DIGITAL DEFENSE®
INCORPORATED

Shrink the Attack Surface™

Webinar: The Wild West of Data Protection and GDPR: *Settle the score with GDPR Compliance to make the grade*

Presenter
Tom DeSot
EVP, Chief Information Officer

Presenter
Kimberly Carlos
Director, Product Marketing

The Wild West of Data Protection and GDPR:
Settle the score with GDPR Compliance to make the Grade

Key items we will cover

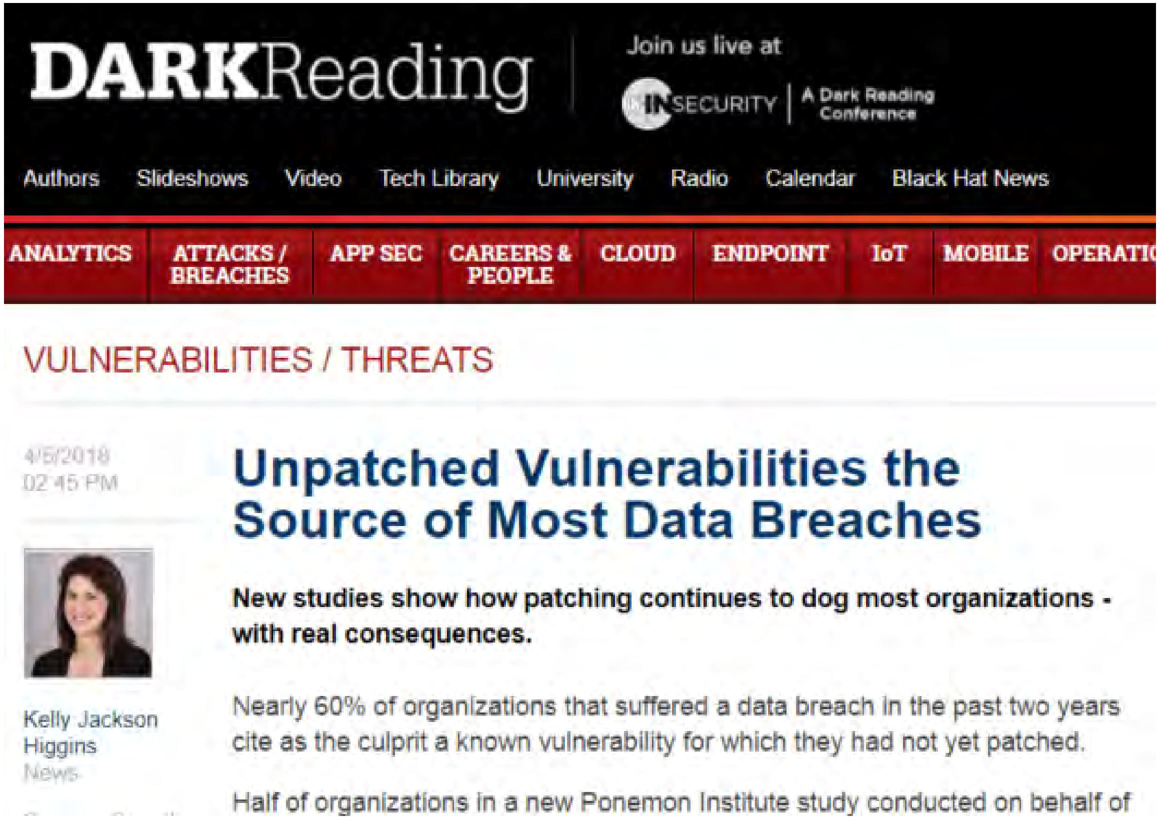
- Walk thru the compliance stages, and learn how to organize the best team internally to attack the GDPR compliance marathon; and
- How to leverage the work you are doing to comply with GDPR to strengthen your security posture, customer trust, and therefore brand resilience;
- Understanding the anatomy of GDPR penalties and fines, and how to avoid them with due diligence planning and risk management;
- How to align your cybersecurity and vulnerability management efforts with your GDPR compliance budget;
- How to leverage new GDPR adherence reports and Frontline Security Grade Point Average (Frontline Security GPA®) reporting to guide you in prioritizing for expedited compliance and internal transparency at all levels;
- Finally, learn which toolbox technologies you can use in complying with GDPR policy and procedure review and security testing of key GDPR-related assets.

What came first?

The Chicken or the Egg?

The Hacker or the Vulnerability?

The Jig is Up



VULNERABILITIES / THREATS

4/6/2018
02:45 PM

Kelly Jackson Higgins
News

Unpatched Vulnerabilities the Source of Most Data Breaches

New studies show how patching continues to dog most organizations - with real consequences.

Nearly 60% of organizations that suffered a data breach in the past two years cite as the culprit a known vulnerability for which they had not yet patched.

