CyberDB

The Cyber Research Databank

security orchestration, automation and response (SOAR)

Facts and Emerging Vendors

April 14th, 2018

Contents

1. Introduction

There are a number of threats to today's complex information systems. An internal employee can download a single instance of ransomware and can have a significant impact on an organization. More complex attacks such as a network exploitation attempt or targeted data breach increases the chaos that a security incident causes.

Having the ability to properly respond to security incidents in an orderly and efficient manner allows organizations to both limit the damage of a potential cyber-attack, but also recover from the associated damage that is caused. To facilitate this orderly response, organizations of all sizes have looked at adding an incident response capability to their existing policies and procedures.

Enterprises are striving to keep up with the current threat landscape with too many manual processes, while struggling with a lack of resources, skills and budgets. Security and risk management leaders should determine which Cyber Incident Detection, Response and Threat Intelligence solution improve security operations efficiency, quality and efficacy.

2. The impacts of cybercrime

The annual cost to the global economy from cybercrime is estimated to be US$445 billion *(1).* As businesses across every industry fall victim to cyber-attack, all corporate officers and functions — from the board, executive management, risk functions and general counsel to business units and information technology (IT) — are being profoundly affected.

Take, for example, a Fortune 50 global retailer that disclosed a data breach in September 2014. After stealing credentials from a vendor, hackers were able to break into the retailer's networks, install malware, and steal 56 million credit card numbers and 53 million email addresses over five months before the compromise was discovered and eradicated. This has had operational, legal and financial impacts. The retailer hired two external forensic investigation firms to investigate and remediate the technical aspects of the breach. In addition, five outside law firms were engaged in order to address the legal ramifications of over 40 civil suits stretching across multiple countries, in which customers and financial institutions have alleged negligence in protecting consumer data. The retailer is further being investigated by several state attorneys general in the United States. As the company's own SEC filing stated, "These claims and investigations may adversely affect how we operate our business, divert the attention of management from the operation of the business, and result in additional costs and fines."

Significant business impacts, however, do not result solely from the release of customer information. A multinational conglomerate became the victim of both data theft and destruction when attackers destroyed an undisclosed number of computers and forced the company to shut down parts of its networks for periods ranging from days to months. From the terabytes of data that attackers claim to have stolen, they have already released emails and documents that contain embarrassing exchanges between company executives, sensitive business information and employees' personally identifiable information (PII). In addition to several class action lawsuits filed by employees who allege that the company did not take sufficient steps to protect their information, industry insiders believe that further lawsuits could emerge based upon the underlying data made public. Moreover, some of the sensitive business information disclosed could impact future contract negotiations with suppliers and partners, not only for the company in question, but also its entire industry.

These breaches demonstrate that it is the breadth of an attack's impact, separate and apart from an attack's sophistication, that must drive the depth of response.

3. Key findings in cyber incident detection, response and threat intelligence

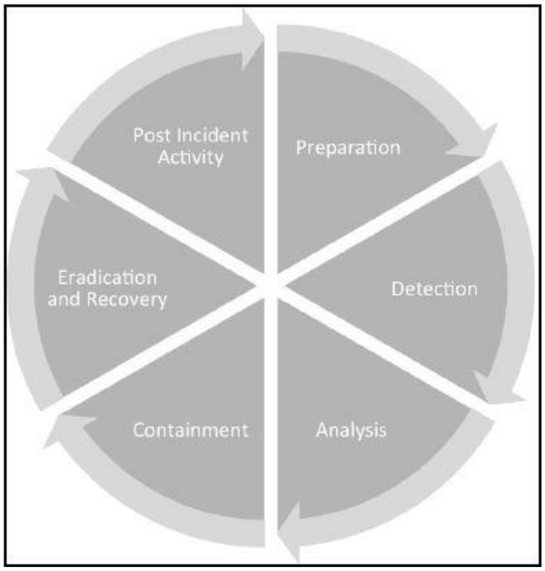
- Security operations teams struggle to keep up with the deluge of security alerts from an increasing arsenal of threat detection technologies.
- Security operations still primarily rely on manually created and maintained, document-based procedures for operations, which leads to issues such as longer analyst onboarding times, stale procedures, tribal knowledge and inconsistencies in executing operational functions.
- The challenges from an increasingly hostile threat landscape, combined with a lack of people, expertise and budget are driving organizations toward security orchestration, automation and response (SOAR) technologies.
- Threat intelligence management capabilities are starting to merge with orchestration, automation and response tools to provide a single operational tool for security operation teams.

