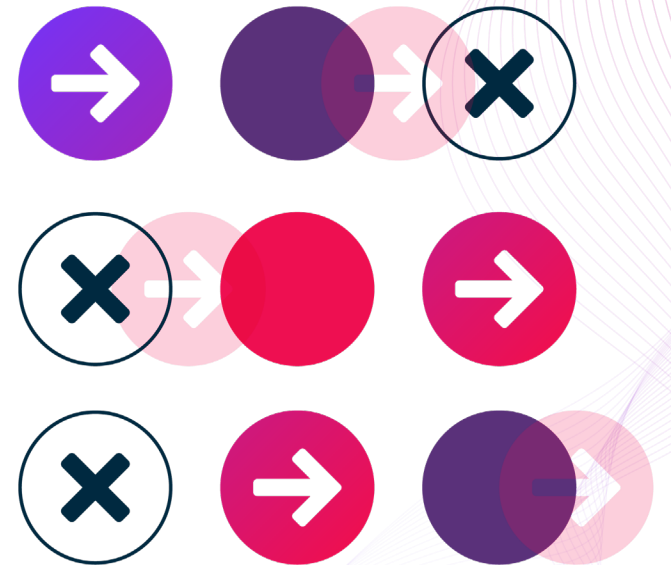
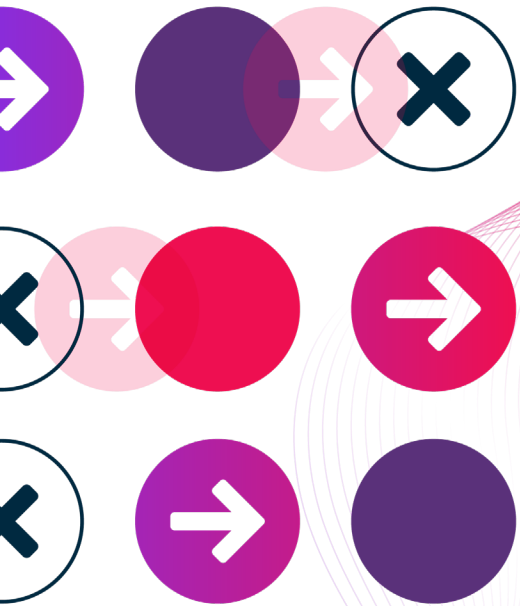


VALIDATE 2022



Prepare to Prevent Business Disruption



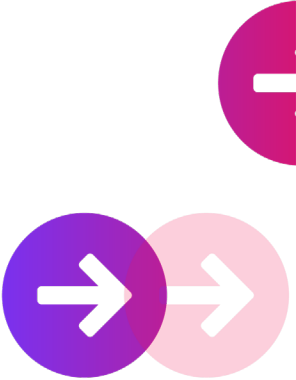


 IBM Security

Srinivas Tummalapenta

*Distinguished Engineer & CTO
IBM Security Services*

This is a practitioner-to-practitioner conversation,
art of possible conversation cannot be treated as
declaration of future capabilities.



Cybercriminals remain adept at successfully infiltrating organizations across the globe

Evolving threat landscape

21%

Ransomware share of attacks

41%

Attacks exploited phishing for initial access

\$401M

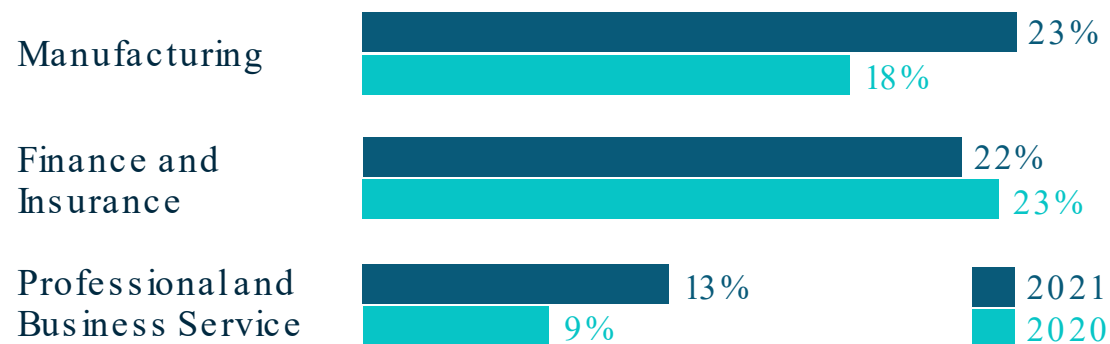
Average cost of a mega data breach (50-65M records)