Half of organizations in a new Ponemon Institute study conducted on behalf of

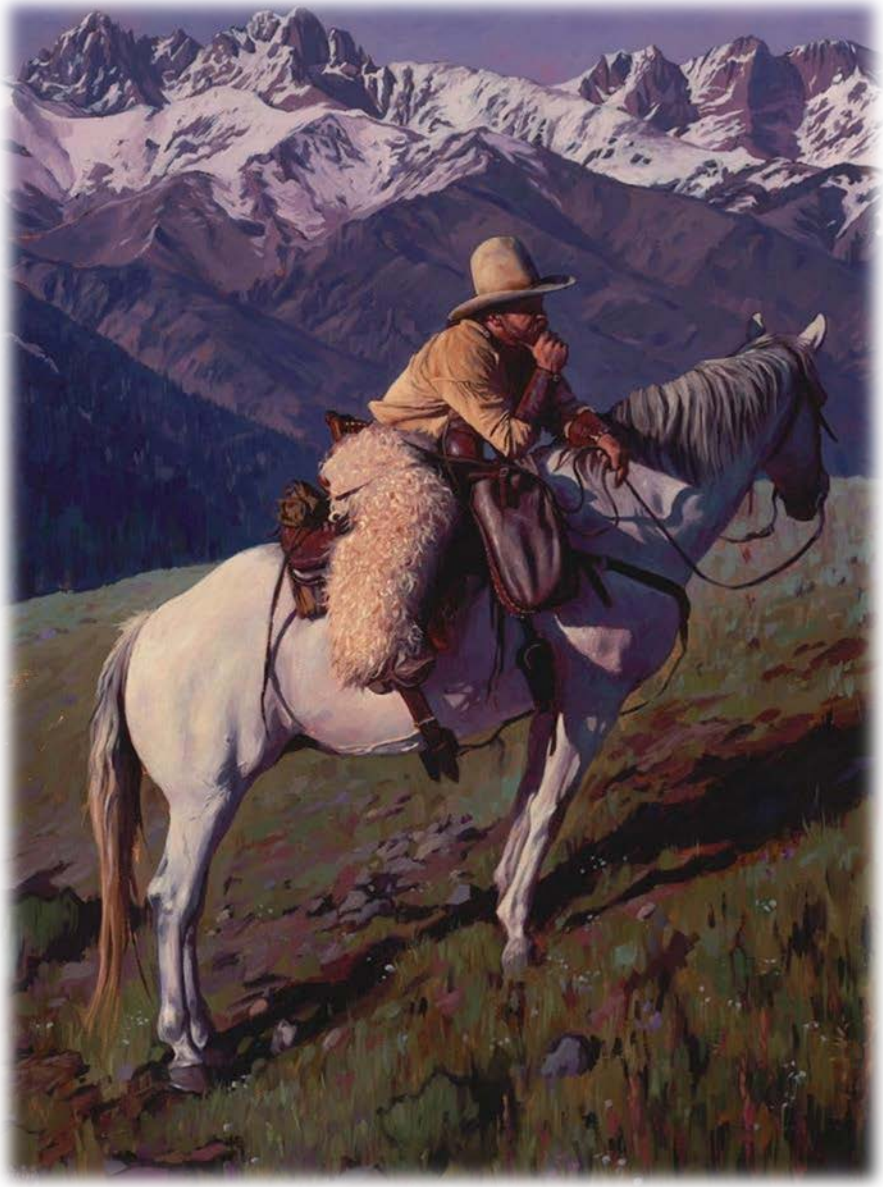
The Jig is Up

The **EU General Data Protection Regulation (GDPR)** is the most important change in data privacy regulation in 20 years - we're here to make sure you're prepared.

There's a New Sheriff in town Named GDPR

- **What's it's purpose**
  - To bring order to the Wild West of data usage Globally.
- **Who it applies to**
  - Any country in the EU.
  - If you hold or process personal EU citizen data no matter where you are located in the world.
- **How we got in this mess**
  - Silos between departments such as IT and Compliance or Marketing and IT for example.
  - The Dark Web Market is growing.
  - It's gotten personal i.e. breaches in healthcare around PHI.
  - The days of data privacy are over.
- **Why now**
  - The EU was fairly behind on security regulations so they needed a large regulation to cover all their bases.
  - The days of data privacy are **over** and data theft is increasing.
  - We continue to add technology to better our lives and create more holes for hackers to exploit.
  - U.S. States are beginning to adopt the GDPR-like best practices.

