

# INCIDENT RESPONDER'S FIELD GUIDE

LESSONS FROM A FORTUNE 100  
INCIDENT RESPONSE LEADER



# TABLE OF CONTENTS

- 03** Introduction & How to Use This Guide
- 04** Introducing Tim Bandos
- 05** Part One: Incident Response Do's and Don'ts
- 08** Part Two: Get Ready
- 18** Part Three: The Five Stages of Incident Response
- 31** Part Four: Advanced Threat Protection as a Service
- 35** Appendix: Digital Guardian – Next Generation Data Protection

# WHY READ THIS GUIDE?

Careful cyber security incident response planning provides a formal, coordinated approach for responding to security incidents affecting information assets. This e-book provides easy-to-follow steps for crafting an incident response plan in the event of cyber security attacks.

## HOW TO USE THIS GUIDE

IF YOU ARE...	GO TO...
<b>New to Incident Response Plan</b>	Part One: Incident Response Do's and Don'ts
<b>Not sure where to start?</b>	Part Two: Get Ready
<b>Familiar with Incident Response Plans, but how do I implement in my organization</b>	Part Three: The Five Stages of Incident Response
<b>Worried about managing Incident Response with limited resources</b>	Part Four: Advanced Threat Protection as a Service
<b>Looking to understand what makes Digital Guardian different</b>	Appendix: Digital Guardian — Next Generation Data Protection

# INCIDENT RESPONSE EXPERT

Tim Bandos is the Director of Cybersecurity at Digital Guardian. He has over 15 years of experience in the cybersecurity realm at a Fortune 100 company with a heavy focus on Internal Controls, Incident Response & Threat Intelligence. At this global manufacturer, he built and managed the company's incident response team.

Tim recently joined Digital Guardian to help build our Managed Security Program (MSP) to deliver advanced threat protection to our global customer base. He brings a wealth of practical knowledge gained from tracking and hunting advanced threats targeted at stealing highly sensitive data.



· To learn why Tim joined Digital Guardian read his blog post, Why I Signed on with an IT Security Vendor.



**TIM BANDOS**  
Director, Cybersecurity  
Digital Guardian CISSP,  
CISA, CEH & CASS



PART ONE

# INCIDENT RESPONSE DO'S AND DON'TS

# 5 THINGS **NOT** TO DO DURING AN INCIDENT

- 1 PANIC**

Do **not** panic. It's the worst thing you can do. You want to remain calm and having an IR plan will help to do just that. An IR plan will provide you with a predefined path that outlines the best course of action to take during an incident.

---
- 2 SHUT DOWN SYSTEMS**

Do **not** shut down infected systems. By shutting them down, you could lose volatile data that contains important forensic information. This information can be essential in determining the timeline of what transpired.

---
- 3 SOCIALIZE**

Do **not** discuss the incident with others unless otherwise directed. It's important to be cautious about the audiences that you choose to communicate with about an incident that has just begun to unravel.

---
- 4 USE DOMAIN ADMIN CREDENTIALS**

Do **not** use domain administrative credentials when accessing systems environment. Threat actors patiently wait for a user with enterprise-wide access to login in order to capture the password to gain complete control over the environment.

---
- 5 NON-FORENSIC TOOL USAGE**

Do **not** execute any non-forensic software on the infected systems because this will overwrite the timelines associated with the attack in the Master File Table.

# 4 THINGS TO DO DURING AN INCIDENT

- 1 COLLECT DATA**

Collect volatile data and other critical artifacts off the system using forensic tools. Forensically sound tools have the ability to connect to the system without modifying any timestamps on the device.

---
- 2 EXTERNAL INTELLIGENCE**

Gather external intelligence based on identified indicators of compromise (IOC). Search the web for intelligence about specific MD5s, IP addresses, domains that you discovered during your initial incident investigation. You are attempting to identify what the potential infection is or what type of malware may have been executed within the environment.

---
- 3 SAFEGUARD**

Safeguard systems and other media for forensic collection.

---
- 4 COLLECT LOGS**

Collect the appropriate logs. This may include Windows Events, Firewall, Netflow, Anti-Virus, Proxy, etc. It is important to view the story both at the network and at the endpoint level.

