THREAT
iNTELLiGENCE

INTELLIGENT
SECURITY AUTOMATION

INTRODUCTION

Ty Miller

- Managing Director
- Threat Intelligence Pty Ltd
  https://www.threatintelligence.com
  https://evolve.threatintelligence.com

- CREST Australia New Zealand
  - Board of Directors
  - Technical Team Lead
  - Assessor

- Black Hat Asia Review Board

Security Researcher, Presenter and Trainer

• Black Hat Training	The Shellcode Lab
• Black Hat Training	Practical Threat Intelligence
• Black Hat Training	The Security Automation Lab
• Black Hat Presentation	Reverse DNS Tunnelling Shellcode
• Black Hat Presentation	The Active Directory Botnet
• Black Hat Webcast	The Best Way to Catch a Thief
• Hack In The Box Training	Practical Threat Intelligence
• Ruxcon Presentation	The Active Directory Botnet
• Ruxcon Presentation	BeEF Bind Shellcode
• Core Impact	DNS Channel Payload
• Co-Author	Hacking Exposed Linux 3rd Edition
• Presentation Mitigations	Machine Learning and Modern Malware
• Presentation	Modern Threat Detection and Prevention
• Presentation	Securing Your Startup to Secure Big Brands
• Presentation	Can your application be breached?

… and many more

OVERVIEW

Key Takeaways

- Understand the driver behind Security Automation and why it is so important
- Learn how to utilize Security Automation to maximize your security skills, resources and budgets
- How to streamline your operational security process through automated intelligence correlation and contextual awareness

WHY SECURITY AUTOMATION?

CYBER CRIME REVENUE

THREATINTELLIGENCE

$1T

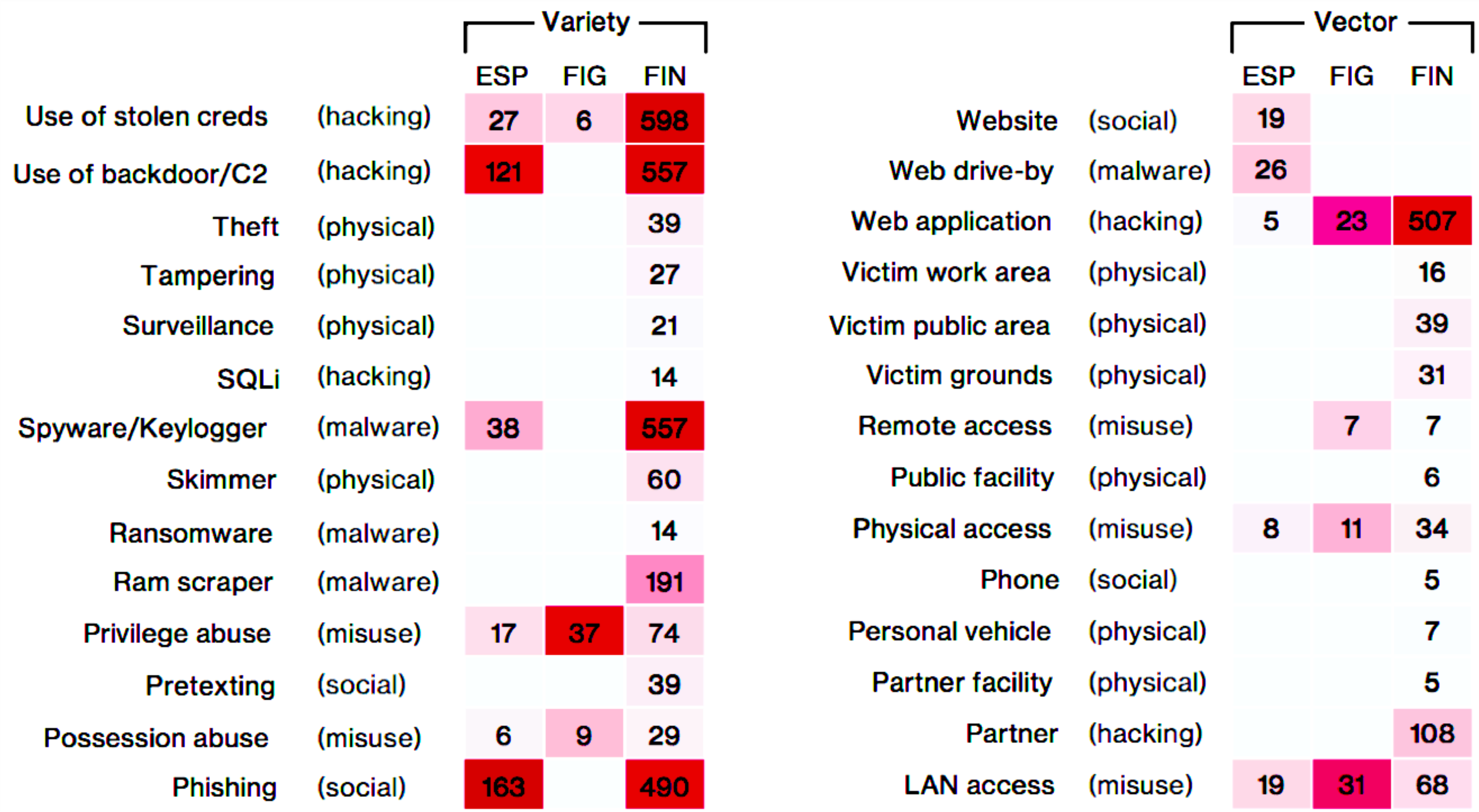
In 2009, revenues from cyber-crime exceeded drug trafficking as the most lucrative illegal global business, estimated at profits of over $1 Trillion annually.

