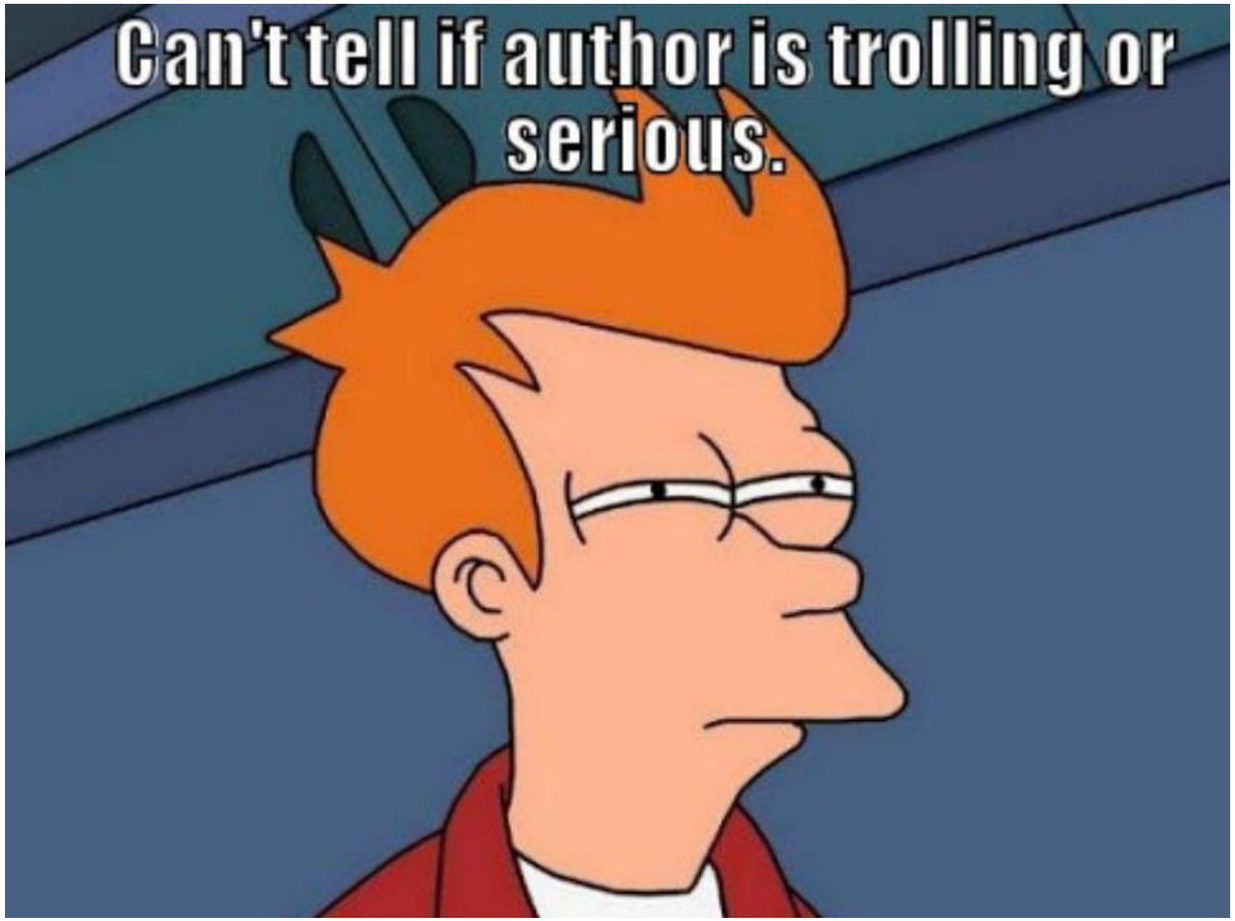
Security Automation – all you need to know

ISSA Polska – Stowarzyszenie ds. Bezpieczeństwa Systemów Informacyjnych,

Lech Lachowicz
Dyrektor ds. Profesjonalnego Rozwoju

Disclaimer



Who am I:
IT Security freak with decent background in dev
Global Threat Defense lead responsible for detections, hunting, automation and breach simulation
Big fan of opensource and automation

Who I'm not:
NOT a full time Developer
NOT A DEVOPS
NOT Alfa and Omega, you can actually do it differently

