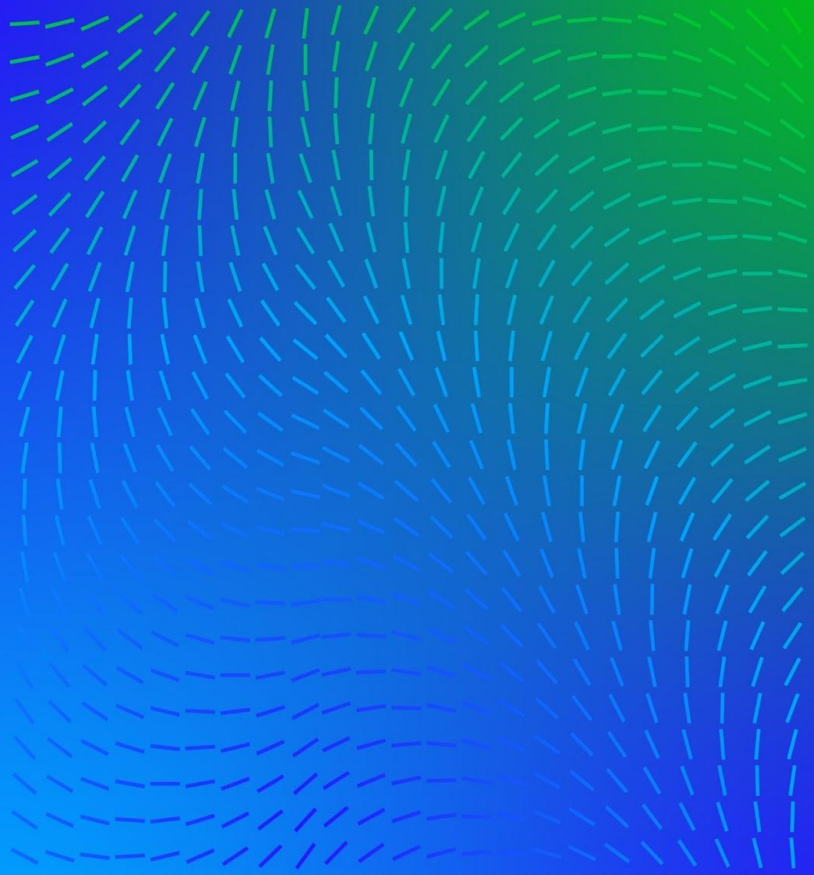
Trellix

AI & Adaptive Security Operations



Advancing Security Operations

Creating an Adaptive Model

Security operations (SecOps) **must find ways to adapt**. To do so, SRM leaders should adopt an exposure-based approach to operations, promoting business relevance. As a primary function, SecOps is **responsible for maintaining visibility** across technology estates for the purposes of monitoring and responding to potential threat activity, and **actively advising and reducing risk through careful orchestration of controls**. To achieve its goals, it's equipped with technologies and services aimed at providing deep visibility of technology networks, assisting with diagnostic outcomes and, in some cases, control implementation.

- 2023 Hype Cycles: Deglobalization, AI at the Cusp and Operational Sustainability

Trellix

Security Operations Revolution

SOC 1.0
Foundation + Discovery

- **Basic** Security concepts, **Legacy AV**, Firewalls
- Appliances **not connected** or talking to each other
- Correlation often after **post mortem forensics**