4. Incident Response Overview

There is a general path that cyber security incidents follow during their lifetime. If the organization has a mature incident response capability, they will have taken measures to ensure they are prepared to address an incident at each stage of the process. Each incident starts with the first time the organization becomes aware of an event or series of events indicative of malicious activity. This detection can come in the form of a security control alert or external party informing the organization of a potential security issue. Once alerted, the organization moves through analyzing the incident through containment measures to bring the information system back to normal operations. The following figure shows how

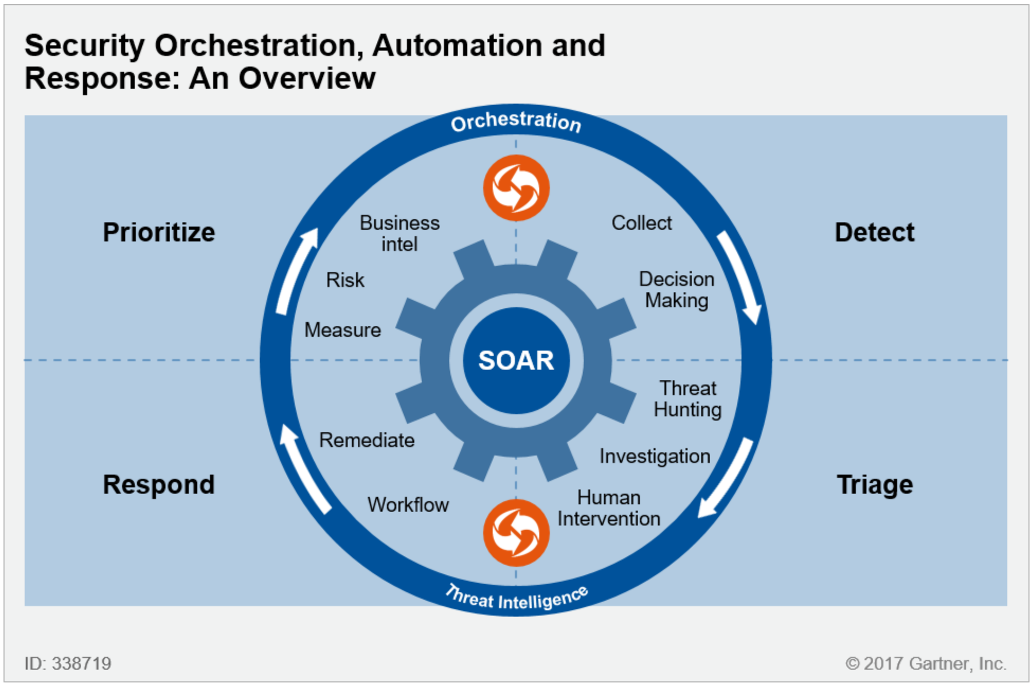
these flow in a cycle with Preparation as the starting point. Closer examination reveals that every incident is used to better prepare the organization for future incidents as the Post Incident Activity and is utilized in the preparation for the next incident.

The incident response process can be broken down into six distinct phases Preparation, Detection, Analysis, Containment, Eradication and recovery and Post-incident activity.



5. What is Security orchestration, Automation and Response?

Gartner defines security orchestration, automation and response, or SOAR, as technologies that enable organizations to collect security threats data and alerts from different sources, where incident analysis and triage can be performed leveraging a combination of human and machine power to help define, prioritize and drive standardized incident response activities according to a standard workflow.



Security Orchestration, Automation and Response: An Overview

ID: 338719

© 2017 Gartner, Inc.

Source: Gartner (November 2017)

6. SOAR tools offering from vendors

The following vendors offer notable service offering:

1. Carbon Black
2. Check Point Software
3. Cyberbit
4. Demisto Inc.
5. Empow
6. Fireeye
7. Phantom
8. Rapid7
9. Resilient Systems
10. SecBI
11. ThreatMetrix, Inc.