It’s a Journey to Compliance

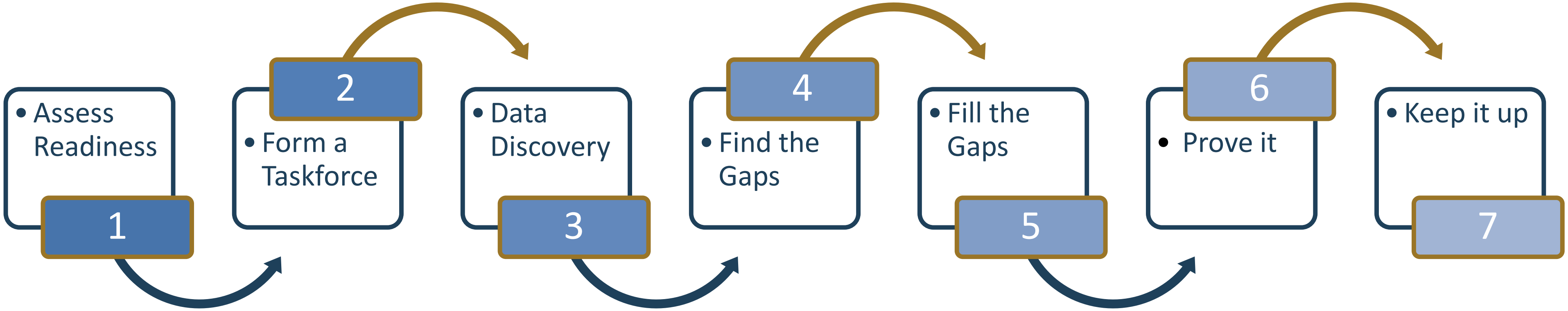


“The journey of 1000 miles begins with a single step.”

- Confucius

Where are you in your GDPR compliance Journey?

The Stages of GDPR Compliance



1
- Assess Readiness

2
- Form a Taskforce

3
- Data Discovery

4
- Find the Gaps

5
- Fill the Gaps

6
- Prove it

7
- Keep it up

Challenges Complying with GDPR

These aren't news to you

- **Experts**: It's a new regulation so finding an expert to help you plan for compliance is difficult.
- **Supervising authority**: Who do you have to attest compliance to?
- **Data Privacy Offers**: This is a role GDPR requires be dedicated to protecting the privacy of data and not all organizations have someone with the skillset.
- **Complex and wide reaching regulation**:
  - Understanding how it effects U.S. companies and at what level.
  - The solutions for complying are often vague and leave you to interpret when creating your action plan.
- **Knowing and Managing the "what ifs"**: What if you do nothing and bank on the adherence to other regulations like PCI?
- **Data Discovery**: identifying where your GDPR related data is, where it isn't, and being able to manage it if a citizen requests to be "forgotten". Dealing with patching legacy systems that hold relevant GDPR data.
- **The Stakeholders**: EU citizen data touches a lot of departments. Discovering who all needs to be involved in your internal GDPR taskforce.
- **Breach Notification**: 72 hours to report a breach doesn't leave much time for investigation and could damage your brand.
- **Fear:** The regulation comes with steep fines and penalties and it's easy to feel paralyzed.

Form Your Own GDPR Posse & Playbook

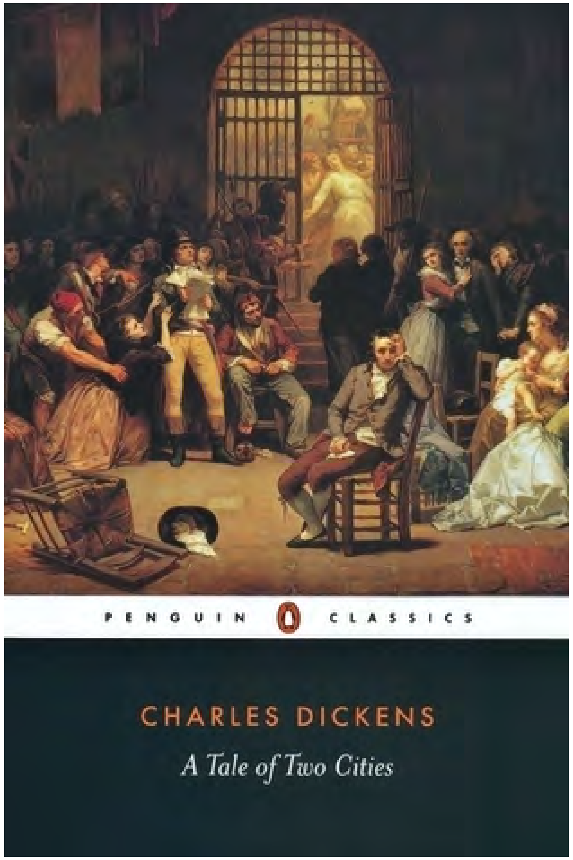
Find the best, rock star players

- **An executive, powerhouse player-** The tone from the top is key
- **A cybersecurity quarterback** – The team leader.
- **A compliance or data privacy guru** -
- **A security operations watchdog** – Security Operations
- **The referee** - loves putting processes into place. They are your stream-liners!
- **The all-star** – It's ok to ask for directions.

A Tale of 2 Regulations

"It was the best of times, it was the worst of times."

- EU GDPR
- California's Consumer Privacy Act of 2018 (CCPA)
  - Both place requirements on companies to protect PII
  - Both carry hefty fines for violations
  - Both require a data privacy program to be in place
  - Primary Difference?
    - GDPR is in effect NOW!
    - The CCPA does not go into effect until 1/1/2020



Anatomy of GDPR: Penalties and Fines

Why everyone is shaking in their boots...

