2022 INFORMS BUSINESS ANALYTICS CONFERENCE

Asking the Right Questions

A Data-Driven Blueprint for Effective Defense

BIONIC

About Me

20 years in cyber defense

Former CTO, Raytheon Cyber

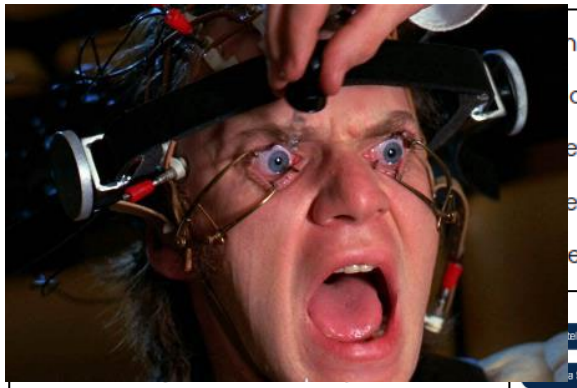
Co-inventor, *Automated Internet threat detection and mitigation system and associated method*

Co-Founder & CEO, Bionic

Certified Instructor and
Course Author @ SANS Institute

BIONIC

Analytics in Cyber Defense



nalyzing network traffic to detect patterns that indicate a po

onitoring user behavior, especially potentially suspicious behavior

etecting **insider threats**

etecting **data exfiltration**

entifying accounts that may have been compromised

Supervised detection

Unsupervised anomaly detection

dentify patterns that may indicate attacks

avior

at data exfiltration

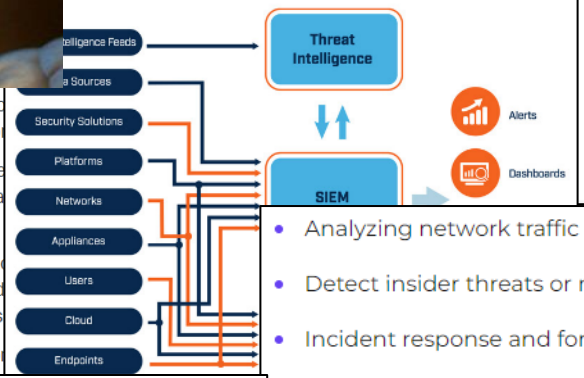
ity of remote and internal employees

reats

7. Detecting accounts that have been compromised
8. Demonstrating compliance to standards such as the Health Insurance Standard (PCI DSS)
9. Investigating incidents
10. Detecting the improper use of user accounts

trends of users, applications and devices to identify abnc
detect anomalies that could indicate a security breach o

- **External threat intelligence:** An external security service intelligence as part of its portfolio. While not security ana supplement the analytical process.
- **Forensics:** Forensic tools are used to investigate past or how attackers infiltrated and compromised systems, and security vulnerabilities that could leave an organization s
- **Network analysis and visibility (NAV):** NAV is a collectio user and application traffic as it flows across the
- **Security information and event management (S** management combines a series of tools to provide real-time analysis of security alerts generated by network devices and applications.
- **Security orchestration, automation and response (SOAR):** Security orchestration, automation and response (SOAR) is the hub that ties together data gathering capabilities, analysis and threat response.



Detection correlation

- Analyzing network traffic to identify patterns that indicate a potential attack
- Detect insider threats or malicious activity
- Incident response and forensics
- Manage third and fourth-party **vendor risk**
- Detect data exfiltration and which accounts may have been compromised
- Governance, risk, and **compliance**
- Identify threat indicators with threat hunting

BIONIC

The Right Questions

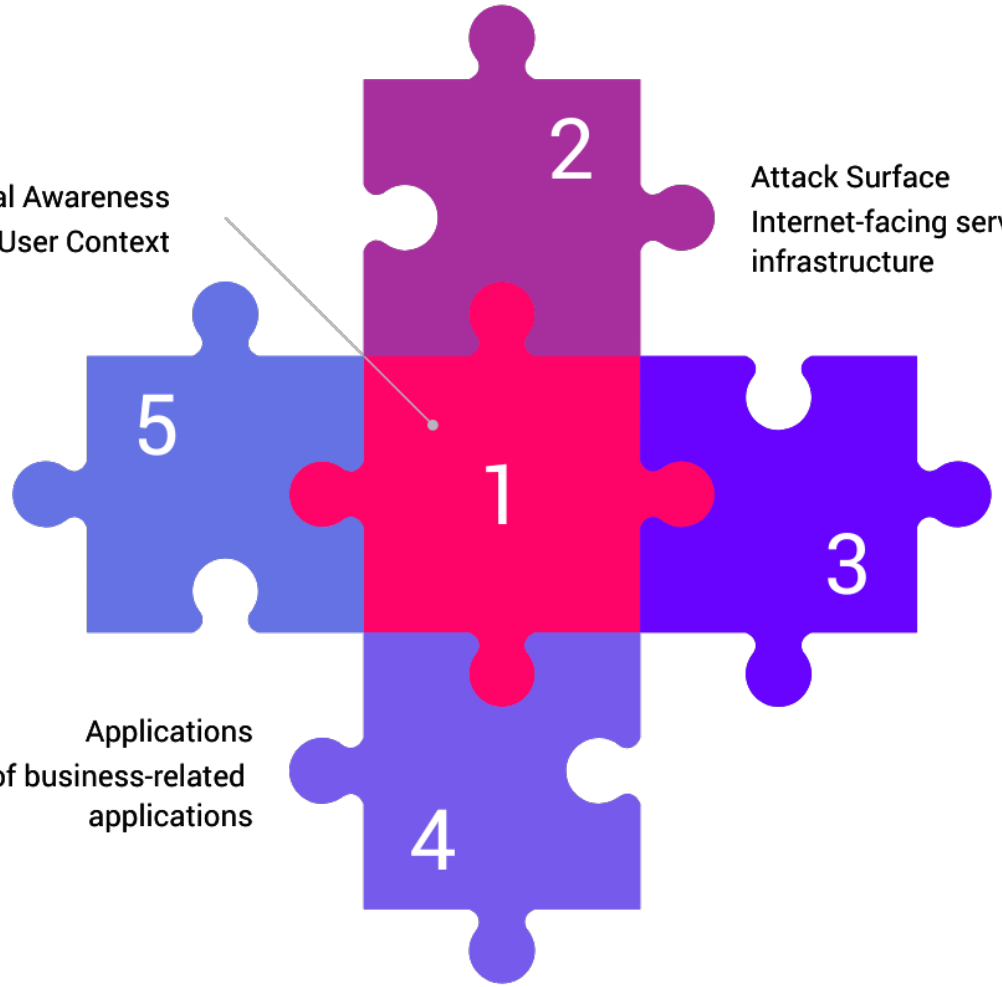
1. What do I have that is worth protecting?
2. How might that value be degraded or destroyed?
3. How likely is that to happen?
4. How much work am I willing to do to keep that from happening?
5. What don't I know?

