GIGAOM RESEARCH

The industry leader in emerging technology research

ADVANCED THREAT DETECTION AND CYBER HUNTING

MARKET LANDSCAPE REPORT

AUTHOR: Simon Gibson - GigaOm Analyst

AUTHORED BY GIGAOM ANALYST, SIMON GIBSON

INTRODUCTION

Cyber threat hunting is the act of proactively searching through systems and networks to detect and isolate cyber threats that manage to evade existing security solutions. Rather than rely solely on traditional solutions such as firewalls, sandboxes, or SIEMs to alert on suspicious activity, hunting puts the security operations team in the driver's seat.

Hunting evolved in part from good threat intelligence used to alert teams to active threats. In this GigaOm, Analyst Simon Gibson examines how the use of threat intelligence in combination with analytic and situational awareness drives early detection of breaches. Learn how to speed up the mean time to detect a compromise by using Indicator of Compromise (IoC), understanding the adversary's Tactics, Techniques and Procedures (TTPs) and combining with good network and system instrumentation. This report looks at different components that make up a complete hunting stack, including:

- Host and network based visibility
- Backend storage
- Data access including cyber hunting specific taxonomy and query language
- Intelligence sharing
- Automation

We discuss where hunting must be manual and how to automate it using vendors and tools as a company's security operations center and network instrumentation matures.

REPORT TOPICS

- Visibility
  - Network or Host based
  - Roll your own vs buy
  - Packet collection
  - Native system log collection
  - Agent based instrumentation
- Backend Storage
  - Scale needed
  - Tamper proofing
- Access to Data
  - Data storage structure
  - Hunting specific query language
- Threat Intelligence
  - Providers and sources for IoCs
  - Information sharing networks and resources
- Analytic Engines
  - Tools to compare and contract system telemetry against threat intelligence

ARE YOU PREPARED?

- **Is your enterprise ready to start a hunting program?**
  - Are the basics covered?
  - Does your team have the capability and appetite to instrument devices connected to the network?
  - Can any existing infrastructure be repurposed?
- **Do you know the best options to gather telemetry based on your network design and usage patterns?**
  - Is it better to focus on deploying a packet based solution or an endpoint based one?
  - What the benefits of an Endpoint Detection and Response (EDR) platform vs an Endpoint Protection Platform (EPP)?
- **What should you consider for storage requirements?**
  - How much scale will you need?
  - What are the read/write requirements for the storage?
  - What are the tools that will be ingesting the data and what must the alerting ecosystem look like?
- **What are the intelligence inputs and output requirements?**
  - What threat data will you consume?
  - How will you baseline your environment?
  - What will the intelligent outputs be?
- **How will you manage the analytics?**
  - What sorts of structures will be needed to test breach hypothesis?
  - How will you script the inputs to refine and test your cyber hunting platform?
  - What will the success criteria of consist of?

ABOUT

ANALYST SIMON GIBSON

Simon Gibson is a **CISO and subject matter expert on security.** He has been responsible for driving security capability into products, enterprises and supporting complex engagements.

Simon led the Information Security Group at Bloomberg and served as their CISO. He has managed attack teams, incident response teams and been responsible for the defensive security posture in the financial, government, manufacturing and PCI industries.

Simon is a **renowned speaker and panel moderator.** He has counseled fortune 100's on building their programs and worked with US Government public private information sharing initiatives.

@simonhg

https://www.linkedin.com/in/simonhg/

INTERESTED IN GIGAOM REPORTS?

To purchase this report, or to explore opportunities to participate in future GigaOm reports, Email a GigaOm Business Development Representative.

GIGAOM

Find us:
gigaom.com

GigaOm provides technical, operational, and business advice for IT's strategic digital enterprise and business initiatives. Enterprise business leaders, CIOs, and technology organizations partner with GigaOm for practical, actionable, strategic, and visionary advice for modernizing and transforming their business. GigaOm's advice empowers enterprises to successfully compete in an increasingly complicated business atmosphere that requires a solid understanding of constantly changing customer demands.

GigaOm works directly with enterprises both inside and outside of the IT organization. To apply proven research and methodologies designed to avoid pitfalls and roadblocks while balancing risk and innovation. Research methodologies include but are not limited to adoption and benchmarking surveys, use cases, interviews, ROI/TCO, market landscapes, strategic trends, and technical benchmarks. Our analysts possess 20+ years of experience advising a spectrum of clients from early adopters to mainstream enterprises.

GigaOm's perspective is that of the unbiased enterprise practitioner. Through this perspective, GigaOm connects with engaged and loyal subscribers on a deep and meaningful level.