
- Rule 5 – If something does fail, you need to learn from that because the next time could be a fall

The People are also similar

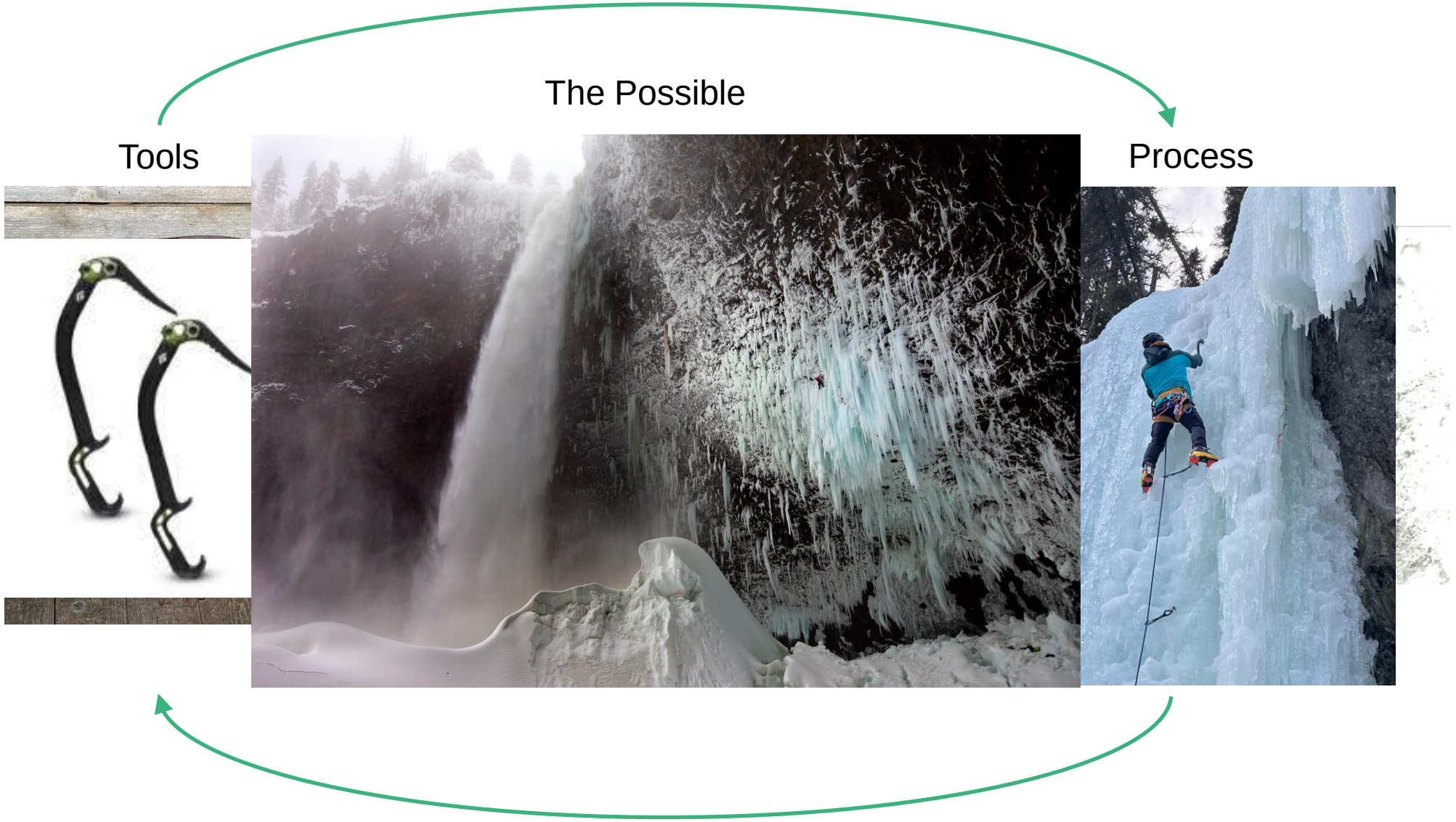
=

A (Very) brief history of ice climbing

Its relevant



The Loop



What's Driving Cybersecurity Decisions?

Driving Infrastructure Evolution

How we interact with customers, suppliers, infrastructure, and employees is changing

Work from Anywhere

Digital Acceleration

Application Journey

Operational Technology Connectivity

Evolving Threat Landscape

Cybercriminals are adopting APT-like tactics to develop and scale attacks faster than ever

Cloud

Kaseya VSA

Nation Sponsored

Hermetic Wiper

Ransom as a Service

REvil

Growing Attack Surface

SolarWinds | Log4j

AI-enabled

Swarmbot

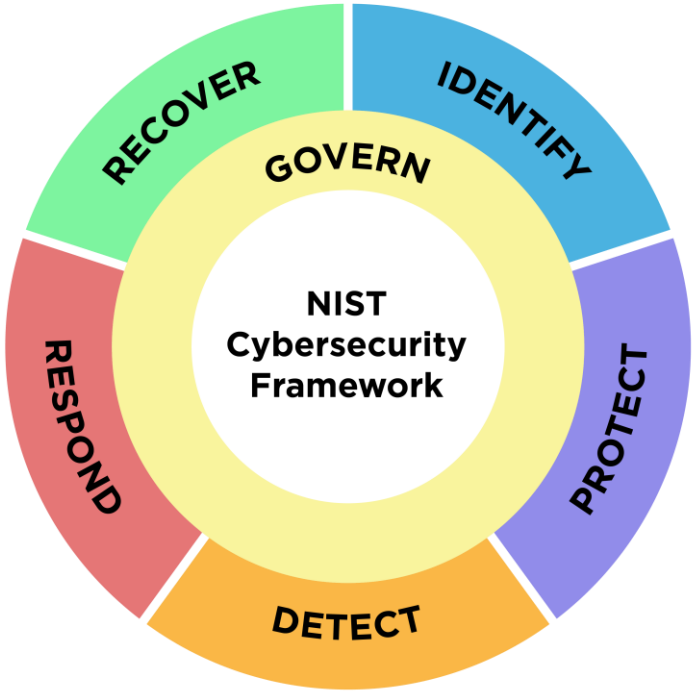
OT

Wipers | Colonial Pipeline

The Process

To a Successful Cybersecurity Strategy

We know the possible. Where do we start?



- Frameworks are a great place to start
  - When you're not sure where you should start
- Its high level and can be used by anyone
  - The more descriptive, the less flexible
- For a board audience
  - Everyone in this room should find some value
- We need to know what the process looks like to select our Products (Tools/Controls)

Governance

- Organizational Context
  - Understand what your business does and what is required of its security team.
- Risk Management Strategy
- Roles, Responsibilities, and Authorities
  - Understand who’s truly accountable; it might surprise them.
- Policy
  - It’s easier for people to follow a policy when you have one.
- Oversight
- Cybersecurity Supply Chain Risk Management
  - This one continues to become more and more important in our “aaS” world.

Identify

- Asset Management
  - It’s hard to protect it if you don’t know it exists or what state it exists in.
- Risk Assessment
  - Understand your Risks
- Improvement [to the CSF Process]
  - And make a plan to improve them

Protect

- Identity Management, Authentication, and Access Control
- Awareness and Training
- Data Security
- Platform Security
  - Read this as security of assets
- Technology Infrastructure Resilience

Detect

- Continuous Monitoring
  - Monitor everything and always
- Adverse Event Analysis
  - Potentially adverse events are analyzed to better understand associated activities
  - Information is correlated from multiple sources
  - The estimated impact and scope of adverse events are understood
  - Information on adverse events is provided to authorized staff and tools
  - Cyber threat intelligence and other contextual information are integrated into the analysis

Respond

- Incident Management
- Incident Analysis
- Incident Response Reporting and Communication
- Incident Mitigation

Recover

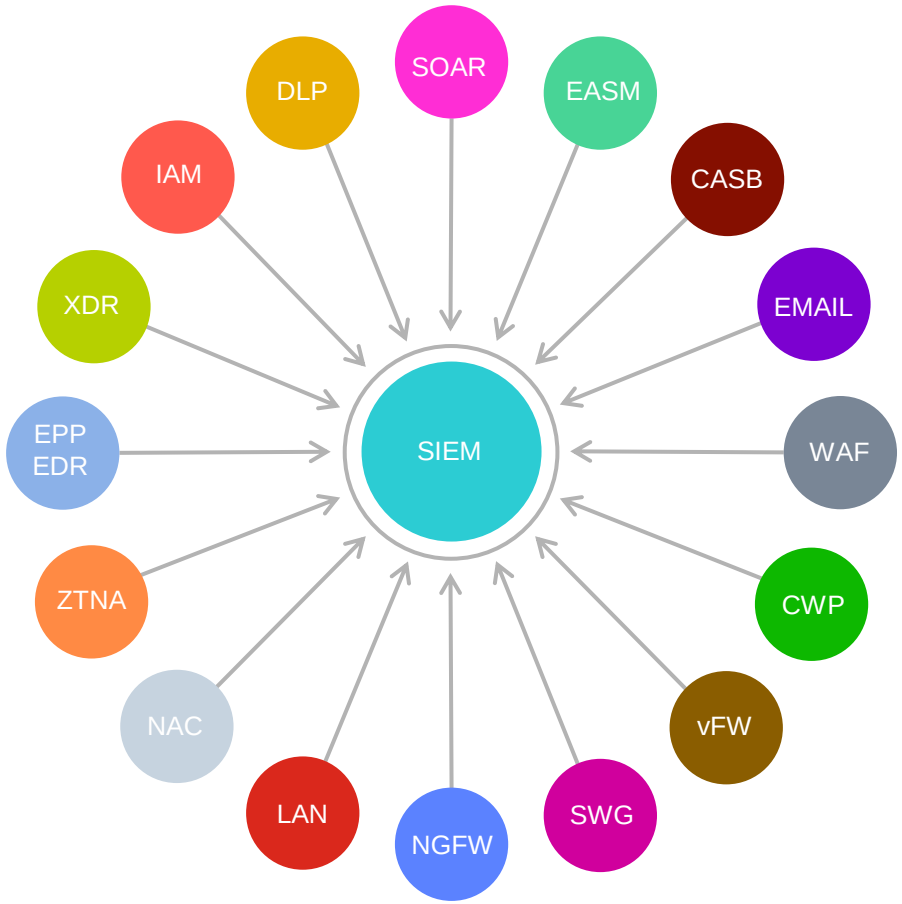
- Incident Recovery Plan Execution
- Incident Recovery Communication