# PART TWO

# GET READY

# BUILD YOUR IR TEAM

An Incident Response team is a centralized team that is responsible for incident response across the organization.

The team receives reports of security breaches, analyzes the reports and takes necessary responsive measures. The team should be composed of:



## INCIDENT RESPONSE MANAGER

IR manager oversees and prioritizes different steps in detection, analysis and containment of the incident. In case of high severity incidents, IR manager also interfaces with the rest of the company, including corporate security, human resources, etc. to convey findings, status, and requirements.



## SECURITY ANALYSTS

These are the cyber-ninjas that go deep down into the weeds to identify when an incident has occurred and what has happened during that period of time. The team consists of:

- Triage Analysts - Filter out false positives and alert on potential intrusions
- Forensic Analysts - Recover key artifacts of data and maintain integrity of evidence to ensure a forensically sound investigation.



## THREAT RESEARCHERS

Threat researchers complement security analysts by providing threat intelligence and context to the incident. They are constantly combing the internet, identifying intelligence that may have been reported externally. They then build an internal database of internal intelligence derived out of prior incidents.

# GET CROSS-FUNCTIONAL SUPPORT

All business representatives must fully understand and advocate the Incident Response plan in order to ensure that the plan is properly executed, smooth information flow occurs and remediation takes place.



## MANAGEMENT

Management buy-in is necessary for provision of resources, funding, staff, and time commitment for incident response planning and execution.



## HUMAN RESOURCES

Human Resources is called upon when an employee is discovered to be involved with the incident.



## AUDIT AND RISK MANAGEMENT SPECIALISTS

The specialists help develop threat metrics and vulnerability assessments, along with encouraging best practices across the constituency or organization.



## GENERAL COUNSEL

The Attorney's role is to ensure the forensic value of any evidence collected during an investigation in the event that the company chooses to take legal action. An attorney can also provide advice regarding liability issues in the event that an incident affects customers, vendors, and/or the general public.



## PUBLIC AFFAIRS

The Public Relations' role is to communicate with team leaders, ensuring an accurate understanding of the issue and the company's status, so as to communicate with the press and/or informing the stockholders about the current situation.

