Threat Detection

Core Practices to Manage Risks and Vulnerabilities

SUDIP SENGUPTA
PRINCIPAL ARCHITECT & TECHNICAL WRITER, JAVELYNN

CONTENTS

- Understanding Threat Detection: Significance and Complexities
  - The Threat Landscape and Evolving Challenges
- Mastering Threat Detection: Basic Techniques and Advanced Practices
  - Core Practices of Threat Detection
    - Exposure Management
    - Proactive Threat Hunting
    - Employing Advanced Threat Detection Systems
    - Effective Incident Response Planning
    - User Behavior Analytics
- Conclusion and Additional Resources

Many leading organizations face complex decisions when dealing with the multifaceted nature of cyber threats. One could approach threat detection and prevention reactively, putting up defenses as threats appear. Alternatively, a more strategic stance could be adopted, using sophisticated systems to predict and prevent threats before they manifest.

But employing these complex mechanisms requires a thoughtful balance of several factors. Most organizations also make the mistake of considering threat detection as a static practice. Instead, it must evolve with your organization's needs and the constantly changing nature of threats.

This Refcard will explore these nuanced methods, discussing how threat detection works and offering guidance on integrating them into your overall security strategy.

UNDERSTANDING THREAT DETECTION: SIGNIFICANCE AND COMPLEXITIES

The complexity of today's cyber threats demands a nuanced approach. It's no longer about merely thwarting attacks but about understanding, predicting, and preempting them. An essential proactive strategy of an organization's cybersecurity structure, threat detection serves as an analytical blueprint for identifying potential security breaches and malicious activities within a system.

Different from threat hunting (proactive search), threat prevention (security enforcement), and threat response (incident management), threat detection ***continuously monitors the environment to detect actual threats already present within the IT service boundaries***.

The practice of employing advanced threat detection systems offers a layered defense strategy against highly sophisticated threats. It also plays a crucial role to safeguard personal and sensitive information — and ensure compliance with regulatory standards, including GDPR, HIPAA, and PCI DSS. The ultimate success factor here is to focus on not merely implementation but also on understanding how threat detection systems align with industry best practices, an organization's unique attributes, and regulatory frameworks.

THE THREAT LANDSCAPE AND EVOLVING CHALLENGES

The threat landscape is as complex and dynamic as the mechanisms designed to detect it. Before delving into threat detection, it's vital to recognize the inherent complexity due to the evolving nature of threats and ever-expanding organizational attack surfaces.

CALIBRATION AND REEVALUATION

The design of a threat detection system requires meticulous planning and continuous fine-tuning. A continuous recalibration of defense mechanisms also helps you optimize your security posture with the changing threat landscape.

censys

Detect More Threats with Leading Internet Intelligence

Censys empowers security teams with the most comprehensive, accurate, and up-to-date map of the internet to defend attack surfaces and hunt for threats.

Learn More →

In the past, simple viruses and malware constituted the primary concerns for security professionals. These rudimentary threats were often tackled with regular updates to virus definitions and relied on relatively straightforward methods, such as signature-based antivirus software that recognized known malicious code. But now, the complexity of the task has increased significantly.

This escalating threat complexity also underscores the importance of comprehensive monitoring and continuous assessment. If a particular threat detection method continuously succeeds without challenge, or without identifying vulnerabilities, perhaps it's time to augment your defenses. Conversely, if a certain area seems persistently vulnerable, it could be indicative of the need for a comprehensive reassessment.

Take, for instance, sophisticated state-sponsored cyber attacks, advanced persistent threats (APTs), and organized ransomware groups. Each of these threats operates on a different level, requiring diverse strategies for detection. APTs might be ongoing, stealthy, and persistent, while ransomware attacks are more immediate and demanding, and state-sponsored attacks can be incredibly complex and covert.

And to make things worse, most of such cyber activities are orchestrated by cross-border entities. Jurisdictional differences in regulations and law enforcement collaboration can impede coordinated response efforts, further complicating the containment and mitigation of such threats.

CHALLENGES OF EMERGING TECHNOLOGIES

The challenges don't stop there. The proliferation of Internet of Things (IoT) devices and cloud services increases the attack surface exponentially, subsequently introducing new vulnerabilities that are difficult to anticipate and monitor. And the growing sophistication of cybercriminal tactics, techniques, and procedures to target unknown vulnerabilities makes threat detection a continuous challenge. Subtle forms of deception, like living-off-the-land attacks, often mimic legitimate activities, making detection even more challenging.