The Tools

To Complete the Process

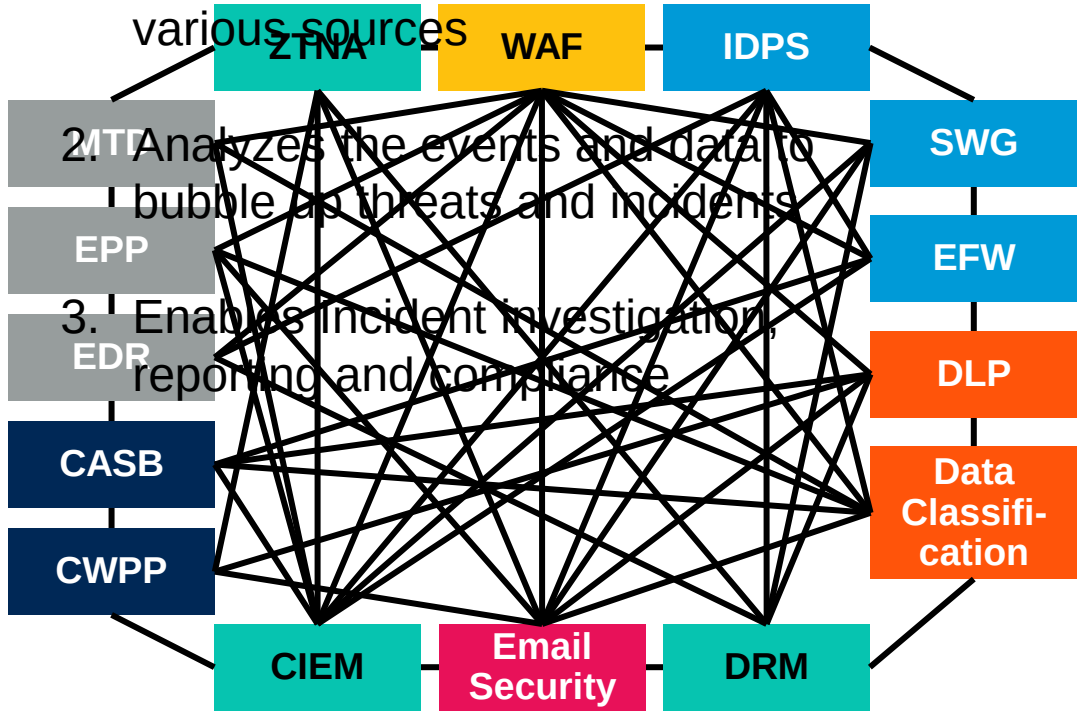
Point Products

Cybersecurity Point Products



20 Vendors

Gartner Cybersecurity Mesh Architecture (CSMA)



What does the SIEM do?

1. Normalizes and ingests logs from various sources
2. Analyzes the events and data to bubble up threats and incidents
3. Enables incident investigation, reporting and compliance

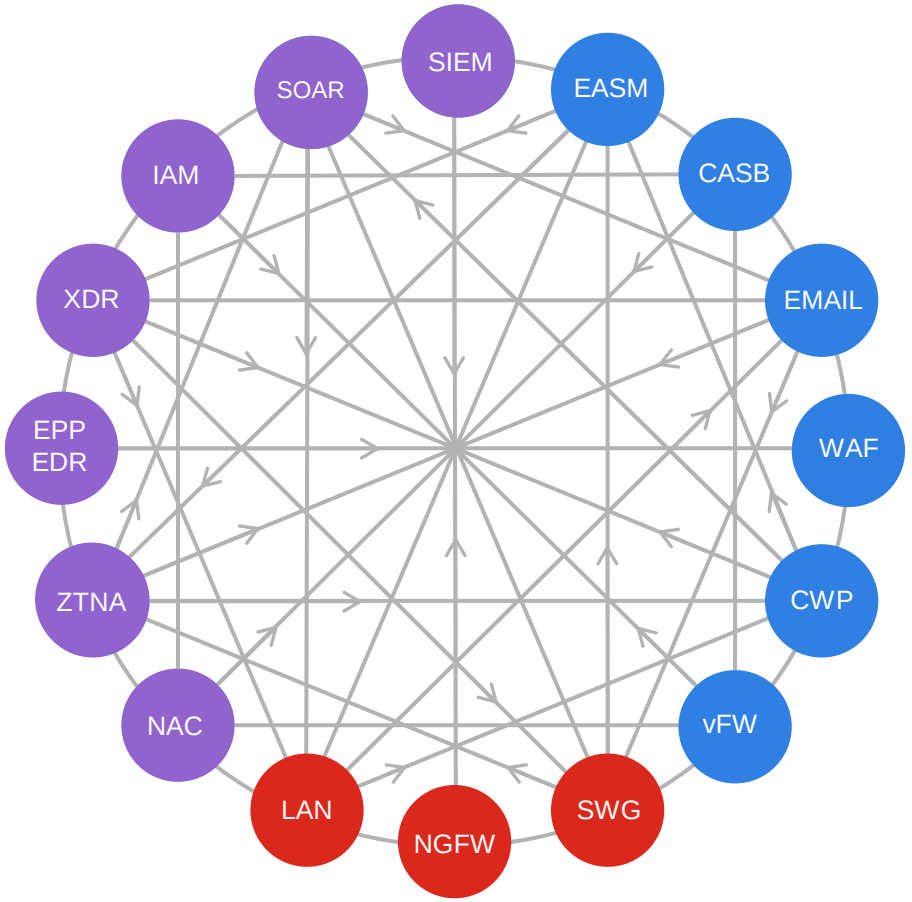
Platforms

“a raised level surface on which people or things can stand”

- Self Contained
  - Easy to use and consume
- Unified Management
  - Less work for a team to manage
- Integrations often (though not always) through proprietary means
  - But often more seamless to the consumer
- Generally made of up multiple Products and Solutions
  - But a unified platform makes it appear as one
- Efficiencies through automation within the solution
  - Focused and easy to utilize

Enabling teams with a Platform

Cybersecurity Platform Approach



4-6 Platforms

- The consolidation of point products into platforms
- Multiple platforms still needed to cover everything
  - But as time goes on their capabilities grow
- But this can also make it difficult to understand where coverage starts and ends
- Still requires SIEM/SOAR to enable inter-platform threat sharing
  - Some platforms might contain SIEM/SOAR functionality natively

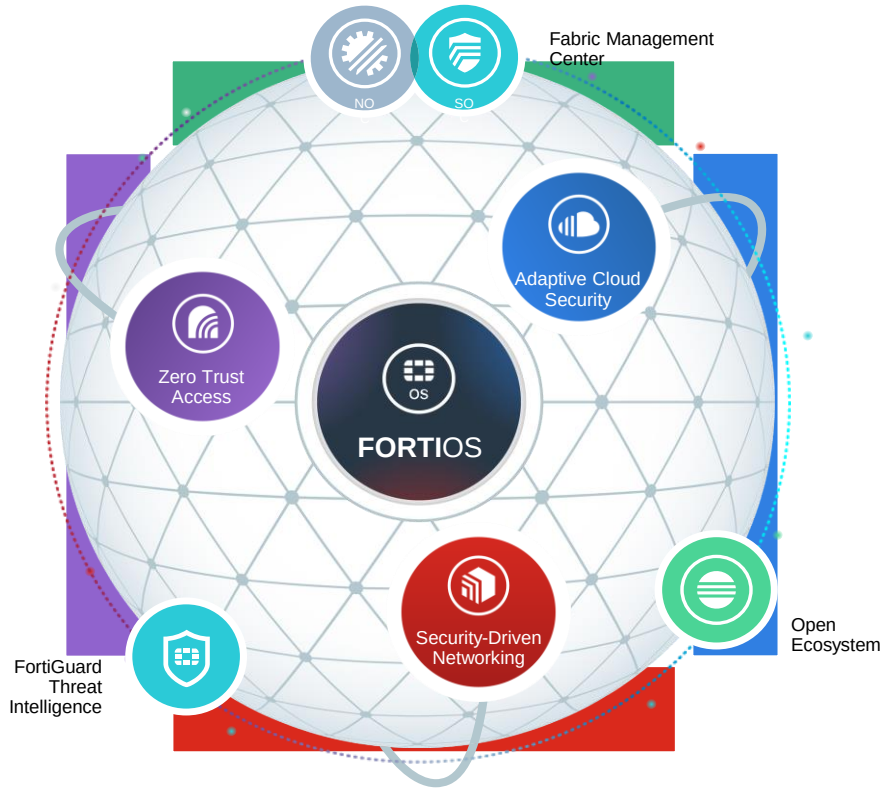
Cybersecurity Fabrics

- Less focused on Unified management
  - More of a focus on interoperability
- Vendor / Solution agnostic
  - Fabrics enable the use of various sources of analytics
- Larger emphasis on gathering and using data (unstructured)
  - Enables the use of LLMs and ML to utilize the large vast data
- The Majority use standard-based ways to communicate
  - Makes it straightforward to connect platforms
- Designed around scalability
  - The more systems you connect the more data you have

The tools we need to make “The Possible”