What is it going to be about:
Better SECURITY

Current security operations challenges

Increasing volume and complexity of attacks

67%

of organizations say volume of attacks is increasing

Expanding compliance and obligations

72 hours

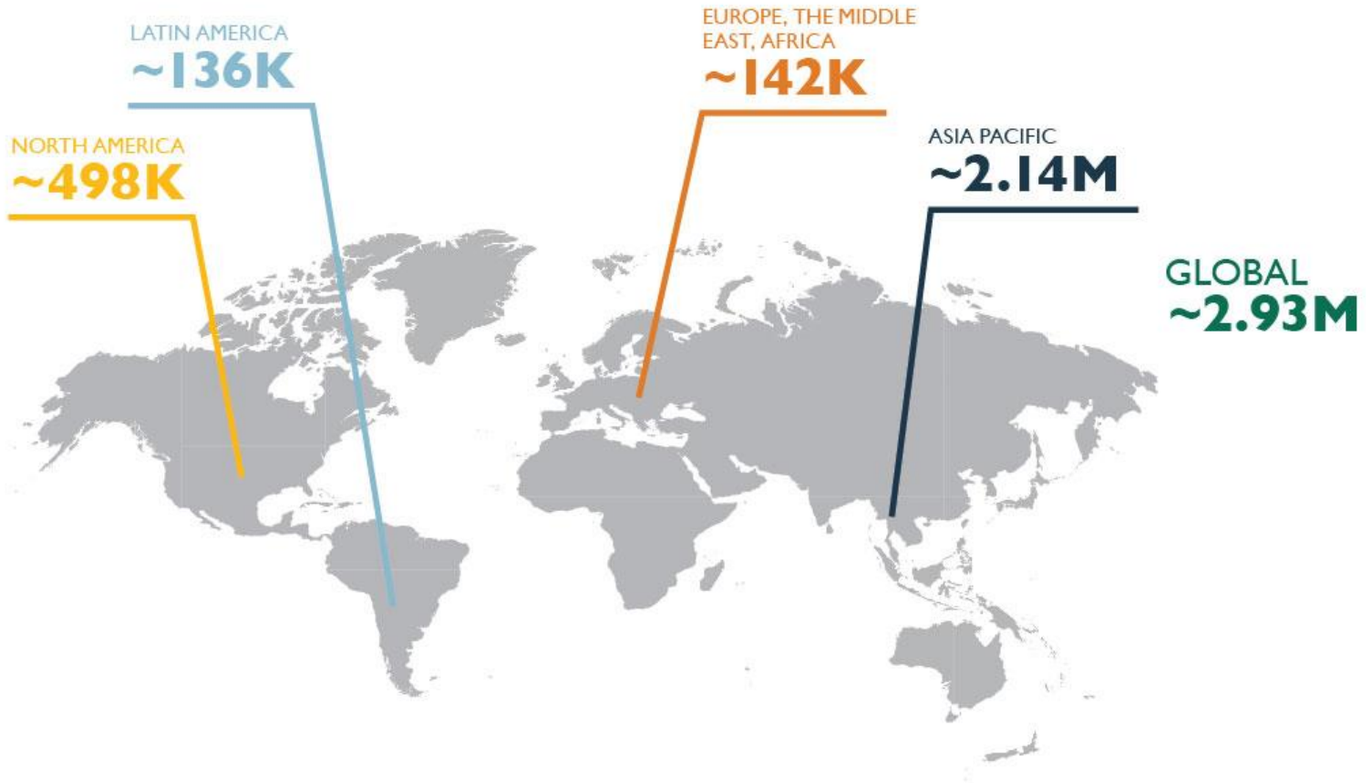
to comply with mandatory breach reporting for GPR