By now, you’re likely making this comparison

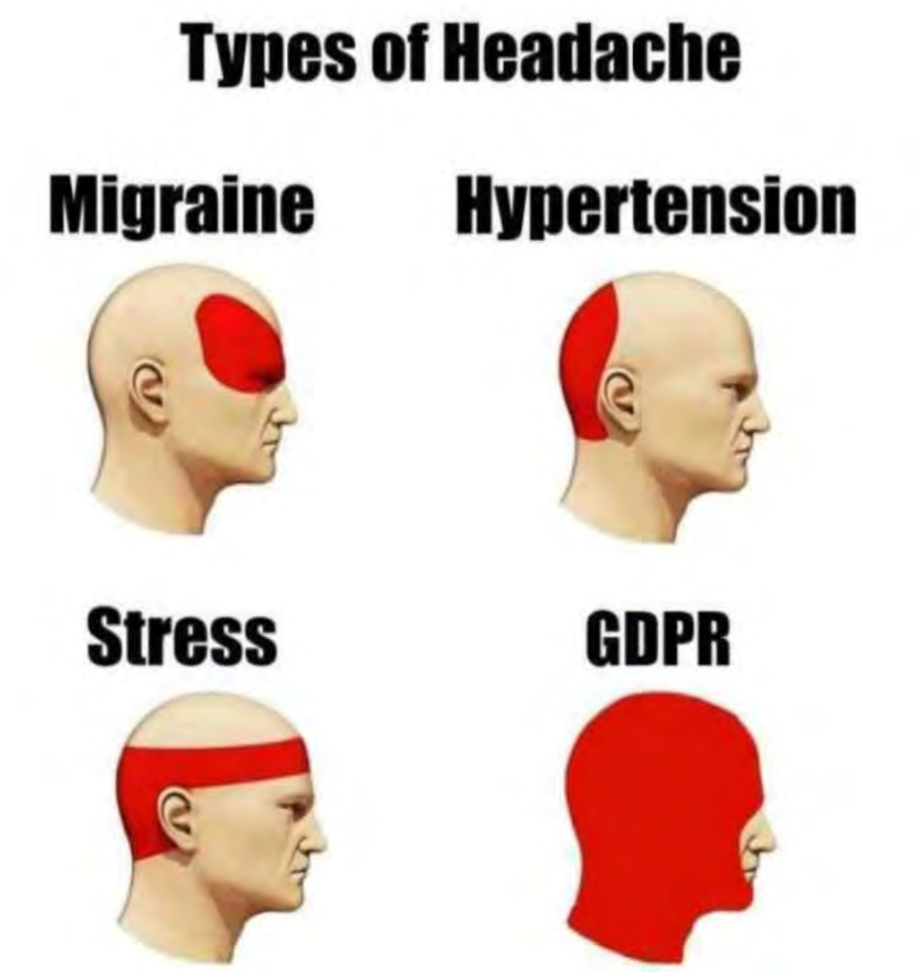


Image from futurecontent.co

Wanted: Dead or Alive

How Are GDPR Fines Determined?

- The nature, gravity and duration of the infringement
- The scope and purpose of the personal data processing
- The number of data subjects
- The degree of damage concerned by an infringement
- The level of cooperation with the data protection authority

Penalties and Fines: How to stay out of trouble

Security Due Diligence

- **GDPR Penalties, liability and requirements and how you can address them:**
  - 3rd and 4th party liability;
  - Both controllers and processors can be held liable for a breach so you must ensure you are all compliant;
  - Conduct risk assessments/audits of relevant internal systems and require evidence of the same from your providers or vendors; and
  - Require your suppliers audit their own supply chains to reduce exposure of fourth-party risks.
- **GDPR Article 32: Security of processing requires controllers and processors implement technical and organizational procedures to ensure suitable security, such as:**
  - Encryption including pseudonymization;
  - Processes and procedures for recurrently testing, assessing, measuring and evaluating their security;
  - Measures to ensure systems' confidentiality, integrity, availability and resilience; and
  - The ability to restore accessibility to personal data in a timely manner.
- **GDPR Articles 33 and 34 - Breach Notifications**
  - 72 hours doesn't leave much time for investigation.

Align GDPR Budget with Security Initiatives

It's raining...

- **Risk Management**
  - Third-Party and Fourth Party Vendor Risk Management
- **Vulnerability Management**
  - Scanning ports
  - Scanning web apps
  - Pen Tests (Internal and External)
- **Environmental & Threat Assessments**
  - Social Engineering
  - Cyber Threat Assessment Report Cards
- **Training and Education**
  - GDPR Data Privacy
  - Security Awareness Training

It's raining...

It’s Time to Settle the Score: Help Make the Grade with Scoring Technology

It's Time to Settle the Score on GDPR

Security Scores, Grades, and Report Cards can demonstrate your due diligence to supervising authorities in a universal language anyone can understand.