# TIPS FROM TIM



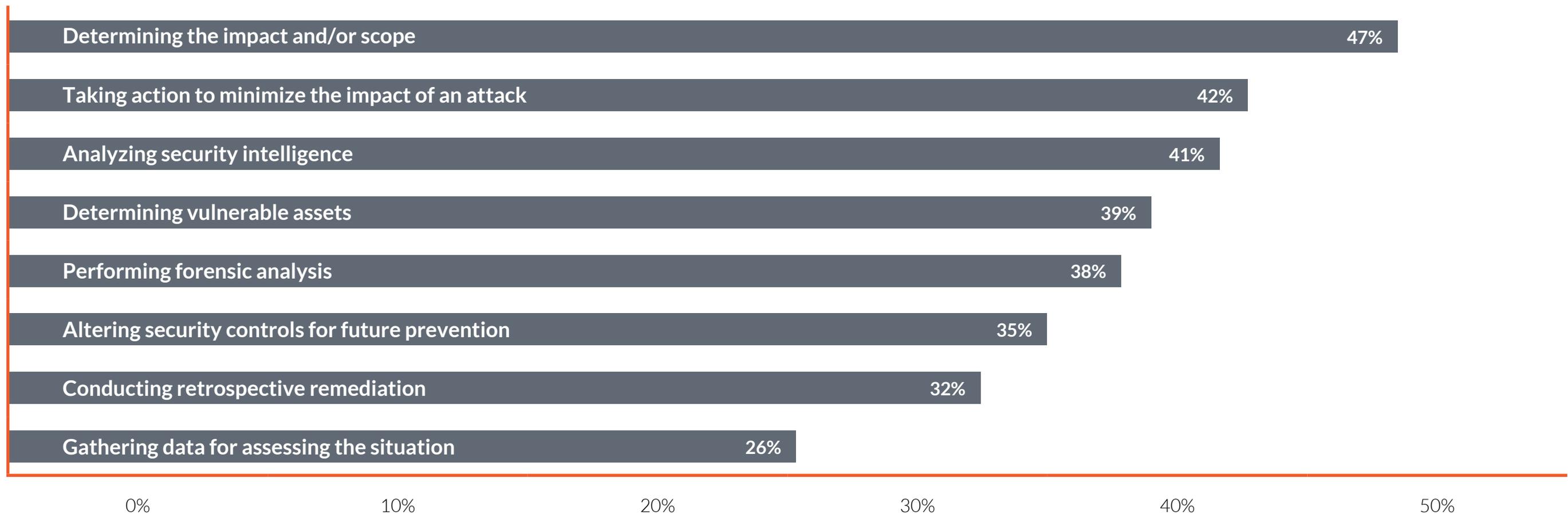
**TIM BANDOS**

Director, Cybersecurity  
Digital Guardian CISSP,  
CISA, CEH & CASS

## COMMUNICATION WITHIN AND ACROSS TEAMS IS CRITICAL

Communications during an incident should be conducted in a manner which protects the confidentiality of the information that is being disseminated. The incident response manager should be the central point of all communication and only those with a valid need-to-know is included in communications regarding key incident details, indicators of compromise, adversary tactics and procedures. Securing this communication so that Mr. Threat Actor is unable to snoop your messages is extremely vital to avoid tipping them off that an on-going investigation is occurring. Any indication that 'You're On to Them' may lead to swift changes by the attackers to further mask their activity.

# MOST TIME CONSUMING IR TASKS



Percent of respondents, N=700, three responses accepted  
(source: Enterprise Strategy Group, May 2015.)

# CREATE YOUR INCIDENT CLASSIFICATION FRAMEWORK

Creating an Incident Classification Framework is a critical component in enabling the proper prioritization of incidents. It will also help you derive meaningful metrics for future remediation purposes. We recommend a two-tiered classification scheme.

## INCIDENT CLASSIFICATION FRAMEWORK

### SECURITY INCIDENT CLASSIFICATION

1. Category
2. Type
3. Severity

### SECURITY INCIDENT TAXONOMY

1. Detection Method
2. Attack Vector
3. Impact
4. Intent
5. Data Exposed
6. Root Cause

**Note:** Incident classification may change several times during the incident management lifecycle as the team learns more about the incident from the analysis being performed.

# INCIDENT CLASSIFICATION FRAMEWORK

This first tier of classification organized by category, type and severity give the information you need to prioritize incident management.



## CATEGORY

- Unauthorized Access of the network
- Malware
- Denial of Service
- Improper Usage by an IT administrator (accidently or intentionally)
- Unsuccessful access Attempt
- Physical Asset Loss
- Explained Anomaly



## TYPE

- Targeted vs Opportunistic Threat
- Advanced Persistent Threat
- State sponsored act of espionage
- Hactivism Threat
- Insider Threat
- Nuisance Threat



## SEVERITY

- **Critical Impact** - Threat to public safety or life
- **High Impact** - Threat to sensitive data
- **Moderate Impact** - Threat to computer systems
- **Low Impact** - Disruption of services

# INCIDENT TAXONOMY

Taxonomy gives you additional information you need to identify root cause, trends and intelligence. It also provides you with the information for essential incident response metrics.



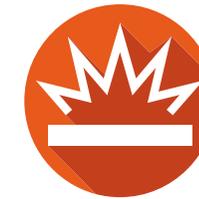
## DETECTION METHOD

- End user
- 3rd Party Service Provider
- Law Enforcement such as the FBI
- Intrusion prevention and detection systems
- Data Loss Prevention system, Firewall, Anti-Virus, Proxy and Netflow



## ATTACK VECTOR

- Viruses
- E-mail attachments
- Web pages
- Pop-up windows
- Instant messages
- End user action
- Exploiting system vulnerabilities
- 3rd party compromises, etc



## IMPACT

- Employee Dismissal
- HR / Ethics Violation
- Loss of Productivity
- Unauthorized Privileges
- Website Defacement
- Brand Image
- Lawsuit
- Denial of Service
- Compromise of IP
- Malicious Code Execution

# INCIDENT TAXONOMY (CONT.)

Taxonomy gives you additional information you need to identify root cause, trends and intelligence. It also provides you with the information for essential incident response metrics.



