Protecting Against the Top 5 Attack Vectors

Stay secure from the most common threats seen by Arctic Wolf's security team

Layer 7 Data Solutions

ARCTIC WOLF

www.arcticwolf.com

Table of Contents

Major Cyberattacks in the News

Uber

57 million users' and drivers' personal data was exposed— addresses, driver license numbers and credit cards were stolen. Hackers gained unauthorized access to customer data via Uber's GitHub instance in AWS to steal data.

WannaCry

Multiple ransomware attacks hit a number of multinational companies across Europe and brought their businesses to a halt. They all exploited a vulnerability in Microsoft Windows that could have been easily patched.

Equifax

145 million consumers' SSNs, addresses, drivers license numbers and credit cards were stolen. An unpatched Apache web server was exploited. It was very similar to intrusions into Anthem and the US Office of Personal Management.

Spectre/Meltdown

Most modern processors are susceptible to malicious code that can gain unauthorized access to portions of memory and steal passwords and crypto-keys. Patches are available for most OS's running on these processors.

The Top 5 Attack Vectors

Here are the five most common attacks Arctic Wolf Networks has detected in our AWN CyberSOC™

As you will see, nefarious hackers, cybercriminals and bad actors seek means, pathways and vulnerabilities to gain unauthorized access to a computer device or network for exploitation purposes.

Malware/Ransomware

Modus Operandi:

Malicious software that spreads via an email attachment or a link to a malicious website. It infects the endpoints when a user opens the attachment or clicks on the link.

1

Ransomware is a specialized malware that encrypts all the files on the system that it infects, and prevents you from accessing data unless you pay a ransom.

Counter-Measure:

Ongoing security awareness training for end users, to teach them not to open email attachments from unknown users and not to click on suspicious URLs and download browser plug-ins from suspicious websites.

The Top 5 Attack Vectors

Password Phishing Attack

2

Modus Operandi:

Malicious email that tricks users to surrender their user credentials. The email may appear legitimate, as if coming from your bank, and ask you to reset your password.

Everything looks above board; it even warns the recipient not to fall for fraudulent emails. The only thing that gives it away is the rogue link asking for confidential information.

Counter-Measure:

Enable 2-factor authentication, biometrics, or other out-of-band authentication methods (one-time passwords via text). Use anti-spam email software to protect against such attacks.

PUP Adware

3

Modus Operandi:

Potentially unwanted programs (PUPs) are trojans, spyware or adware that surreptitiously monitor your keystrokes, scan files on your hard drive, and read your browser cookies.

Hackers make money using PUPs by marketing software products with annoying ads that pop up on your screen.

Counter-Measure:

Avoid downloading and installing apps, browser extensions and programs from untrusted websites. Backup your system to an external drive or online backup service.

The Top 5 Attack Vectors

4 Account Hijacking

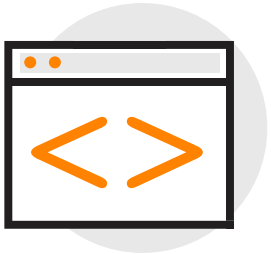
Modus Operandi:

Hackers gain access to user accounts by repeatedly entering in different "guesses" of stolen passwords or words from the dictionary with combinations of numbers until they successfully log in.

Such attacks are typically launched with automated tools, where thousands of passwords are submitted from multiple bots (botnets) in a matter of seconds.

Counter-Measure:

Brute-force attacks can be prevented, by 1) account lockout after designated number of failed login attempts; 2) using a challenge-response test (reCAPTCHA) to prevent automated submission.



5 Unpatched/Outdated Software

Modus Operandi:

Hackers exploit vulnerabilities in systems software and web applications to execute unauthorized code, enabling them to gain extra privileges or steal information.

