edgescan

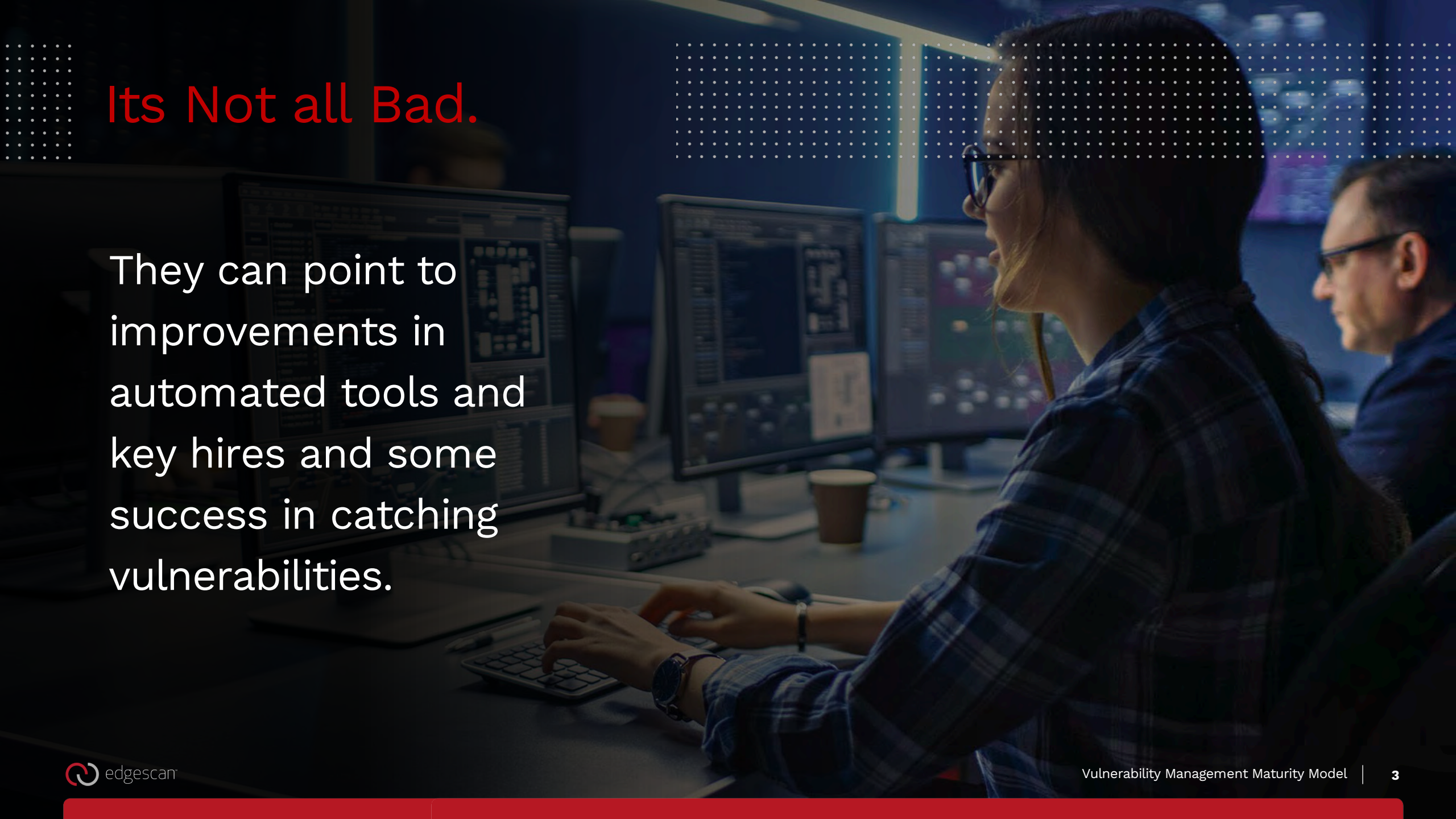
# Vulnerability Management Maturity Model

A Framework to Determine your Cyber Security Maturity

# Is Your Vulnerability Management Program Mature?

While Corporations are advancing to meet the ever expanding cyber threat – there is uncertainty whether they are actually prepared.

# Its Not all Bad.



They can point to improvements in automated tools and key hires and some success in catching vulnerabilities.