SOC 2.0
XDR - Operational

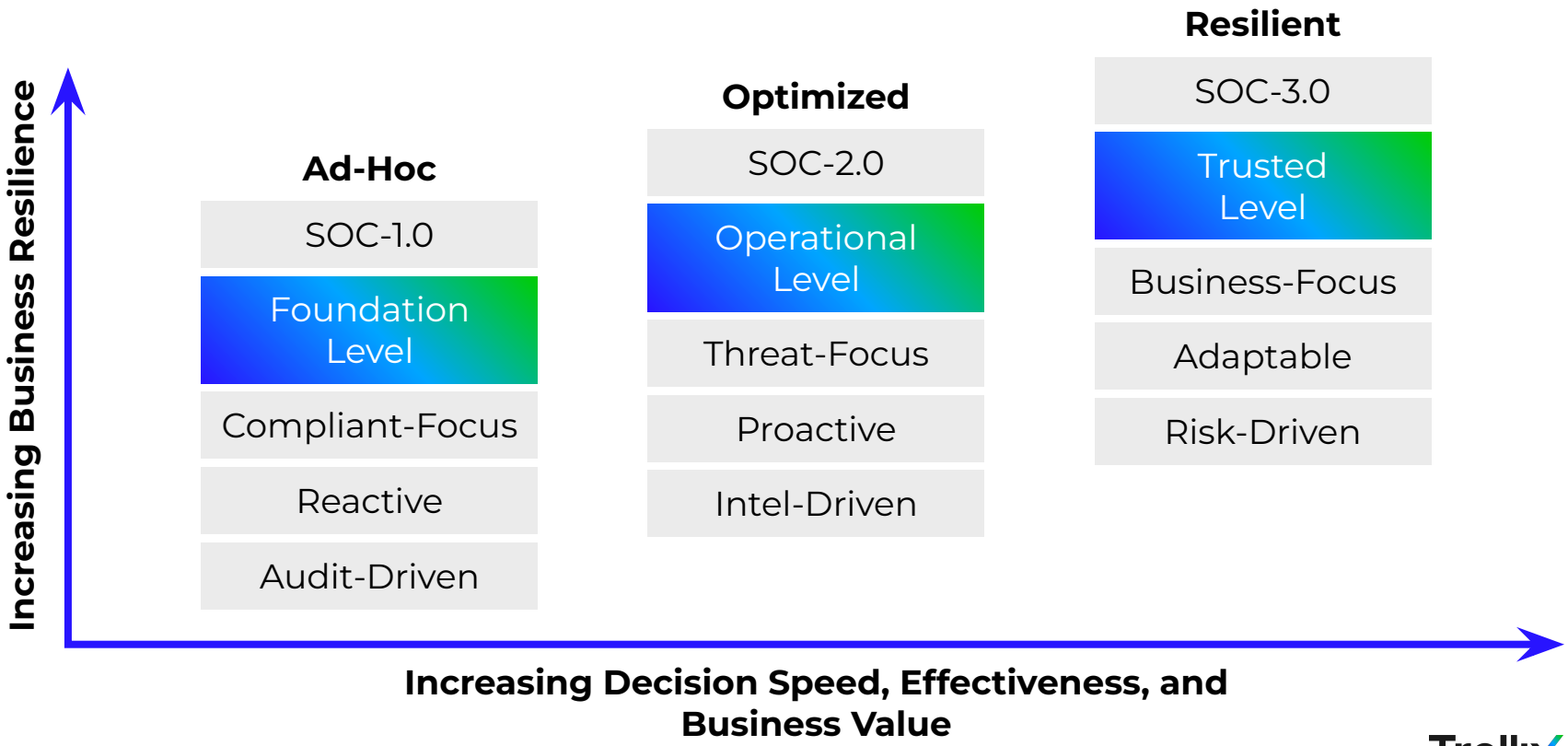
- **Alerts correlated** and accurately diagnosed
- **IR Focused**
- **Best Detection**
- **Best Response** countermeasures and Playbooks
- **Limited** in **Proactive** approach, Intelligence is **alert driven** (data-enrichment)

SOC 3.0
Aimed at Longevity Adaptive platform (XDR+Insights + AI)

- **Proactive**, **and Adaptive**, measure and check-up (Threat Intel, Threat modeling, Attack surface monitoring, automated red teaming etc.)
- **In control of your Security posture, limit the chance of any of breach to occur and have an adaptable mindset to limiting RISK.**