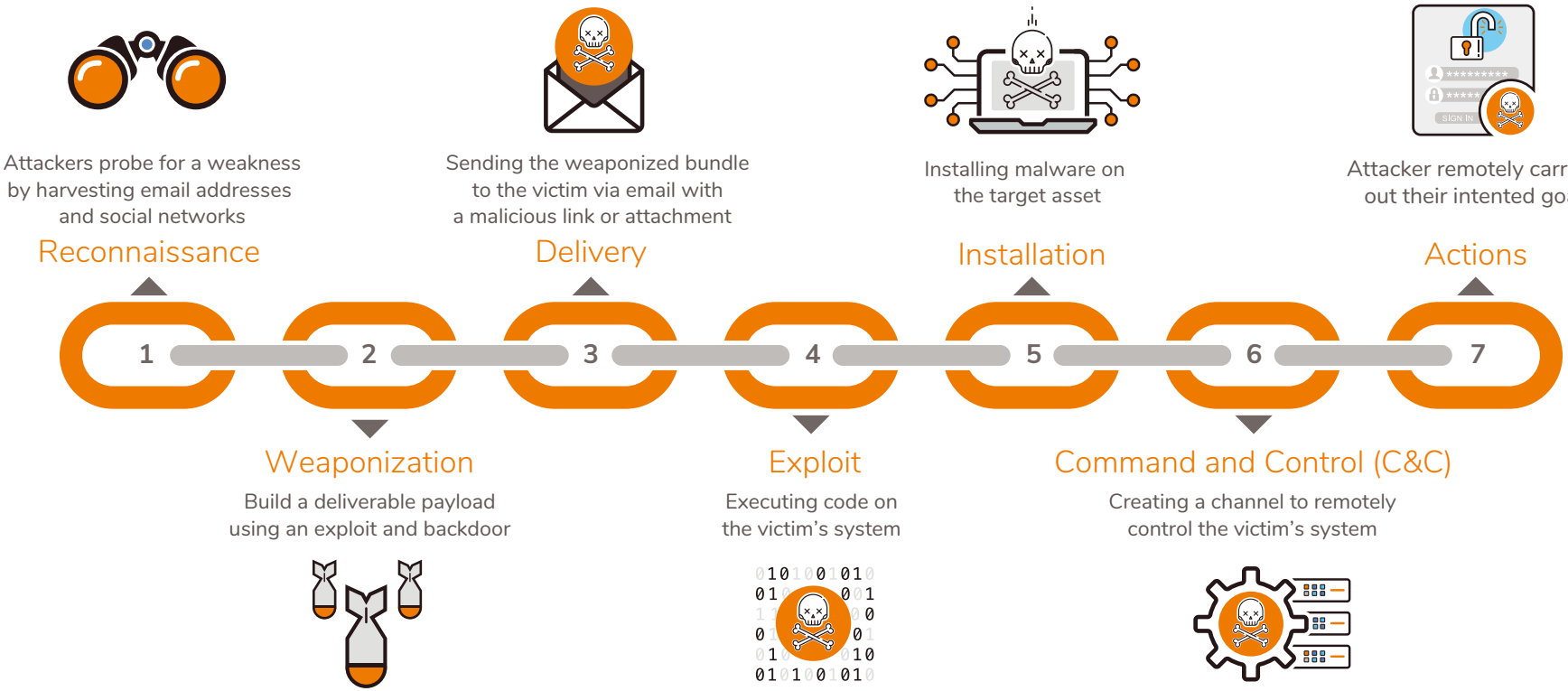
Shellshock exploited a bug in Unix in 2014 to take over systems and convert them to bots. SQL-injection attacks are used to exploit vulnerable web applications.

Counter-Measure:

Run vulnerability scanning software at regular intervals, and patch all systems which have high-priority vulnerabilities.