Challenging operational environments

26 or more

security products managed on average by organizations

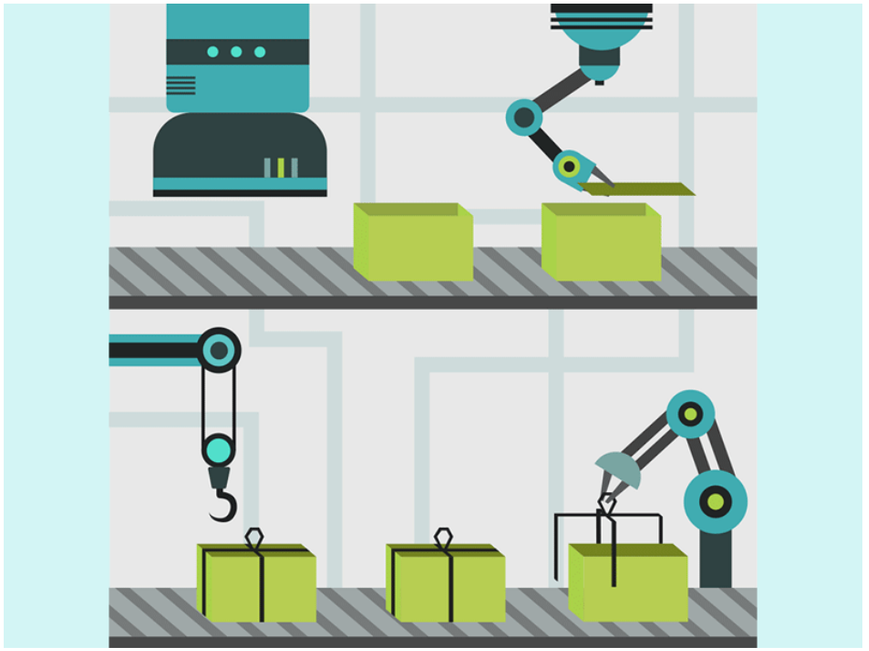
Skills shortage



Source: (ISC)²'s Cybersecurity Workforce Study, 2018

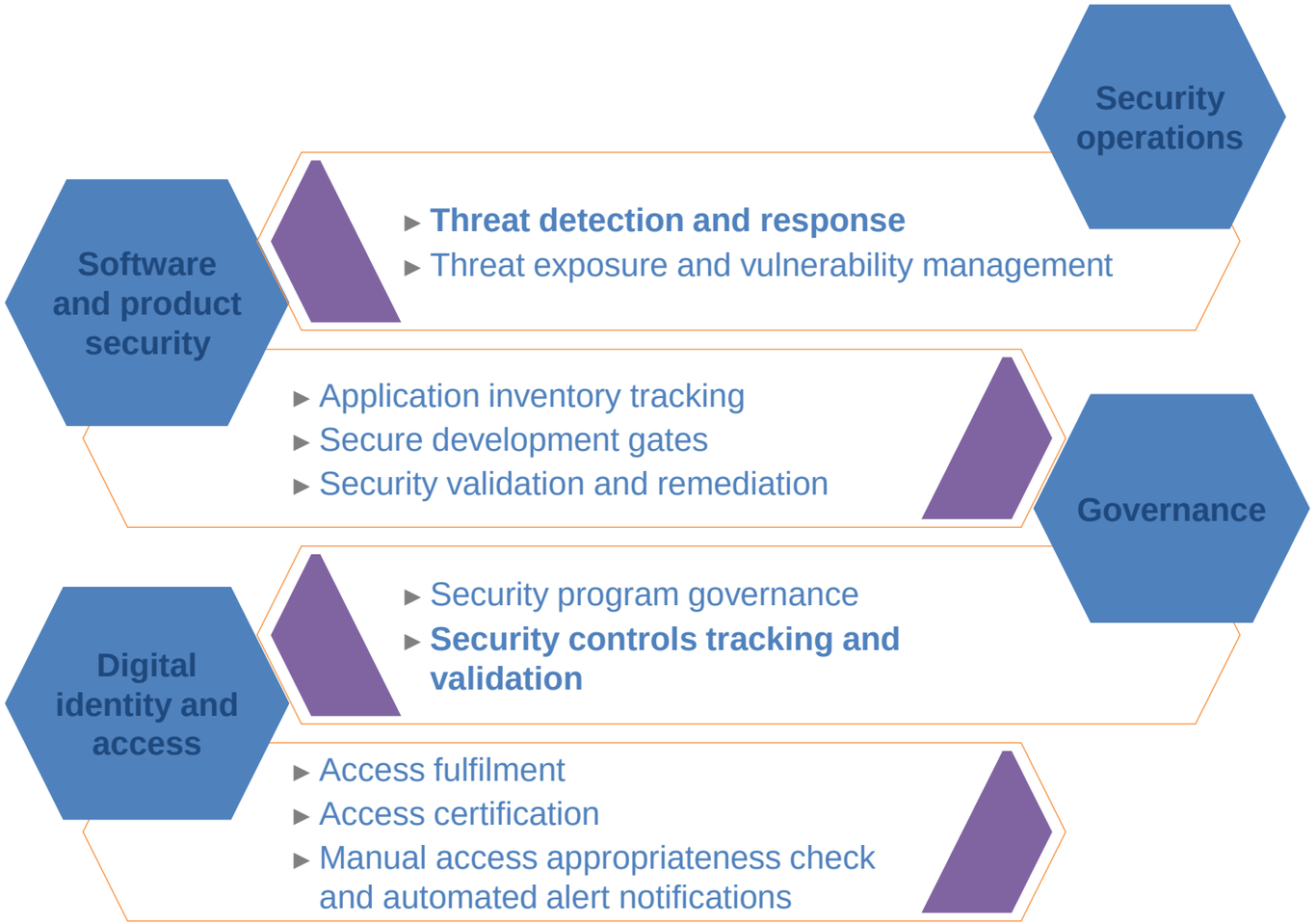
Security Operations need to

- **Minimize** duration and impact of cyber attacks
- **Optimize** SecOps and reduce staff burnout
- **Address** breach reporting requirements and show compliance
- **Maximize** security investments and scale insights across teams