In 2018, according to the UN, $800 billion - $2 trillion is laundered annually, mainly through crypto-currencies with an increase via in-game purchases.

$2T

ATTACKER MOTIVATIONS

THREATINTELLIGENCE



		Variety		
		ESP	FIG	FIN
Use of stolen creds	(hacking)	27	6	598
Use of backdoor/C2	(hacking)	121		557
Theft	(physical)			39
Tampering	(physical)			27
Surveillance	(physical)			21
SQLi	(hacking)			14
Spyware/Keylogger	(malware)	38		557
Skimmer	(physical)			60
Ransomware	(malware)			14
Ram scraper	(malware)			191
Privilege abuse	(misuse)	17	37	74
Pretexting	(social)			39
Possession abuse	(misuse)	6	9	29
Phishing	(social)	163		490

		Vector		
		ESP	FIG	FIN
Website	(social)	19		
Web drive-by	(malware)	26		
Web application	(hacking)	5	23	507
Victim work area	(physical)			16
Victim public area	(physical)			39
Victim grounds	(physical)			31
Remote access	(misuse)		7	7
Public facility	(physical)			6
Physical access	(misuse)	8	11	34
Phone	(social)			5
Personal vehicle	(physical)			7
Partner facility	(physical)			5
Partner	(hacking)			108
LAN access	(misuse)	19	31	68

** Verizon 2017 Data Breach Investigations Report - 10th Edition*

OPERATIONAL SECURITY TEAMS

Limited Security Budgets

- Security is an expense
- This means security budgets will always be limited

Limited Security Skills

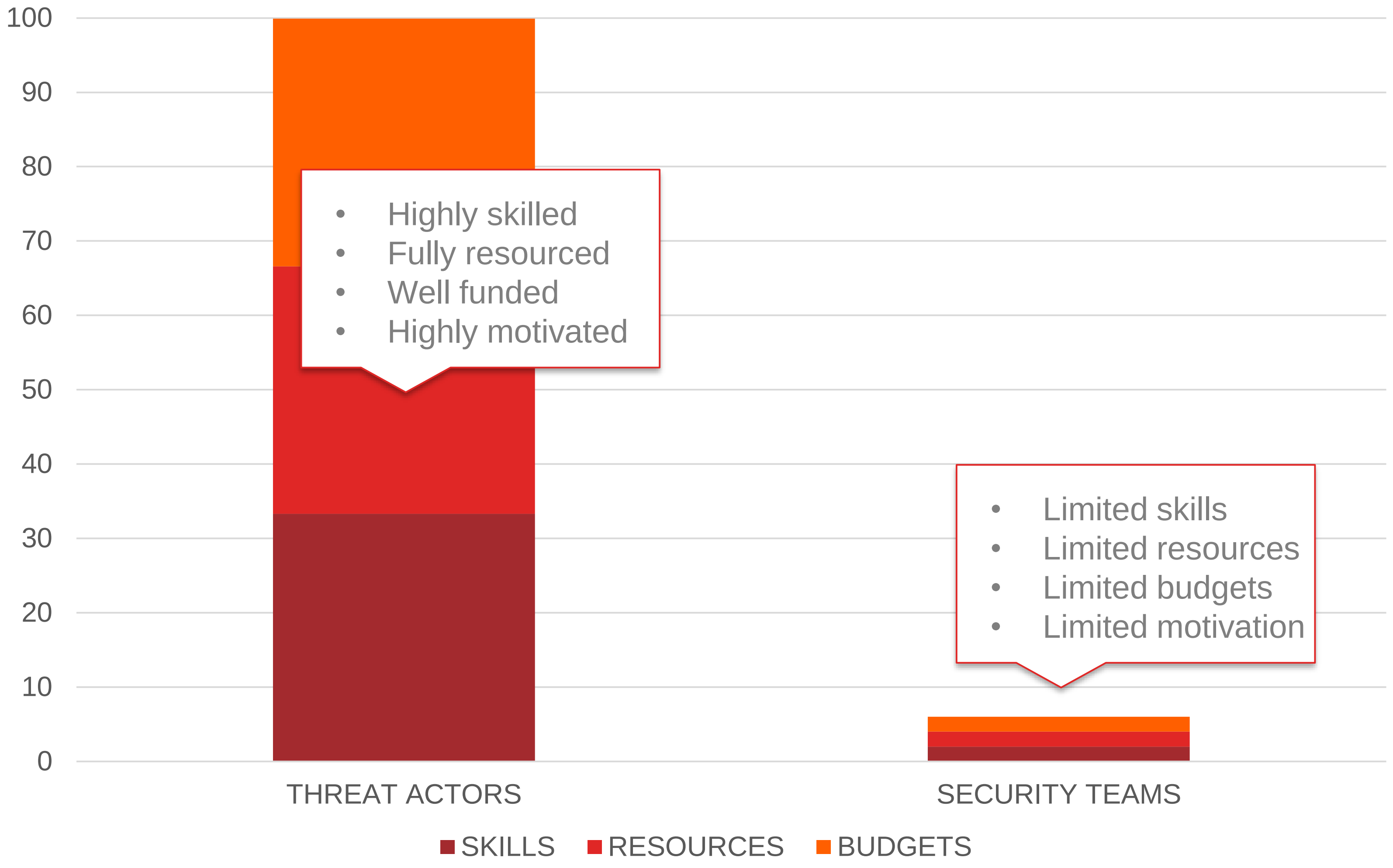
- No offence intended! Our industry has a very real security skills shortage
- Risk Managers, Security Managers and Security Officers have a wide range of security skills
- Often gaps in deep technical expertise, such as in-depth incident analysis and bypass techniques