2,204%

Increase in reconnaissance against Operational Technology (OT) devices

Top industries targeted

Percentage of attacks



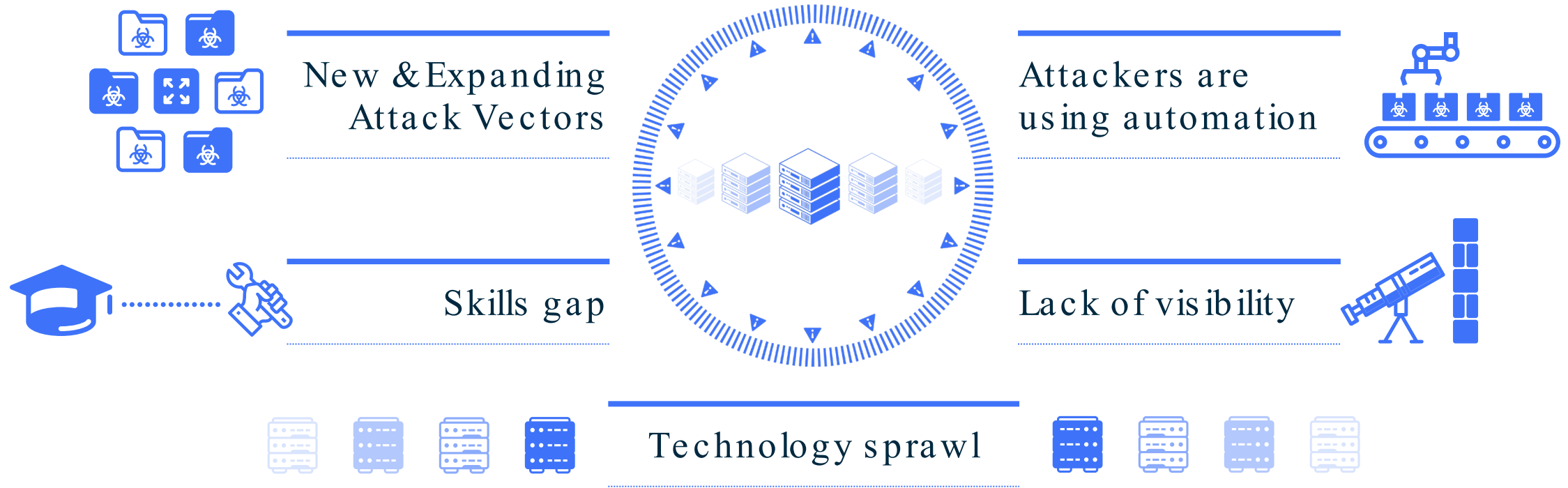
Linux threats on the rise

Year-over-year increase in Linux ransomware innovation across cloud environments

Sources: 2022 IBM X-Force Threat Intelligence Report; 2021 IBM Security Cost of a Data Breach Report