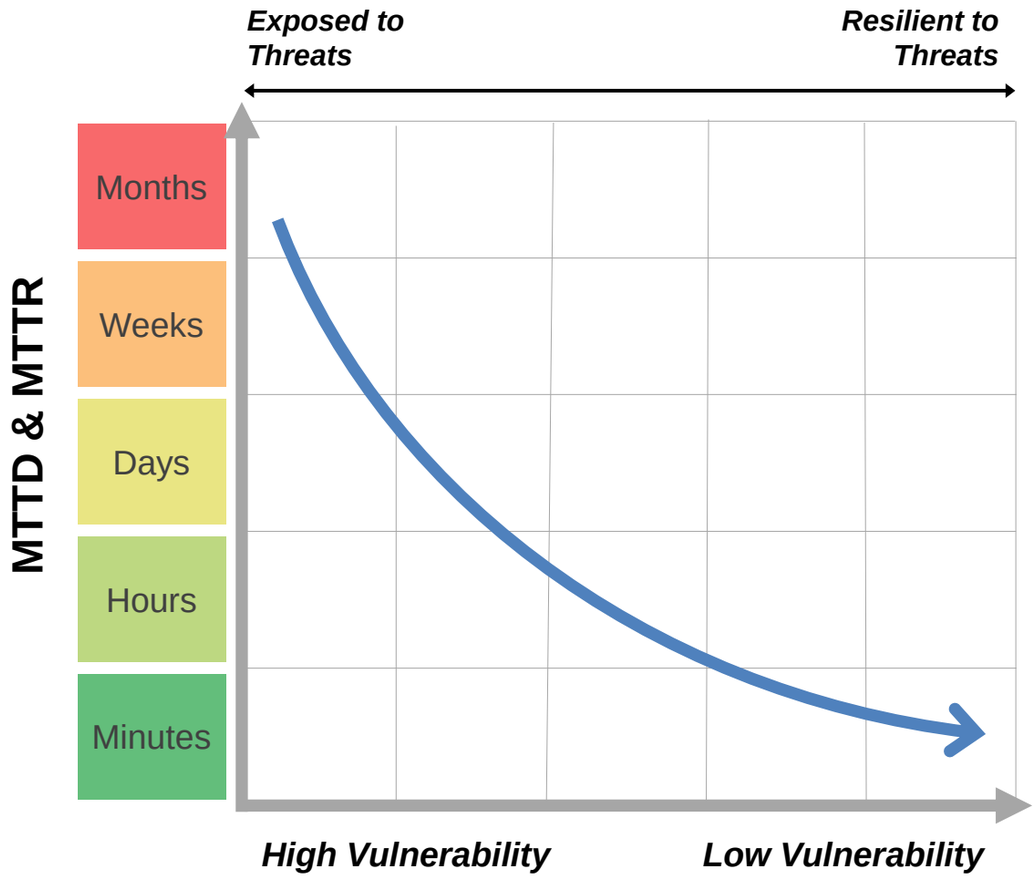
So we automate

Areas to automate



Threat Detection and Response

Key Parameters

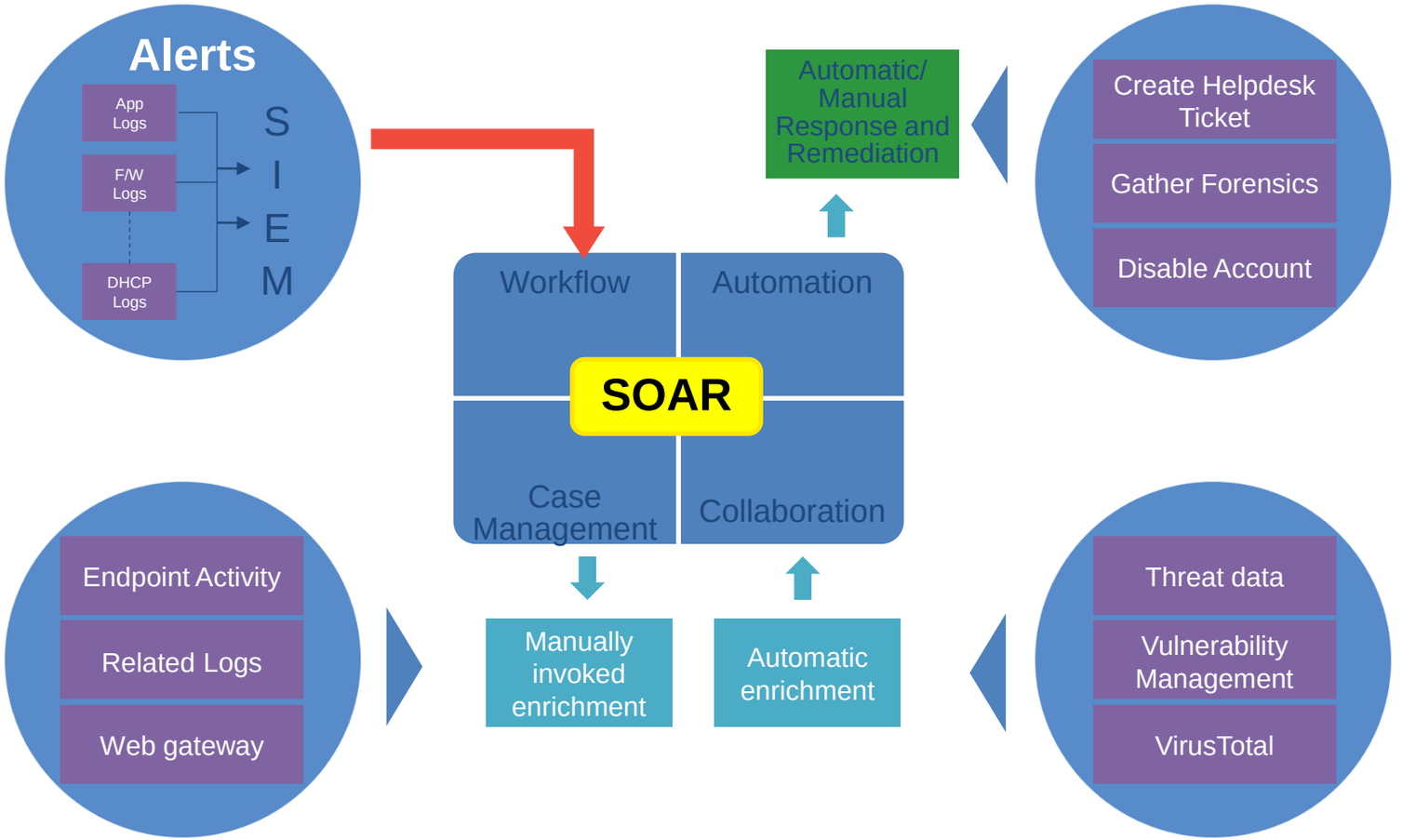


MEAN-TIME-TO-DETECT (MTTD)
The average time it takes to recognize a threat requiring further analysis and response efforts