## INTENT

- Non-Malicious
- Malicious
- Theft
- Accidental
- Physical Damage
- Fraud
- Defamation
- Espionage



## DATA EXPOSED

- Public
- Confidential
- Export Control
- Financial Reporting
- Unknown



## ROOT CAUSE

- Unauthorized Action
- Vulnerability Management
- Theft
- Security Control Failure/Gap
- Disregard of Policy
- User Negligence
- Non-Compliance to Standards such as PII, PCI, HIPPA
- Service Provider Negligence

# TIPS FROM TIM



**TIM BANDOS**  
Director, Cybersecurity  
Digital Guardian CISSP,  
CISA, CEH & CASS

## DETECT THREAT ACTORS THROUGH ANTIVIRUS LOGS

Your good ol' antivirus solution may only detect 10 to 15 percent of malware, but your antivirus logs may contain critical indicators of the attack.

When threat actors break into your environment, one of their first objectives is to acquire passwords by running a credential dumping program. Your antivirus might detect this activity the first time and block the program from executing. But further executions of different credential dumping programs may go unnoticed, so it's important to alert on any activity associated with these types of malicious tools. Having the log of the first attempt is critical because that might be the single thread that you need to pull and unravel to identify a potential incident.

PART THREE

# 5 STAGES OF INCIDENT RESPONSE



**1** PREPARATION



**2** DETECTION AND REPORTING



**3** TRIAGE AND ANALYSIS



**4** CONTAINMENT AND NEUTRALIZATION



**5** POST-INCIDENT

# 1. PREPARATION

“Preparation is the key to effective incident response.”

## DEVELOP AND DOCUMENT IR POLICIES

Establish policies, procedures, and agreements regarding incident response management.

## CONDUCT CYBER HUNTING EXERCISES

Conduct operational threat hunting exercises to find incidents occurring within your environment. This will enable you to be more proactive in your incident response.

## DEFINE COMMUNICATION GUIDELINES

Create standards and guidelines to enable effective communication flow during and after the incident.

## ASSESS YOUR THREAT DETECTION CAPABILITY

Assess your current threat detection capability and accordingly influence risk assessment and improvement program.

## INCORPORATE THREAT INTELLIGENCE FEEDS

Perform ongoing collection, analysis, and fusion of your threat intelligence feeds.

## SAMPLE TEST PLAN

### NIST GUIDE

- Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities

### SANS GUIDE

- SANS Institute InfoSec Reading Room, Incident Handling Annual Testing and Training

# TIPS FROM TIM



**TIM BANDOS**  
Director, Cybersecurity  
Digital Guardian CISSP,  
CISA, CEH & CASS

## 5 TIPS TO MAKE INCIDENT COMMUNICATION EFFECTIVE



**1** Avoid using speakerphones. You don't want people in the hallway to overhear your discussions.

---



**2** Avoid using instant messenger systems unless they are encrypted end to end or secure in some other way.

---



**3** Try to avoid using email as much as possible because threat actors may have access to your email systems ("Man in the Mailbox") watching every message coming in and out.