We attribute these security exposures to these key dynamics

Organizations lack reliable controls to prevent business disruption





What we're hearing from clients

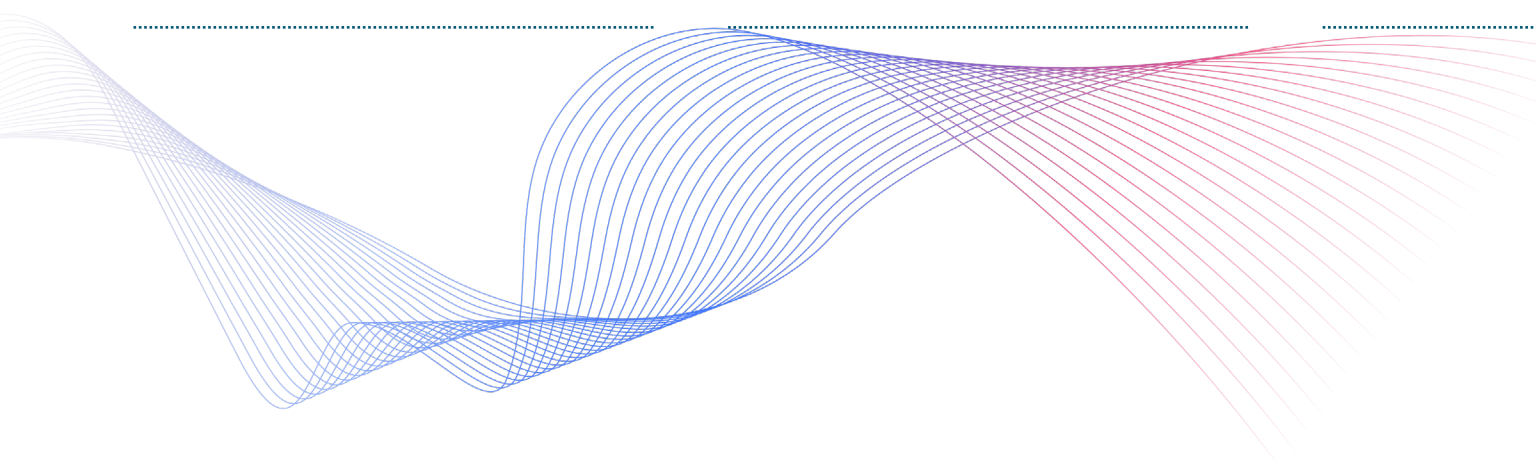
From thousands of engagement across the world, we've heard some common security concerns.