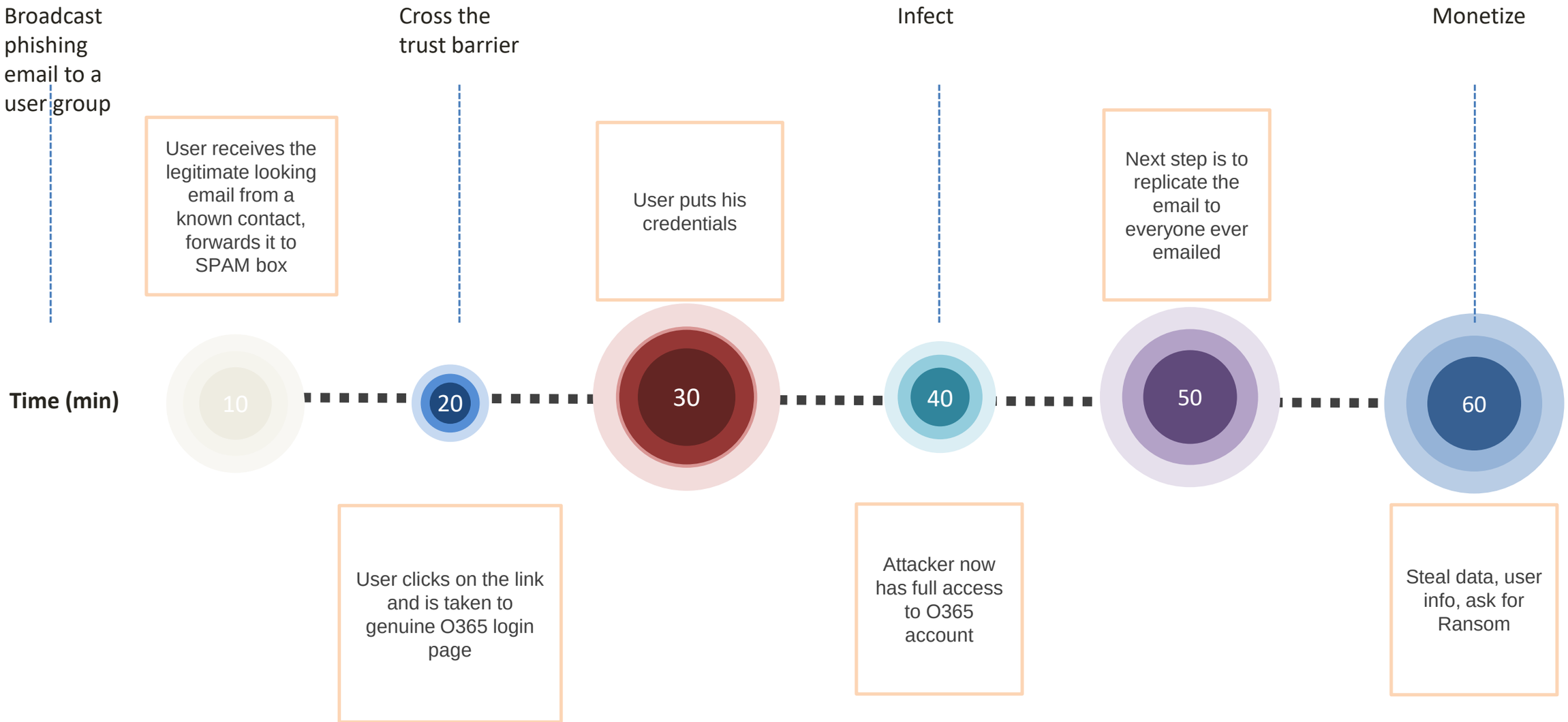
MEAN-TIME-TO-RESPOND (MTTR)
The average time it takes to respond and ultimately resolve the incident

As organizations improve their ability to quickly detect and respond to threats, the risk of experiencing a damaging breach is greatly reduced

Security Orchestration Automation and Response



Anatomy of phishing attack



The process for handling Phishing emails

#	Action	Current manual time spent (sec)	Current manual time spent - Explanation
A	Have a look at the email content	30	Need to download the email, open it and save a screenshot
B	Collect email header	60	Need to grab the email header then run it into a parsing script/tool and finally attach the data into the ticket
C	Check URL & determination	300	Need to manually check it against VT/OSINT, test it within Safe Browser and document it into IOC feeds. Finally determine if bad
D	Check attachment & determination	300	Need to grab the sample, detonate it manually in Sandbox, create IOC and attach the report into Incident
E	Check downloaded malware & determination	300	Need to grab the sample, detonate it manually in Sandbox, create IOC and attach the report into Incident

The times after automation

#	Action	Current manual time spent (sec)	Current manual time spent - Explanation	New manual time spent (sec)	New manual time spent - Explanation	Manual time saved (sec)
A	Have a look at the email content	30	Need to download the email, open it and save a screenshot	5	Screenshot already present in the Incident	**25**
B	Collect email header	60	Need to grab the email header then run it into a parsing script/tool and finally attach the data into the ticket	5	Header already displayed in the Incident, with quick spoof check for determination	**55**
C	Check URL & determination	300	Need to manually check it against VT/OSINT, test it within SafeBrowser and document it into IOCs. Finally determine if bad	120	OSINT is automatically gathered, and IOCs created. URL is detonated in Sandbox. Use Sandbox score and OSINT for determination.	**180**
D	Check attachment & determination	300	Need to grab the sample, detonate it manually in Sandbox, create IOC and attach the report into Incident	60	IOC already created with Sandbox report, for quick determination	**240**
E	Check downloaded malware & determination	300	Need to grab the sample, detonate it manually in Sandbox, create IOC and attach the report into Incident	60	IOC already created with Sandbox report, for quick determination	**240**

Demo

- Lets build a sample playbook.


Breach Attack
SIMULATION

Breach and attack simulation platform

A tool for Security Control Validation

Simulate TTPs to test defenses

Visualize exposures with data-driven results

Holistically remediate to defend infrastructure

Sample Breach Simulation Scenarios

Security Control Validation

- Organization wide Security Posture
- Posture Assessment per OU/BU
- Environmental Drift Detection
- MITRE ATT&CK Assessment
- Endpoint Techniques Assessment
- Email Security Assessment
- Perimeter Validation
- Data Leakage Assessment
- Segmentation Control Validation
- Compare Security Controls Efficacy
- SOC/IR Validation
- M&A Risk Assessment

Threat Assessment

- Imminent Threat Assessment
- MITRE Threat Actor Assessment
- TI Integrated Assessment

Cloud Security Assessment

- Cloud Threats Assessment
- CWPP Control Validation
- Configuration Control Validation

Risk Based VM

- Vulnerability Prioritization
- Vulnerability Prioritization by Threat

Organization wide Security Posture

Description

- Assessment of overall **security posture** based on continuous baseline assessment and **tracking over time**
- Produce **risk reports** to track at the executive level
- Produce **operational reports** to drive remediation processes

Benefits

- **Uniform KPIs** across organization and programs
- **Common terminology** across different teams
- Track program **progress over time** against a clear target
- Proven **attack surface reduction** based on data
- Prove overall **effectiveness**

Examples

- Validating security controls effectivenes for different assets and environments

