CAPCO

ADVANCED THREAT DETECTION THROUGH USER BEHAVIOR ANALYSIS

CAPCO'S CYBERSECURITY INSIGHT SERIES

ADVANCED THREAT DETECTION THROUGH USER BEHAVIOR ANALYSIS

As the frequency and magnitude of cybersecurity incidents increases, the mean time to detect threats is becoming critical. Financial institutions need to respond by investing in advanced threat detection capabilities, including user behavior analysis.

INCREASE IN CYBERSECURITY INCIDENTS

As the focus on digitization accelerates across financial institutions, the threat of a significant cybersecurity incident continues to loom larger each year. In 2019, 61 percent[1] of firms surveyed reported that they were subject to a cybersecurity incident, which is up from 45 percent in the prior year.

A cybersecurity incident in today's landscape can have a significant financial, regulatory, and reputational impact on a financial institution, and in cases, even systemic effects on the financial industry. In response, security teams at financial institutions are building capabilities to have clear visibility into all forms of activities taking place within the technology environment.

The number of firms that experienced cybersecurity incidents has risen to 61% in 2019 from 45% in the prior year.

With threat actors becoming increasingly sophisticated and easy access to advanced attack toolkits, the industry continues to struggle with the complexity and challenge of detecting cybersecurity incidents in the early stages and responding to attacks with minimal business disruption. As Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) cite inadequate or inexperienced staffing and outdated security technology as top concerns, investments in the next generation of detection technology need to be prioritized to upgrade the effectiveness of the limited personnel guarding the technology environment.

IMPORTANCE OF COMPREHENSIVE MONITORING AND DETECTION PROGRAM

A robust detection program is critical to maintaining a safe and trusted environment that can support business operations. Without the ability to effectively detect unauthorized activity, there would be no way to activate incident response efforts until it is too late. Additionally, the longer a threat actor persists on the organization's environment, the more familiar and entrenched they become, which consequently increases the difficulty in removing the bad actor and preventing them from returning in the future.

Analysis from publicly available threat intelligence reports[2] illustrates that the amount of time taken by various threat actors from the initial point of compromise to lateral movement across the network to more valuable targets can occur in as little as twenty minutes by the most sophisticated actors, up to an average of four hours 37 minutes industry-wide.

The speed of past cyberattacks provides a benchmark of the maturity required to sustain business operations against increasingly sophisticated threats. If the time to detect and time to respond are higher than the known benchmarks of threat actor propagation, the organization will continuously be operating from a reactive stance.

Amount of time between the initial compromise as indicated in system logs and the detection time when the security analyst initiated an action to address the alert

Amount of time between the initial action taken by the security analyst until the incident is addressed and closed as remediated

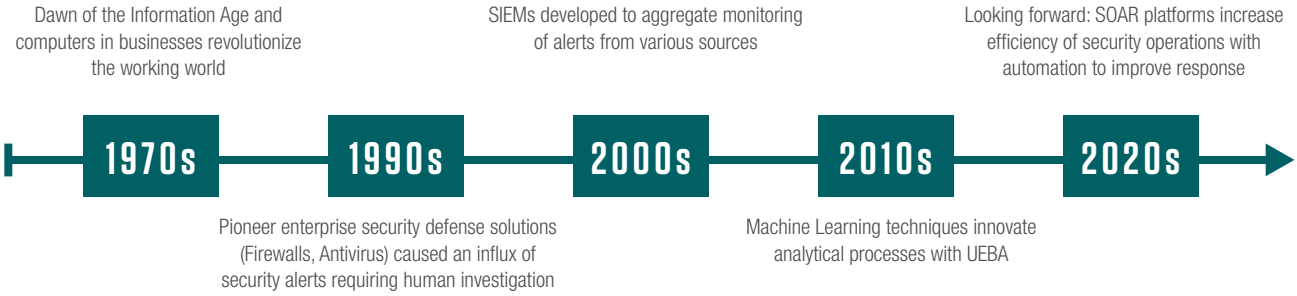
Figure: Key metrics to measure detection and response capabilities

In addition, cybersecurity incident detection capabilities are also considered as fundamental requirements to satisfy regulatory mandates, and is defined as a core security function:

Regulatory Requirements	**New York State Department of Financial Services 500** • Section 500.02 – Cybersecurity Program must be designed to detect cybersecurity events • Section 500.06 (a)(2)(b) – Audit Trails to detect and respond to Cybersecurity Events and shall maintain records for not fewer than three years • 500.14 (a) – Monitoring the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users
Industry Best Practices	**NIST Cybersecurity Framework (CSF) Detect Function** • Anomalies and Events – Anomalous activity is detected and the potential impact of events is understood. • Security Continuous Monitoring – The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures. • Detection Processes – Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.