In addition, the interplay between **maintaining security** and **respecting privacy** is a highly nuanced aspect of modern threat detection. Encryption remains fundamental to ensuring data privacy and integrity, yet it simultaneously cloaks the malicious activities within the very secure channels designed to protect information. Penetrating this cloak without infringing privacy rights or undermining trust requires a fine balance that demands advanced analytical tools and intelligent inspection methodologies.

TRANSLATING INSIGHTS INTO ACTION

Translating an understanding of the threat landscape into actionable insights is another significant challenge. It's not enough to merely grasp the complexity; the real task lies in converting this abstract concept into practical applications.

Advanced threat detection platforms are needed to transform this knowledge into robust defense mechanisms. Failure to do so can render the understanding ineffective, making it more of a theoretical exercise rather than a vital component of an effective cybersecurity strategy.

MASTERING THREAT DETECTION: BASIC TECHNIQUES AND ADVANCED PRACTICES

Threat detection requires a multifaceted approach that constantly adapts to the ever-changing cyber landscape. It is also important to note that recognizing the "what" through indicators of compromise (IOCs) and known malicious patterns is only half the equation. The ability to identify the "how" via predictive analytics, anomaly detection, and threat intelligence feeds — all aligned with strategic incident response planning — forms the other essential half.

The progression from foundational techniques, like signature- and behavior-based analysis, to advanced machine learning (ML) and heuristic methods highlights the industry's gradual innovation over the years. The tables below summarize these methodologies and the purposes they serve:

Table 1

PRIMARY THREAT DETECTION METHODOLOGIES			
APPROACH	**ATTRIBUTES**	**PURPOSE**	**USE CASES**
Signature-based detection	Relies on known patterns and definitions to identify threats	Identify and block known malicious codes and viruses	• Antivirus software • Intrusion detection systems
Behavior-based detection	Monitors and analyzes unusual system behavior to detect anomalies	Detect new or unknown threats through behavior analysis	• Anomaly detection in network traffic • User monitoring

Table 2

ADVANCED THREAT DETECTION METHODOLOGIES			
APPROACH	**ATTRIBUTES**	**PURPOSE**	**USE CASES**
Heuristics	Utilizes rules and patterns to identify suspicious activities	Quick identification of potential threats with less data	• Email scanning for spam and phishing • Fraud detection
Anomaly detection	Detects deviations from established baselines, revealing potential threats	Detecting unknown threats by identifying behavioral anomalies	• Network security • Fraud detection • System monitoring
ML algorithms	Employs algorithms that learn and adapt to detect new and evolving threats	Adapting to evolving threat landscape with continuous learning	• Adaptive threat detection • Predictive threat analysis

CORE PRACTICES OF THREAT DETECTION

Effective threat detection relies on a cohesive set of core practices that collectively form the defense against cyber threats. The following practices are essential pillars that represent a multifaceted defense strategy, each one tailored to address specific challenges in the modern cyber environment.

EXPOSURE MANAGEMENT

Exposure management functions as a critical threat detection pillar that focuses on the comprehensive assessment of an organization's external-facing attack surface. Representing a strategic alignment of technology and process, the primary purpose of this stage is to understand the scope of what needs to be protected, optimizing response mechanisms against an ever-changing cyber environment.

This is typically achieved by implementing the following measures:

1. **Scoping exposure and identifying blind spots** – Contrary to popular belief, even the most advanced tools can render an organization vulnerable if they are misconfigured or fall outside of organizational bounds (e.g., cloud services, other IT assets).
   - Detailed and ongoing mapping of exposures is essential. It's critical to understand context like ownership and connections, especially for complex organizations that may have branches, made acquisitions, or have other complicated ownership structures.
2. **Building and refining risk mitigation processes** – Subsequent to identifying gaps, efforts must be made to bridge them and enhance existing risk mitigation processes.
   - Delineating accountability based on security roles is vital as it both instills a sense of responsibility and refines the risk mitigation blueprint into a more agile and adaptive system.
3. **Measuring and aligning remediation efforts** – Metrics play a crucial role in this stage, tracking remediation processes (e.g., response times) to critical vulnerabilities.
   - Continuous monitoring and alignment of these metrics with changes in the security infrastructure ensure that the exposure management strategy remains robust and agile.