Blueprint for a Better Night's Sleep

- Know what you have
- Understand how it is being used
- Know what is leaving your network
- Revisit your assumptions (constantly)
- Trust but verify
- Learn from what you have done
- Measure and improve

BIONIC

What Do You Have?



Situational Awareness
Asset and User Context

Attack Surface
Internet-facing services and infrastructure

Configurations
Operating System settings and configurations

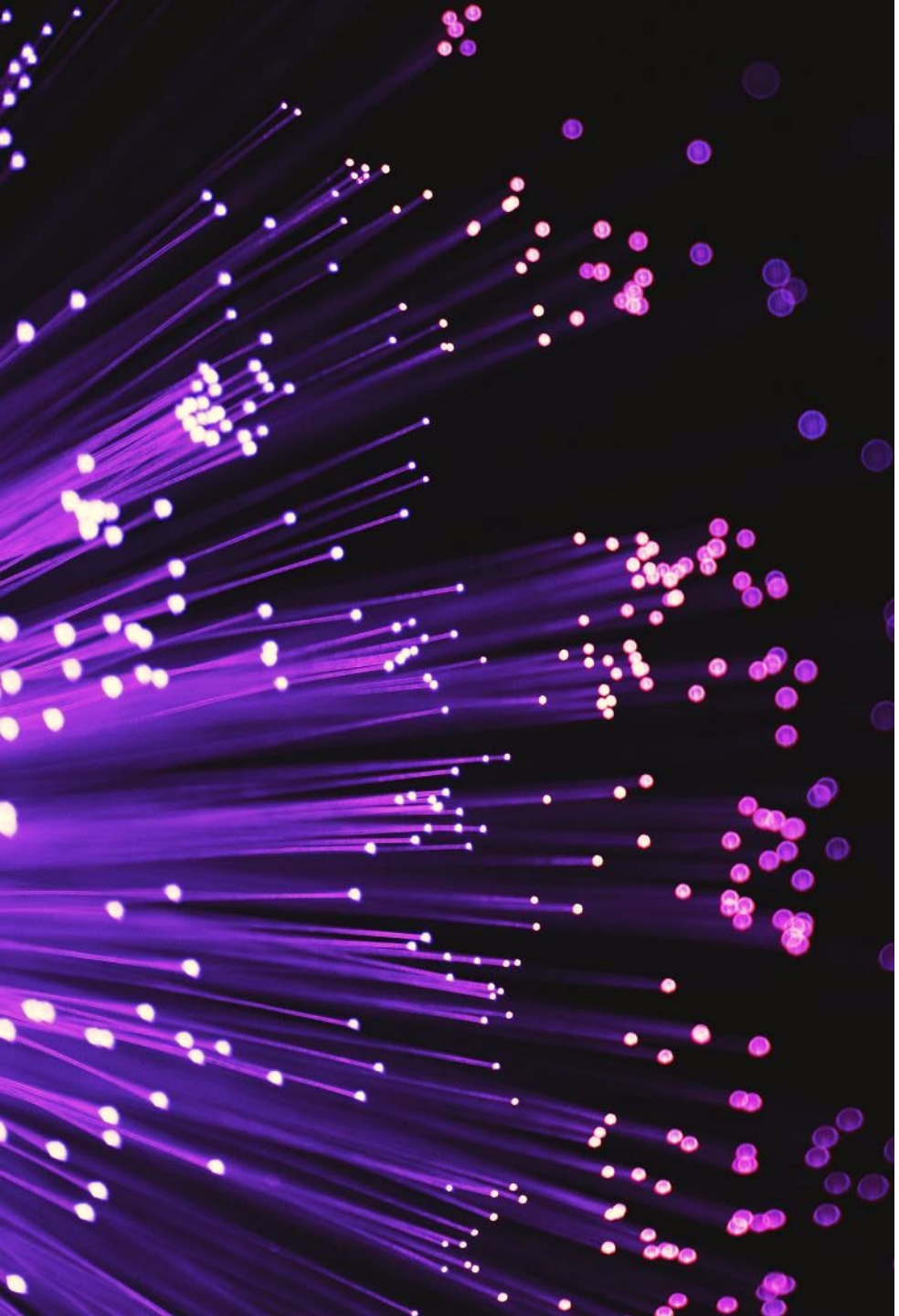
Users
Groups, roles, rights and permissions

Applications
Baseline of business-related applications

BIONIC

How Are Your Assets Being Used?