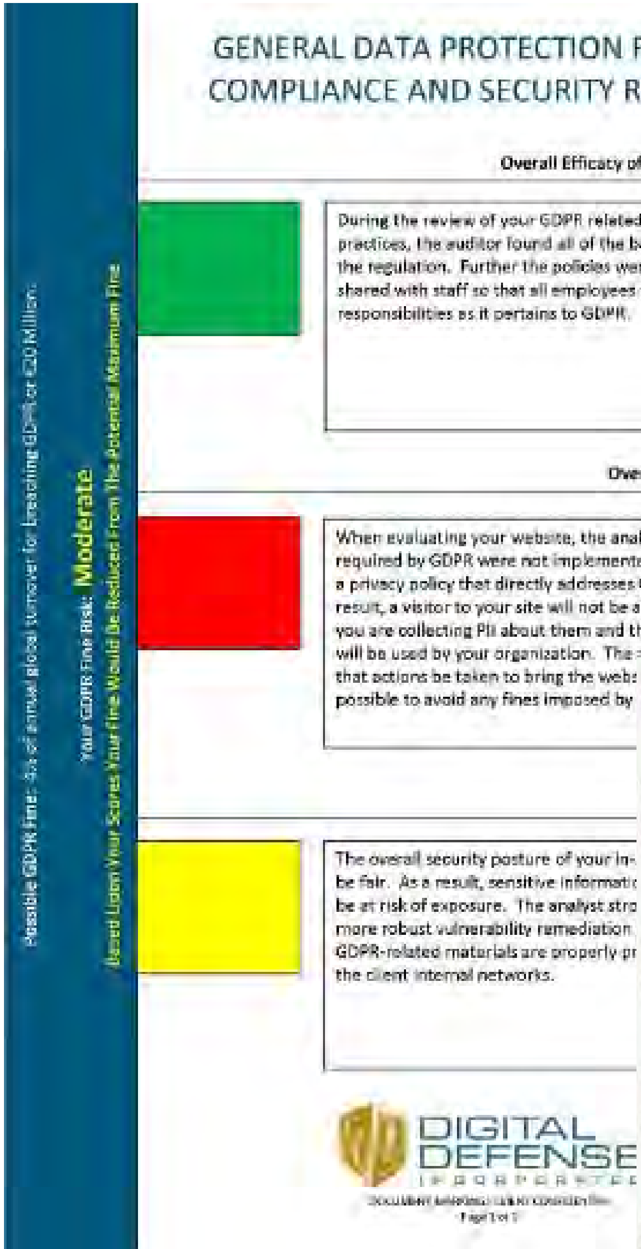
This technology is also beneficial when communicating with non-security experts and even board members about your security posture health and risk management.

- **How to obtain a score**
  - Vulnerability Scanner
    - Types of reports Scanners can provide to tell the security health story.
- **Why leverage scoring**
  - Communicating cross departmental in a way everyone can understand.
  - Understanding your security posture health.
- **Scoring Algorithms**
  - These vary based on what you are trying to measure, but the end goal is to tell the story so everyone can be on the same page when making savvy business decisions.

The Journey to the “Wild West” Began with a Plan

Much like the early Pioneers, the Journey to GDPR compliance needs a plan, and many questions had to be answered before, during and after to avoid threats.

Preparedness: The Fast Track to GDPR Compliance



Possible GDPR Fine: 4% of annual global turnover for breaching GDPR or €20 Million.

Your GDPR Fine Risk: **Moderate**

Based Upon Your Scores Your Fine Would Be Reduced From The Potential Maximum Fine

GENERAL DATA PROTECTION REGULATION
COMPLIANCE AND SECURITY REPORT CARD

Overall Efficacy of GDPR Related Internal Controls

🟩	During the review of your GDPR related policies, procedures and practices, the auditor found all of the basic tenets that are required by the regulation. Further the policies were well drafted and had been shared with staff so that all employees were aware of their roles and responsibilities as it pertains to GDPR.

Overall Efficacy of Website Controls

🟥	When evaluating your website, the analyst found a number of items required by GDPR were not implemented. As an example, there is not a privacy policy that directly addresses GDPR requirements. As a result, a visitor to your site will not be able to ascertain whether or not you are collecting PII about them and then understanding how that PII will be used by your organization. The analyst strongly recommends that actions be taken to bring the webs possible to avoid any fines imposed by
🟨	The overall security posture of your in be fair. As a result, sensitive informatic be at risk of exposure. The analyst stro more robust vulnerability remediation GDPR-related materials are properly pr the client internal networks.

DIGITAL DEFENSE INCORPORATED

DOCUMENT MARKING: CLIENT CONFIDENTIAL

Page 1 of 1

Advisera

CERTIFICATE

JOHN DOE

has successfully completed the

EU GDPR DATA PROTECTION OFFICER COURSE

by passing the written examination on 2018-XX-XX
Date of issuing the certificate: 2018-XX-XX