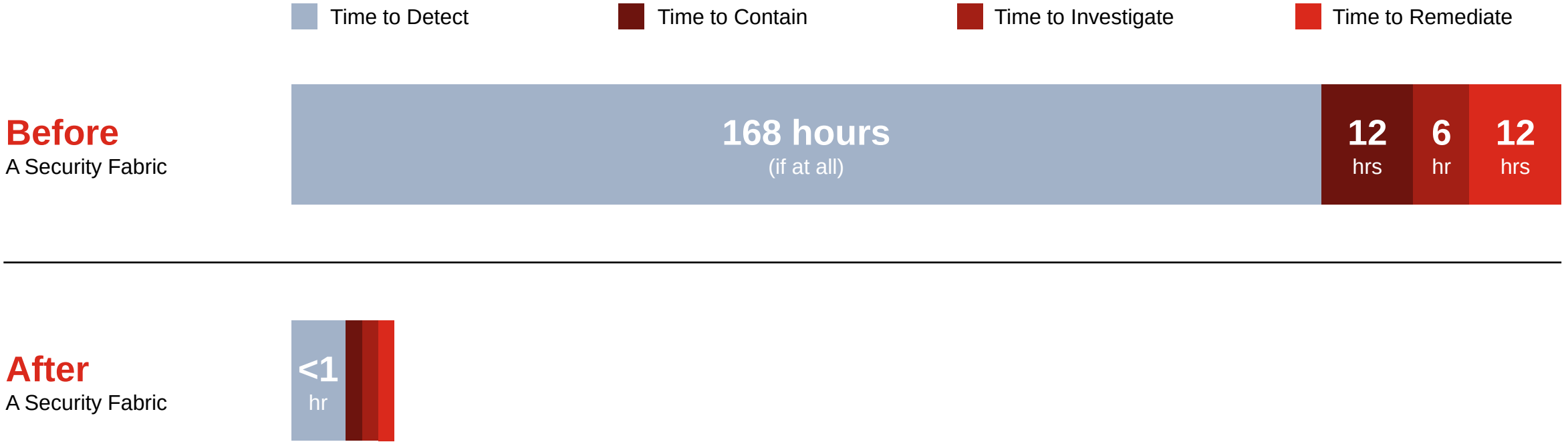
- The process for cybersecurity today requires tools that enable each other
  - With the enormous amount of data produced, it’s easy to get buried
  - Platforms handle some aggregation, but a fabric enables you to extract enrichment data from those solutions
  - Reducing the time your analysts spend doing busy work increases the time they have to make decisions that require a human
  - Tighter integrations also make compliance and governance a more manageable task

Cybersecurity Fabric



Fabric Benefits

Massively Improved MTTD, MTTR and Productivity



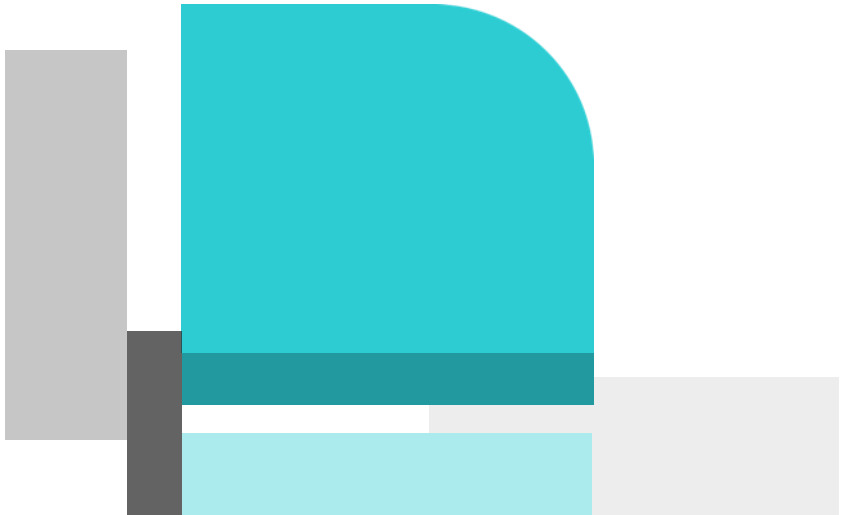
Source: Enterprise Strategy Group, a division of Tech Target, Inc.

So, use Products and Platforms to build a Fabric?

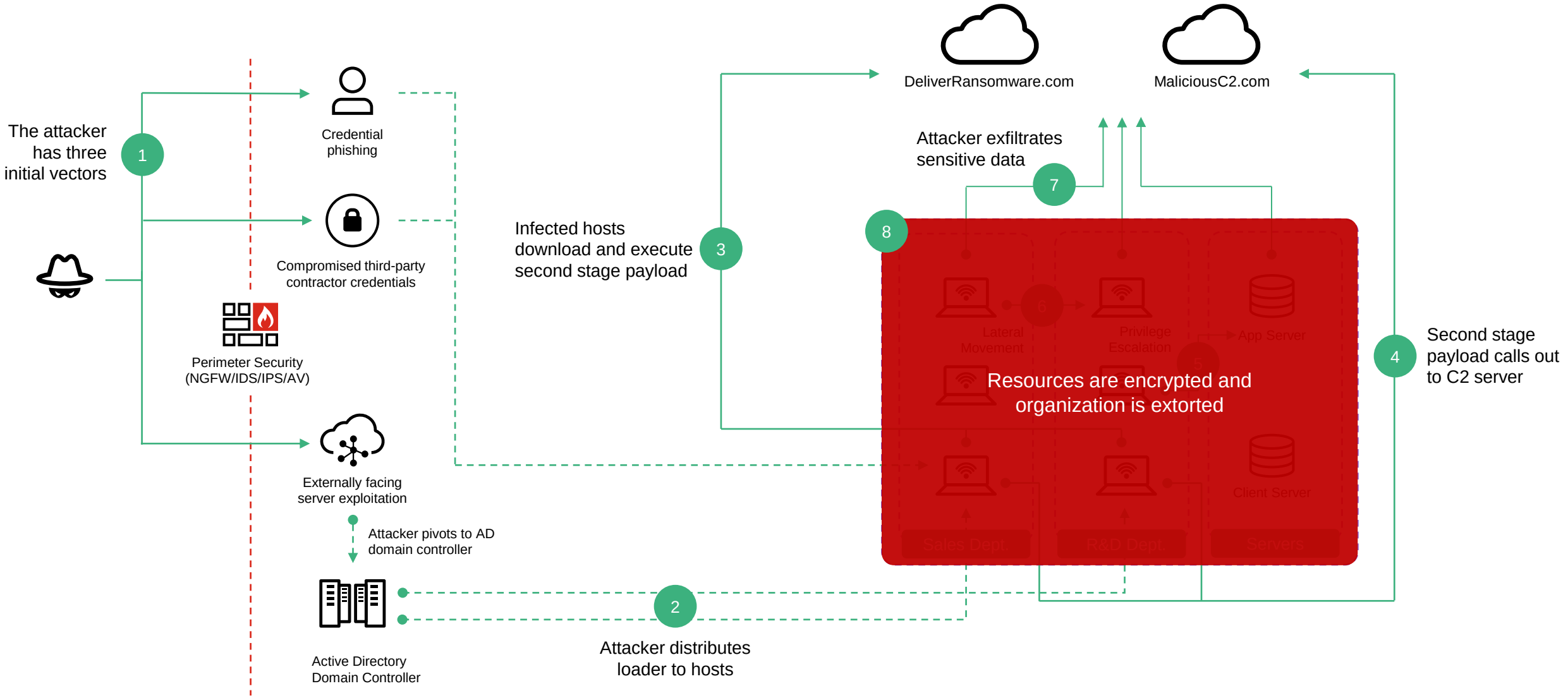
And why does it matter what we call them?

- Save time and effort with pre-built solutions
- Better evaluate a vendor's product
  - What areas does it cover?
- Determine where in your Strategy this tool fits.
  - Can it be used to enhance my existing fabric
- Cut through marketing
  - We make it sound attractive, but sometimes that makes it hard to understand

Fabric In Action



Anatomy of a Ransomware Attack



Some might say…

“The attacker only has to get it right once while the security team has to get it right 100% of the Time.”