The Cyber Kill Chain®

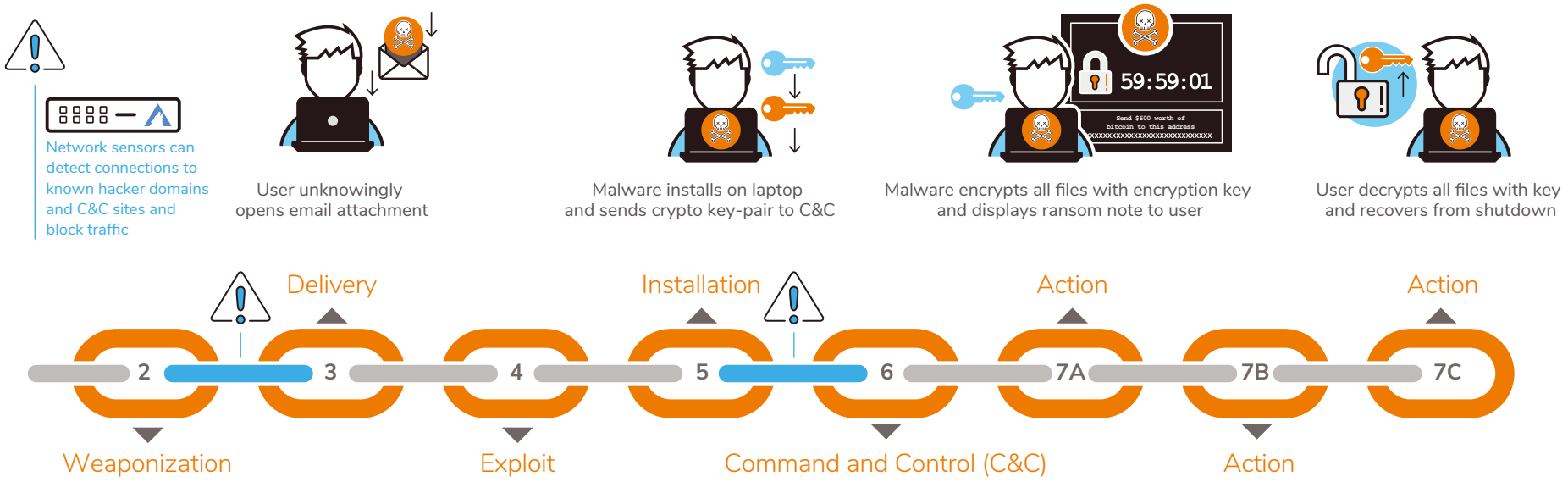
The cyber kill chain, created by Lockheed Martin, describes the seven stages of any targeted attack. Each stage presents an opportunity to detect and mitigate that attack.



Protecting Against

Malware/Ransomware

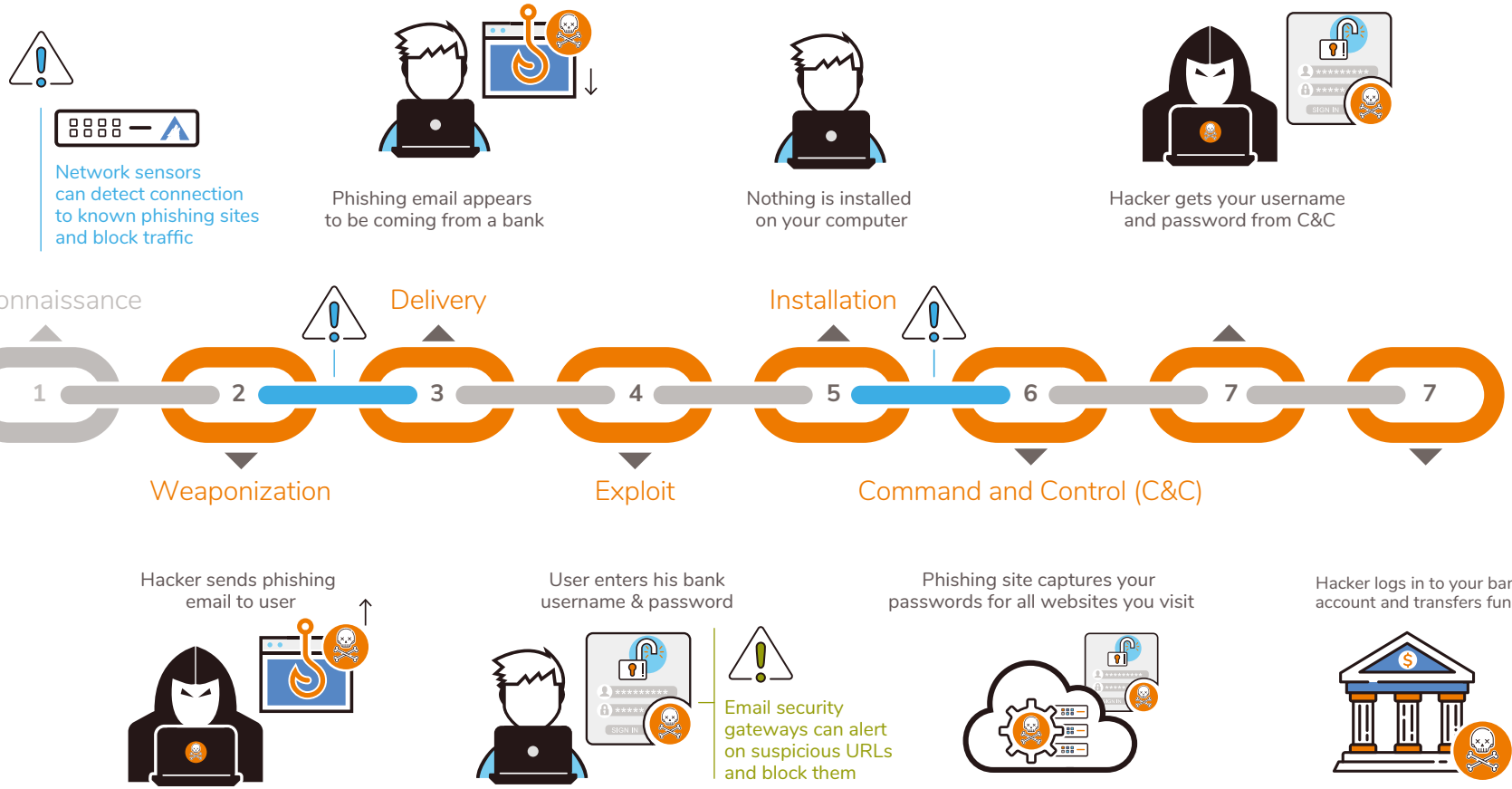
Malicious software that spreads via an email attachment or a link to a malicious website. It infects the endpoints when a user opens the attachment or clicks on the link.