- Application control
- Executables, scheduled tasks, autoruns, scripts
- Administrative functions and commands
- Login activity



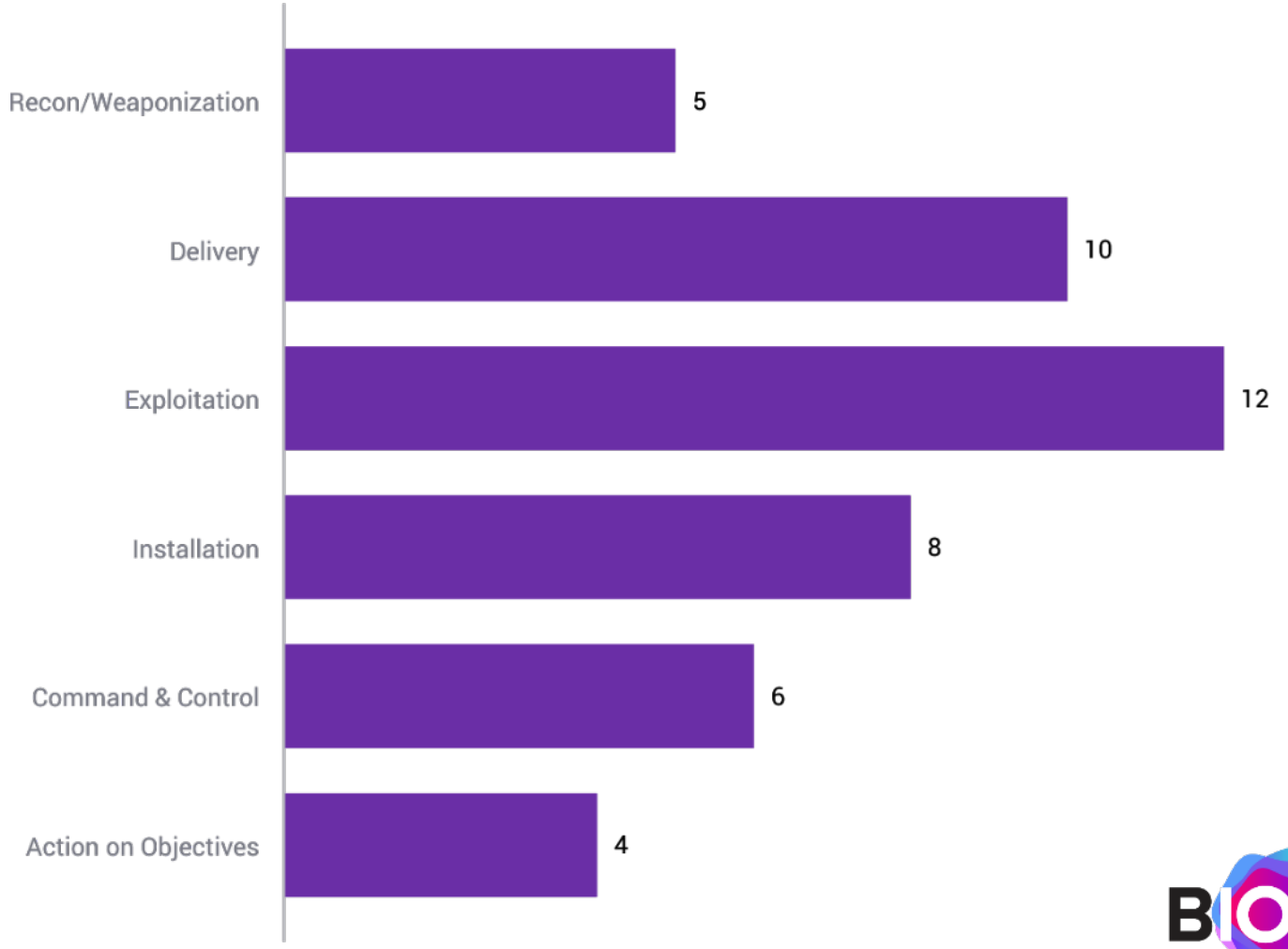
What Is Leaving Your Network?

- Watch your outbound communications
- Long term retention is not as important as complete data
- New implementations of DNS, HTTP, TLS are making this harder

BIONIC

How Many Chances Do You Have?

Detection Capabilities
by Kill Chain Phase



BIONIC

Are You Sure Your Defenses Work?