PROACTIVE THREAT HUNTING

Going beyond exposure management's focus on known vulnerabilities and visible attack surface, proactive threat hunting delves deeper to actively detect unknown, concealed threats within the network. Unlike traditional methods that react to security incidents as they occur, proactive threat hunting searches through networks to detect and isolate advanced threats that evade existing security solutions.

Consider the complex role that threat feeds, IOCs, and indicators of attack play together. A diligent analysis of these components can provide significant and actionable insights. The real challenge, instead, is to separate valuable signals from inconsequential noise, a task demanding both technical expertise and strategic insight.

For a more comprehensive approach, consider the following actions:

- **Understand the unusual** – Delve into endpoints, network architecture, and typical user behavior to spot the unusual. This understanding is tested by simulating cyber attacks through red teaming exercises in a controlled environment, revealing weaknesses that might not be apparent otherwise.
- **Challenge the standard** – Reject the notion of a universal method that fits all use cases. Embrace constant evaluation and change by utilizing key performance metrics and keeping an observant eye on the shifting threat landscape.
- **Employ agile tactics** – Adapt techniques and maintain vigilance toward evolving cyber threats. Ensure that the threat hunting process remains as adaptable and formidable as the ever-changing cyber environment itself.

EMPLOYING ADVANCED THREAT DETECTION SYSTEMS

Evolved cyber threats extending beyond traditional perimeters to target both physical and virtual infrastructures demand an adaptive response. Intrusion detection systems (IDSs) with advanced persistent threat (APT) correlation, and intrusion prevention systems (IPSs) with stateful protocol analysis, serve this purpose by administering a continuous surveillance mechanism against network anomalies.

IDSs' behavior-based detection models raise the alarm on suspicious activity, and IPSs neutralize the threat swiftly. But the dynamics change with the adoption of hybrid cloud and bring-your-own-device (BYOD) approaches, opening up new threat vectors that require specialized attention.

Understanding these vectors is crucial as they can ***extend into previously secure areas***, thus demanding a ***broader perspective on threat management***. Endpoint detection and response (EDR) solutions and cloud access security brokers (CASBs) are designed to tackle these unique vulnerabilities:

- An **EDR** monitors and mitigates device-level threats through graph-based analytics and automated playbooks.
- **CASBs** safeguard cloud accounts from malicious activities, including advanced persistent threats and malware, administering a resilient security architecture.

The integration of these systems is as critical as their individual roles. When properly aligned, they create a holistic security environment that adapts to changing threats, recognizing patterns that might be missed in isolation. For example, combining insights from EDRs and CASBs can provide a complete view of both internal and external threat movements, enhancing the reaction time to incidents.

But in the face of advanced threats, are traditional security systems completely irrelevant? ***Not really.*** Despite their conventional nature, security information and event management (SIEM) systems continue to add depth by correlating and analyzing security events across the organization.

Through integration with various security sources and threat intelligence feeds — and employing complex event processing (CEP) — SIEMs detect subtle, sophisticated attacks, ensuring a uniform security posture across all assets.

This layered approach to threat detection, integrating both new solutions and augmenting existing tools, creates a robust, flexible defense strategy capable of not only reacting to current threats but also anticipating future challenges.

EFFECTIVE INCIDENT RESPONSE PLANNING

The foundation of an effective incident response is a robust incident response plan (IRP), which guides swift action during a security incident, supported by the specialized skills of an incident response team. Regular incident response drills take this preparedness a step further, replicating potential threats and solidifying a proactive stance.

However, it's important to note that creating a resilient and agile response strategy **does not follow a linear path**. Instead, it's a continuous cycle that demands both strategic foresight and multi-layer execution. The real art also lies in balancing the readiness with continuous adaptation to new threats and vulnerabilities, ultimately crafting an incident response that evolves with the cyber threat landscape.