Protecting Against

Phishing Attacks

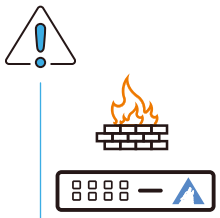
Malicious email that tricks users to surrender their user credentials. The email may appear legitimate, as if coming from your bank, and ask you to reset your password.



Protecting Against

Potentially Unwanted Programs/Adware

Potentially unwanted programs (PUPs) are trojans, spyware, or adware that surreptitiously monitor your keystrokes, scan files on your hard drive, and read your browser cookies.



Firewalls or network sensors can detect connections to known PUP download sites and C&C servers

PUP is delivered as update from known software download portals

PUP as a startup program annoying you with a pop-up at regular intervals

Hacker makes money by getting you to purchase software products

PUP/adware is bundled with "free" apps on suspicious software portals

No exploit required since you have approved the software download

PUP contacts C&C sites to download actual app for purchase

Protecting Against

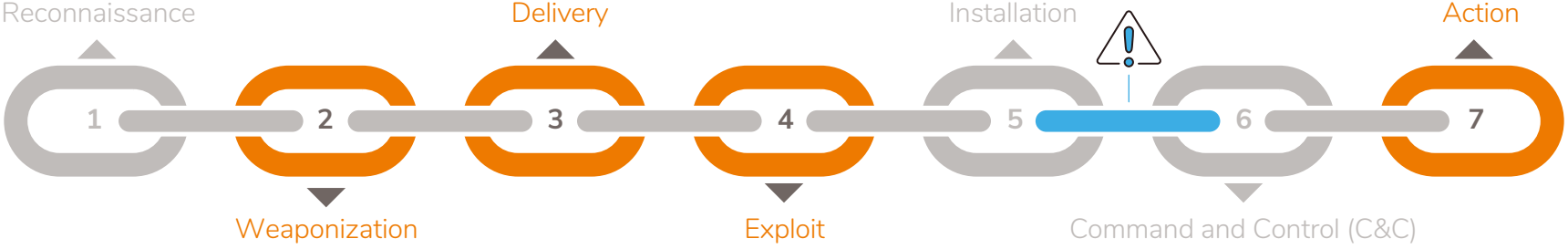
Account Hijacking

Hackers gain access to user accounts by repeatedly entering in different “guesses” of stolen passwords or words from the dictionary with combinations of numbers until they successfully log in.