Authorized representative

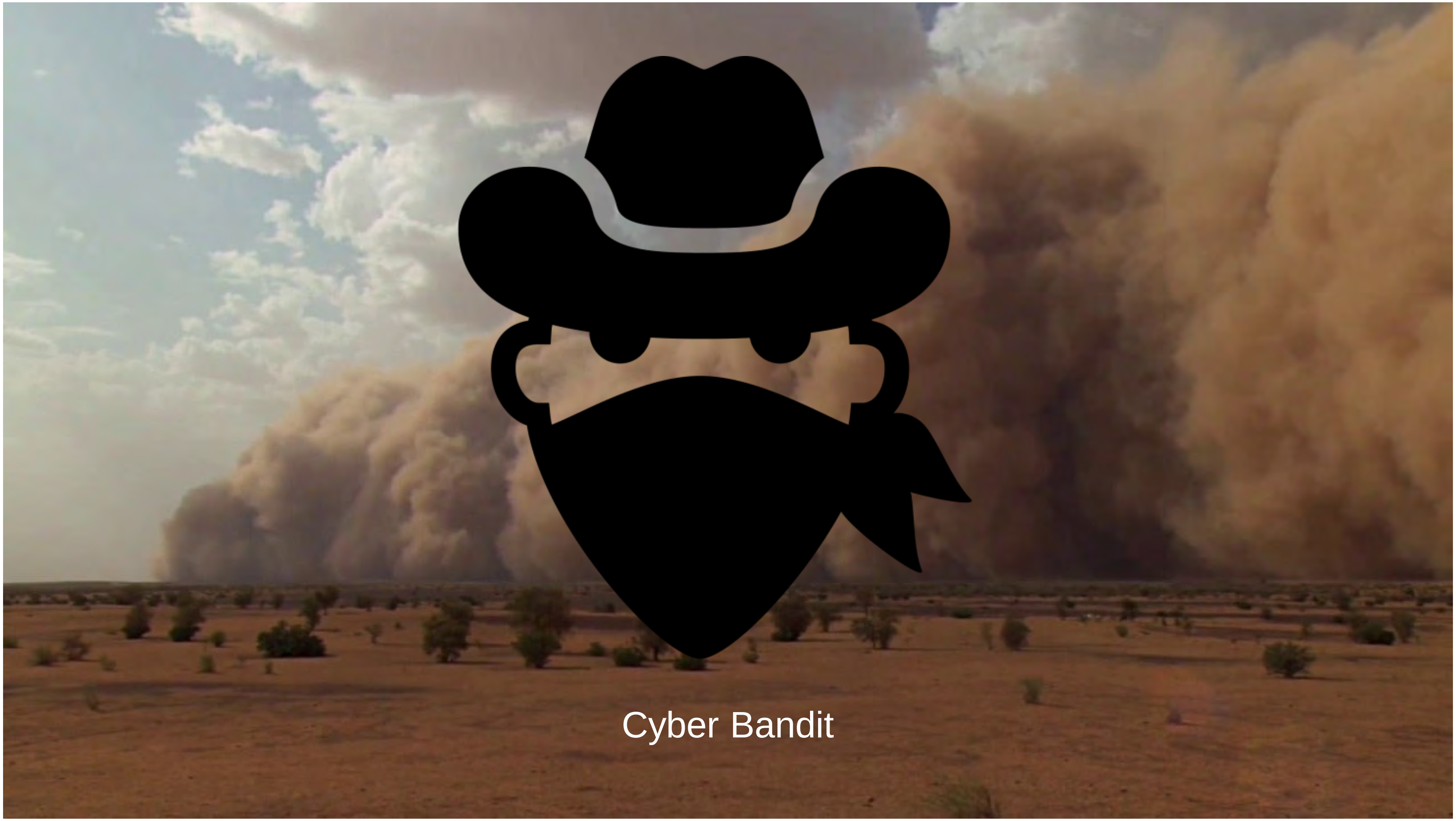
Dejan Kosutic

Know where you stand first

Whether you are a small, medium or larger sized organization, we have a solution to fit your needs for securing data and complying with GDPR.

- On-site evaluation performed by a Certified GDPR Data Protection Officer.
- Experts employ a combination of risk assessments and policy evaluations to identify gaps and vulnerabilities vis-a-vis adherence to GDPR regulations.