Limited Security Resources

- Limited security budgets result in under-resourced security teams
- This means security teams focus on BAU or fight fires
- No time to implement strategic security, fix security flaws, threat hunt, or perform breach response

THREATS VS. DEFENDERS

THREATINTELLIGENCE



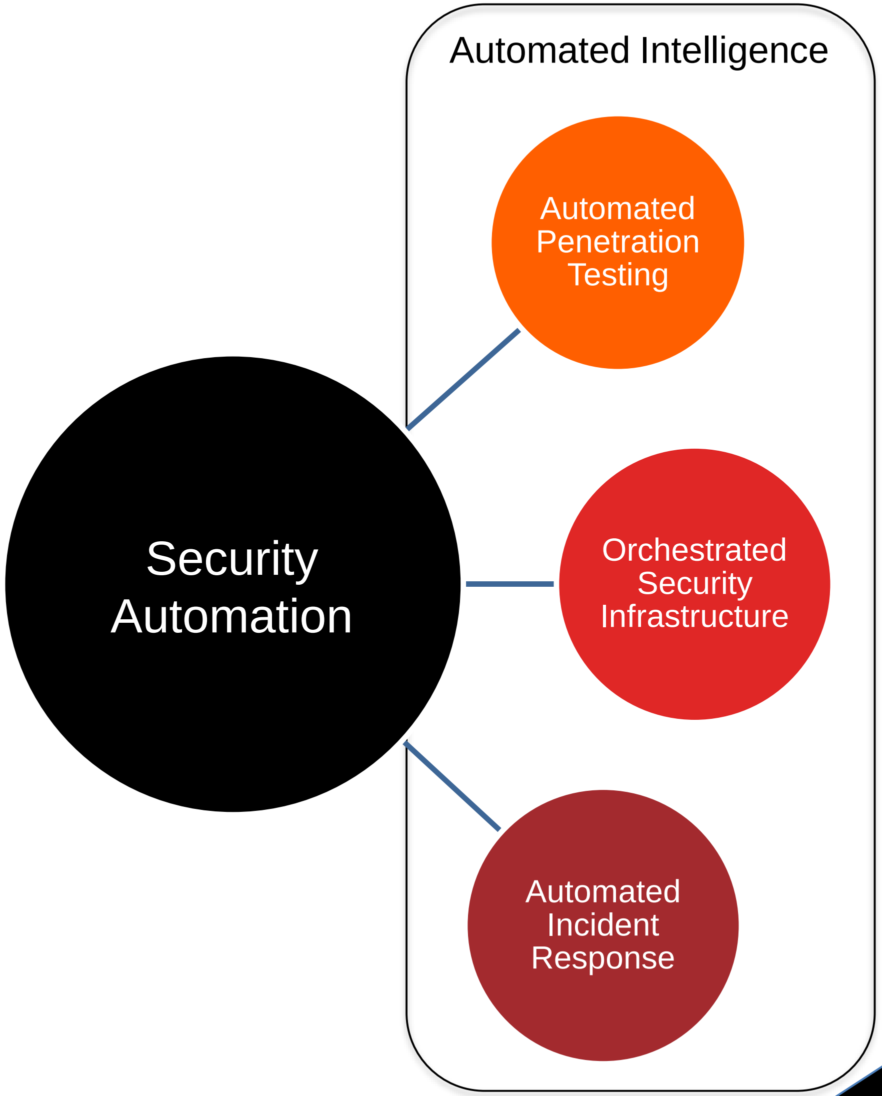
- Highly skilled
- Fully resourced
- Well funded
- Highly motivated