Detect and respond to threats faster

Reduce mean time to resolution

Safeguard workloads in hybrid multi-cloud environments

Enhance and leverage existing security investments





What we hear from our analysts



Reduce
noise, enrich
with intel and
context



Better tools
for triage,
investigation
and response



Immersive and
hands-on
learning of
latest attacks

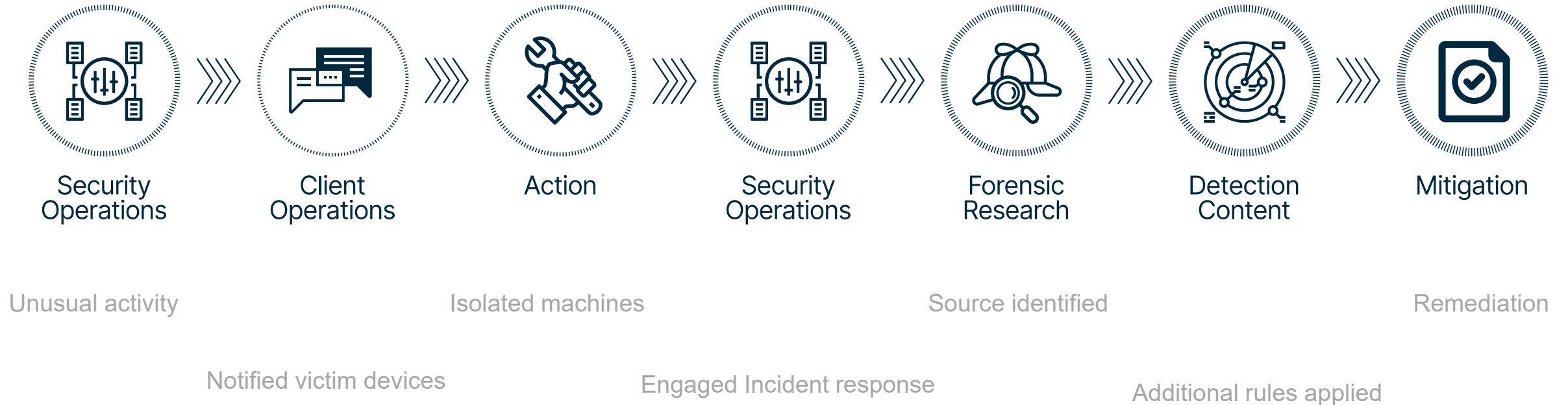


Make
the security
technologies
effective

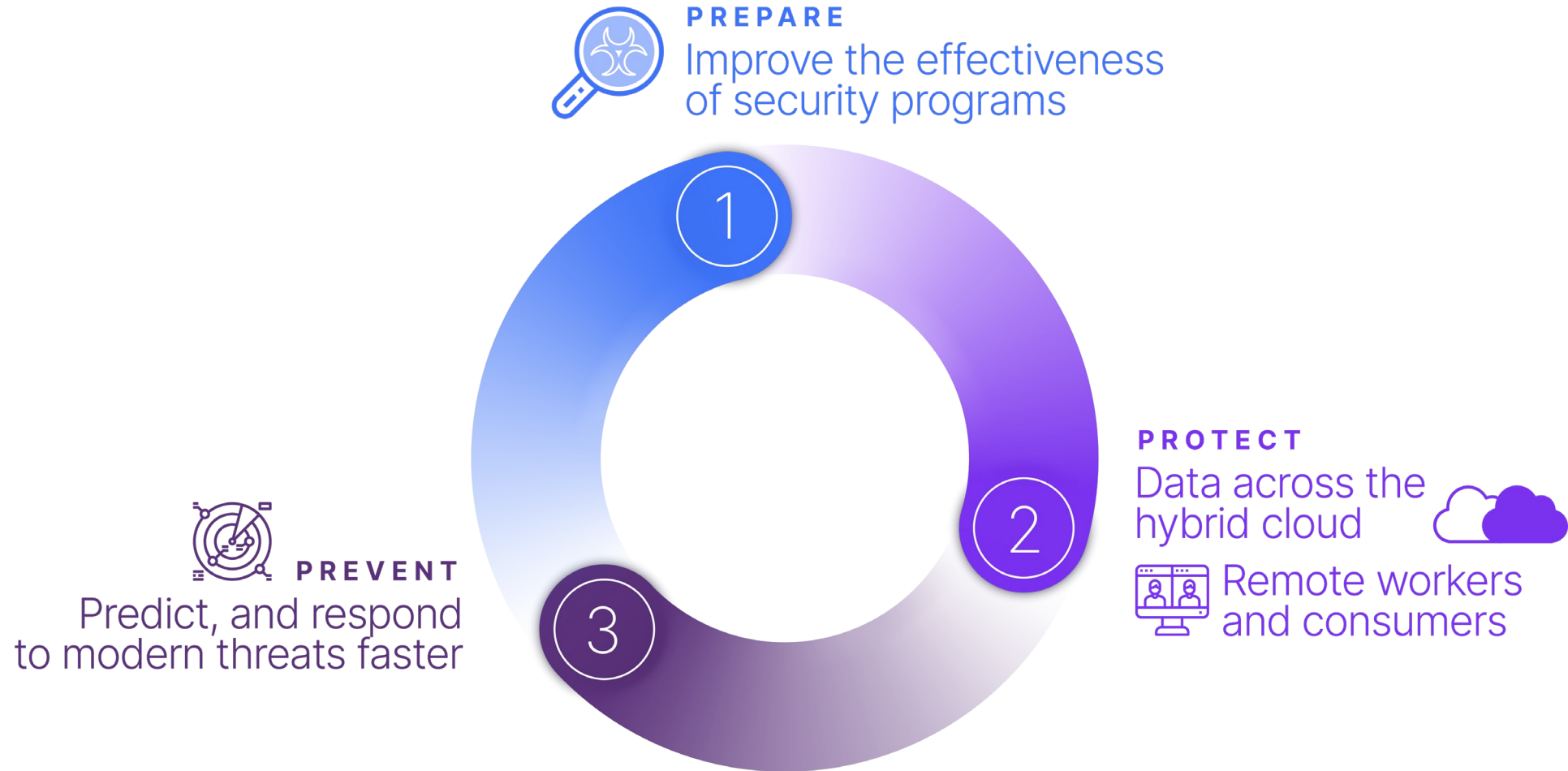
Under prepared client was at risk of major financial opportunity