Users / Roles

- Security Operations
- CISO & Executives

Environmental Drift Detection

Description

- Continuous evaluation of security posture on a **target environment** against a **baseline performance**
- **Monitoring deviations** from the baseline performance
- Baseline performance can be defined in terms of **detection, prevention or both**
- Can target **static/dynamic threat landscape** to measure

Benefits

- Ensure a certain **performance level** is maintained against a threat or a reference set of attacks.
- **Alert on deviation** and reduce time to resolution
- Clear **remediation steps** to return to baseline

Examples

- Corporate network vs. Remote Workforce Threats
- Production DC vs. Data Theft
- Corporate vs. Credential Access
- Validating Alerting state

Users / Roles

- Security Engineering
- SOC
- Security Managers

Segmentation Control Validation

Description

- Comprehensive validation of **Network security** against Lateral Movement attacks and techniques
- **Lateral movement** and **credential abuse** validation
- Wide **threat coverage** and **malware infection** techniques between hosts in the network

Benefits

- **Focus** on **segmentation** security and ability to enhance email security gateway coverage
- Validation of segmentation security posture over time against an evolving **threat landscape**
- Enablement of remediation efforts on a **defined scope**

Examples

- Validation of network security vs. Brute Force techniques
- Validation of windows networks remote control techniques
- Validation of network inspection vs. Ransomware propagation attacks
- Validating Azure NSG Deployment.

Users / Roles

- Security Operations
- Network Security
- Security Managers

MITRE Threat Actor Assessment

Description

- Assessment of overall **security posture** vs. a **threat actor** TTPs
- Evaluate overall **organization risk vs. a threat actor.**
- Produce **operational reports** to understand gaps and plan remediation

Benefits

- **Consistent** assessment and ability to review change over time
- **Focus** on relevant threats for the organization
- Clear **quantifiable data** on security posture

Examples

- Assessment of security posture vs. APT29 TTPs

Users / Roles

- Security Operations
- Threat Intelligence
- CISO & Executives

Cloud Threats Assessment

Description

- Assessment of **cloud security** posture vs. cloud specific threats.
- Evaluate overall cloud security posture vs. a **cloud baseline** set of attacks and techniques.
- Produce **operational reports** to understand gaps and plan remediation

Benefits

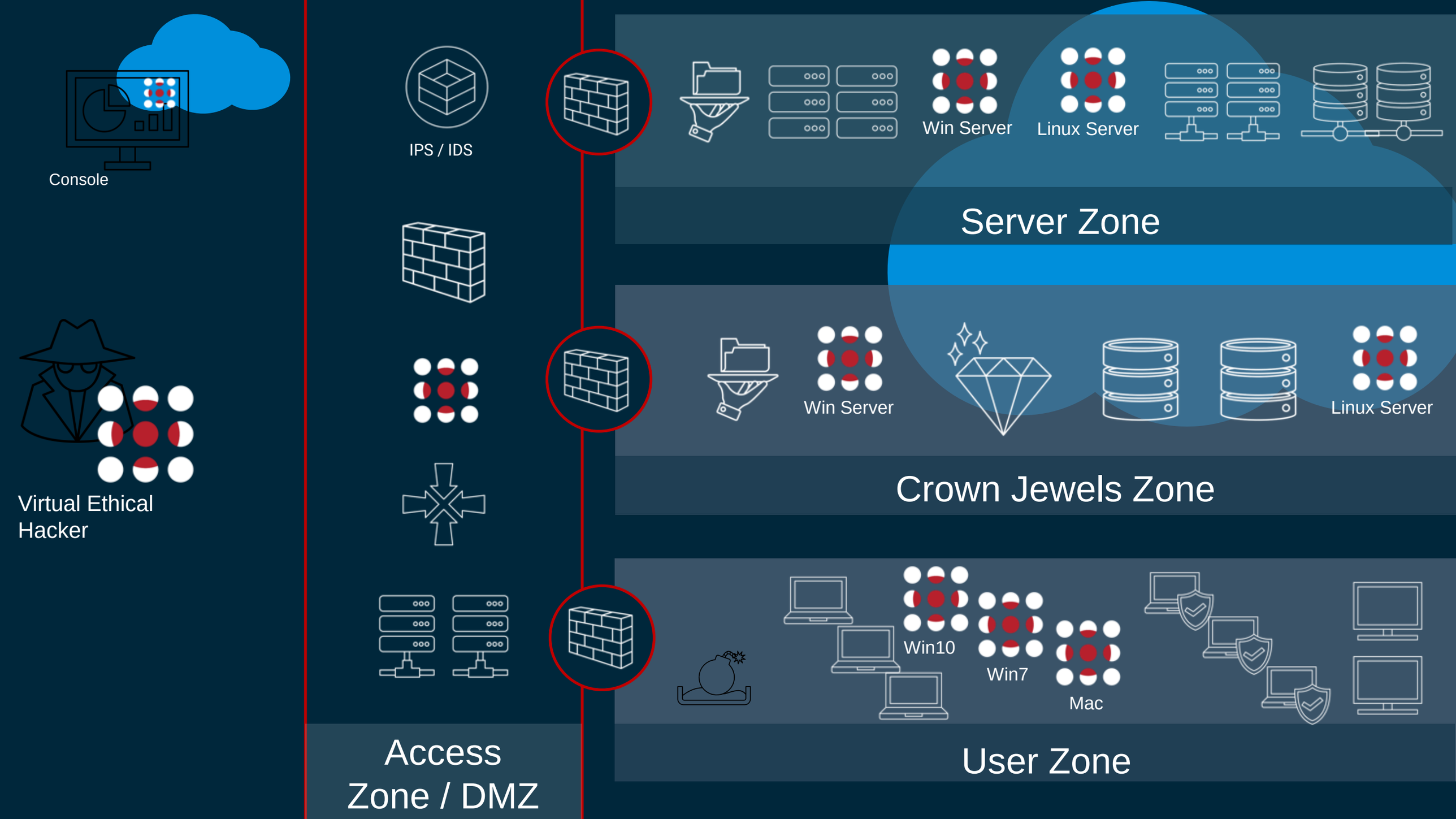
- **Consistent** assessment and ability to review change over time
- Ability to take a data driven approach to **enable cloud transition**
- Validate **enforcement of cloud policies** and generate **visibility to effectiveness**