- Limited skills
- Limited resources
- Limited budgets
- Limited motivation

SECURITY AUTOMATION AND INTELLIGENCE

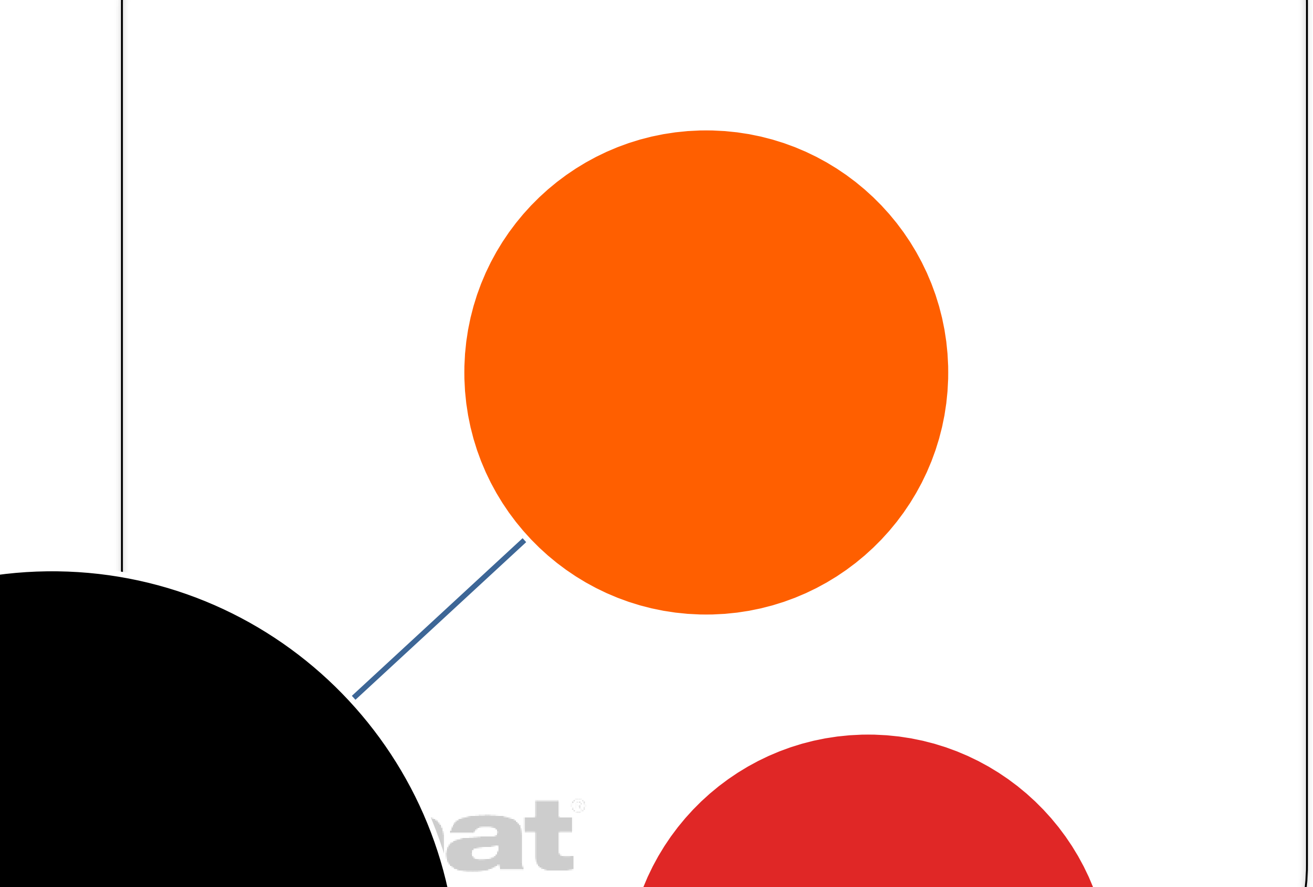
SECURITY AUTOMATION

- **What areas of security are prime for automation and orchestration?**
    - Automated Cyber Threat Intelligence
    - Orchestrated Security Infrastructure
    - Automated Incident Response
    - Automated Penetration Testing


Automated Intelligence
Security Automation
Automated Penetration Testing
Orchestrated Security Infrastructure
Automated Incident Response

AUTOMATED INTELLIGENCE

Automated Intelligence



- Automated Intelligence Collection
- Automated Intelligence Transformation
- Automated Intelligence Aggregation
- Automated Intelligence Analysis
- Automated Intelligence Sharing

EXTERNAL INTELLIGENCE

- **External Intelligence Sources**

A wide range of intelligence sources exist that can be used to:

- Gain an insight into threats
- Prevent attacks
- Detect security breaches
- Identify risky systems
- Identify risky employees
- Gain an insight into industry-based threats

- Malware Feeds
- Botnet Feeds
- TOR Feeds
- Phishing Feeds
- Scanner Feeds
- Spam Feeds
- Social Media Data
- Online Dump Sites
- Offline Password Dumps
- Defacement Archives
- Dark Web
- Vulnerability Feeds
- Exploit Feeds
- Intelligence Sharing

INTERNAL INTELLIGENCE

- **Internal Intelligence Sources**

Massive amounts of intelligence data exists within your organization that can be used to:

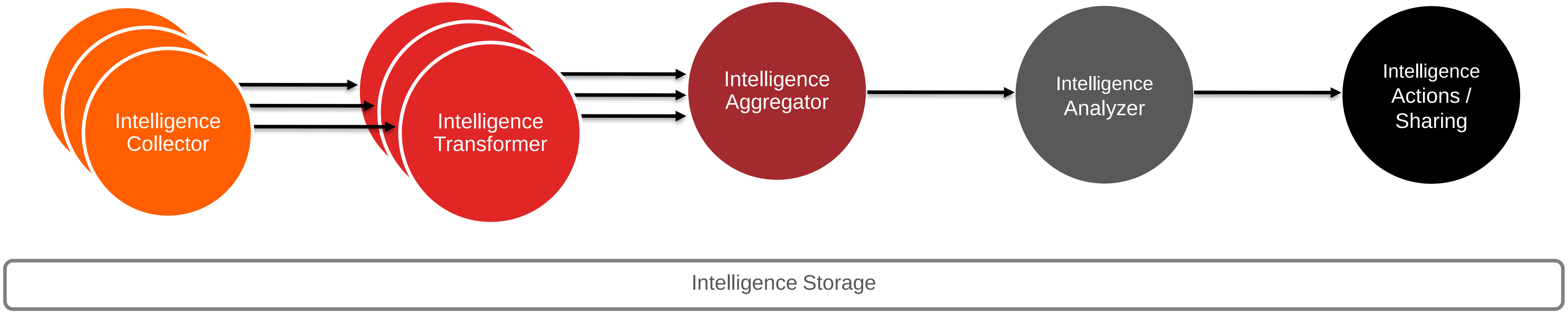
- Identify security incidents
- Provide context to threat activity
- Generate internal intelligence feeds
- Detect malicious network traffic
- Detect anomalous traffic
- Detect security breaches
- Identify risky systems
- Identify risky employees
- Identify compromised accounts
- Generate industry-based threat data

- Intrusion Detection
- Firewall Logs
- Web Application Firewall
- SIEM
- File Integrity Checks
- Application Whitelisting
- Anti-Virus
- Honeypots
- Honey Tokens
- DNS Sinkhole
- Web Proxy Content Filter
- Network Traffic Monitor
- Vulnerability Scanners
- Authentication Logs
- Host Events