---



**4** Communicate in-person if possible and use secure lines for phone conversations.

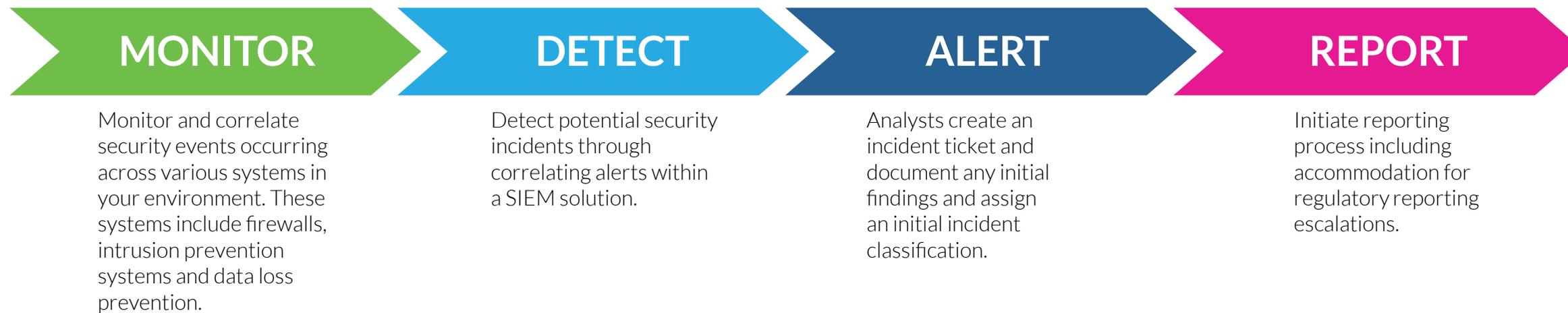
---



**5** Use pre-shared access codes for authenticating users for bridge/conference calls.

# 2. DETECTION AND REPORTING

The focus of this phase is monitoring and correlation of security events in order to detect, alert, and report on potential security incidents.



# TIPS FROM TIM



**TIM BANDOS**

Director, Cybersecurity  
Digital Guardian CISSP,  
CISA, CEH & CASS

## CENTRALIZED LOGS CAN OFTEN TELL YOU THE STORY

A centralized SIEM that ingests logs from all of your security systems—such as antivirus, firewall, intrusion prevention systems, data loss prevention, is a critical tool.

A SIEM enables you to search across all devices within your enterprise to identify malicious activity and enable you to trace back and determine how a potential threat gained access. What boxes did they touch? What firewall did they go through or what data leak prevention logs may have been generated when they were on a system. Incident Responders need to answer these types of questions and having a SIEM will make it easier in doing so.

# 3. TRIAGE AND ANALYSIS

The triage and analysis phase initiates the bulk of the effort in properly scoping and understanding the security incident. Resources should be engaged to collect data from tools and systems for further analysis and identifying Indicators of Compromise. These individuals should have in-depth skills and a detailed understanding of **Live System Response, Digital Forensics, Memory Analysis, and Malware Analysis.**

As evidence is collected, the analyst will now focus on 3 primary areas:





# 3. TRIAGE AND ANALYSIS (CONT.)

## END POINT ANALYSIS

- Determine what tracks may have been left behind by the threat actor.
- Gather the artifacts needed to build a timeline of activities.
- Analyze a bit-for-bit copy of systems from a forensic perspective & capture RAM to parse through and identify key artifacts of what occurred on a device. RAM is feature rich with data on activities executed by a threat.

## BINARY ANALYSIS

- Investigate malicious binaries or tools leveraged by the attacker in order to document the purpose and functionality of those programs. This analysis is performed in two ways:
  1. **Behavioral Analysis** - Executes malicious program in a VM to monitor its behavior.
  2. **Static Analysis** - Reverse engineer the malicious program in order to scope out the entire functionality.

## ENTERPRISE HUNTING

- Enterprise hunting is performed to identify all systems impacted by a security incident.
- Analyze existing systems and event log technologies to determine machines in scope of a compromise.
- This will allow the responder to document all compromised accounts, machines, malware used, etc. so that effective containment and neutralization can be performed.

# 4. CONTAINMENT AND NEUTRALIZATION

This is one of the most critical stages of the incident to ensure that a malicious infection is completely eradicated from the environment. The strategy for containment and neutralization is based on intelligence and indicators of compromise developed throughout the incident analysis phase. After the system is restored and verified that there are no further security compromises, normal operations can resume.

## COORDINATED SHUTDOWN

Once you have identified all systems within the environment that have been either accessed or compromised by a threat actor, perform a coordinated shutdown of these devices at the same time. When performing the coordinated shutdown, a notification is sent out to all IR team members to gain alignment on timing and the resources required to perform the remediation.

## WIPE AND REBUILD

Wipe the infected devices and rebuild the operating system from the ground up. Change passwords of all compromised accounts.

## THREAT MITIGATION REQUESTS

If you have identified domains or IP addresses that are known to be leveraged by threat actors for command and control, issue threat mitigation requests to block the communication at all egress channels.