Well prepared client avoided business disruption through faster detection and response



We should Prepare to address evolving threats, respond and protect faster



Take a two-pronged approach through the threat management lifecycle to improve enterprise resiliency

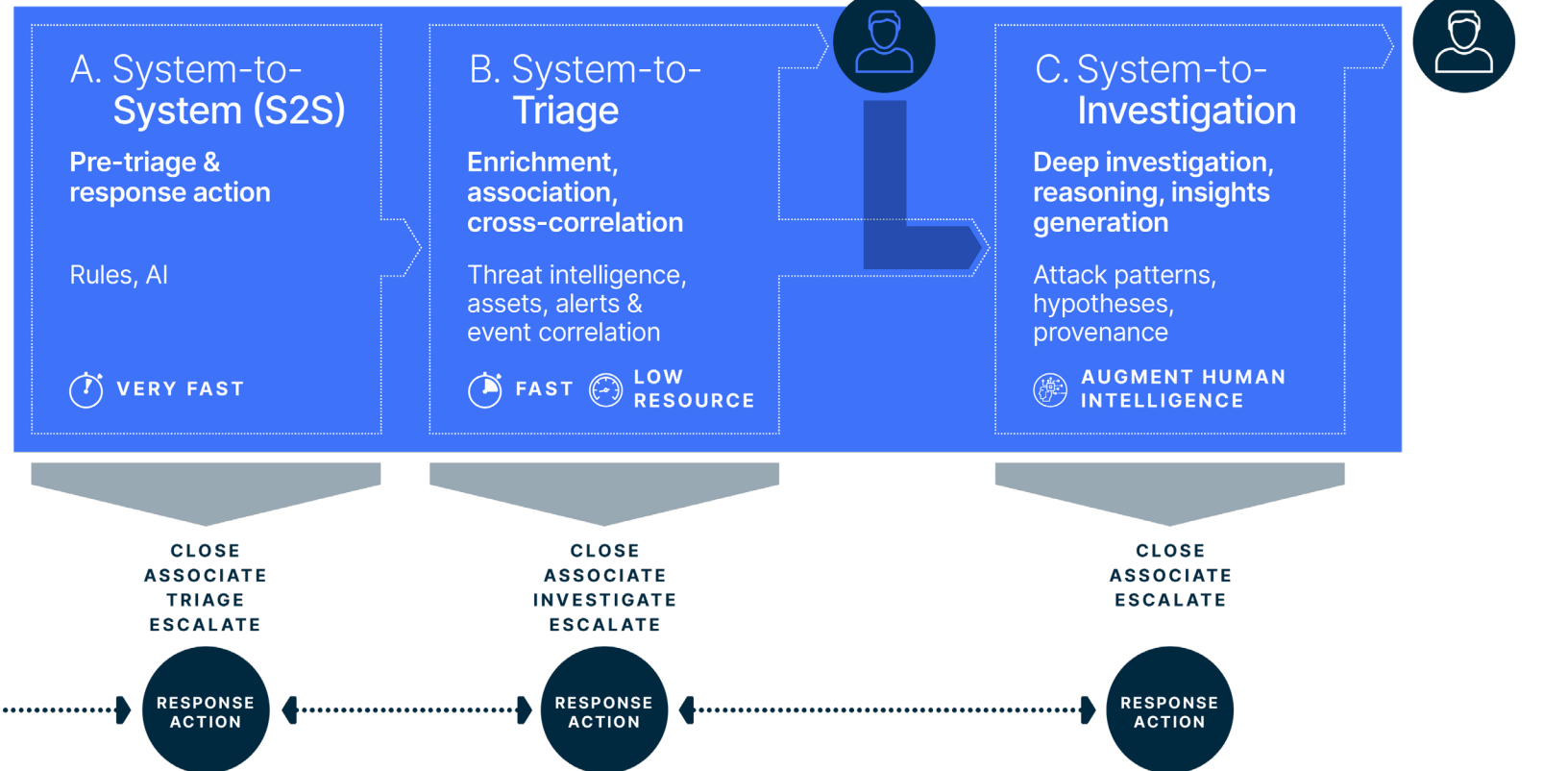
Protection & Detection Tech

In system
Protection & Detection

Rules, hygiene, rapid testing, response automation

EFFECTIVE

Analytics & analysts support engine



1. Prepare the detection and protection technologies

Adopt a risk based approach

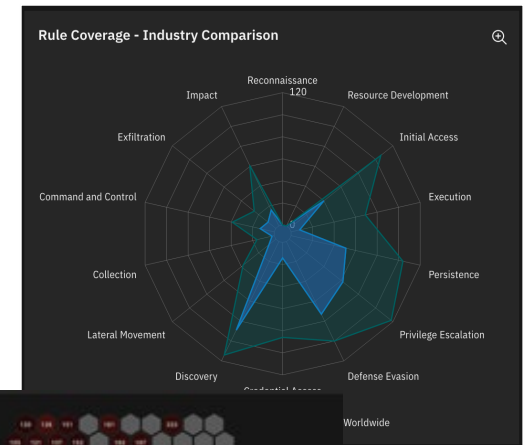
Harden systems, detect drift and automate to remediate

Weaponized Exploits (WX) centric risk-based approach to vulnerability Management