Harden the Attack Surface and Block Attacks

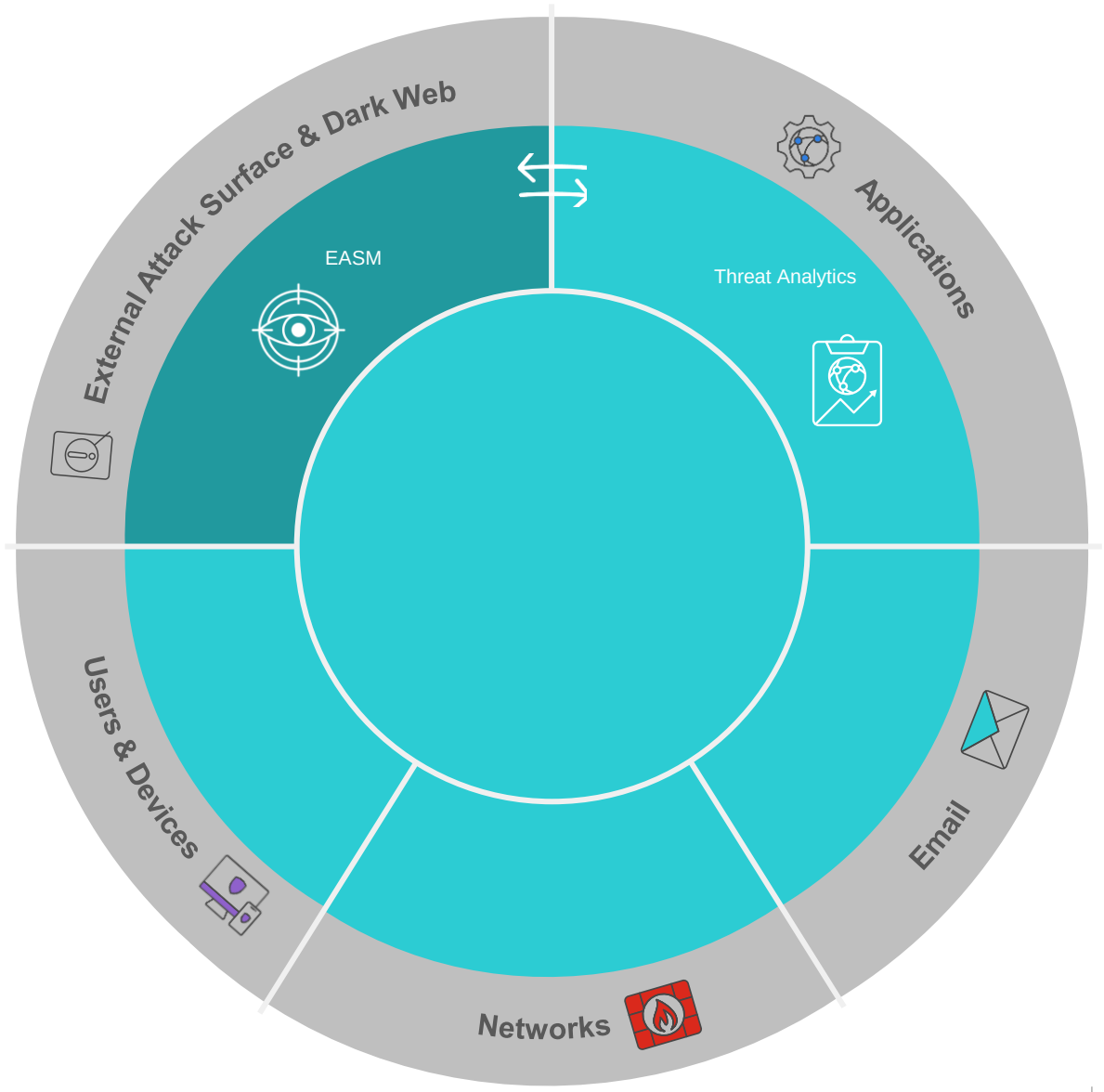
NIST Cybersecurity Framework

NIST Cybersecurity Framework

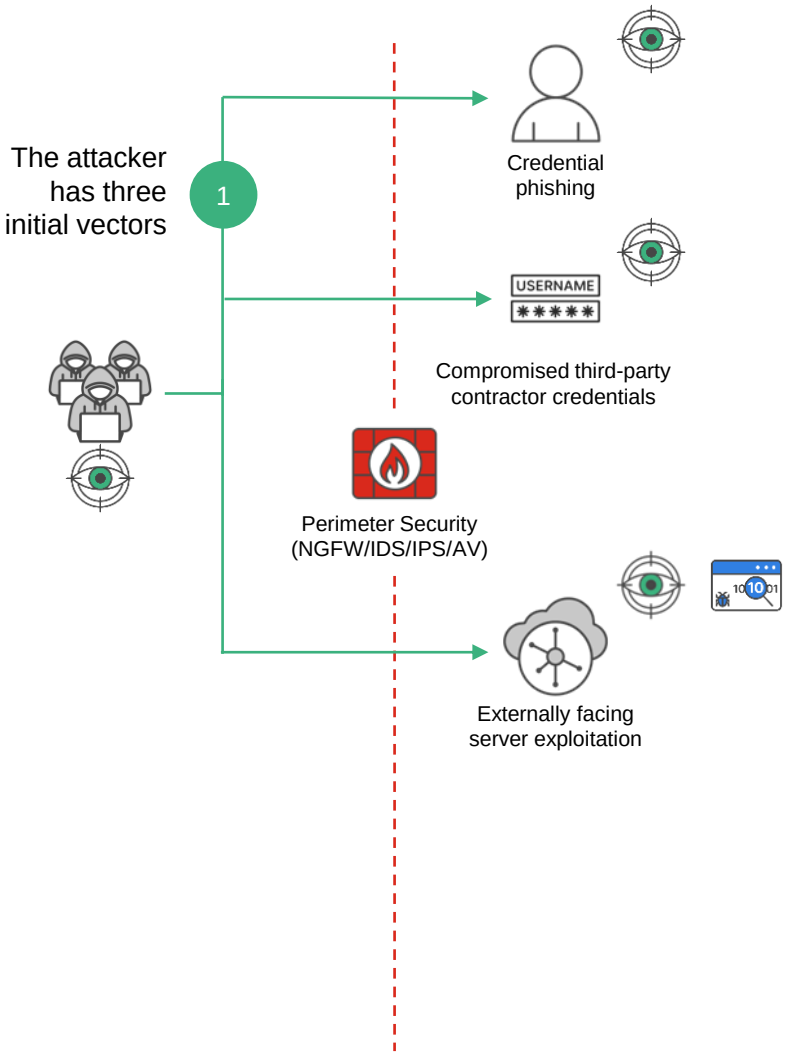
Identify

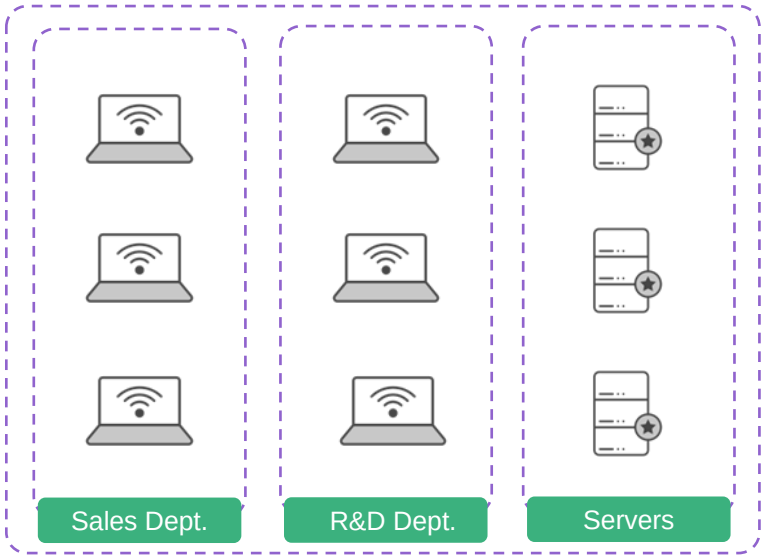
Technologies & Services

EASM
DRPS
Threat Research
Application Testing



Identify Cyber Threats and Exposure





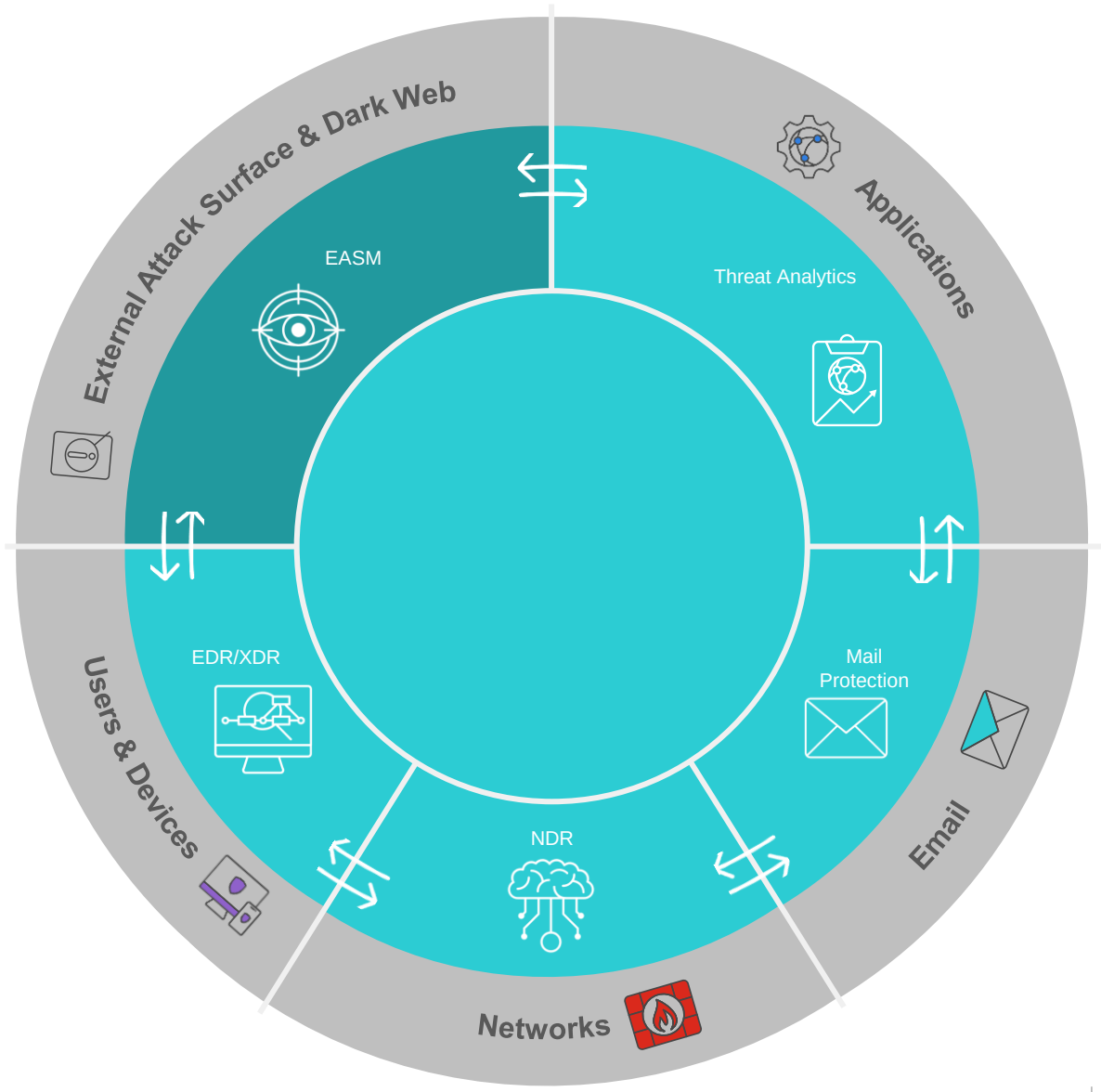
Harden the Attack Surface and Block Attacks