6.1 Carbon Black (https://www.carbonblack.com/)

Headquartered in Waltham, Massachusetts, USA, Carbon Black having offices in Asia, Europe and Australia. Carbon Black was founded as Bit9, Inc. in 2002 by Todd Brennan, Allen Hillery, and John Hanratty. The company changed its name from Bit9, Inc. to Carbon Black, Inc. on February 1, 2016.

The company develops endpoint security software that detects malicious behavior and prevents malicious files from attacking an organization. It is an actor in the antivirus, endpoint detection and response and endpoint protection platform space. Carbon Black has more than 2,500 customers, including 30 of the Fortune 100.

With Carbon Black's Cb Response, Investigations that typically take 78 hours can be completed in 15 minutes. Cb Response captures more information about more events than any other solution, giving incident responders the most complete picture possible.

Cb helps maintain continuous compliance with numerous regulatory standards and frameworks, such as PCI-DSS, HIPAA/HITECH, SOX, NERC CIP, NIST 800-53, and more

6.2 Check point Software Technologies Ltd. (https://www.checkpoint.com/)

Check Point headquarters are located internationally in Tel Aviv, Israel, and in the United States in San Carlos, California. The Company has offices in the U.S. as well as in Canada. The Company also has international subsidiaries located in Europe, Australia, and Asia.

Check Point's ThreatCloud Incident Response is a collaborative network and cloud-driven knowledge base that delivers real-time dynamic security intelligence to security gateways. That intelligence is used to identify emerging outbreaks and threat trends. Since processing is done in the cloud, millions of signatures and malware protection can be scanned in real time. Three different blades IPS, Anti-Bot and Antivirus Software Blades defend network against both external and internal (bot) threats.

ThreatCloud incident Response offers following two types of service levels that fits different customers' needs.

- Monitoring & Alert Service (Standard and Premium): The Standard level provides automated IPS log analysis and provides alerts to you when a significant event is detected. The Premium level adds the benefit of a Check Point analyst reviewing all alerts in order to determine if immediate action is required.

- Fully-Managed Threat Prevention Service (Elite) Includes a dedicated Check Point security appliance, premium support including on-site replacement, licenses for the IPS, Anti-Bot, and Antivirus Software Blades, and remote management of the appliance.

6.3 CyberBit (https://www.cyberbit.com/)

CyberBit Founded in 2015, Cyberbit is a subsidiary of Elbit Systems (NASDAQ: ESLT), one of the top-30 global providers of defense technologies, and a world-leading provider of simulation systems and large-scale command and control centers. CyberBit has offices in Israel, the US, Europe, and Asia.

Their products are developed with MSSPs in mind. Cyberbit EDR provides an approach for detecting and responding to advanced threats at the endpoint level. It is based on a hybrid detection engine, which combines behavioral analysis with machine learning algorithms that use statistical modeling to identify abnormal activity. This hybrid approach detects a broader range of malicious activities, including threats that have never before been encountered, and is more effective at differentiating between normal and abnormal activity.

6.4 Demisto (https://www.demisto.com/)

Demisto is backed by Accel, ClearSky and other prominent investors and has offices in Silicon Valley and Tel Aviv. Demisto Enterprise offers Security Operations Platform to combine security orchestration, incident management, machine learning from analyst activities, and interactive investigation. Demisto’s orchestration engine automates security product tasks and weaves in the human analyst tasks and workflows.

Demisto tracks numerous metrics including incident open rate, close rate, open time, mean time to respond, analyst load, analyst respond time and many more. These metrics are available through built-in reports and dashboards out of the box.

6.5 Empow Cyber Security (https://www.empownetworks.com)

empow is a cybersecurity company founded in October 2014 in Tel Aviv – with funding from the Office of the Chief Scientist – with the mission of helping enterprises and governments "make more of what they already have." Forbes recently singled out empow's technology as one of the few disruptive technologies at RSA, in the "software-defined cybersecurity" arena.

empow's solution comes with adaptive behavioral analysis service that adds visibility to internal network's traffic and detects unknown threats in it. Based on empow's network DPI software engines, the network traffic analytics service learns and profiles the normal patterns of behavior of users and servers inside the network, and identifies behavior anomalies that can be associated with various threat categories.