Security technology optimization (ex. FW rule optimization)

Continuous improvement through MITRE ATT&CK-based SIEM posture assessment and recommendation

Automate adversarial simulation with BAS to proactively assess and enforce



2. Prepare the analysts

Skills and expertise through immersive education and training

Happy analysts, happy clients;
Quality of Experience improvement
for Clients and IBM'ers

Learn latest and greatest attacks
through Breach Attack Simulation on
representative Hybrid cloud lab

Information curated in single pane of glass,
reduce screen surfing and steps



3. Prepare AI

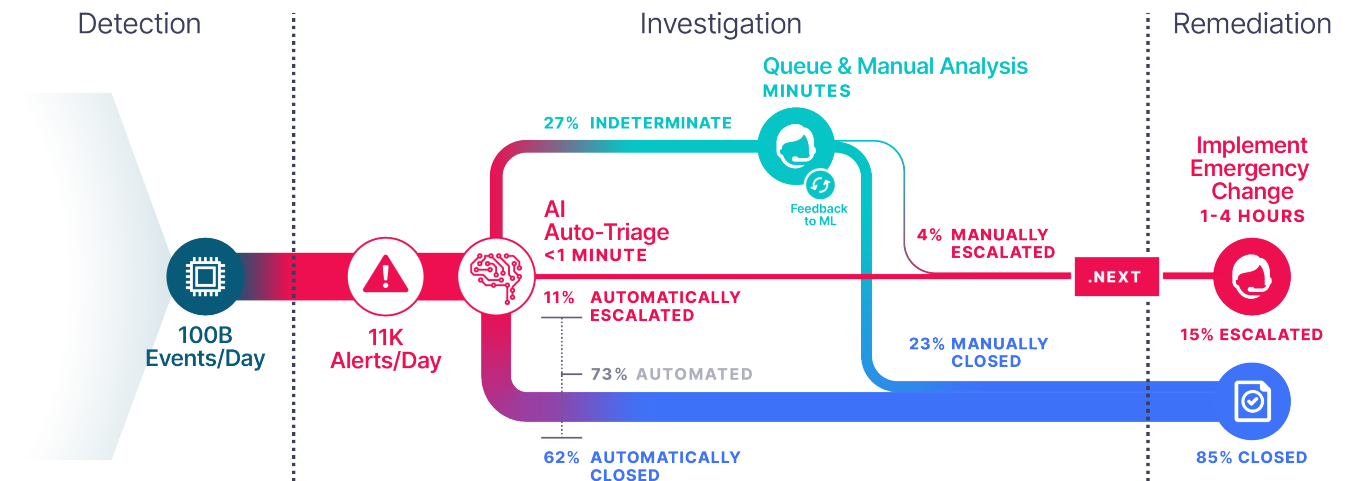
Improve response time through AI-enabled multilateral detection and response