NIST Cybersecurity Framework

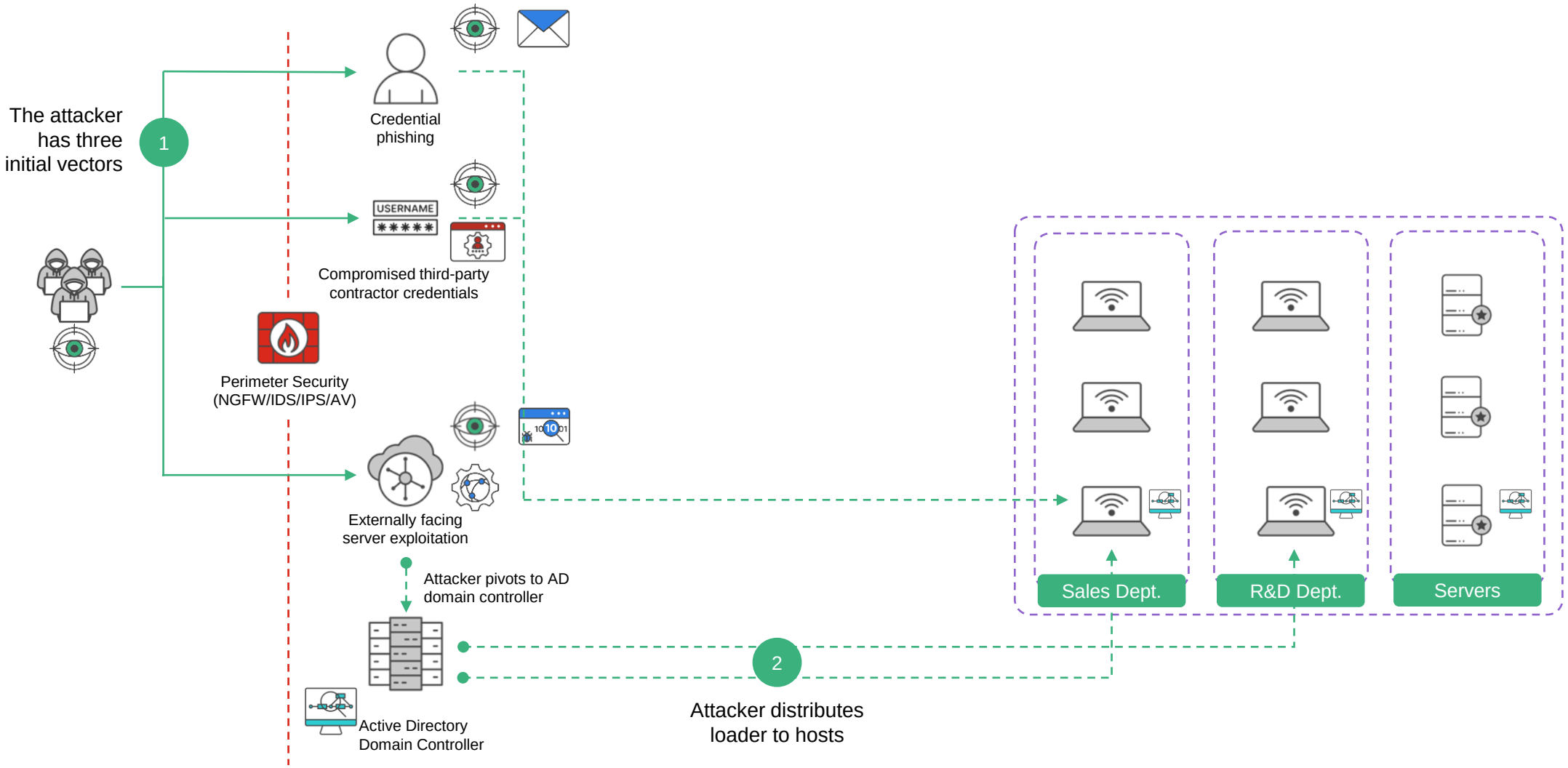
NIST Cybersecurity Framework

Technologies & Services

EASM DRPS Threat Research Application Testing	NGFW SEG WAF EPP VMS ZTNA PAM



Harden the Attack Surface and Block Attacks



Detect and Disrupt Threat Actor Intrusion

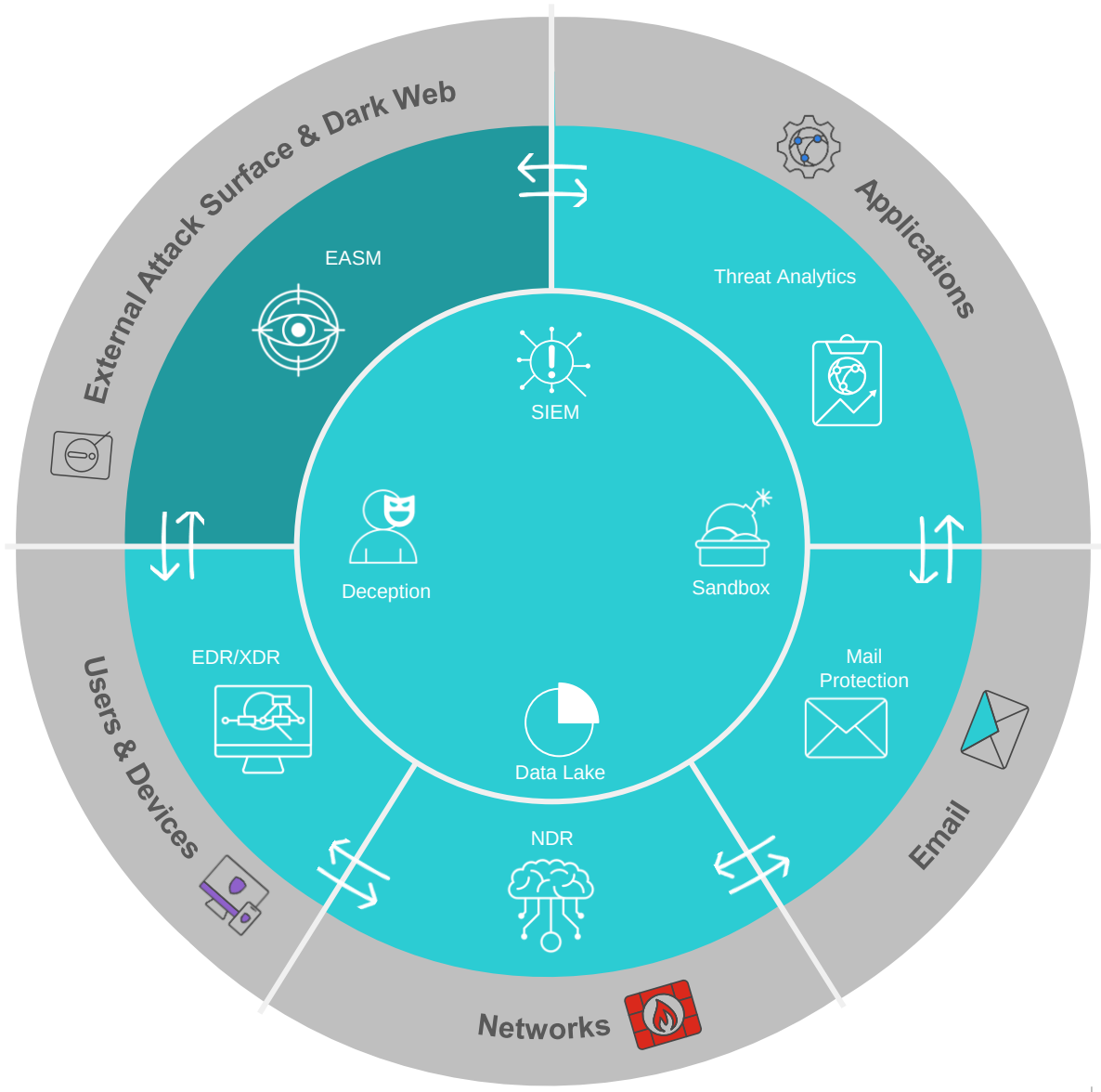
NIST Cybersecurity Framework

NIST Cybersecurity Framework

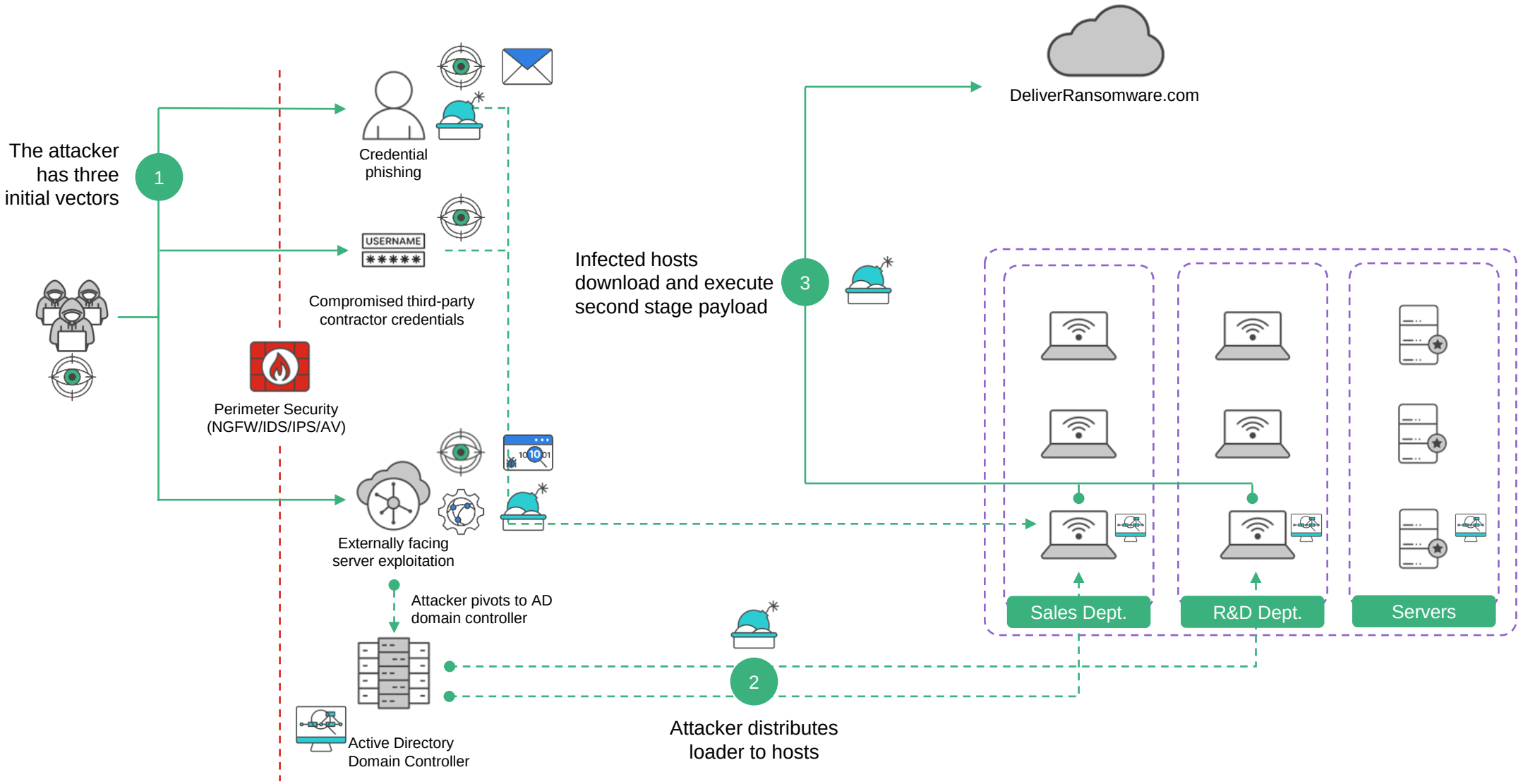