# TIPS FROM TIM



**TIM BANDOS**

Director, Cybersecurity  
Digital Guardian CISSP,  
CISA, CEH & CASS

## COORDINATE SYSTEM SHUTDOWN

I recall once during an incident that a compromised server was not shutdown during a coordinated effort. It actually alerted the threat actors and they knew that something was going on within our environment and that we were attempting to kick them out. So they immediately came back in, not even within 10 minutes of those servers being shut down to move laterally again within the environment and installed a whole set of new malware and tools. We had to go through the entire process again of conducting triage and analysis. Therefore, it is extremely important that all parties involved in a neutralization process follow the instructions carefully to avoid this from happening.

# TIPS FROM TIM



**TIM BANDOS**

Director, Cybersecurity  
Digital Guardian CISSP,  
CISA, CEH & CASS

## NEVER LET A GOOD INCIDENT GO TO WASTE

Now is the time to answer those critical questions: How did this happen? What were they targeting? What controls should we have had in place that would've prevented this intrusion from occurring in the first place? Are there specific areas within our security that require additional resources or funding to cover those gaps? As you think through these questions that relate to the Incident at hand, also begin to think about the organization in general and what security metrics could be reported each week/month/quarter to further shed light on any chinks in the armor. Develop a heat-map of your Cyber Security Readiness Scorecard and include areas such as Vulnerability Assessments / Remediation, SIEM Event Collection, Continuous Visibility, Security Configurations, etc. A scorecard that appears to have been dipped in red paint, indicating serious control gaps, will undoubtedly get the attention that it deserves.

# 5. POST-INCIDENT ACTIVITY

## 1. COMPLETE INCIDENT REPORT

Documenting and disseminating the incident will help improve the incident response plan and to augment additional security measures to avoid such security incidents in the future.

## 4. IDENTIFY PREVENTATIVE MEASURES

Identify new security initiatives to prevent future incidents.

## 2. MONITOR POST-INCIDENT

Closely monitor for activities post-incident since threat actors will re-appear again. We recommend a security log hawk analyzing SIEM data for any sign of indicators tripping that may have been associated with the prior incident.

## 5. GAIN CROSS-FUNCTIONAL BUY-IN

Coordination across the organization is critical in order to implement new security initiatives.

## 3. UPDATE THREAT INTELLIGENCE

Update the organization's threat intelligence feeds.

# TIPS FROM TIM



**TIM BANDOS**

Director, Cybersecurity  
Digital Guardian CISSP,  
CISA, CEH & CASS

## BE SURE TO RESET CREDENTIALS

You have to be sure to reset any passwords that may have been compromised during the incident. It's important to note though that, once a threat actor has gained access to a system they immediately dump the credentials. Consequently, they have a whole bunch of credentials and it might not just be the one or two that they've used. Therefore as part of the post-incident monitoring, identify any failed login attempts with those accounts. It could be a potential indication that they're back in within the environment attempting to use what they've previously harvested.

# PART FOUR

# ADVANCED THREAT PROTECTION AS A MANAGED SECURITY PROGRAM

# WHEN DOES IT MAKE SENSE TO CONSIDER ATP AS A SERVICE?

If any of these apply to your organization it may make more sense to outsource or augment your Incident Response team with an Advanced Threat Protection Managed Security Program:



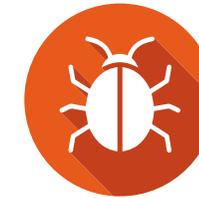
## **SECURITY TALENT SHORTAGE**

The severe security talent shortage, especially for cyber security professionals, is preventing you from finding and retaining the people you need to build an IR team.



## **HEADCOUNT CHALLENGES**

The political climate of your organization makes it difficult to gain approval for the 3-5 people you need to build an effective IR team.



## **COMPLEXITY OF STAYING ON TOP OF SOPHISTICATED MALWARE**

Modern malware is sophisticated, targeted and difficult to detect. According to Verizon's latest Data Breach Investigations Report, companies on an average went more than 200 days between the time they were breached and the day they discovered the malware. As malwares get smarter, your ability to prevent the loss of sensitive data on your own gets harder and harder.

# ADVANCED THREAT PROTECTION MANAGED SECURITY PROGRAM

## THE LATEST DEFENSE STRATEGIES AND INTELLIGENCE

Our Advanced Threat Protection Managed Security Program is led by Tim Bandos, Director of Cybersecurity. The program combines security researchers and analysts' expertise, Digital Guardian's Next Generation Data Protection Platform and a centralized threat intelligence management system. This combination enables Digital Guardian to detect and remediate threats faster and more efficiently. You can expect the highest level of protection from threats including polymorphic malware, zero-day attacks, advanced persistent threats (APTs), ransomware and attacks involving sophisticated data theft methods.