Reduce noise for analysts with AI so they can focus on high value alerts

Reduce triage time through recommendations with explanation and reasoning

Faster investigation through structured playbooks with intel enrichment and intuitive visualization

Automated response through fact-based enrichment

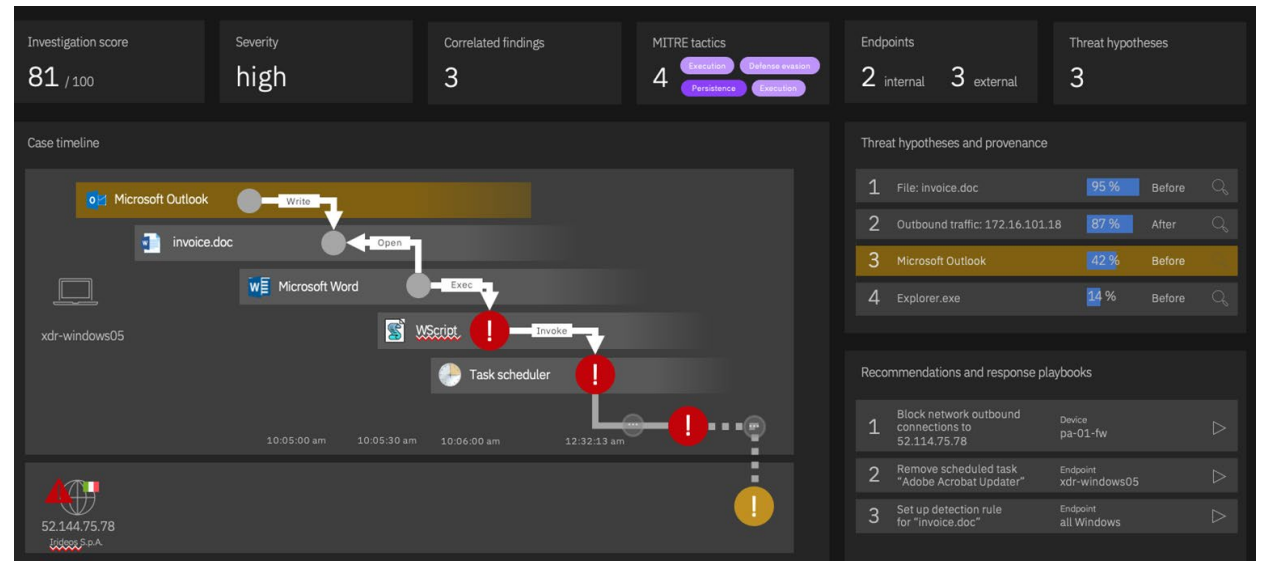


Can we predict to prevent ?

Use simulation data from Breach & Attack Simulation to train and test AI models. Use it for early warning?

Proactively assess security controls posture and remediate

Speculative cause (before) and effect (after) hypotheses



Ready for future battles

Thousands of IBM Researchers in 12 labs across 6 continents are busy working on security projects that will shape our future

Good AI versus bad

IBM researchers are finding ways to address the weaknesses found in AI systems

Quantum-safe cryptography

Lattice cryptography will protect organizations from quantum-enabled hackers

Blockchain for security

IBM invented the way to share threat intelligence that's anonymous and trusted

Securing the world of things

IBM researchers are working on cryptographic algorithms and protocols, and key management to enable end-to-end IoT security



Q&A



FOLLOW US ON:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

[@ibmsecurity](https://twitter.com/ibmsecurity)

youtube.com/user/ibmsecuritysolutions

SafeBreach

FROM DEFENSE

VALIDATE 2022

TO OFFENSE

Elevating Your Proactive Security Program

© Copyright IBM Corporation 2019. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.