Table 3

INCIDENT RESPONSE STAGES		
STAGE	**KEY ACTIONS**	**CONSIDERATIONS**
Preparation	• Developing policies, guidelines, and procedures • Assigning roles • Acquiring tools	• Ensuring alignment with legal requirements • Training staff • Implementing readiness measures
Identification	• Recognizing signs of an incident • Analyzing system logs	• Timely detection • Accurate assessment • Proper communication
Containment	• Implementing short- and long-term strategies • Isolating systems	• Balancing immediate containment with preserving evidence • Planning long-term containment strategies
Eradication	• Identifying root cause • Removing malware • Restoring functionality	• Ensuring full eradication • Validating system integrity • Avoiding future recurrence
Recovery	• Monitoring systems • Verifying functionality • Implementing additional security measures	• Confirming restoration of all functionalities • Ongoing monitoring • Adjusting based on lessons learned
Lessons learned	• Analyzing incidents • Documenting insights	• Utilizing insights for future prevention • Updating and adapting strategies and plans

USER BEHAVIOR ANALYTICS

Adapting to the dynamic nature of users and triggered transactions, user behavior analytics (UBA) analyzes user activities and interactions to establish a baseline of normal behavior. Anomalies from this baseline signify potential threats, even if they originate from a seemingly legitimate user account.

- **Holistic understanding of user behavior** – Traditional security measures often miss sophisticated threats as they focus on predefined rules and signatures.
  - UBA provides a nuanced understanding of user behavior by continuously monitoring and learning from user interactions within the network. This understanding goes beyond mere rules, capturing subtle behavioral patterns that could signal malicious activities.
- **Detection of insider threats** – Whether malicious or accidental, insider threats pose significant risks. UBA's focus on behavior allows it to detect suspicious activities, even from authenticated users, making it a powerful tool against insider threats.
- **Adaptive and proactive security** – UBA adapts to the ever-changing threat landscape by dynamically learning from user behavior and updating its baseline understanding. This proactive approach keeps defenses aligned with emerging threats, making an organization more resilient.
- **Enhanced incident response** – The real-time monitoring and intelligent alerting offered by UBA enable faster detection and response to suspicious activities. Prompt action can mitigate potential damage and reduce the overall risk.
- **Integration and synergy** – UBA's strength lies in its ability to integrate smoothly with existing security systems, such as SIEM and EDR, within an enterprise. This synergy amplifies the overall protective measures, creating an enriched layer of defense.

CONCLUSION

Enterprises often regard cybersecurity as merely a technical concern, overlooking its strategic role in safeguarding assets and reputation. In contrast, the fabric of modern cybersecurity extends into intelligence, adaptability, and continuous improvement to maintain a layered defense strategy.

The real strength of your cybersecurity posture lies in the ability to detect unknown, shifting threats. While the challenge of administering such a robust posture is unending, this dynamic approach paves the way for continuous growth and readiness.

But as you embrace sophisticated threat detection mechanisms, it is worth recognizing that although they furnish enterprises with robust defenses, they can't fully contain the volatility of the evolving threat landscape.

This doesn't diminish the vitality of these security practices, though. Instead, it highlights the need to reinforce them with advanced technologies, contextual intelligence, expert insights, and an organizational culture that nurtures vigilance, resilience, and innovation.

Additional resources:

- *MalSpot: Multi2 Malicious Network Behavior Patterns Analysis* – https://www.cs.ucr.edu/~epapalex/papers/malspot_PAKDD14.pdf
- *Mobile Device Security: Corporate-Owned Personally-Enabled (COPE)* – https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-21.pdf
- *Threat Detection for Containers* Refcard – https://dzone.com/refcardz/threat-detection-for-containers
- "Threat Hunting Uncovered: Innovative Strategies for Cybersecurity" – https://dzone.com/articles/threat-hunting-uncovered-innovative-strategies-for-cybersecurity
- *Threat Modeling: Core Practices to Securing Applications* Refcard – https://dzone.com/refcardz/threat-modeling-1

WRITTEN BY SUDIP SENGUPTA,
PRINCIPAL ARCHITECT & TECHNICAL WRITER, JAVELYNN

Sudip Sengupta is a TOGAF Certified Solutions Architect with more than 18 years of experience working for global majors such as CSC, Hewlett Packard Enterprise, and DXC Technology. Sudip now works as a full-time tech writer, focusing on Cloud, DevOps, SaaS, and cybersecurity. When not writing or reading, he's likely on the squash court or playing chess.

DZone
3343 Perimeter Hill Dr, Suite 100
Nashville, TN 37211
888.678.0399 | 919.678.0300

At DZone, we foster a collaborative environment that empowers developers and tech professionals to share knowledge, build skills, and solve problems through content, code, and community. We thoughtfully — and with intention — challenge the status quo and value diverse perspectives so that, as one, we can inspire positive change through technology.