AUTOMATED INTELLIGENCE

THREATINTELLIGENCE

How to automate the collection and analysis of intelligence data



- Collect relevant intelligence data for your strategic purpose

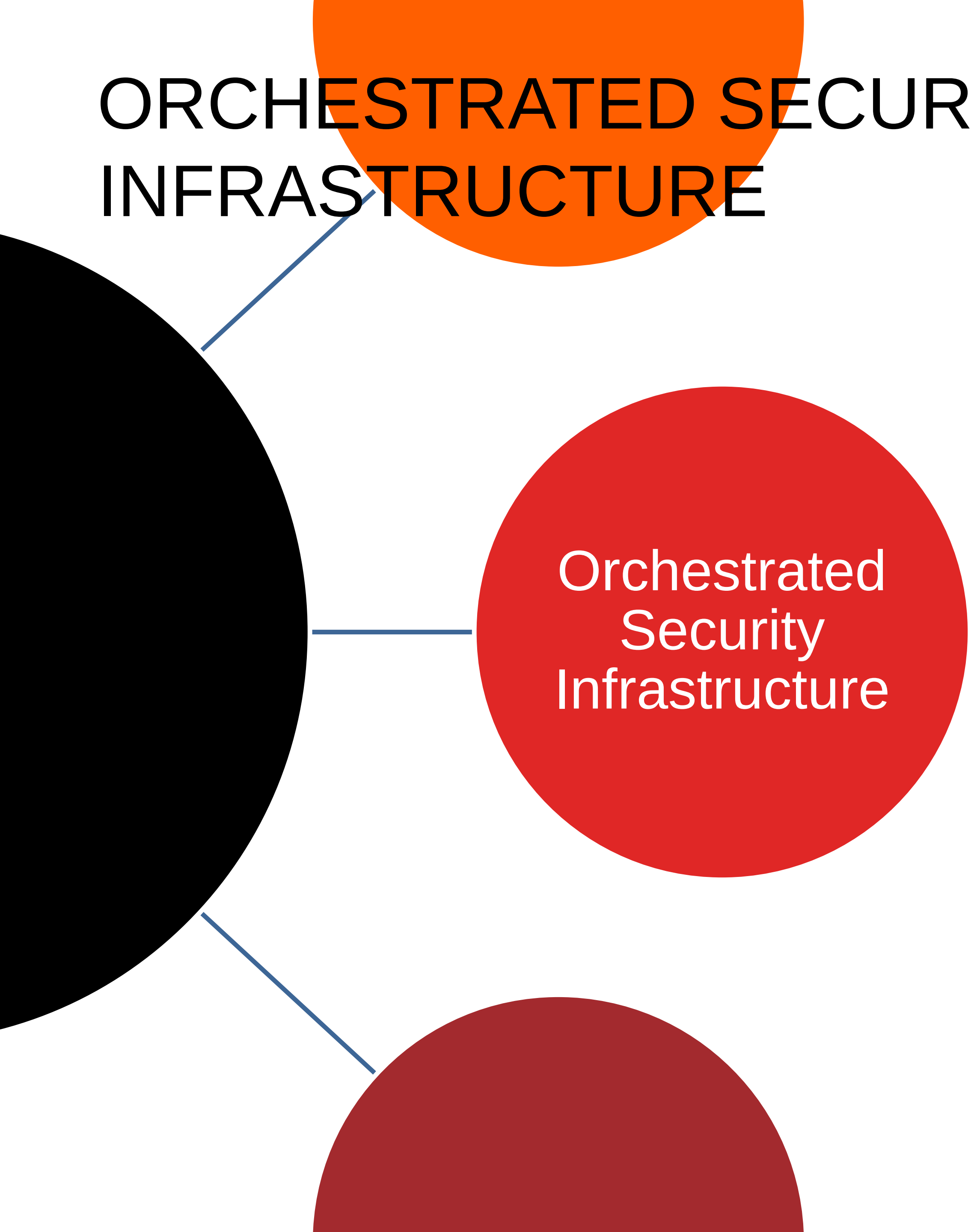
- Transform intelligence data into a normalized format removing irrelevant data and formatting

- Aggregate intelligence data into central data storage, such as a file or database

- Analyse the intelligence data potentially by correlating it with other data or intelligence sources

- Make a security decision based on the intelligence data and action it to prevent threats or contain breaches, or share the intelligence

ORCHESTRATED SECURITY INFRASTRUCTURE



- Orchestrated Security Infrastructure
- Automated Intelligence Integration
- Automated Incident Detection

INTELLIGENCE INTEGRATED SECURITY INFRASTRUCTURE

THREATINTELLIGENCE

- **DNS Sinkhole**
  - Utilize intelligence feeds to detect malicious domains and IP addresses being requested by internal systems to automatically identify security breaches.
- **Syslog Collector**
  - Utilize intelligence feeds to map internal syslog entries, such as proxy logs, to automatically identify security breaches.
- **Block List Server**
  - Utilize intelligence feeds to be served up by a block list server and pulled directly into firewalls and web application firewalls for automated protection.