Identify	Protect	Detect

Technologies & Services

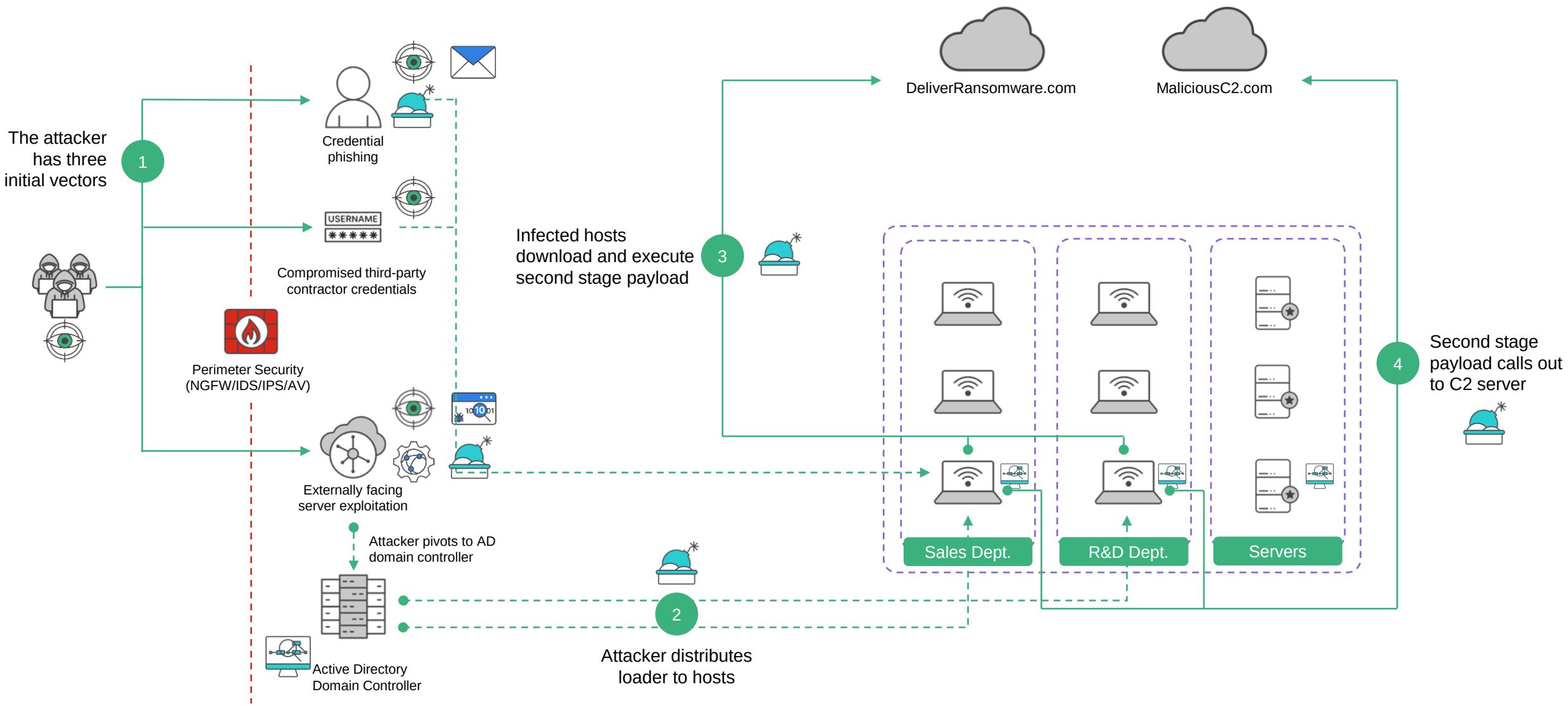
EASM DRPS Threat Research Application Testing	NGFW SEG WAF EPP VMS ZTNA PAM	EDR/MDR UEBA NDR Mail SIEM Analytics Deception Sandbox SOCaaS



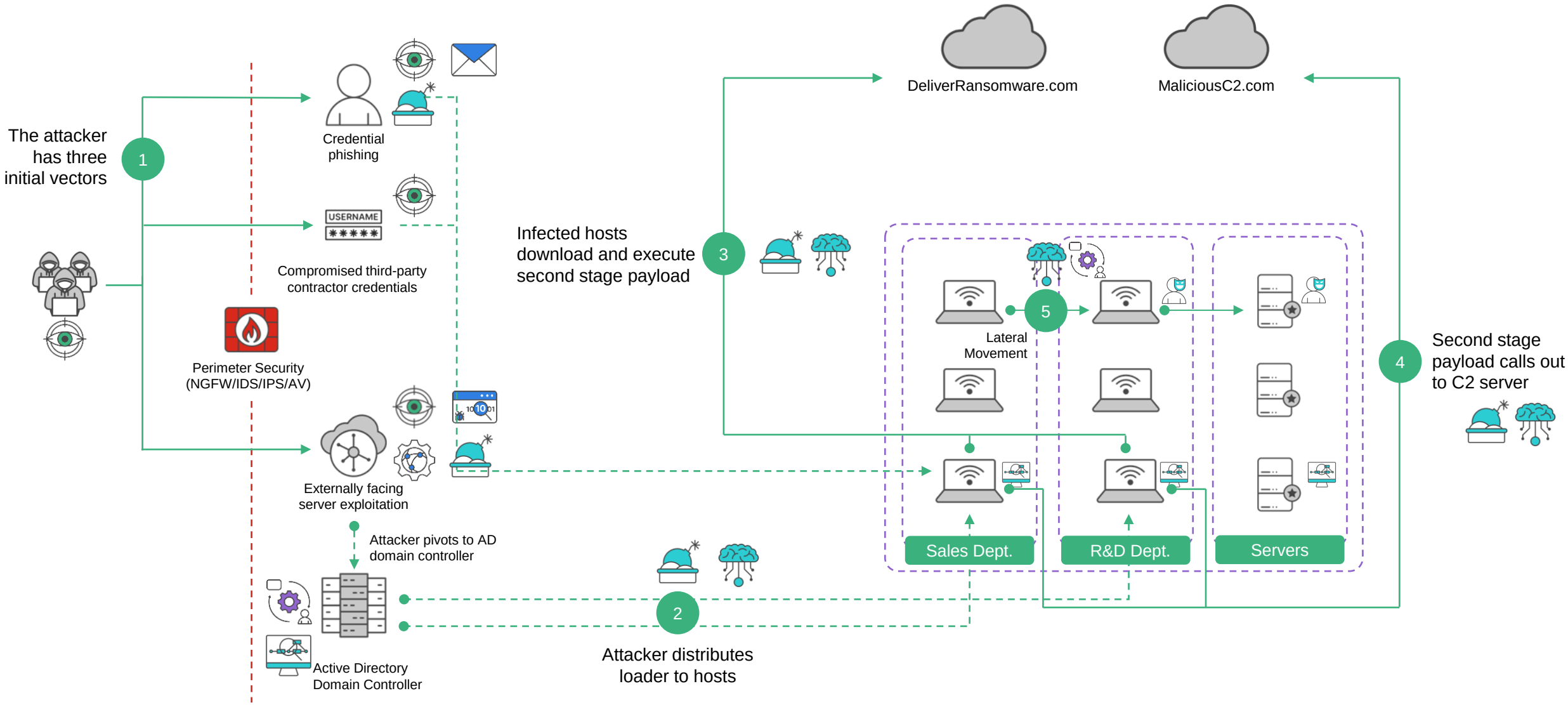
Detect and Disrupt Threat Actor Intrusion



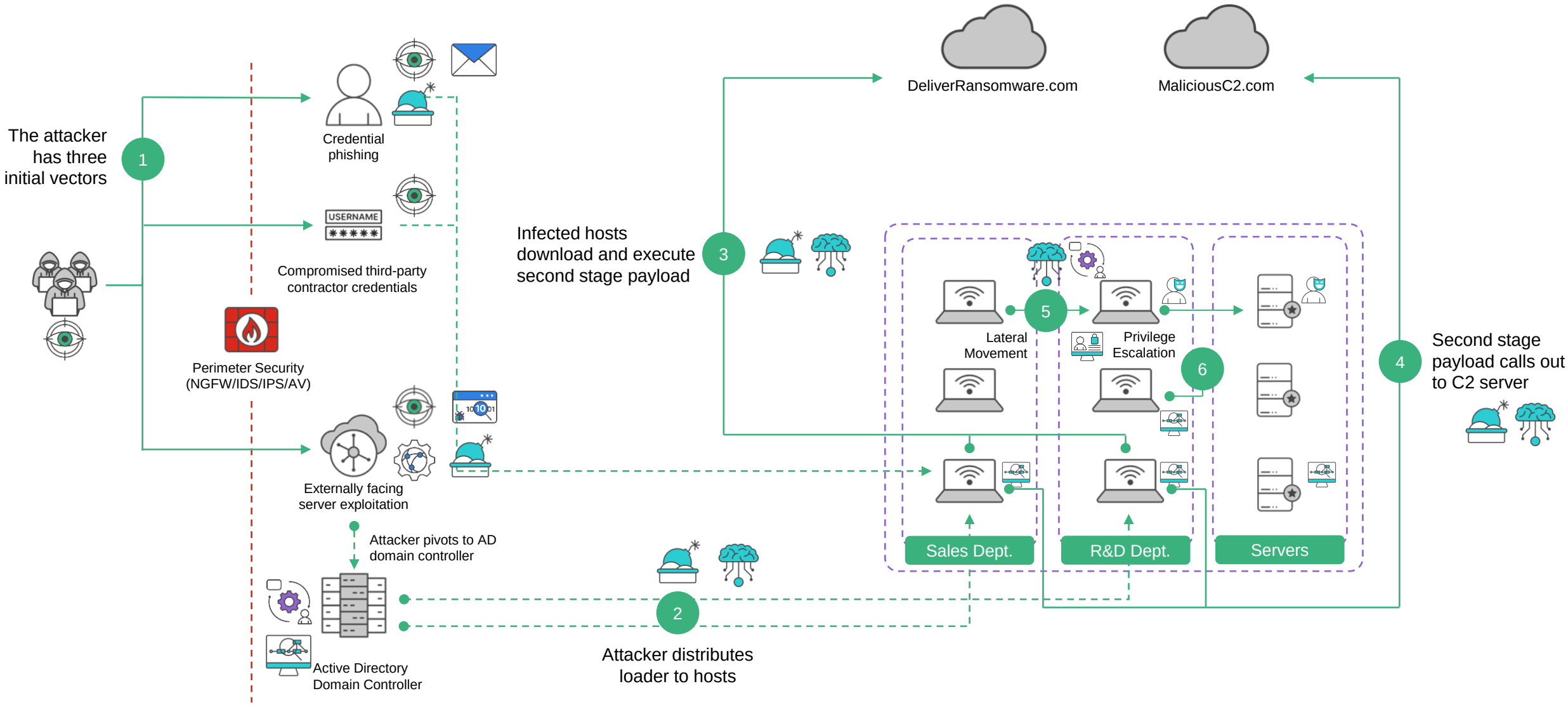
Detect and Disrupt Threat Actor Intrusion