1. Atomic tests for your analytics

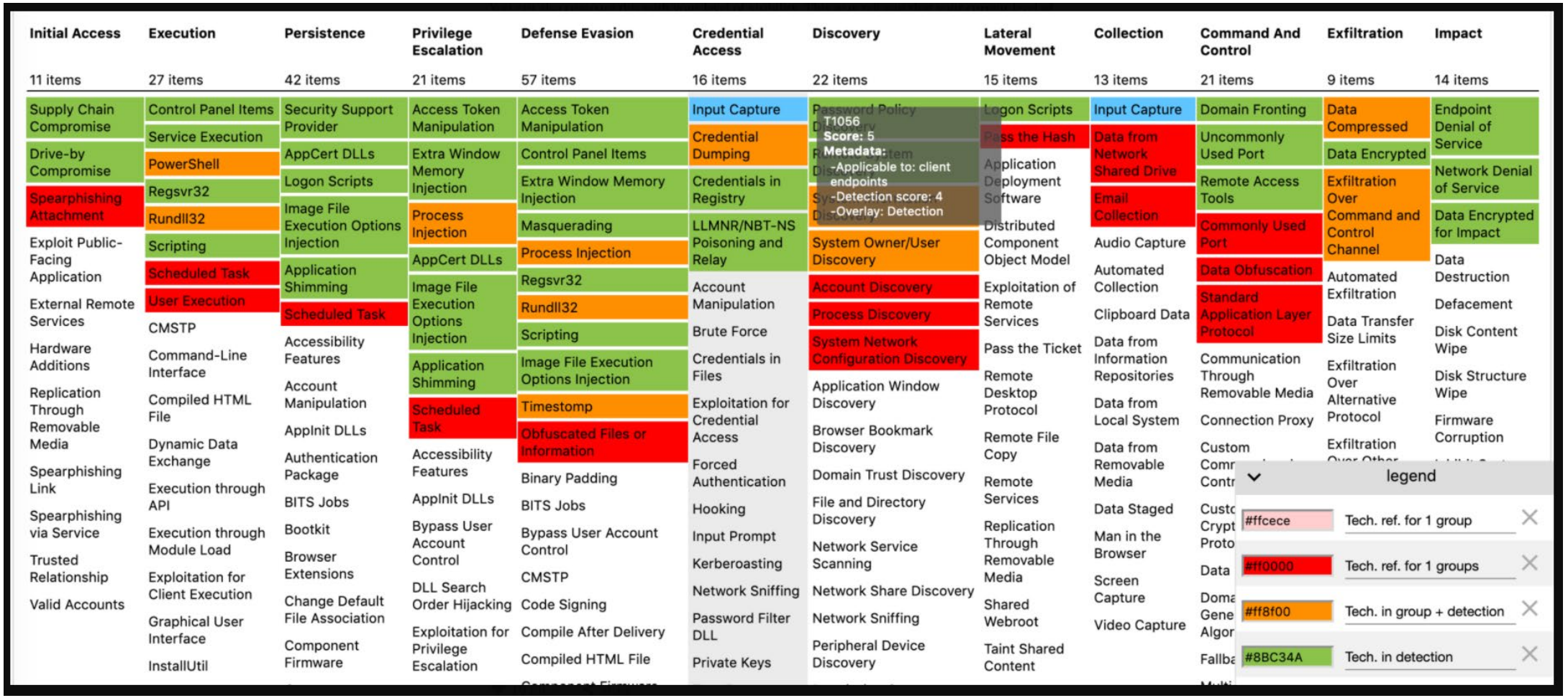
2. Purple team assessments for your enterprise logging and detections

3. Red team assessments for your preventative controls

4. Adversary emulation for your enterprise controls and detections

BIONIC

Visualizing Detections with MITRE ATT&CK



Source: https://www.mbsecure.nl/blog/2019/5/dettact-mapping-your-blue-team-to-mitre-attack

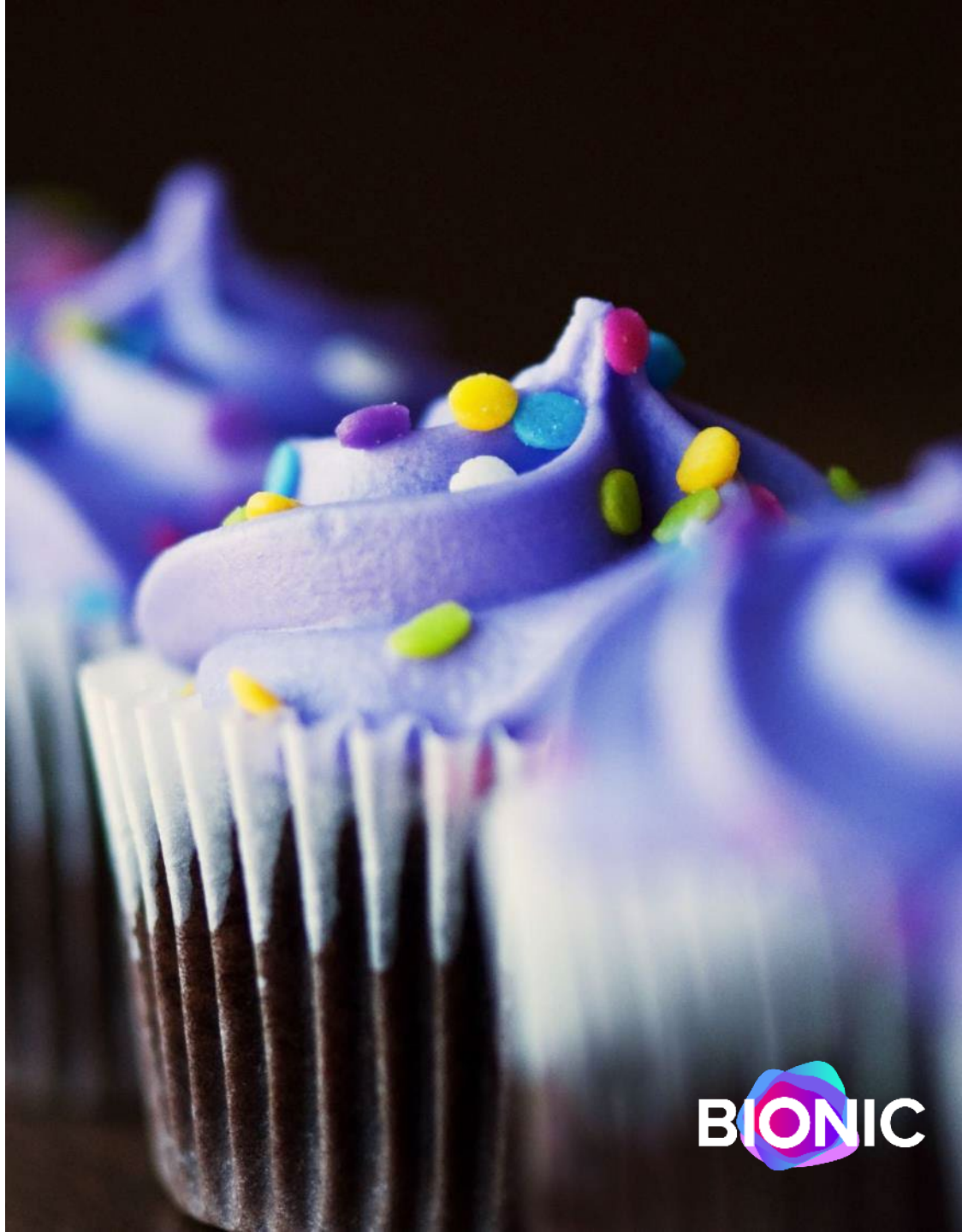
Are You Learning?