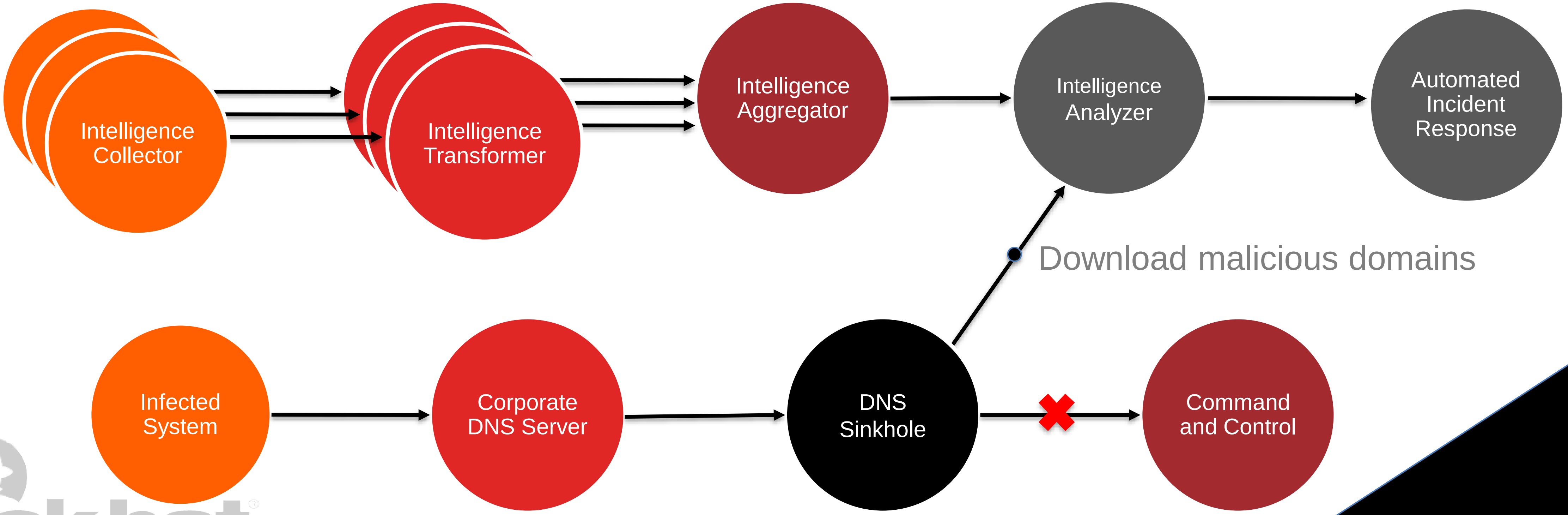
DNS SINKHOLE

Common Security Breach Flow

- Security Breach occurs
- Implant embedded into the system
- DNS lookup for Command and Control
- Connection to Command and Control
- Attacker remotely accesses the system

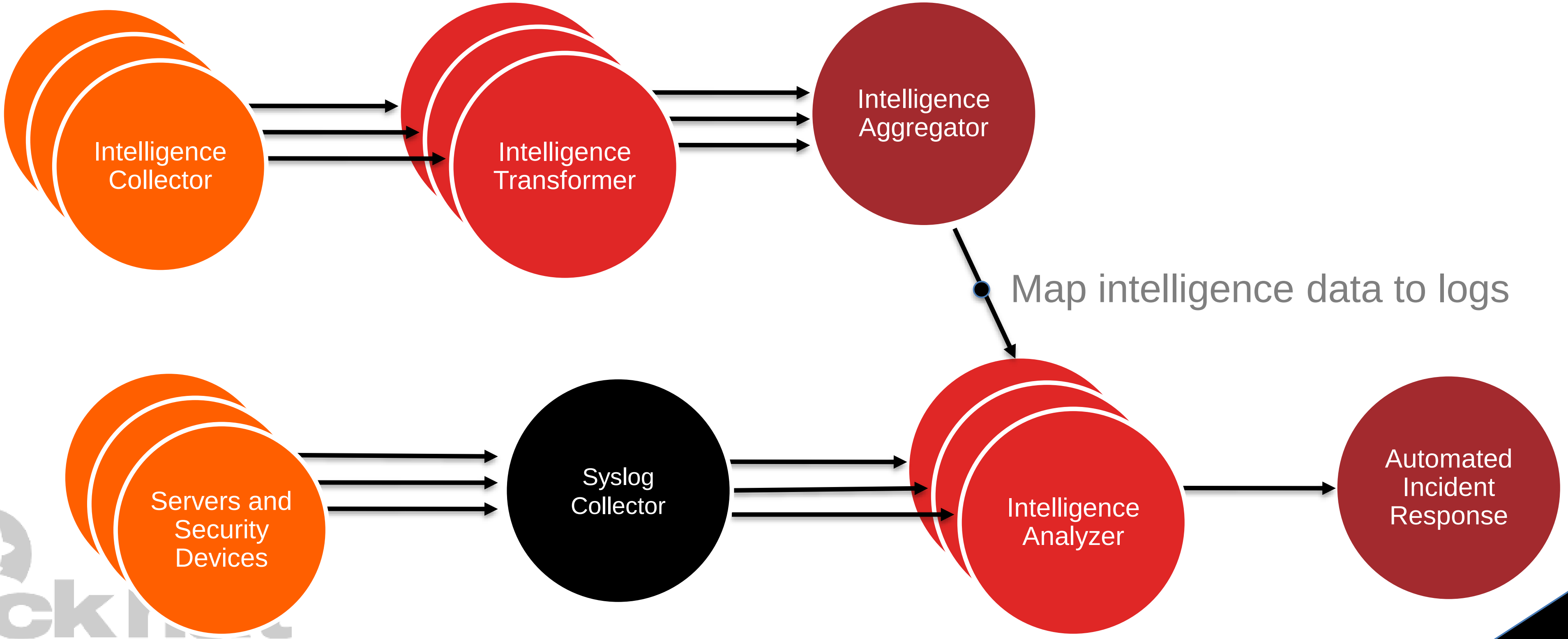
DNS Sinkhole Flow

- Security Breach occurs
- Implant embedded into the system
- DNS lookup for Command and Control
- Sinkhole blocks identified malicious domains