Examples

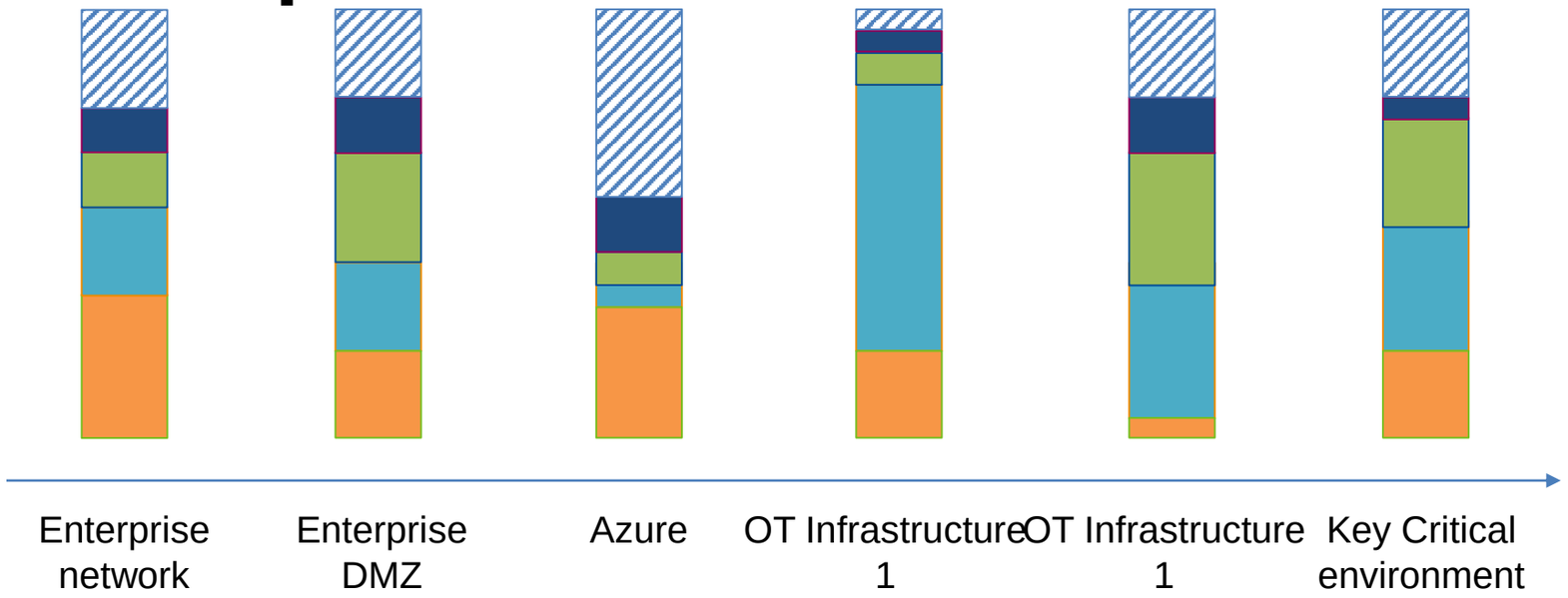
- Assessment of overall cloud security posture vs. SafeBreach cloud baseline
- Assessment of overall cloud security program based on MITRE ATT&CK
- Assessing visibility and understanding the gaps in newly created Azure subscriptions.

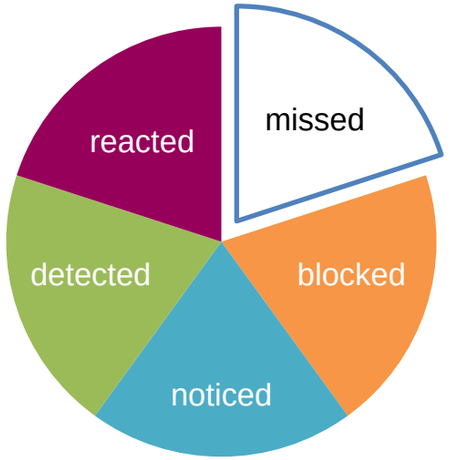
Users / Roles

- Security Operations
- Cloud Security
- CISO & Executives


Console
IPS / IDS
Win Server
Linux Server
Server Zone
Virtual Ethical Hacker
Win Server
Linux Server
Crown Jewels Zone
Win10
Win7
Mac
User Zone
Access Zone / DMZ

Sample Dashboard





Detection efficacy for “in the wild” scenarios

Missed – no signals from security tools

Noticed – security tools signaled activity (event has been generated) but no alert has been generated

Blocked – security tools blocked the threat

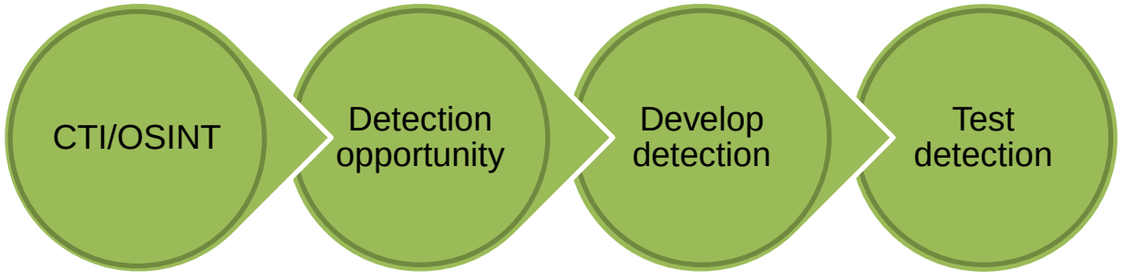
Detected – security tools signaled activity and alert has been generated but not escalated for remediation