**DIGITAL GUARDIAN**  
MANAGED SECURITY PROGRAM  
FOR ADVANCED THREAT PROTECTION

## WHY DIGITAL GUARDIAN?

### REAL-TIME VISIBILITY

Digital Guardian continues endpoint monitoring includes real-time and historic visibility into more than 200+ parameters associated with system activities. Visibility into the entire kill chain lifecycle means more effective detection & analysis by our team.

### THREAT INTELLIGENCE

Our team harnesses both externally and internally generated intelligence feeds for immediate detection based on known threat activity.

### EYES ON GLASS IDENTIFYING YOUR REAL RISKS

Our analyst team is constantly reviewing your data for anomalous behavior and alerting you immediately upon discovery. Alerts generated by your team will provide you with a summary of what's been detected and details around the type of alert.

### INDICATORS OF EXECUTION

Our service utilizes behavioral-based signatures based on profiled malware and threat actor activity that is delivered via your content feeds. Your team is constantly researching emerging threats and developing these signatures to keep up with the dynamic & evolving world of threats.

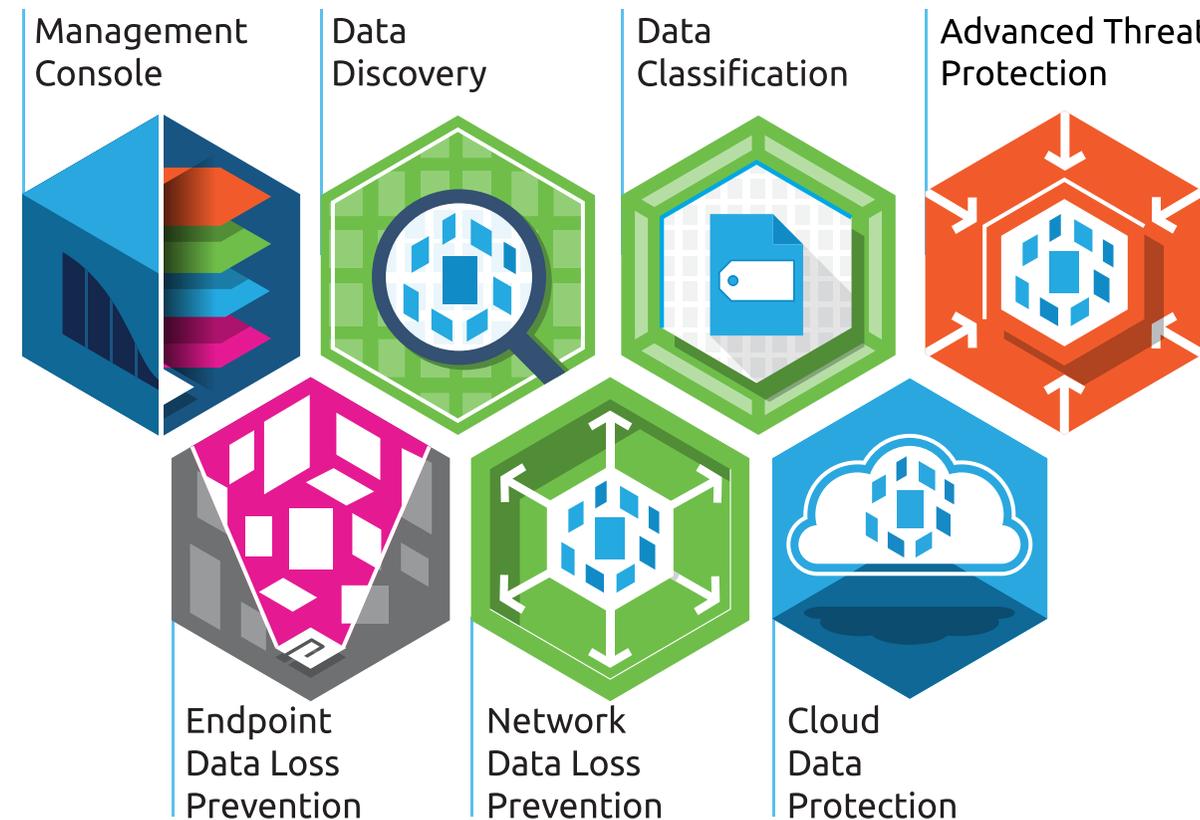
# APPENDIX

# DIGITAL GUARDIAN NEXT GENERATION DATA PROTECTION

# NEXT GENERATION DATA PROTECTION

Data protection is at the core of our company mission. Our next generation data protection platform is purpose built to stop data theft. This platform is designed to:

- Discover and protect sensitive data through out the data lifecycle and across the enterprise
- Protect sensitive data on the network at the endpoint, in storage and in the cloud
- Provide automated classification
- Provide integrated advanced protection to protect data from external threats
- Provide flexible deployment options including a managed security service manned by our peerless analyst team with deep, real-world expertise



 **FREE DOWNLOAD**

Digital Guardian Platform Technical Overview

 **FREE DOWNLOAD**

Digital Guardian Managed Security Program Technical Overview

# A LEADER IN THE GARTNER MAGIC QUADRANT QUADRANT

- “Digital Guardian offers one of the most advanced and powerful endpoint DLP agents due to its kernel-level OS integration. In addition to Windows, both Apple OS X and Linux are supported.”
- **“The Digital Guardian solution for endpoint covers DLP and endpoint detection and response (EDR) in a single agent form factor...”**
- “...Digital Guardian [is one of] two vendors most frequently mentioned by clients looking for a managed services option.”



• Gartner 2016 MQ for Enterprise DLP

Gartner 2016 Magic Quadrant for Enterprise Data Loss Prevention, 1 February, 2016, Brian Reed and Neil Wynne.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and is used herein with permission. All rights reserved.

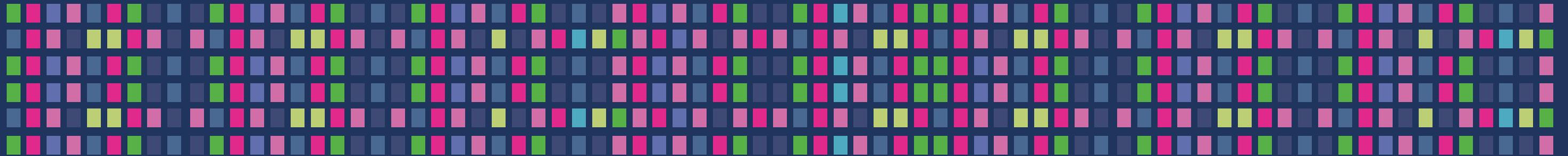
Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Digital Guardian.

2016 GARTNER MAGIC QUADRANT FOR ENTERPRISE DATA LOSS PREVENTION



# 60 MILLION TERABYTES OF SENSITIVE DATA IS PROTECTED DAILY BY DIGITAL GUARDIAN AGENTS



OVER **2.5 MILLION** AGENTS DEPLOYED WORLDWIDE TRUSTED DAILY BY MORE THAN **450** OF THE LARGEST BRANDS IN THE WORLD



...ONE OF THE LARGEST AND MOST RESPECTED COMPANIES IN THE WORLD HAS DEPLOYED OVER **300,000** AGENTS

INCLUDING... 7 OF THE TOP 10 PATENT HOLDERS

AND 7 OF THE TOP 10 AUTO COMPANIES

THE ONLY AGENT-BASED TECHNOLOGY COVERING **250,000 EMPLOYEES** USING A SINGLE MANAGEMENT SERVER

WE ARE THE DATA PROTECTOR OF CHOICE IN

- ENERGY
- FINANCIAL SERVICES
- GOVERNMENT
- TECHNOLOGY
- HEALTHCARE & LIFE SCIENCES
- MANUFACTURING

BECAUSE WE'RE FOCUSED ON PROTECTING ONE THING:



# INCIDENT RESPONDER'S FIELD GUIDE

QUESTIONS?

1-781-788-8180

[info@digitalguardian.com](mailto:info@digitalguardian.com)

[www.digitalguardian.com](http://www.digitalguardian.com)