Trellix

SOC Maturity Journey

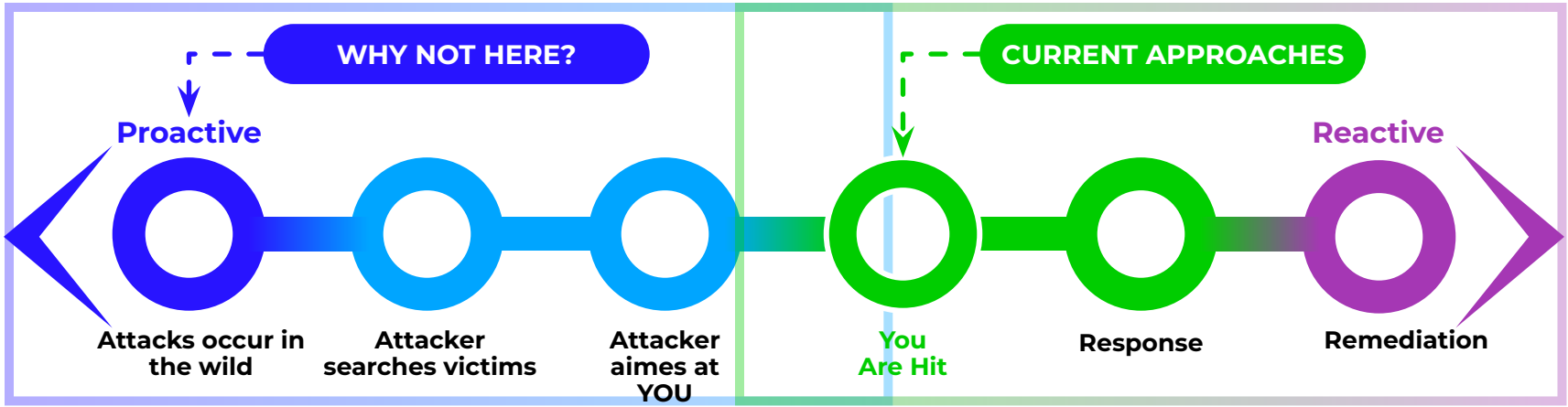


Trellix

SECOPS Readiness (Adaptive XDR)

Pro-Active/ Adaptive (Insights)

XDR Platform

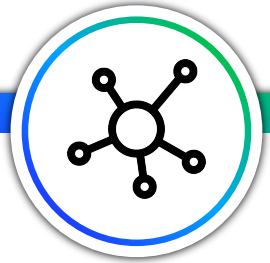


"Thanks to Trellix Insights, we can confidently answer questions from upper management, such as 'Are we protected against this?' It helps us focus on what to do next and informs our cybersecurity strategy."

— Karsten L., CISO at SMS Group

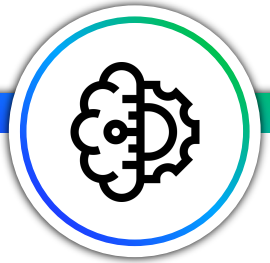
Trellix

Leading Security Forward



Trellix Xtend

A Connected Security Ecosystem



Trellix GenAI

Amazon Bedrock

A Virtual Analyst that is always learning

Trellix ADVANCED RESEARCH CENTER

An elite team of security researchers

AI Drivers

Reducing Risk

Robust Data Security for GenAI use

Leverage Capability

Use GenAI for greater efficacy & efficiency

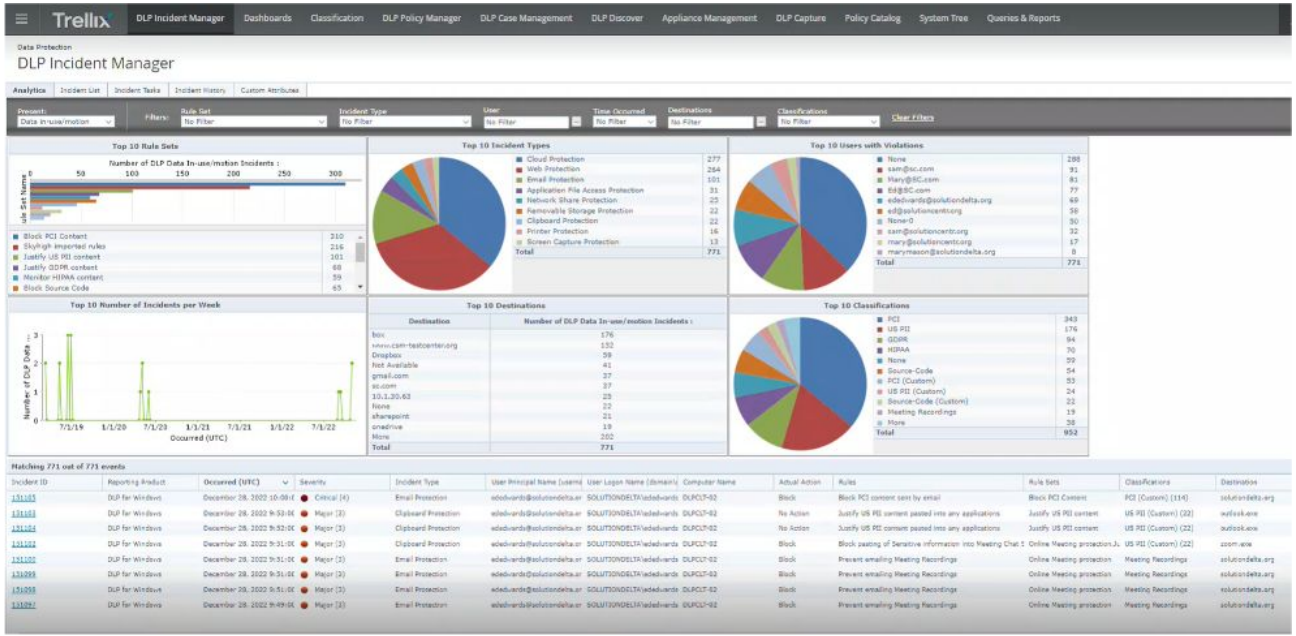
Enhance Posture

Create New Security Content

Trellix

AI: Reduce Risk

Protect Data exposure through GenAI Inter



Reduce risk of data leakage in GenAI

Trellix

AI: Leverage Capability

AI Augmented Personnel

Employees utilizing for their jobs LLM's significantly outperformed those who did not.