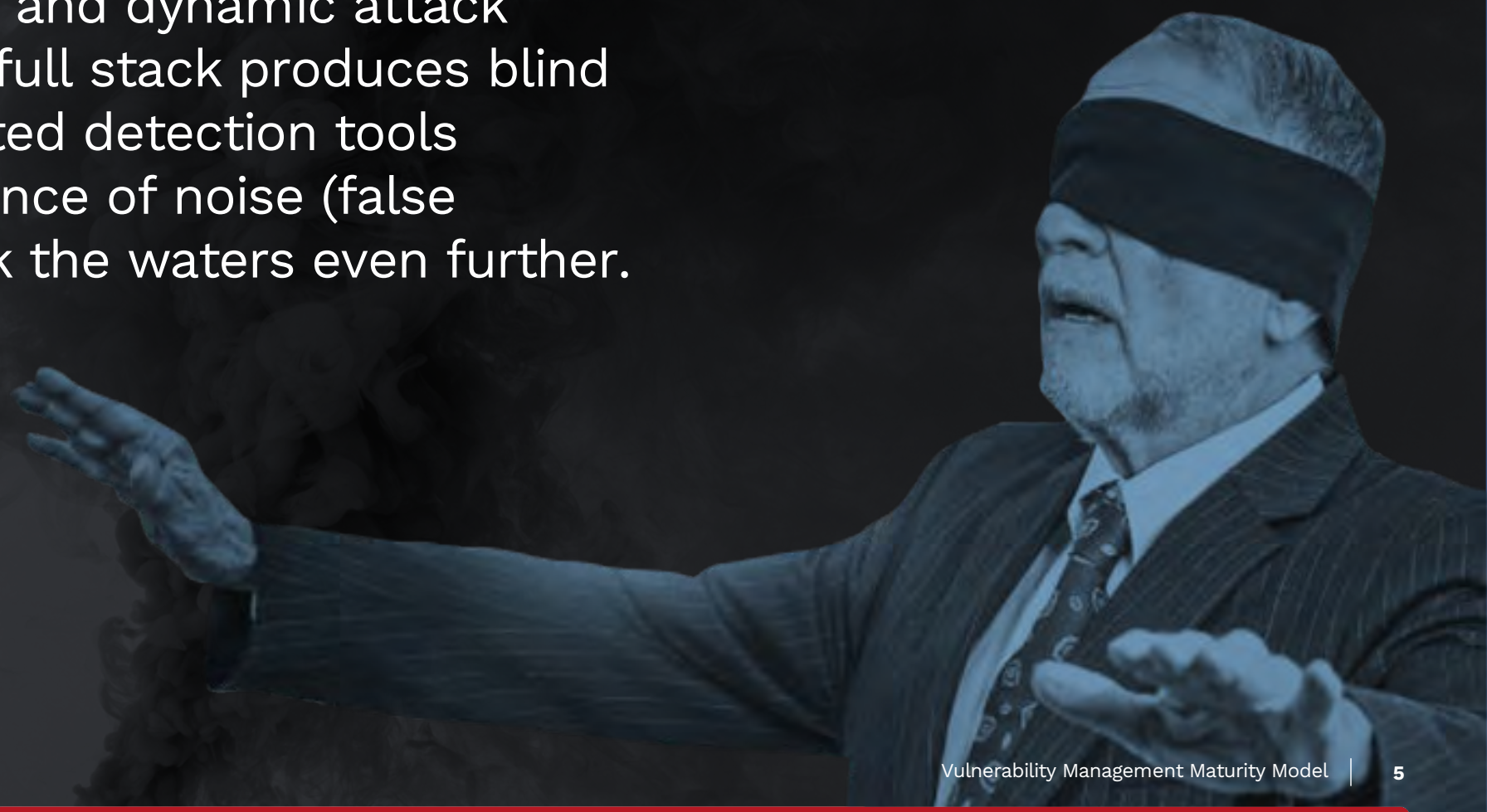
# What the Enterprise DOES Know

They DO know that major Cyber Security incidents are happening on a daily basis just by reading the front page of the news.

And they do know that they are not prepared to avoid being the next front page news

# The Problem

The ever expanding and dynamic attack surface across the full stack produces blind spots. And automated detection tools produce an abundance of noise (false positives) that murk the waters even further.