The Journey to Compliance Won’t Always Be Clear

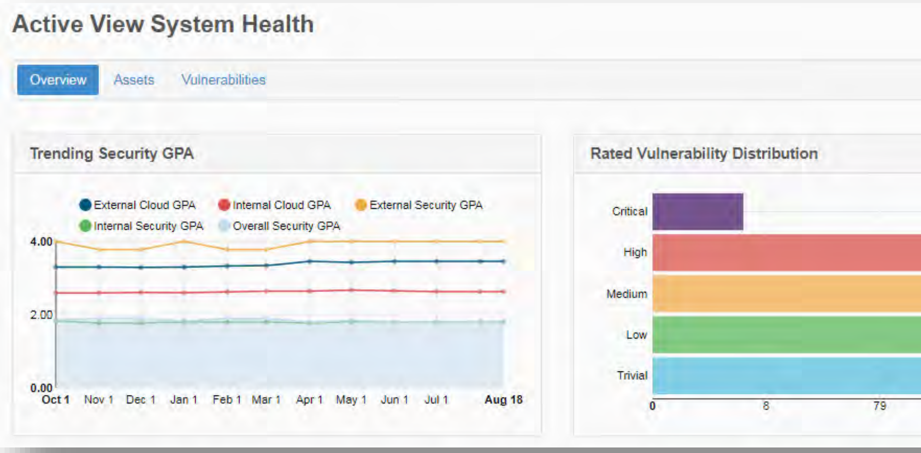


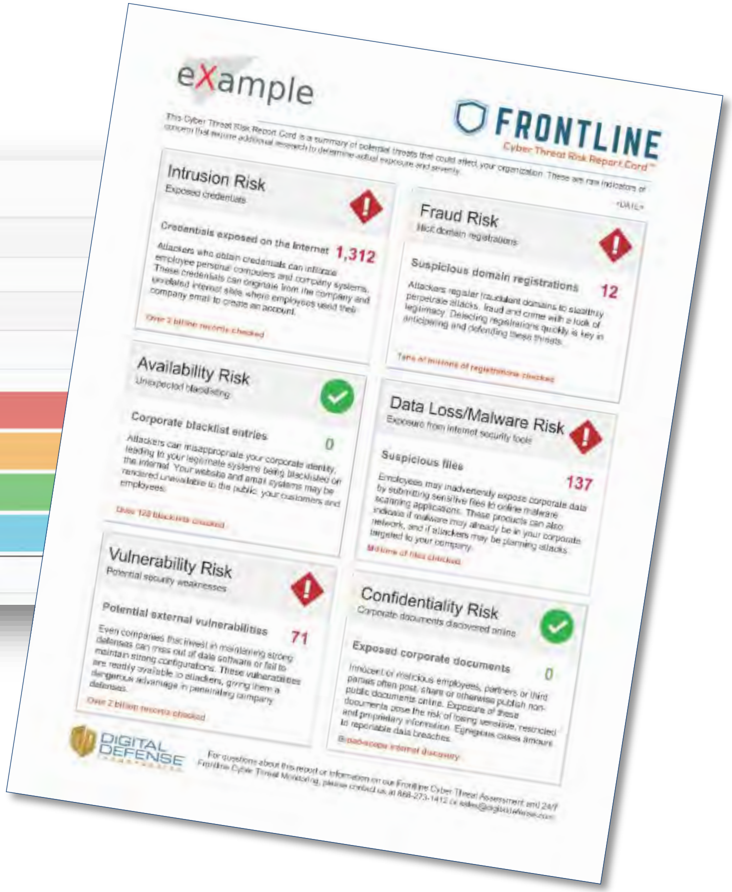
Other Cybersecurity Scores and Grades to Leverage

Settle the GDPR score by leverage security scoring and grading technology

Digital Defense specific

- Frontline Security GPA ™
- Cyber Threat Risk Report Card


Active View System Health


eXample

FRONTLINE
Cyber Threat Risk Report Card™

This Cyber Threat Risk Report Card is a summary of potential threats that could affect your organization. These are raw indicators of concern that require additional research to determine actual exposure and severity.

«DATE»

Intrusion Risk
Exposed credentials

Credentials exposed on the Internet 1,312

Attackers who obtain credentials can infiltrate employee personal computers and company systems. These credentials can originate from the company and unrelated internet sites where employees used their company email to create an account.

Over 2 billion records checked

Fraud Risk
Illicit domain registrations

Suspicious domain registrations 12

Attackers register fraudulent domains to stealthily perpetrate attacks, fraud and crime with a look of legitimacy. Detecting registrations quickly is key in anticipating and defending these threats.

Tens of millions of registrations checked

Availability Risk
Unexpected blacklisting

Corporate blacklist entries 0

Attackers can misappropriate your corporate identity, leading to your legitimate systems being blacklisted on the internet. Your website and email systems may be rendered unavailable to the public, your customers and employees.

Over 120 blacklists checked

Data Loss/Malware Risk
Exposure from internet security tools

Suspicious files 137

Employees may inadvertently expose corporate data by submitting sensitive files to online malware scanning applications. These products can also indicate if malware may already be in your corporate network, and if attackers may be planning attacks targeted to your company.

Millions of files checked

Vulnerability Risk
Potential security weaknesses

Potential external vulnerabilities 71

Even companies that invest in maintaining strong defenses can miss out of date software or fail to maintain strong configurations. These vulnerabilities are readily available to attackers, giving them a dangerous advantage in penetrating company defenses.

Over 2 billion records checked

Confidentiality Risk
Corporate documents discovered online

Exposed corporate documents 0

Innocent or malicious employees, partners or third parties often post, share or otherwise publish non-public documents online. Exposure of these documents pose the risk of losing sensitive, restricted and proprietary information. Egregious cases amount to reportable data breaches.