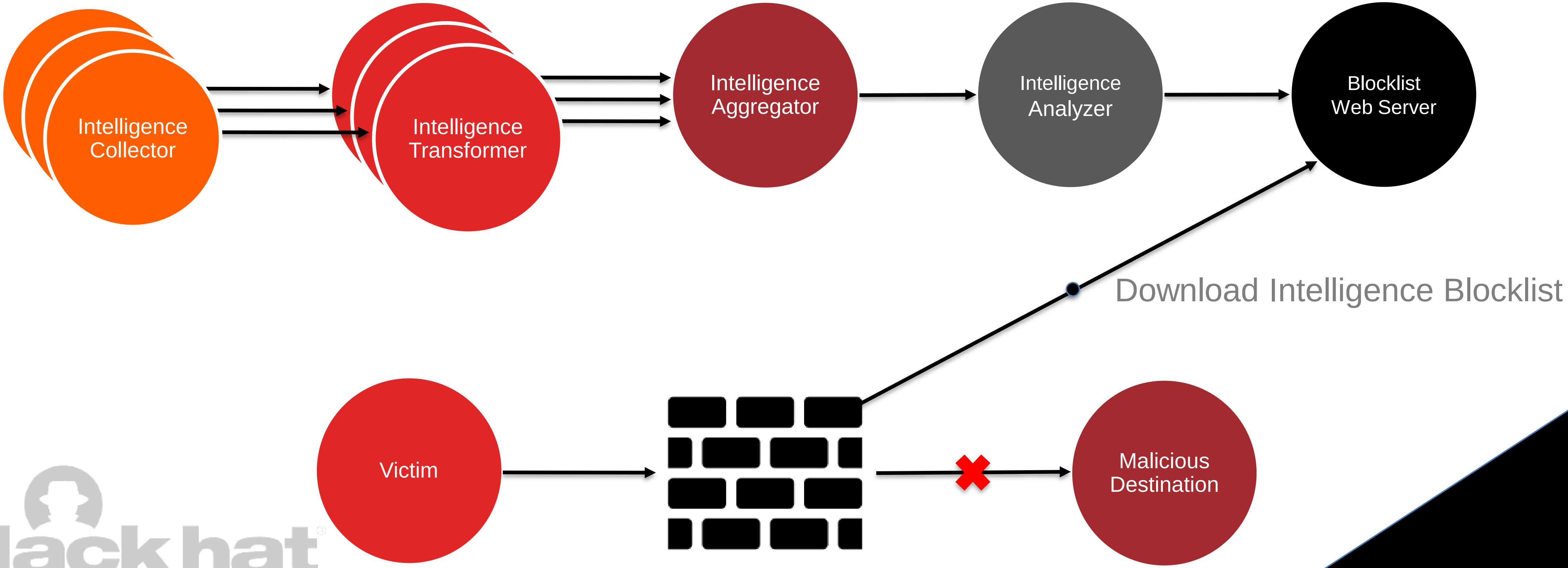
INTELLIGENT SYSLOG COLLECTOR

- Central log collection for evidence preservation and trust protection
- Long-term storage for compliance requirements
- Automated intelligence-integration for log analysis for automated breach detection
- Trigger security automation and incident response from logging events



INTELLIGENCE BLOCKLIST SERVER

- Cyber threat intelligence data collected and made available via a web interface
- Security devices, such as firewalls and WAFs, automatically download the intelligence data
- Malicious IP addresses, URLs or domain names are automatically blocked



AUTOMATED INCIDENT RESPONSE

THREATINTELLIGENCE

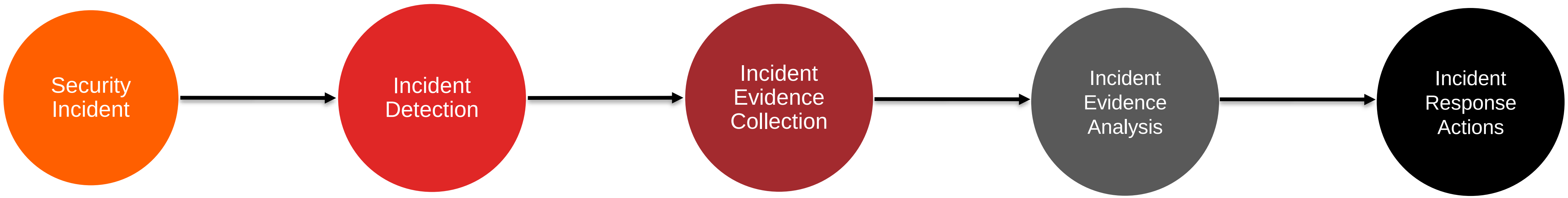
Automated Incident Response

- Automated Evidence Collection
- Automated Evidence Analysis
- Automated Incident Response Actions

black hat

AUTOMATED INCIDENT RESPONSE

End-to-End Automated Incident Response Activities



Security Incident → Incident Detection → Incident Evidence Collection → Incident Evidence Analysis → Incident Response Actions