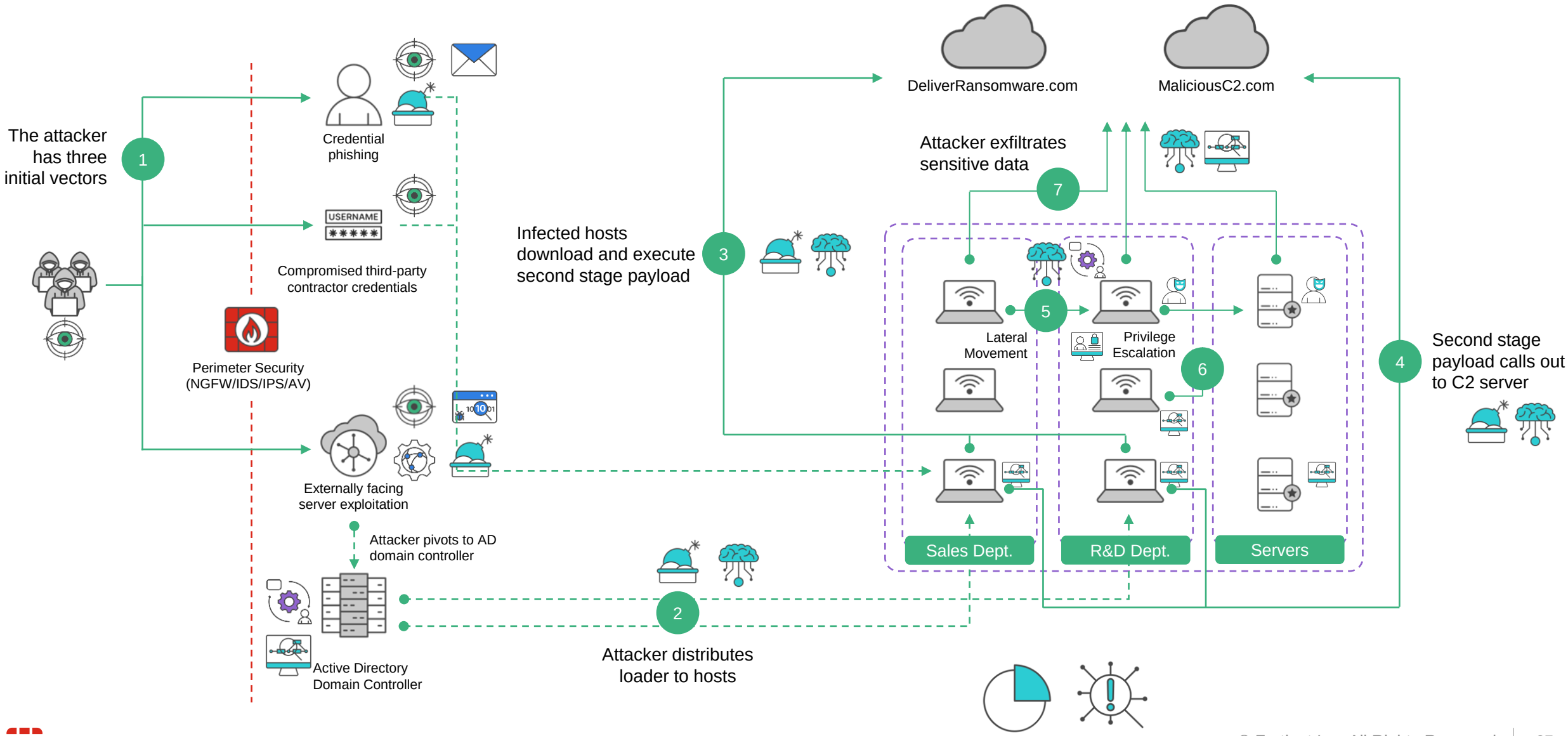
Detect and Disrupt Threat Actor Intrusion