Broad-scope internet discovery

DIGITAL DEFENSE

For questions about this report or information on our Frontline Cyber Threat Assessment and 24/7 Frontline Cyber Threat Monitoring, please contact us at 888-273-1412 or sales@digitaldefense.com

How to Mind the Gaps:

Compliance and Security Toolkit

Compliance and Security Best Practices

- Scan
- Automate
- Analyze
- Test
- Score
- Educate
- Compliance

Vulnerability Scanning

What you need in a Vulnerability Scanning Solution

- Intelligent and Accurate Scanning Capabilities
- Responsive Modern Intuitive Interface
- Executive Dashboards
- Grading and Scoring universal language that translates to all levels of stakeholders
- Management Guidance & Oversight
- Technical Detail & Remediation Progress
- Custom Report Generation
- Powerful, Flexible Data Filtering
- Recurring Assessment Service

SCAN

ANALYZE

AUTOMATE

SCORE

Network Penetration Testing

What you need in an External and Internal Penetration Testing

- Certified Security Analysts and Ethical Hackers (in house or remote)
- Coverage of a vast array of systems
- Experience with variety of testing frameworks
- Robust Executive and Technical Reporting
- Recommendations for remediation

On-Site and Remote Social Engineering

What you need in Social Engineering Solution

- Identification of gaps in security policies and personnel awareness
- Balancing of investments in security technology versus personnel training
- Identification of the absence of necessary physical safeguards
- Obtaining records, equipment, sensitive information, unauthorized access, etc.

TEST

About Digital Defense, Inc.

DIGITAL DEFENSE® INCORPORATED

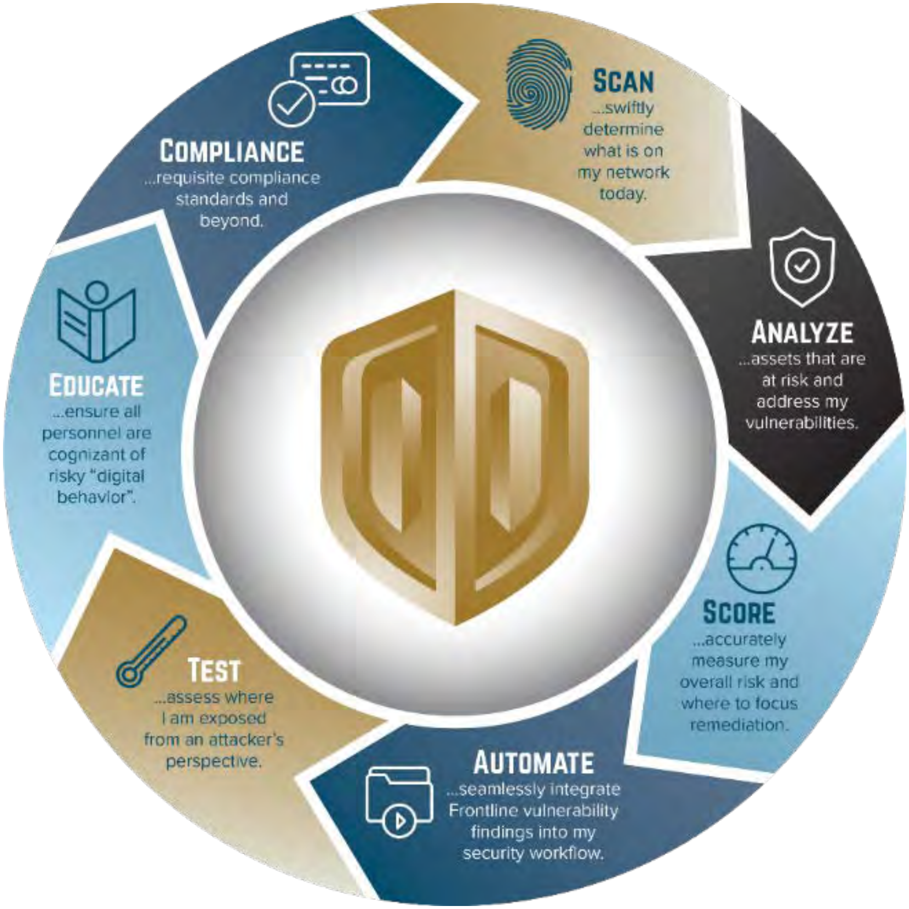
- Premier provider of security risk assessment solutions
- 19 years in the security industry
- Serving all industry verticals

- Industry recognized
- 99% customer satisfaction
- Net Promoter Score® of 74

For a Secure and Compliant Business

DIGITAL DEFENSE INCORPORATED

Shrink the Attack Surface™


SCAN
...swiftly determine what is on my network today.
ANALYZE
...assets that are at risk and address my vulnerabilities.
SCORE
...accurately measure my overall risk and where to focus remediation.
AUTOMATE
...seamlessly integrate Frontline vulnerability findings into my security workflow.
TEST
...assess where I am exposed from an attacker's perspective.
EDUCATE
...ensure all personnel are cognizant of risky "digital behavior".
COMPLIANCE
...requisite compliance standards and beyond.

Superior Technology & Results

- Frontline Security GPA®
- Patented Advanced Network Endpoint Identification and Correlation
- Zero-Tolerance False Positive Program (<0.01%)
- Automated Vulnerability Results and Remediation Management
- Standalone or Fully Managed Service

More

- Questions/Comments/Suggestions to:
  - webinars@digitaldefense.com

- Follow us:
  - www.digitaldefense.com
  - @Digital_Defense