The empow Security Platform enables a detailed Security Diagnostics Service that provides fact-based analysis of the security apparatus and security tools, effectiveness against threat scenarios and compliance models.

6.6 FireEye Cyber Security Company (https://www.fireeye.com/)

FireEye, Inc. is a publicly listed enterprise cybersecurity company[1] that provides products and services to protect against advanced cyber threats, such as advanced persistent threats and spear phishing. Founded in 2004, the company is headquartered in Milpitas, California. FireEye has over 6,600 customers across 67 countries, including more than 45 percent of the Forbes Global 2000.

FireEye Helix is a security operations platform deliver advanced security to any organization. FireEye Helix surfaces unseen threats and empowers expert decisions with frontline intelligence, to help organizations take back control and capture the untapped potential of their security investments.

FireEye Helix collects event data from FireEye and non-FireEye components of a security infrastructure and overlays frontline intelligence, rules, and analytics to give organizations the context to determine which threats present the greatest risk and how to subsequently respond. From within a single interface, FireEye Helix facilitates all Security Operation Center (SOC) functions including alert management, search, analysis, investigations, and reporting.

Their Mandiant’s Incident Response Services handle critical security incidents, resolve immediate issues and put long-term solutions in place to address systemic causes of the incident.

6.7 Phantom Cyber (https://www.phantom.us)

Phantom was founded in 2014 by enterprise security veterans Oliver Friedrichs and Sourabh Satish. Phantom Named Forbes Cloud 100 Rising Stars in 2017.

The Phantom Platform integrates existing security technologies of SOC, providing a layer of connective tissue between them. With Phantom, you can automate tasks, orchestrate workflows, and support a broad range of SOC functions including event and case management, collaboration, and reporting.

6.8 Rapid 7 (https://www.rapid7.com/)

Rapid7, Inc. provides security data and analytics solutions that enable organizations to implement an analytics-driven approach to cyber security and IT operations. It offers threat exposure management solutions, including Nexpose, which enables customers to assess and remediate their exposure to cyber risk; Metasploit, a penetration testing software solution; and AppSpider, an application security testing solution.

The company also provides incident detection and response solutions, such as InsightIDR, a cloud based offering for incident detection and response; Managed Detection and Response, a managed service, which provides customers with attacker behavior analytics, machine learning algorithms, and threat intelligence to hunt attackers; and incident response services that provide customers with access to security experts and experience. In addition, it offers Logentries, a cloud-based solution for collecting, searching, visualizing, and analyzing log data, as well as enables organizations to store and search data; and InsightOps, an IT operations solution to centralize machine data from organizations' IT environments for operational awareness and control.

6.9 Resilient Systems (https://www.resilientsystems.com/)

Resilient System was a privately-held company founded in 2010 in Cambridge, Massachusetts. IBM acquired this company in 2016. Resilient has more than 100 global customers, including 30 of the Fortune 500 and partners in more than 20 countries. Resilient specializes in incident response, which helps IT security teams bolster their defenses against data breaches. The Resilient incident response platform is deployed in more than 100 of the Fortune 500 corporations - which is IBM's sweet spot.

Bruce Schneier, Chief Technology Officer at Resilient, is an internationally renowned security expert, cryptographer, and author of numerous books covering security. With Schneier, IBM Security adds one of the top minds in cyber to its team.

In 2015, the team introduced the latest evolution in incident response – the Action Module, which empowered customers to automate and orchestrate their incident response workflows and processes.

Five years ago, IBM Resilient pioneered the market for incident response technology. Today, they are leading the decade of incident response.

6.10 SecBI (https://www.secbi.com/)

SecBI solves the most complex challenge in the daily operations of a SOC or MSSP by automating threat detection and investigation with machine-learning-based technology. Our value is best understood in contrast to solutions that offer detection via random alerts and anomalies requiring manual correlation and investigation. Our Autonomous Investigation™ technology uncovers the full scope narrative on every suspicious incident, including all affected entities (e.g. users, domains, devices) within minutes. Automated investigation saves chunks of time for analysts and hunters by providing them with all the information for rapid and complete remediation. The automated investigation also reduces the need to hire skilled hunters. Without the need to deploy special appliances or agents, the solution can be deployed on-premise or in the cloud within seconds, and is currently used by financial institutions, telecoms, retailers, and manufacturing enterprises worldwide. SecBI was co-founded by two veterans of RSA who experienced the pain of a long detection and remediation process following the company's well publicized breach in 2011. With its corporate headquarters based in Tel Aviv, SecBI also has an office in Connecticut, USA.