Detect and Disrupt Threat Actor Intrusion



Detect and Disrupt Threat Actor Intrusion



Investigate & Remediate Incidents, Return to Safe Operation

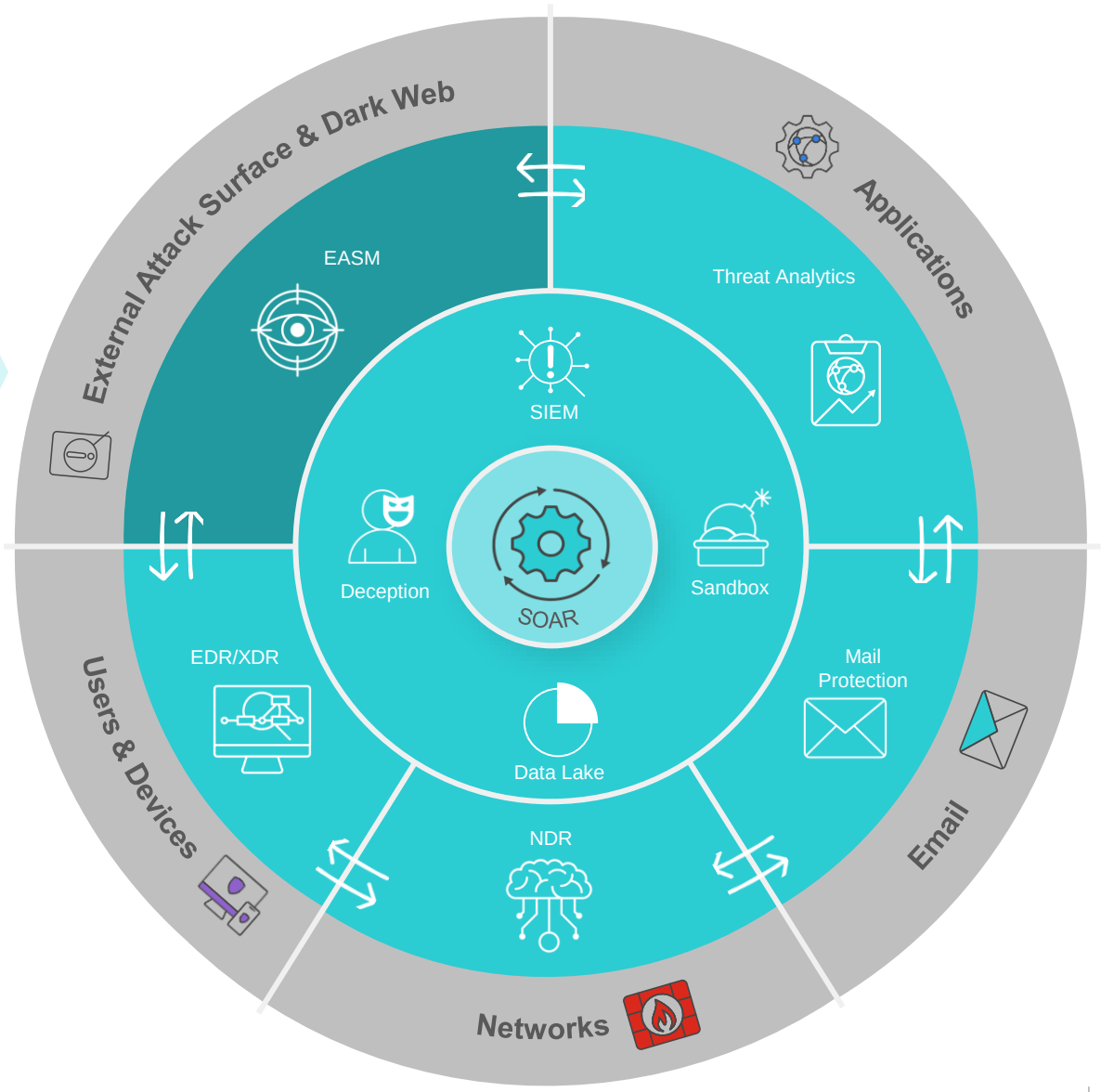
NIST Cybersecurity Framework

NIST Cybersecurity Framework

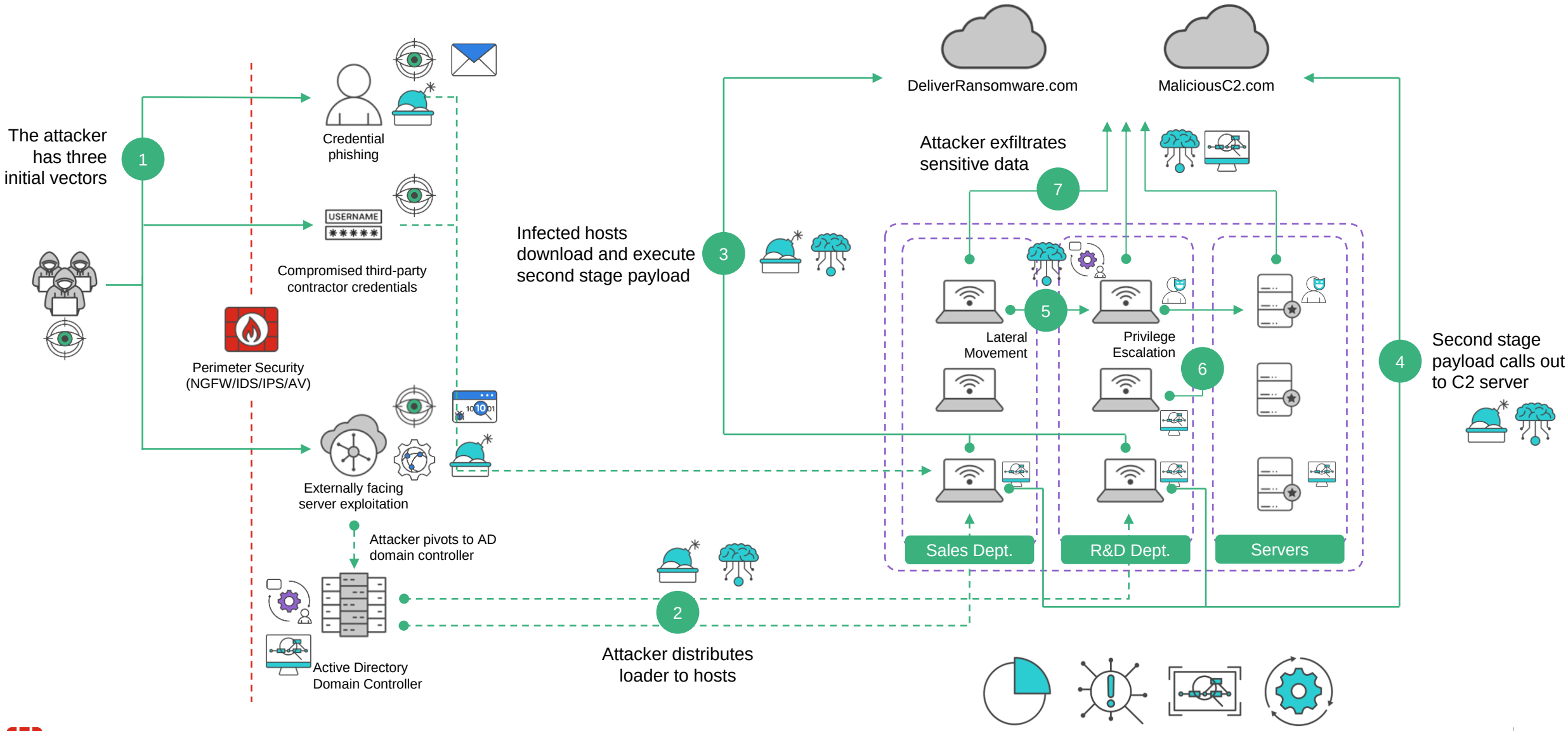
Identify	Protect	Detect	Respond	Recover

Technologies & Services

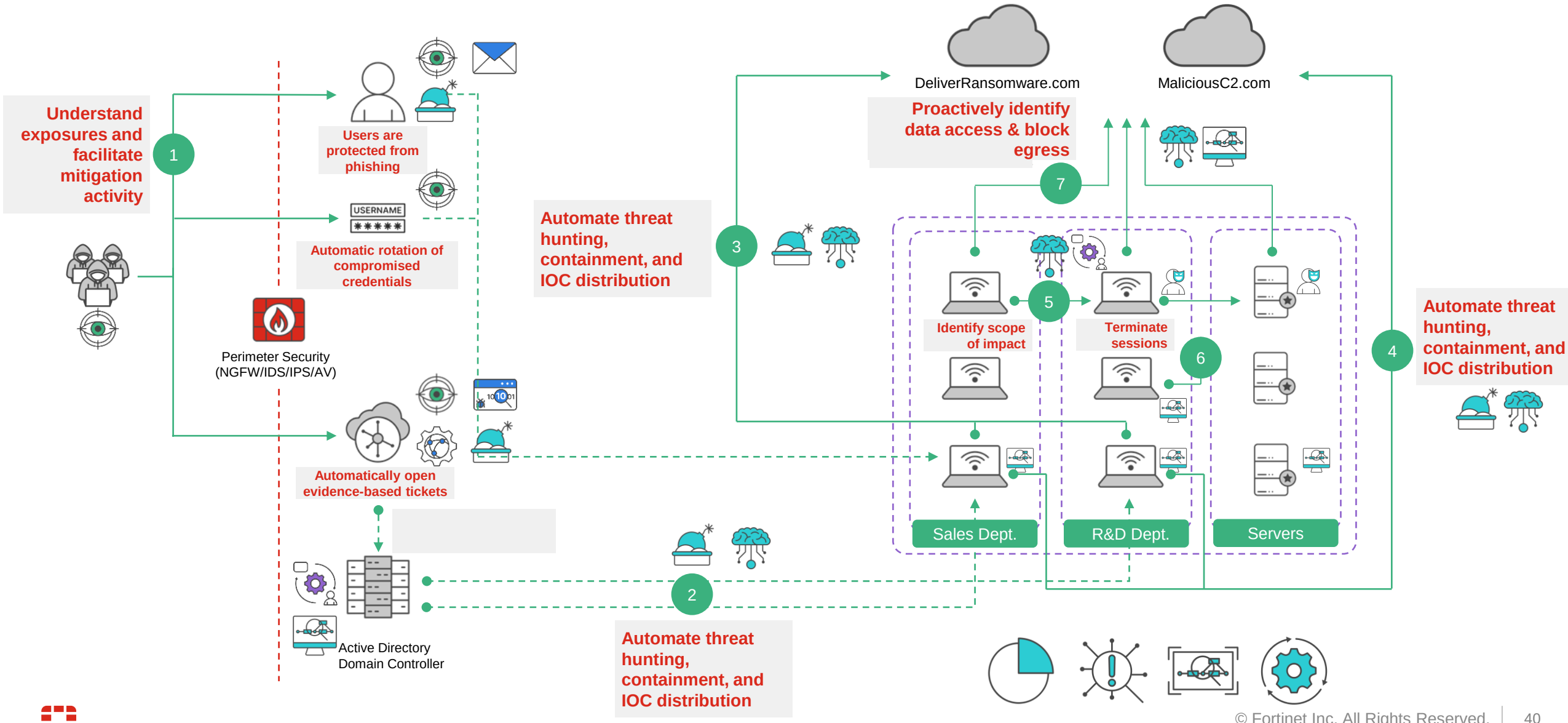
EASM DRPS Threat Research Application Testing	NGFW SEG WAF EPP VMS ZTNA PAM	EDR UEBA NDR Mail SIEM Analytics Deception Sandbox	SOAR XDR	Partner Ecosystem IR Services



Investigate & Remediate Incidents, Return to Safe Operation



Investigate & Remediate Incidents, Return to Safe Operation



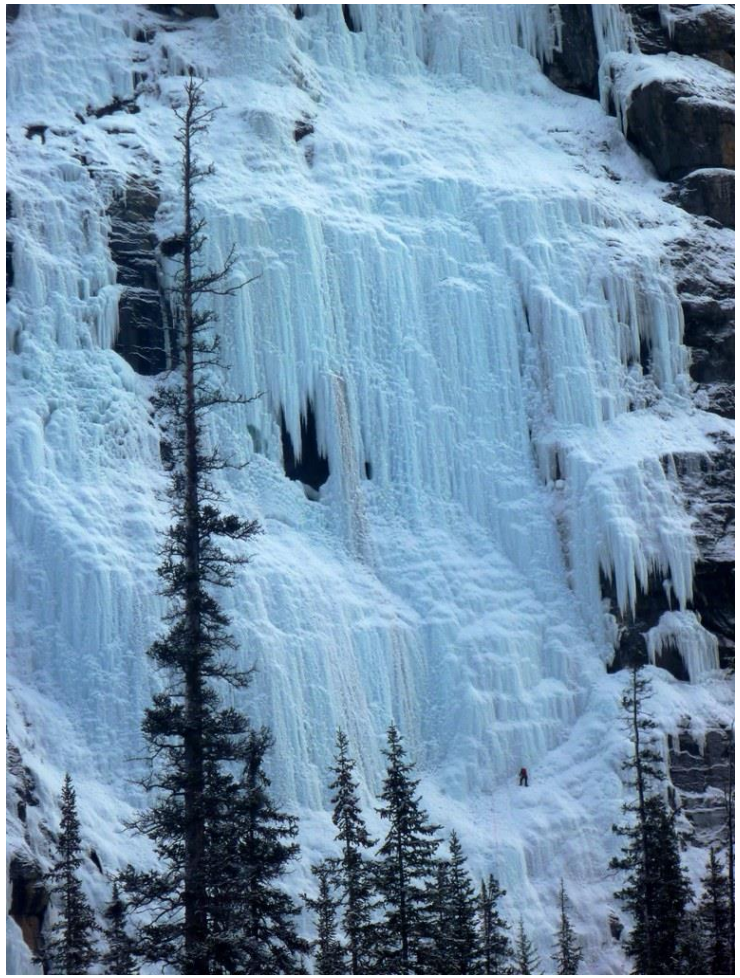
Lets Flip the Script

“The attacker only has to get it right once while the security team has to get it right 100% of the Time.”

When you connect your network through a fabric of cybersecurity protections you change the conversation.

“Once the attacker is in, they have to get it right 100% of the time to avoid network detection, but the security team has multiple chances to catch an attacker in the act”

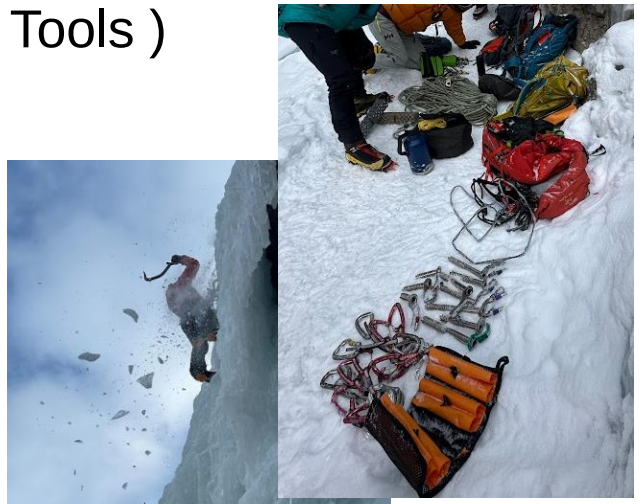
Cybersecurity Strategy

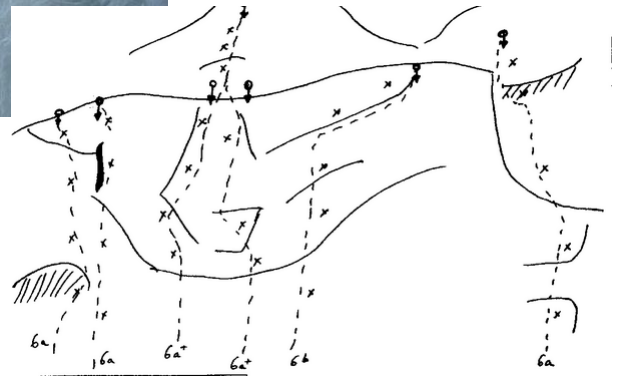


Products (Tools)

People

Processes





Q&A


FORTINET