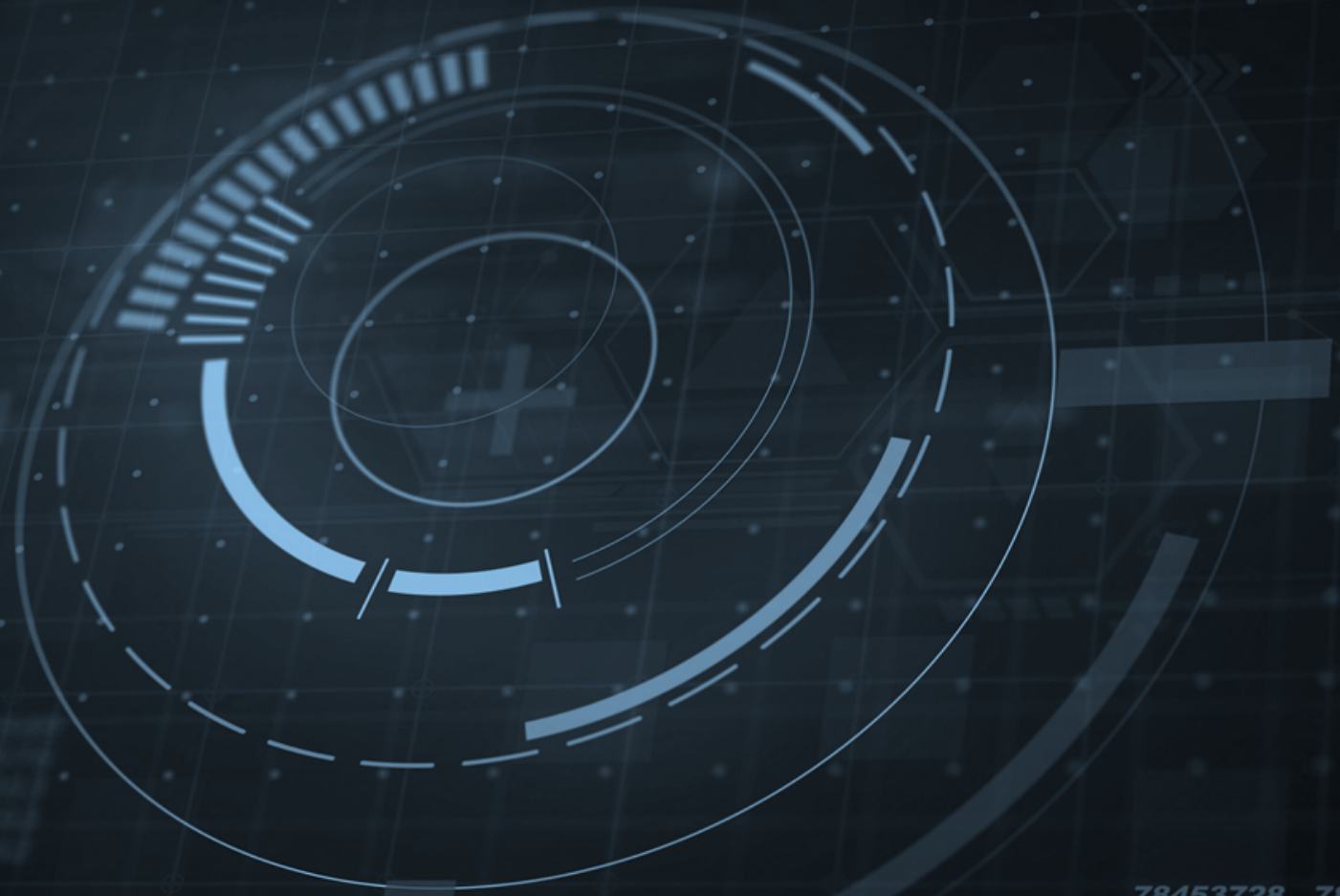
# Blind Spots

The Global 3000 Enterprise simply does not know what it does not know

# And Companies are Simply Not Ready

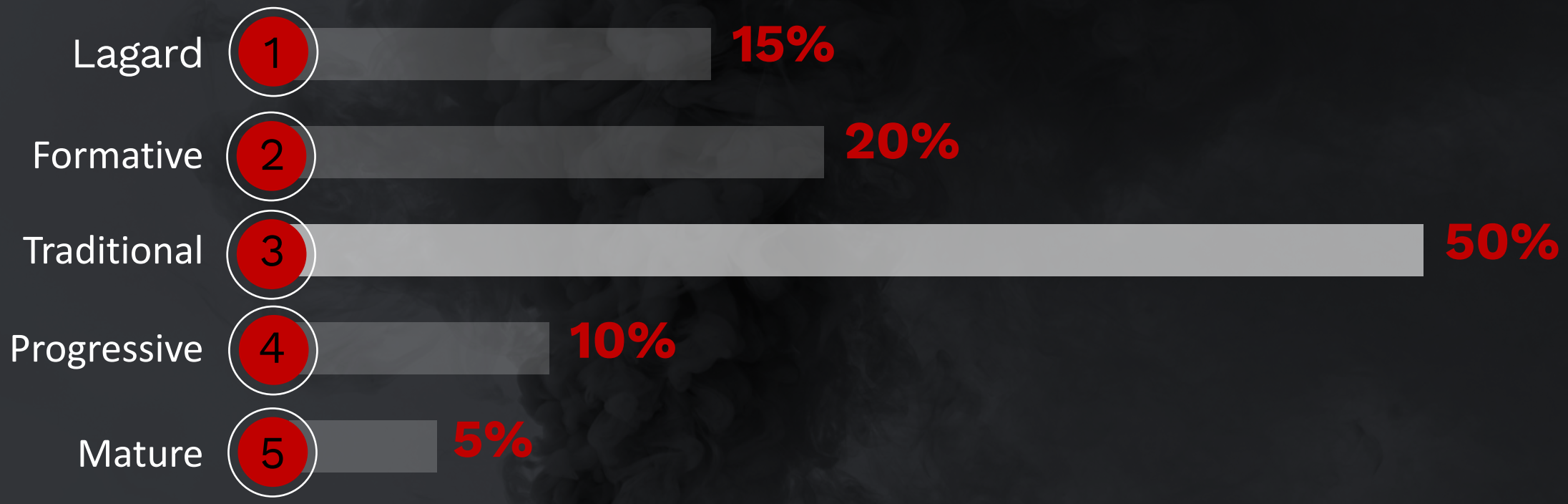
"More than half of businesses are not prepared for Cyber Attacks"

*(Cyber Trendscape Report 2020)*



# So We Developed a Maturity Framework

Based on Eight Evaluation Criteria, we developed a model that places each company into five categories:



# Your Vulnerability Management Maturity

Let’s discuss your maturity level with the following framework

| | Evaluation Criteria | Lagard | Formative | Traditional | Progressive | Mature |
|---|---|---|---|---|---|---|
| Management | Who is the most senior cyber security executive? | Nobody | An IT Manager | A team Lead/Senior Manager | A VP/Director | CISO - Implicit throughout organization. |
| Staffing | What is your current cyber security staffing makeup? | None | 1 Cyber Security Professional | 1-4 Cyber Security Professionals | 5-8 Cyber Security Professionals | 9+ Cyber Security Professionals |
| Goals | What is the primary goal of your current cyber security program? | Non-Existent | Ad-Hoc | Assessment & Compliance | Attack Management | Business Risk Management |
| Intelligence | How comprehensive is your intelligence view? | No intelligence/ business context | No full stack coverage | No full stack vulnerability view | Risk Based View | Validated vulnerability intelligence & business context |
| Processes | How proactive and automated are your cyber security processes? | Ad-hoc Patching/mitigation No process | Haphazard mitigation/patching Ad-hoc assessment cadence | Compliance Driven Infrequent process | Scheduled & on-demand Proactive Patching | Scheduled, Continuous & On-demand Assessments |