6.11 ThreatMetrix Inc. (https://www.threatmetrix.com/)

ThreatMetrix is a security technology company headquartered in San Jose, California, with offices in New York City, Toronto, Hong Kong, Singapore, Sydney, Tokyo, London, Paris, Munich and Amsterdam. ThreatMetrix provides software as a service (SaaS) technology that profiles online transactions and activities to determine whether they initiate from fraudsters or legitimate customers. The technology is supported by a global network, which analyzes more than 40 billion annual transactions and protects more than 210 million active user accounts across 6,000 customers and 40,000 websites.

ThreatMetrix Dynamic Decision Platform provides enhanced authentication, identity verification and fraud decisioning. Integrating Digital Identity Intelligence with behavioral analytics and machine learning capabilities, the platform also incorporates third-party data sources for exception handling. Case management helps to isolate and investigate transactions that require further review.

This approach helps overcome operational silos, combining dynamic data with information from legacy systems for optimized decisioning and a better digital experience.

Other notable SOAR vendors:

Other vendors that we did not discuss in this report, but are not less relevant, are:

Ayehu Software Technologies, Bluecoat (Acquired by Symantec), Bricata, Cyber Triage, D3 Security, DFLabs, Encode, Hexadite (Acquired by Microsoft), Hexis Cyber (Acquired by WatchGuard), Ideagen, information security exchange, LockPath, LogRhythm, MetricStream, NexThink, NowSecure, Panaseer, Radar, Raytheon, Redlock, SecDo, ServiceNow, Siemplify, Swimlane, SySS GmbH, TaaSera, Tanium, UpLevel and Veriato

For more information please contact us at **https://www.cyberdb.co/contacts/**

7. Description and Functional Components

SOAR can be described by the different functions and activities associated with its role within the SOC, and by its role with managing the life cycle of incident and security operations:

- **Orchestration** — How different technologies (both security-specific and non-security-specific) are integrated to work together
- **Automation** — How to make machines do task-oriented "human work"
- **Incident management and collaboration** — End-to-end management of an incident by people
- **Dashboards and reporting** — Visualizations and capabilities for collecting and reporting on metrics and other information

Orchestration

orchestration as the ability to coordinate informed decision making, and formalize and automate responsive actions based on measurement of the risk posture and the state of an environment.

Automation

Some vendors use the terms "automation" and "orchestration" interchangeably as synonyms, although they are not the same concept.

Automation is a subset of orchestration. It allows multiple tasks (commonly called "playbooks") to execute numerous tasks on either partial or full elements of a security process. The security operations teams can build out relatively sophisticated processes with automation to improve accuracy and time to action. For example, a SIEM could check if an IP addresses has been seen, or block an IP address on a firewall or intrusion detection and prevention system (IDPS), or a URL on a secure web gateway. It can then create a ticket in your ticketing system or connect to Windows Active Directory, and lock or reset the password for a user's account.

Incident management and collaboration

Incident management and collaboration comprises several activities, i.e.

- Alert processing and triage
- Journaling and evidentiary support
- Case management and workflow
- Analytics and incident investigation support
- Management of threat intelligence

Dashboards and reporting

SOAR tools are expected to generate reports and dashboards for at least three classes of persona: analyst, SOC director and chief information security officer (CISO).