Note: Regulatory Requirements and Industry Best Practices are indicative and not exhaustive

EVOLUTION OF THREAT DETECTION TECHNOLOGIES



When businesses first became aware of information security risks and sought to protect their technology assets with firewalls and antivirus, security information and event management (SIEM) software were initially introduced as a means to aggregate log and event data from various sources into a single console to simplify analysis and triage of alerts.

Modern SIEM solutions have become more sophisticated and are increasingly equipped with features to correlate information, visualize data for analysis, and automate response actions. With the sheer amount of data surpassing thousands of events per second, security analysts are incorporating user and entity behavior analytics (UEBA) modules that leverage machine learning to process information. Additionally, security orchestration, automation, and response (SOAR) tools are the next-generation features that integrate with existing tools to reduce manual workloads and automate responses to stop attacks as they are identified.

A FRAMEWORK TO IMPLEMENT, ASSESS, AND IMPROVE DETECTION CAPABILITIES

Capco's approach focuses on a risk-based understanding of likely adversary activity in order to define the data analytics-based detection program, which is continuously tested for effectiveness. A comprehensive threat detection approach should consider four critical steps – (1) identify behaviors, (2) acquire data, (3) develop analytics, and (4) test detection.

Figure: Threat analytics maturity scale

1. IDENTIFY BEHAVIORS

Detection relies on a risk-based understanding of the techniques, tactics, and procedures (TTPs) a threat actor can use to compromise business objectives and critical assets.

The first step is to prioritize behaviors for detection based on factors such as:

- Most commonly used threat vectors by likeliest threat actors
- Most adverse impacts on the organization
- Most likely indicators of adversary behavior (i.e., fewest false positives)

In our experience, industry frameworks such as MITRE ATT&CK®[3] can be leveraged as an excellent starting point to identify specific adversary behaviors for prioritization.

2. ACQUIRE DATA

With a defined mandate of prioritized behaviors for detection, a gap assessment should be conducted on the inventory of data sources to determine whether the necessary data is readily available or if sensors need to be implemented to collect additional data.

Furthermore, the quality of available data should be assessed for immediate usability across the following dimensions relevant for threat hunting[4]:

- Completeness – Is the data comprehensive with all necessary information?
- Consistency – Are the data types and naming conventions standardized across different sources?
- Timeliness – Is the necessary data available consistently on-time when it is needed?

The quality of data is absolutely critical for fine tuning detection capabilities. Without clean data, the organization will suffer from excessive false positives, or worse still, be blind to adversarial activities occurring within the technology environment.

3. DEVELOP ANALYTICS

The next step is to determine if all available data is in use by the organization's detection processes. As a result of disparate teams and processes across data collection, aggregation, and analysis, many organizations often collect logs from data sources that do not feed any analytical capabilities.

An assessment of current analytics should be conducted to identify the current level of maturity.

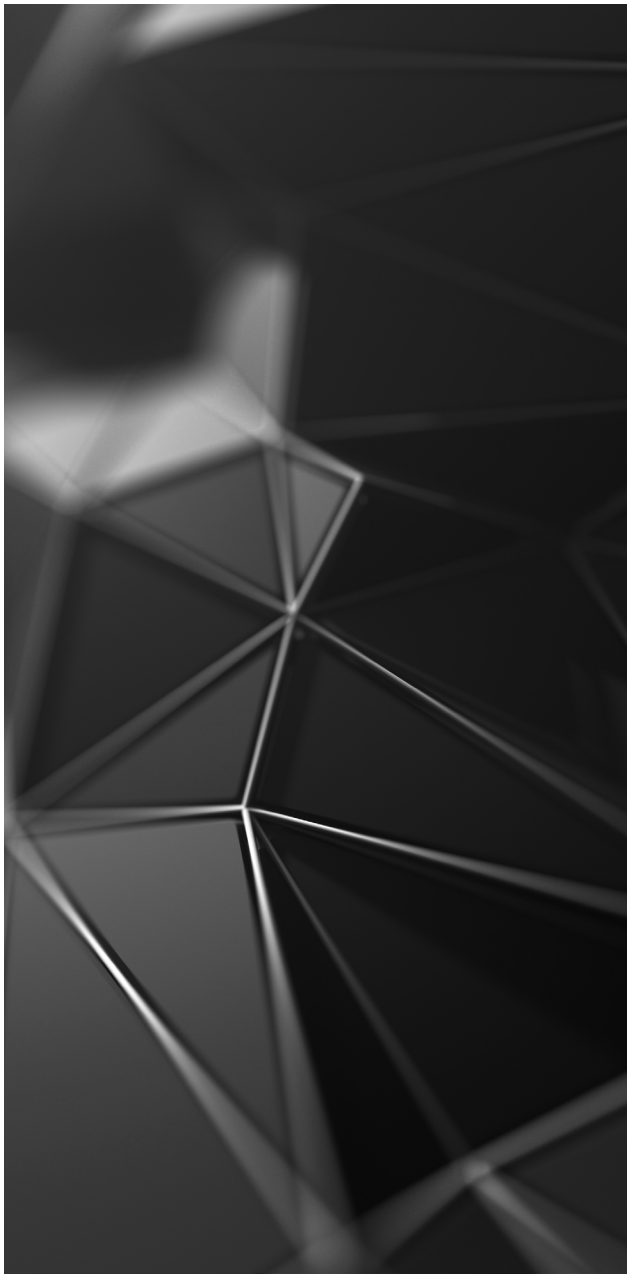
Depending on the level of maturity, incremental steps should then be taken to improve the detection capabilities.