Uses command & control server to recruit botnets to do his dirty work

Security Operations Center (SOC) can detect account hijacking when it sees a successful login after multiple failed login attempts in a span of couple of minutes

Hacker breaks in to your account after trying 20 other accounts, transfers funds



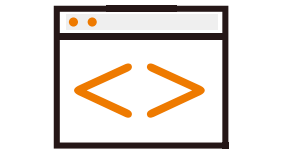
Hacker purchases a trove of stolen usernames/passwords from the dark web

Botnets try multiple usernames/ passwords to break into bank website

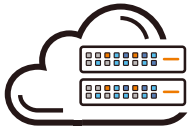
Protecting Against

Unpatched/Outdated Software

Hackers exploit vulnerabilities in systems software and web applications to execute unauthorized code, enabling them to gain extra privileges or steal information.

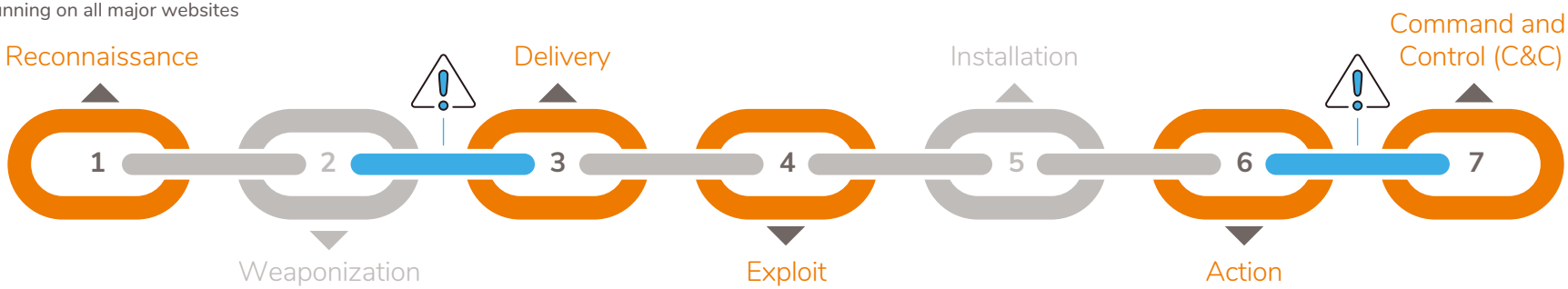


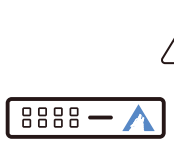
Hacker gets version number of web servers running on all major websites



Identifies unpatched version of Apache Struts web server

Hacker sells customer data for top dollars on the dark web





Network sensors detect anomalous probing requests to web servers, and connections to known C&C sites during customer data theft

Runs remote command to access database sitting behind web server

Hacker transfers customer confidential data from database to C&C sever

Why Focus on Detection and Response?

Identify

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

Protect

- Access Control
- Awareness and Training
- Data Security
- Information Protection Processes and Procedures
- Maintenance
- Protective Technology

Detect

- Anomalies and Events
- Continuous Monitoring
- Detection Process

Respond

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

Recover

- Recovery Planning
- Improvements
- Communications

Requires Managed Detection and Response

Why Focus on Detection and Response?

Lower Your Cost of Handling Security Breaches by Speeding Up the Time to Identify and Contain the Attack