8. Solution Offering of Selected Products

The table below is a competitive analysis for a selected list of vendors in this market. For wider and deeper analysis, please contact us

Company	Orchestration	Automation	Dashboards and reporting	Platform
Carbon Black	- Flexible API customization - Automate software approvals and updates via IT and cloud-driven policies - FIM/FIC capabilities	- Correlate network, endpoint, and SIEM data through open APIs - Play Book	- Meet IT risk and audit controls across major regulatory mandates - Unlimited data retention for investigating long-term attacks with extreme dwell time	- SaaS & On-premises
CheckPoint	- Flexible API - Remediation for several different types of threats including: IPS/IDS, Firewall, Apps, Data loss, Malware, Botnets, unauthorized access, DoS.	- Correlate network, endpoint, and SIEM data through open APIs - Play Book	- Provides full forensic awareness - Table Top Exercises - Post-Attack Analysis and Incident response analysis and recommended remediation	- SaaS & On-premises
Cyberbit	- Integrate alert feeds, data enrichment sources and response tools	- Playbooks - Standard protocols and interfaces including Rest API, SOAP, SSH/CLI interface or even custom APIs	-Preset and custom investigation dashboards including MSSP	- SaaS

Company	Orchestration	Automation	Dashboards and reporting	Platform
Demisto Inc.	- Extensible bidirectional Integration Framework -	- Playbooks - Standard protocols and interfaces including Rest API, SOAP, SSH/CLI interface or even custom APIs	- Capturing knowledge base from security analysts	- SaaS
Empow	- Bidirectional & feature rich integration	- Workflow with multilevel automation - Playbook and App configuration	- Threat Analytics Reporting and Security Diagnostics	- SaaS
Fireeye	- Flexible API customization	- Organize, assign, collaborate and action steps through the investigative process through automated and manual workflows	- Predefined or custom dashboards and widgets to visually aggregate, present and explore the most important information	- SaaS
Phantom	- Use any type and source of security data with Bidirectional API	- Playbook and App configuration	- Predefined or custom dashboards	- SaaS

Company	- Orchestration	- Automation	- Dashboards and reporting	- Platform
Rapid7	- Integrations, unify and detect across network, endpoint, others IDRs and cloud with APIs	- Playbook and App configuration	- Dashboards to view asset, user, and behavioral data into a single instance with customized reporting	- SaaS
Resilient Systems	- Integrations, unify and detect across network, endpoint, others IDRs and cloud with APIs	- Dynamic Playbooks	- Predefined or custom dashboards and widgets to visually aggregate, present and explore the most important information	- SaaS
SecBI	- Increased efficiency and consistency in orchestration and automation of threat intelligence management, security event monitoring and incident response processes.	- Automation of the most complex aspect of a SOC – the investigation processes saving large blocks of analysts' time and enabling complete remediation	- Dashboards and reports intended for different tiers of the security operations, from prioritized lists of incidents for the tiers, down to reports of operational efficiency of incident handling, TTD and TTM.	- On-prem or cloud
ThreatMetrix, Inc	- Packaged integration technology services, integrates with third-party data sources	- Workflow with multilevel automation	- Dashboards to view asset, user, and behavioral data into a single instance with customized reporting	- SaaS

9. References

Claudio Neiva, C. L. (2017). *Innovation Insight for Security Orchestration, Automation and Response.* Gartner.

Johansen, G. (2017). *Digital Forensics and Incident Response.* Birmingham, UK: Packt Publishing Ltd.

NICE Cybersecurity Workforce Framework 2.0. (2014). Gaithersburg, MD: NIST.

10. About CyberDB

CyberDB (www.cyberdb.co) is the leading global research databank for Cyber solutions and vendors.

CyberDB database includes over 1,600 vendors and 6,000 products, categorized into 8 main cyber categories and 146 sub-categories. The company publishes market researches and summaries on bi-weekly basis on cyber categories.

The database is being used by VC's, multinationals, CISO's and system integrators worldwide to help them navigate through the dynamic cyber landscape.

In addition, CyberDB offers its customers Consulting Services for Cyber Product Strategy, Cyber Technology Scouting and tailored Market researches.

CyberDB is established by the founders of Stratechy, strategy consulting practice that has been working with management teams of Hi-Tech vendors to shape their product strategy turn-around and design and execute their Go-To-Market plan

Among its customers, are Deloitte, NEC Corporation, Samsung, Rafael, Amdocs, ClearSky VC, Commonwealth Bank of Australia and S21Sec

Please contact CyberDB at **info@cyberDB.co** or visit us in **www.cyberdb.co**, on **Twitter** or **LinkedIn**