Based on the research by Harvard Business School that was published recently.

25.1% increase in speed

+40% improvement in output quality

12.2% more tasks completed

Skill Leveling Effect of AI:

AI augmented staff demonstrated a skill-leveling effect where lower-performing consultants experienced a 43% performance boost, diminishing the performance gap between top and bottom consultants.

Trellix

AI: Enhance Posture

Security Content Creation

Create a Trellix Endpoint Security Expert Rule to block JavaScript files from launching in the user directory

```
ExpertRule {
  Class "Process"
  Id 1000001
  Rule {
    Process {
      CommandLine {
        Include { -v "*.js" }
      }
    }
    Target {
      FilePath {
        Include { -v "%USERPROFILE%\\*" }
      }
    }
  }
  Reaction {
    Block
  }
}
```

Create a Yara rule for CVE-2018-4878

```
rule CVE_2018_4878
{
    meta:
        description = "Yara rule for CVE-2018-4878"
        author = "Your Name"
        reference = "CVE-2018-4878"
    strings:
        $string1 = "swf" wide ascii
        $string2 = "AS3" wide ascii
        $string3 = "LoaderInfo" wide ascii
    condition:
        $string1 and $string2 and $string3
}
```

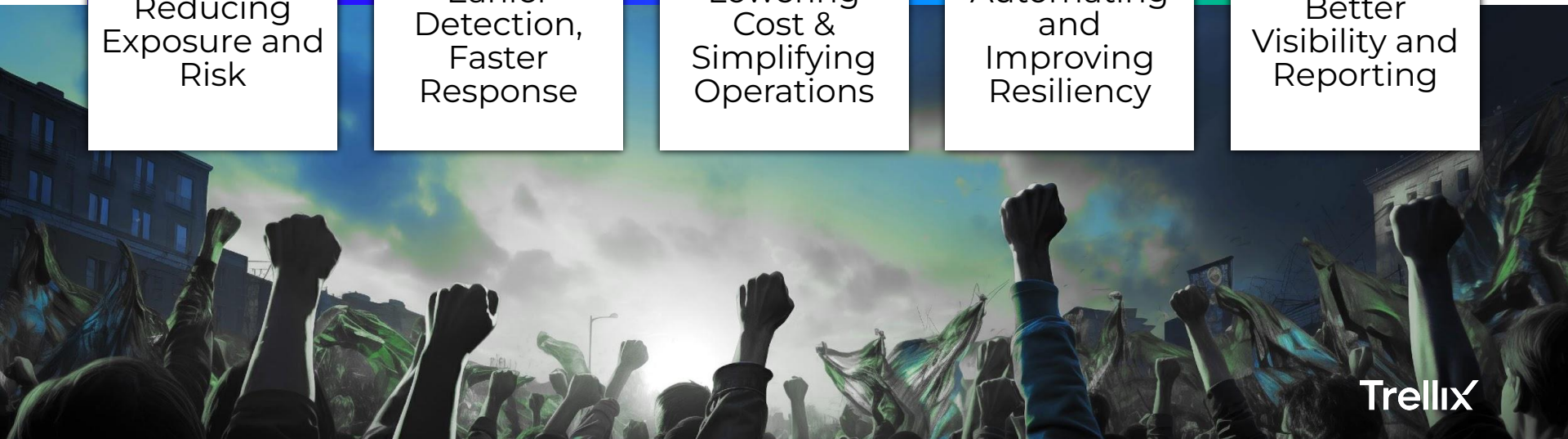
Create a SNORT Rule for DoS attacks using Docker honeypots

```
alert tcp any any -> any any (msg:"DoS Attack against Docker Honeypot"; flow:established, to_server; content:"GET"; nocase; pcre:"/\/containers\/(.*\/)*(\w+)\.json/"; sid:1000001; rev:1;)
```

Trellix

Where Do You Want to Start Your Revolution?

- Reducing Exposure and Risk
- Earlier Detection, Faster Response
- Lowering Cost & Simplifying Operations
- Automating and Improving Resiliency
- Better Visibility and Reporting



Trellix

Thank You

Trellix