- Ensure use cases are defined over available log sources to improve monitoring coverage
- Ensure that all identified behaviors are covered by use cases
- Ensure that thresholds for rules are adequately optimized to minimize false positives

It is important to note that analytics are only as good as the data, the logic, and threat intelligence feeding the system.

4. TEST DETECTION

Regardless of all the analytics and detection capabilities in place, the only way to know if the detection capabilities are sufficient is to conduct a test. Aside from a full-fledged 'Red Team' exercise, the security team can generate test events within a controlled environment to replicate specific adversary tactics, such as privilege escalation, to validate if the analytics previously developed to capture such activity is performing as designed.



IMPLEMENTING A SUCCESSFUL THREAT DETECTION PROGRAM

From our experience with leading global financial institutions, addressing the top three challenges plaguing security organizations head-on is critical to implementing a successful threat detection program.

DEVELOP STRONG DATA GOVERNANCE

The biggest problem with effective detection is the poor quality of the data underlying detection processes. This can manifest itself in unreliable, inconsistent, or incomplete data, which do not provide the information necessary to identify suspicious activity effectively. Data can also be located in siloes across the organization, which may only be reviewed on a periodic or an ad-hoc basis. This ends up promoting a reactive stance over proactive detection. To make matters worse, the data may simply not be available, which can have further ramifications during forensic investigations and incident postmortem reviews. As the end-user of security information, the security team needs to define requirements for the data owners and validate data quality to ensure usability. Strong data governance should be embedded throughout the data lifecycle from data generation to aggregation, to normalization, and analysis.

INCORPORATE ACTIONABLE THREAT INTELLIGENCE

With the ever-evolving nature of the threat landscape, adversary TTPs are continually changing. Different malware strains are released faster than defenses can react, and threat actors are getting more sophisticated in their delivery mechanisms. It is imperative to feed detection processes with actionable threat intelligence to filter out the noise and ensure that the latest malware signatures, suspicious IP addresses, and relevant insights are incorporated into processes by the SOC. Having a risk-based understanding of the most critical assets across the enterprise and the likeliest TTPs that a threat actor may use are foundational to anticipating cyber threats before they occur.

AUTOMATE MANUAL TASKS TO COMBAT ALERT FATIGUE

Responding to constant alerts every single day can get repetitive, especially when a large number of alerts could end up as false positives due to poorly set thresholds or data quality issues. However, security operations teams have to maintain vigilance in reviewing each and every alert, as the downside of missing an actual cybersecurity event can be devastating for the financial institution or the industry as a whole. Searching for true cybersecurity events can become akin to finding a needle in a haystack, and automation of repetitive tasks/workflows is critical to free up analyst time for higher-value tasks.

REFERENCES

[1]Hiscox Cyber Readiness Report 2019

[2]Crowdstrike 2019 Global Threat Report: Adversary Tradecraft and the Importance of Speed

[3]MITRE ATT&CK® is a curated knowledge base and model for cyber adversary behavior.

[4]Depart of Defense (DOD) Guidelines of Data Quality Management

CONTACTS

Julien Bonnay
Partner
julien.bonnay@capco.com

Jayadevan Vijayakrishnan
Principal Consultant
jayadevan.vijayakrishnan@capco.com

Timothy Sheng
Consultant
timothy.sheng@capco.com

ABOUT CAPCO

Capco's Cybersecurity Practice brings deep industry expertise, proven risk management capabilities, security technology expertise, and regulatory compliance experience. We have extensive experience advising financial institutions on strengthening their security posture by building a business case to secure funding and identifying strategic investments for the years ahead to stay ahead of the ever-evolving threat landscape.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Hong Kong
Kuala Lumpur
Pune
Singapore

EUROPE
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO
THE FUTURE. NOW.

JN_1760