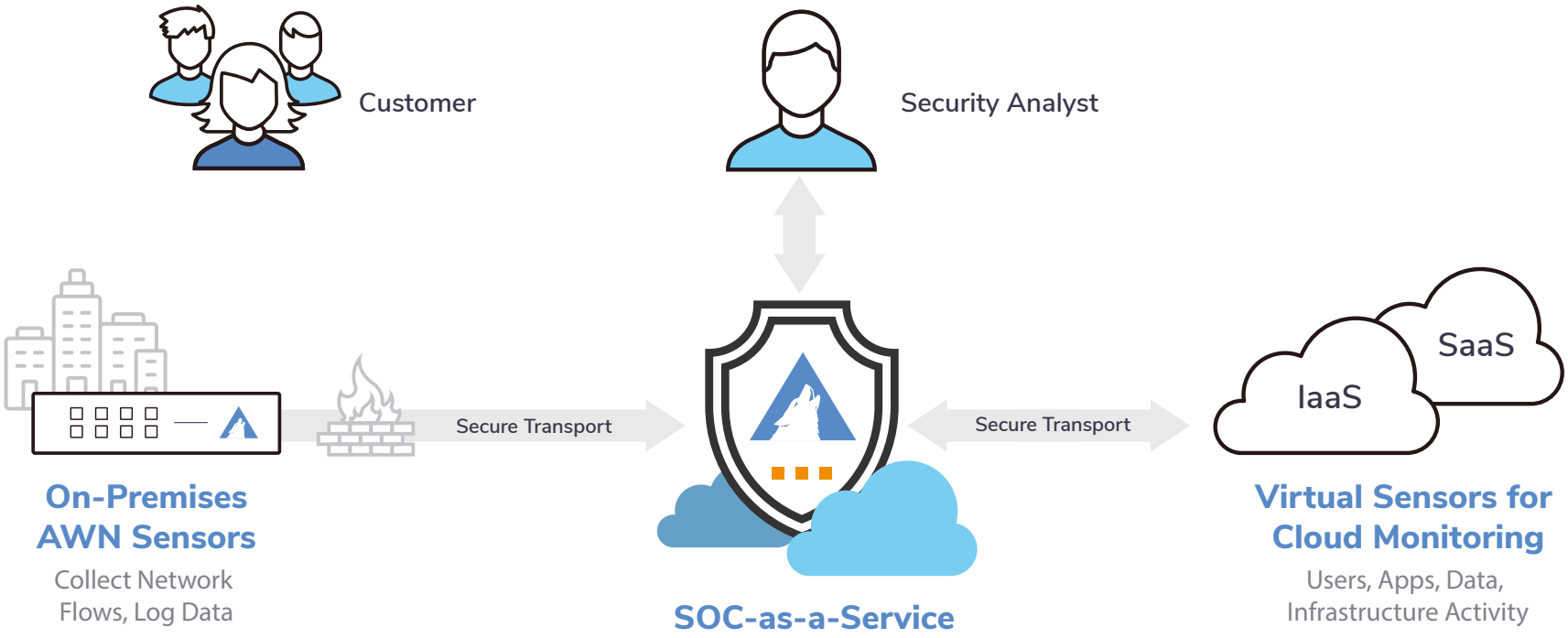
53%
of Cost Per Breach Is Spent on Detection and Response

Mean Time to Identify (MTTI) Malicious and Criminal Attacks

Mean Time to Contain (MTTC) the Attack

Source: 2017 Ponemon Cost of Data Breach Incident Report

Essential Components for Protection



- Managed detection and response
- Fully managed cloud-based SIEM
- Human-assisted machine learning
- External threat intelligence included
- 24x7 monitoring and alerting
- Compliance reporting
- Cloud monitoring – IaaS, SaaS, SecaaS
- Periodic external vulnerability scans
- Advisory services – FW, AD, IR audits
- Simple, predictable pricing

Industry's Most Fierce SOC-as-a-Service

A security operation center (SOC) is the most essential element of modern security. But SOCs are expensive, complicated, and far beyond the reach of most small to medium enterprises (SMEs). So, many take the easy route and invest in security products, but not in the people and processes required to manage a SOC.

AWN CyberSOC™ differs from traditional managed security services. It is a dynamic combination of world-class Concierge Security Engineers (CSEs), advanced machine learning, and comprehensive, up-to-the-minute threat intelligence. Your CSE conducts both routine and non-routine tasks to protect you from known and emerging threats.

AWN CyberSOC™ provides:

- Dedicated security experts
- Managed detection and response
- Security incident and crisis support
- Regulatory compliance
- Simple, predictable pricing

For More Information
Call: 1-888-272-8249

Contact us
arcticwolf.com
ask@arcticwolf.com

Layer 7 Data Solutions
ARCTIC WOLF

www.arcticwolf.com