- Strategic intelligence
- Operational intelligence
- Collaborative intelligence

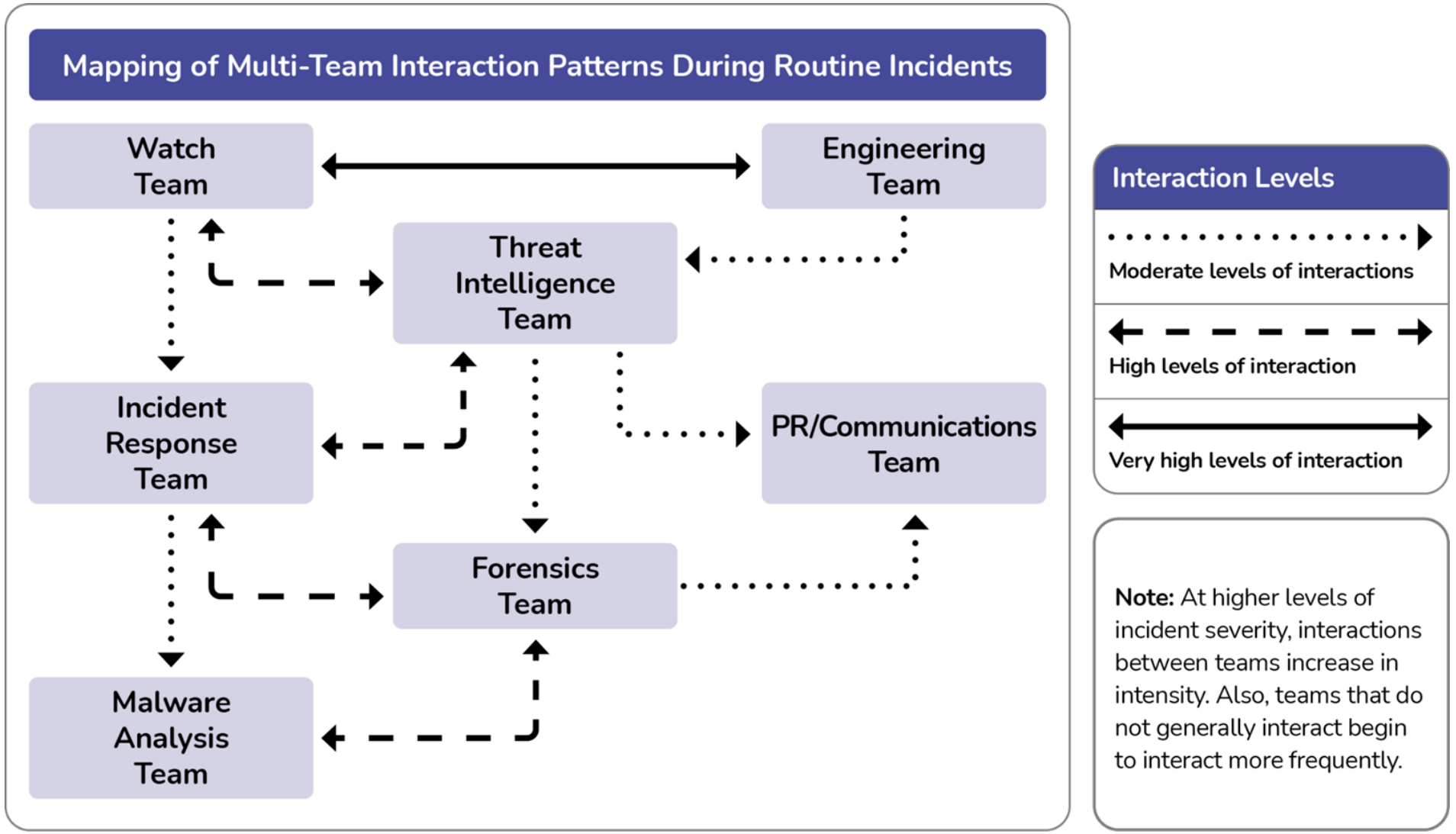
BIONIC

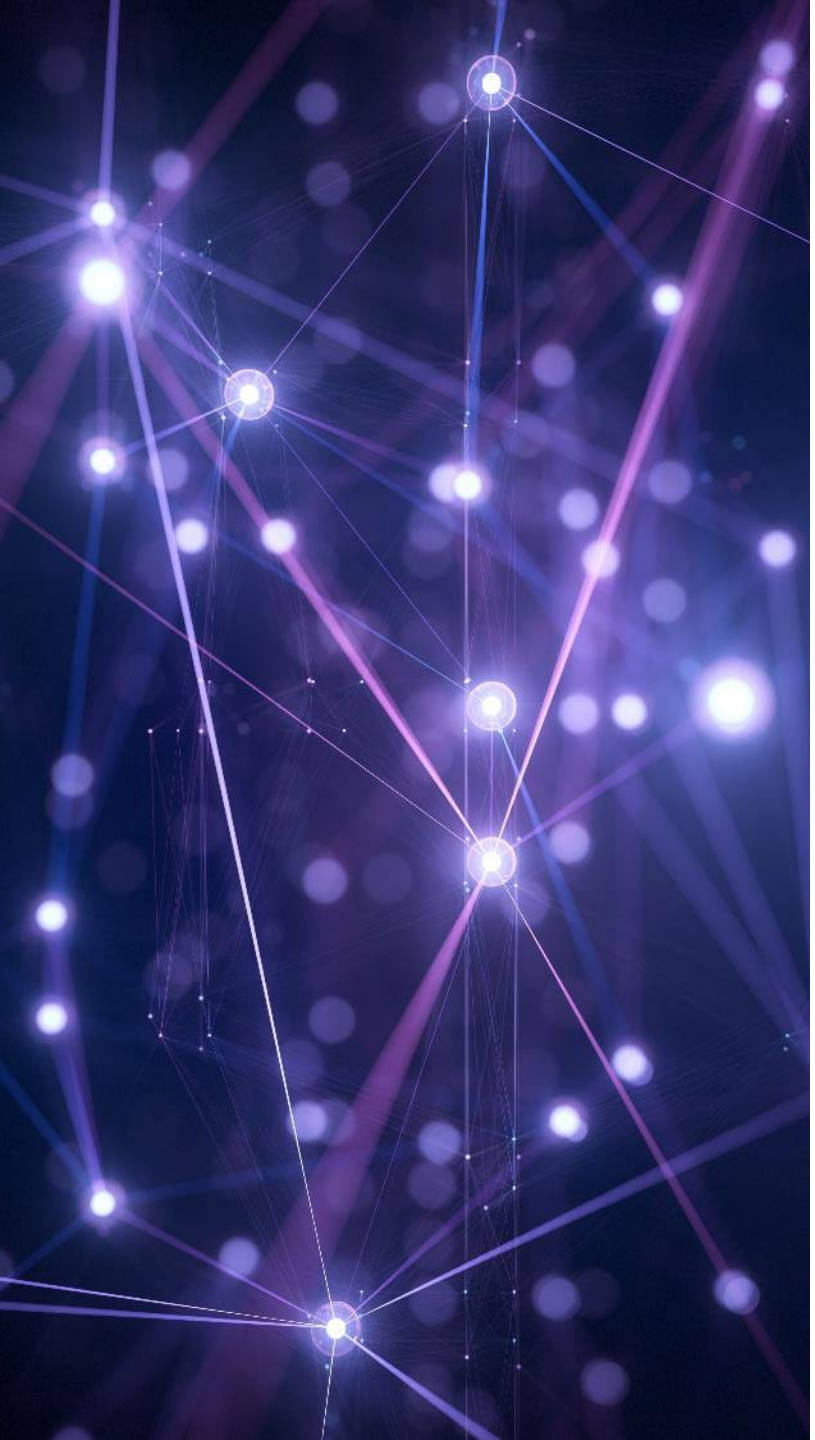
Is Your Team Collaborating?

- Increase trust and shared knowledge of unique expertise (SKUE)