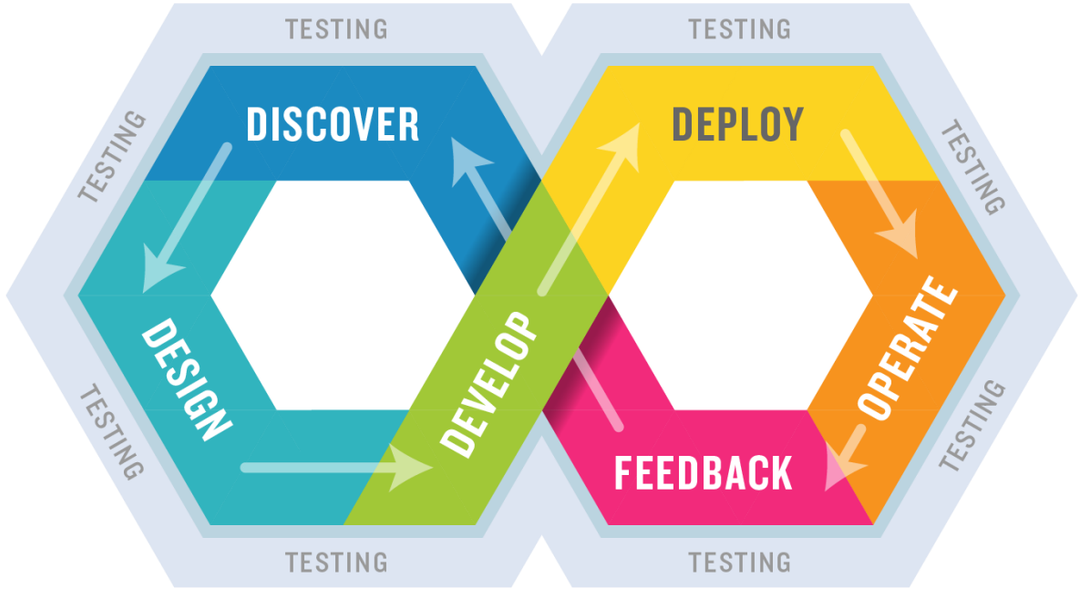
Reacted – security tools signaled activity and alert has been generated, IR has been notified via SIR

Demo

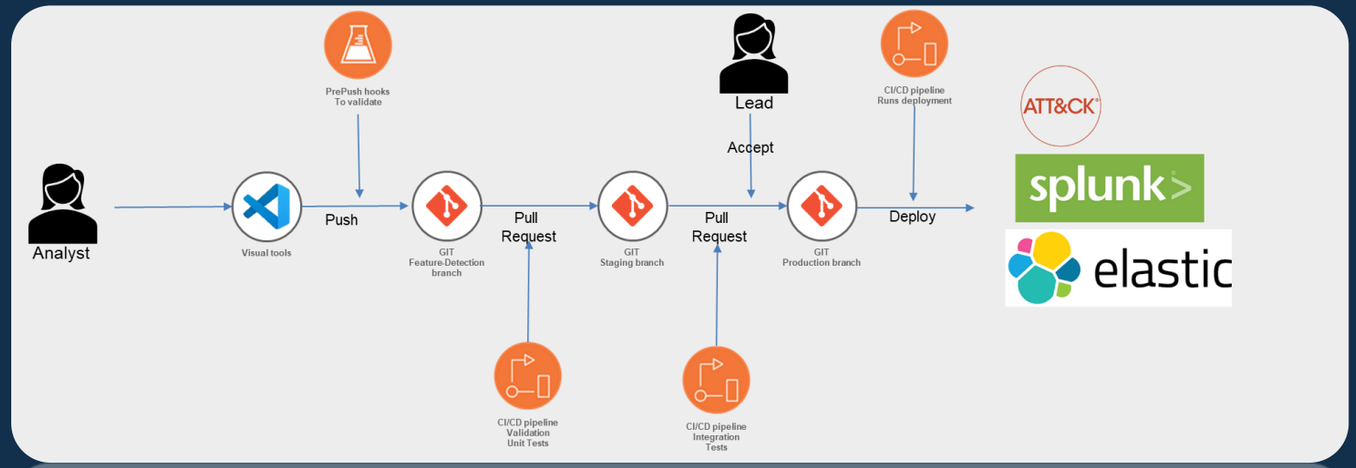
- Lets build a sample scenario.

Shift Left Detection





Detection Pipeline



- Multiple approvers
- Automated testing (basic linting and integrations)
- Importers from other detection sources (Sigma, SSC etc).
- Reporting
- Continuous validation

The benefits

Reliable

Operate 365 days a year!

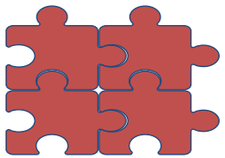
Retention

Freed up human resources for higher value-added tasks

Productivity

Accelerate detection and response

Consistent



Eliminating variations in processes

ROI

20–35% savings

Fast

Automatically deploy security controls

Audit trail

Fully maintained logs for compliance

Scalable

Ramp up and down to match demand

Visibility

Single pane of glass

Questions

Thank you

Lech Lachowicz
Mail to: lech.Lachowicz@issa.com.pl