- System is breached / Incident occurs

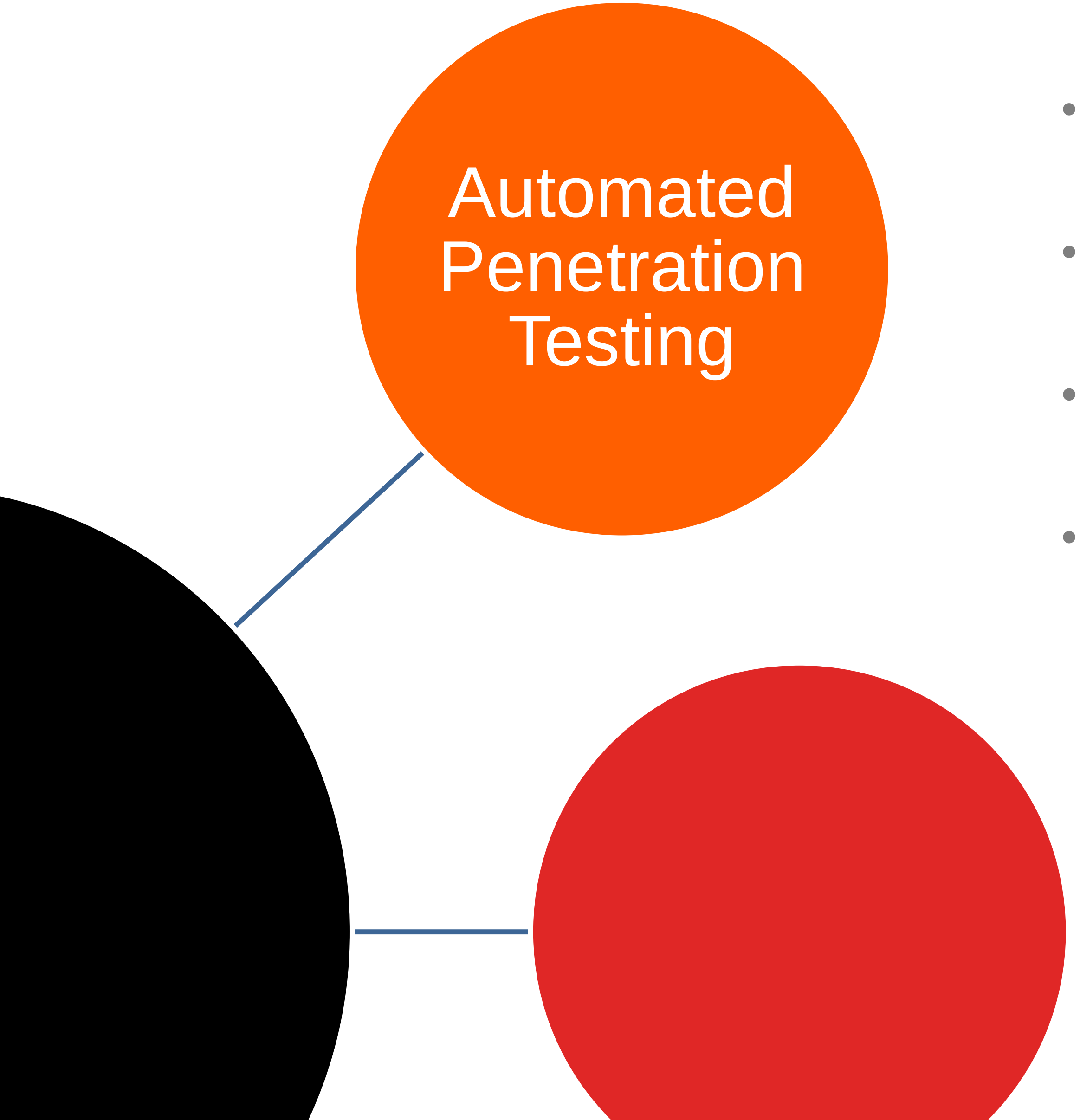
- Internal and external incident detection techniques used to automatically detect the security incident

- Automated evidence collection triggered to capture the security incident data from the victim system

- Collected evidence is then automatically analysed to identify various indicators of compromise and determine whether a breach has occurred

- Automated incident response actions are then triggered for compromised systems and accounts, customised for each business need

AUTOMATED PENETRATION TESTS

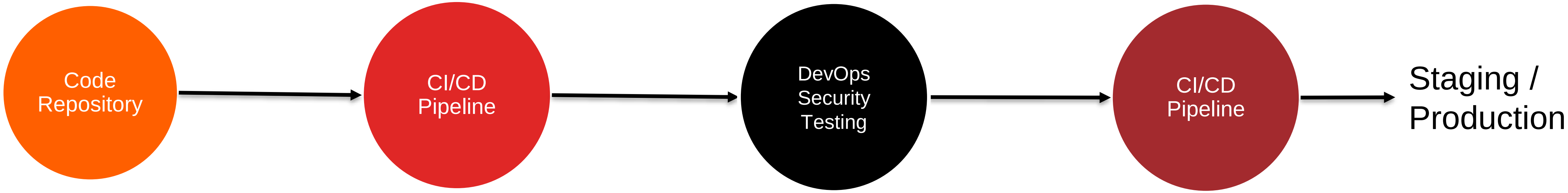


Automated Penetration Testing

- Automated Reconnaissance
- Automated External Infrastructure Penetration Testing
- Automated Internal Infrastructure Penetration Testing
- Automated DevOps Application Security Testing

AUTOMATED DEVOPS APPLICATION SECURITY TESTING

- **What is Automated DevOps Application Security Testing?**



Code Repository → CI/CD Pipeline → DevOps Security Testing → CI/CD Pipeline → Staging / Production

- Developer commits new code

- CI/CD pipeline detects new code
- Runs automated functional tests

- CI/CD pipeline runs automated application vulnerability scanner
- Import results into CI/CD pipeline

- CI/CD pipeline stops vulnerable code going into production

SECURITY AUTOMATION BUSINESS BENEFITS

- Repeatable and automated specialist security capabilities to immediately enhance your organization’s skills and capabilities

- Streamlines your security operations by automating security tasks, allowing security resources to focus on business-specific strategic security activities

- Security budgets are maximized by reducing the need for additional security resources, combined with subscription or usage-based billing

THANK YOU FOR ATTENDING

TY MILLER
MANAGING DIRECTOR

ty.miller@threatintelligence.com
https://www.threatintelligence.com
https://evolve.threatintelligence.com

THREAT
INTELLIGENCE