- Reduce friction in crisis situations
- Promote learning and teamwork
- Track when and how often your team collaborates

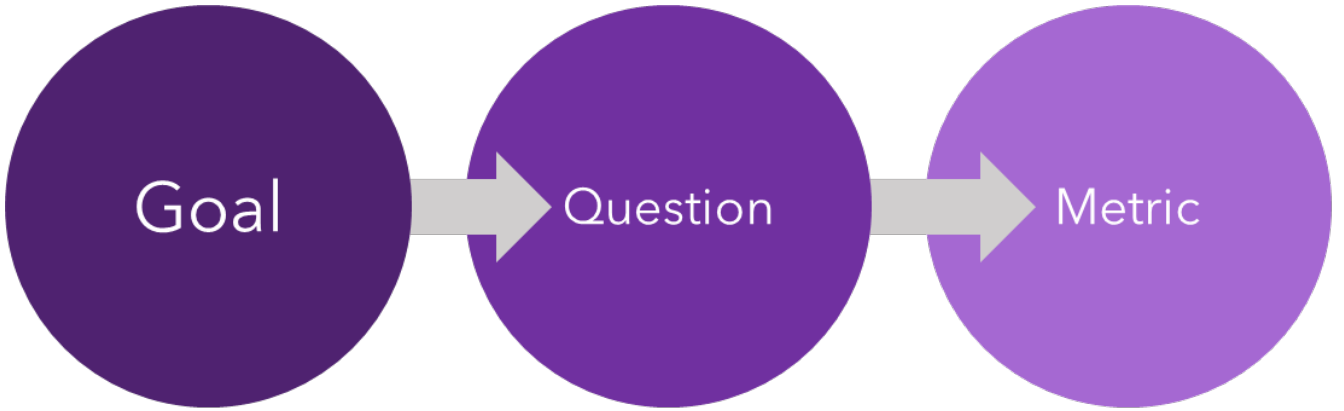


Mapping Team Interaction





Are You Improving?