| Resilience | How prepared are you to react to a cyber event? | Unknown | Unprepared | Recovery Capabilities | Detection and Protection Capabilities | Adaptive strategies & mature actionable intelligence available. |
| Operational Workflow | How do you put your cyber security intelligence into actual operational remediation? | None | Manual | Some automated integration | Full Automated | Fully automated integrated with expert remediation guidance |
| Tools Capability | What are your current VM tools capabilities? | • No Metrics<br>• No Attack Surface Visibility<br>• Desktop Tool based. | • No Metrics/improvement tracking<br>• No Attack Surface Visibility<br>• External scanning only<br>• Desktop Tool based. | • Weak metrics<br>• Weak visibility /Attack surface management<br>• No schedule / Not continuous / Ad-hoc<br>• Weak coverage / Not full stack<br>• No Integration to ticketing<br>• External and Internal assessments<br>• SaaS based tooling | • Metrics and trending<br>• Vulnerability Tracking<br>• Full stack correlation and coverage<br>• Self-validated vulnerability intelligence<br>• Integration to ticketing<br>• Ad-hoc Visibility<br>• Manual ad-hoc pen testing<br>• SaaS based Service | • Integrated systems and Alerts in real-time<br>• Optimum visibility / Attack Surface Management<br>• API Discovery & vulnerability management<br>• Expert Support on demand<br>• On-demand Pen testing as a Service (PTaaS)<br>• VM & PTaaS in single view<br>• Compliance Mapping |

* BASED ON A SAMPLE SIZE OF 789 GLOBAL 3000'S

edgescan

# Human Touch

## “Human Expertise is the Key To Effective Cybersecurity Automation”

“Getting real value and effective cybersecurity from these tools require a human touch” (Tom Gorup, Security Boulevard)


edgescan™