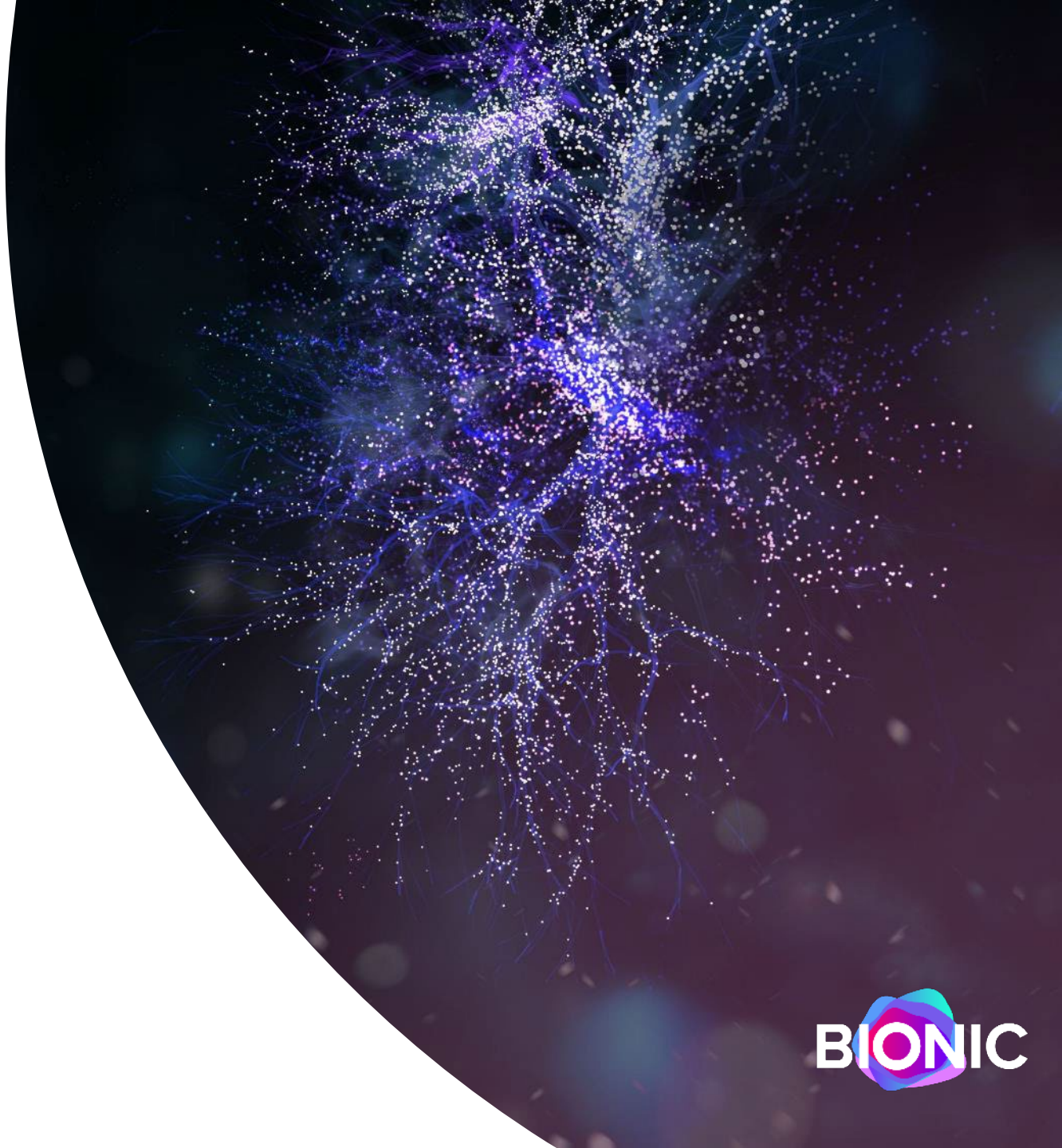


Goal	Question	Metric
"Reduce successful phishing attacks."	What is our target range? What impact constitutes a successful attack? What attempt constitutes a successful attack?	KPI is <5 per week Number of infections Number of messages delivered

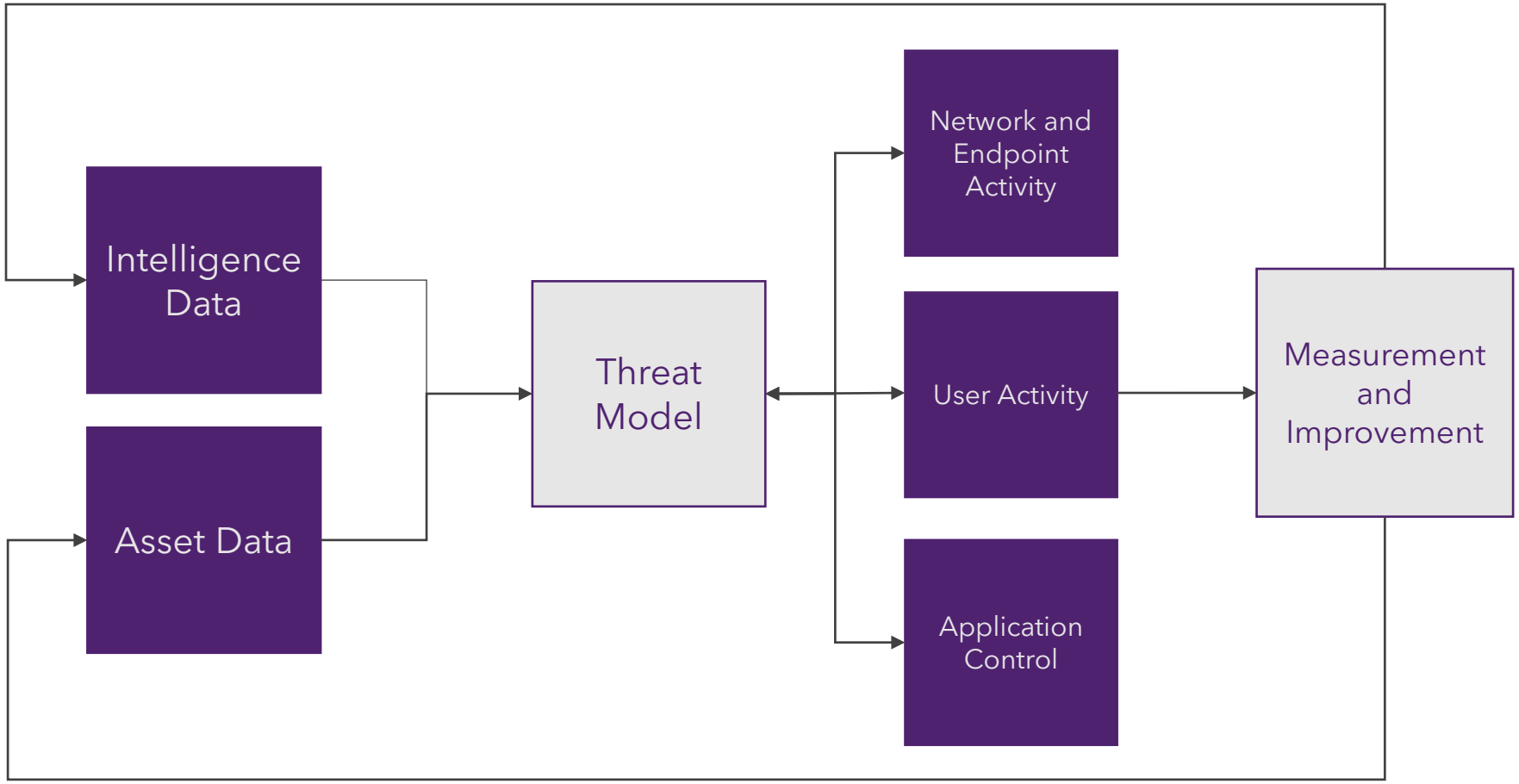
BIONIC

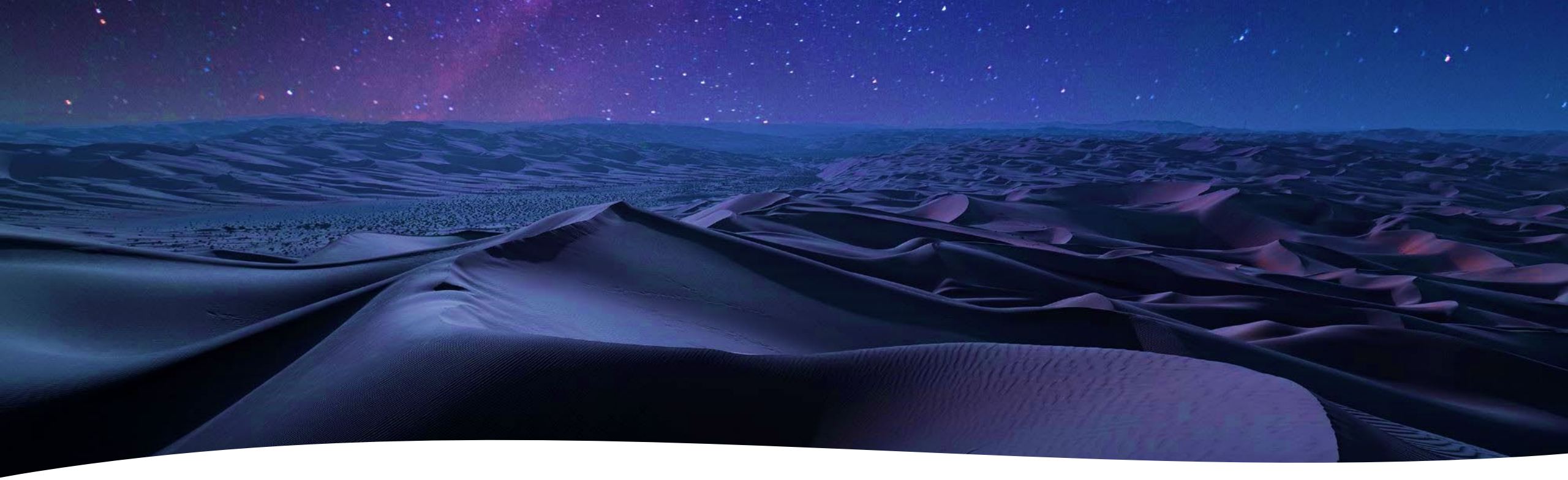
What Are You Assuming?

- Security tools will save you
- Your data is not desirable to an attacker
- Users will not find a way around your security
- Security is more important than productivity
- You know what's going on



Blueprint for a Data-Driven Defense





Summary

- Analytics are decision support, not easy buttons or products.
- They can give defenders superpowers if driven by the right questions.
- Collect some data. Process, interpret, repeat.
- Start with your goals and security “hygiene”, not vendor use cases.

BIONIC

Thank You

Email: mark@bioniccyber.com
LinkedIn: https://www.linkedin.com/in/marko16/
Web: https://bioniccyber.com

BIONIC