



Offensive Cybersecurity Maturity:

A Security Leaders Roadmap
To Advancing Cyber Resilience

Author

Marc Brown

Contributors

Kai Pfiester, CEO, Protexity

John Hammond, Principal Security Researcher, Huntress

Bryson Bort, SCYTHE Founder/CEO

Trey Billbrey, SCYTHE Labs

scythe.io

Table of Contents

Introduction	3
Level 1: Unstructured & Nascent Offensive Security: Laying the Foundation	5
Level 2: Repeatable & Process-Driven Offensive Security: Building a Red Team Capability	9
Level 3: Operationalized & Measured Optimized Offensive Security: Elevating Capabilities for Transformational Benefits	13
Level 4: Predictive Offensive Security: Advancing with Sophistication	17
Level 5: Optimized and Automated Offensive Security: Achieving the Zenith	21
Closing Summary and Recommendations	24
References	26

Introduction

It's common knowledge that cyber threats are becoming more sophisticated and evolving at an unprecedented pace. The importance of robust offensive cybersecurity capabilities cannot be overstated.

For security leaders looking to navigate this challenging landscape, developing a comprehensive, forward-looking strategy is essential. This strategy must assess the current state of your organization's offensive cybersecurity capabilities and outline a clear, actionable roadmap for advancement. A well-structured 18-24 month roadmap, focusing on the critical triad of people, process, and technology, is indispensable for guiding your journey from foundational reactive practices to a state of mastery and autonomy in offensive cybersecurity.

The journey towards achieving a mature offensive cybersecurity posture can be envisioned across five distinct levels, each representing a milestone in the organization's capability and maturity. Interestingly, many of the most sophisticated security teams today are still only at a foundational, nascent level of offensive cybersecurity, primarily driven by compliance requirements more than security resilience improvement efforts. The maturity spectrum spans easy-to-deploy or outsourced endpoint scanning and tabletop exercises to advanced adversarial behavior detection, AI-analyzed CTI, and more.

Our offensive security maturity model is defined across the following levels:

LEVEL
01



Non-Existent

(Ad-hoc Scanning)

Unstructured and nascent security. At this level, organizations focus on assessments (i.e., risk and tabletop) and vulnerability scanning, laying the groundwork for more advanced practices. This stage is crucial for establishing an understanding of the organization's current vulnerabilities and potential threats.

LEVEL
02



Process-Driven

(Repeatable PenTest & Vuln Mgmt)

Repeatable and process-driven. Organizations begin to build a red team capability, focusing on the basics and centered around penetration testing. This stage is about moving from reactive security measures to a more planned and organized stance, where potential threats are identified and actively exploited in controlled environments to understand their impact better.

LEVEL
03



Collaborative

(Measured, Threat Intelligence, ASM, Purple Teaming)

Collaborative and measured. The focus shifts towards operationalizing Cyber Threat Intelligence (CTI) and expanding red team operations, with an emphasis on purple teaming. This level is characterized by a mature understanding of the threat landscape, where offensive and defensive teams collaborate closely to identify, assess, and mitigate cyber threats in a more integrated and strategic manner.

LEVEL
04



Predictive

(Dynamic Threat Modeling, Adversarial Simulation, Continuous Learning)

Predictive methods are deployed. At this stage, comprehensive adversarial threat emulation and adversarial behavior detection engineering are integrated into the cybersecurity framework alongside continuous collaborative purple teaming. This level is about not just responding to threats but predicting and preparing for them through a deep understanding of adversarial tactics, techniques, and procedures (TTPs).

LEVEL
05



Autonomous

(AI/ML-Informed Strategy, Automated Feedback, Real-Time Threat Neutralization)

Optimized and automated. Organizations at this level are focused on continuous improvement and optimization, leveraging automation and advanced analytics to respond to cyber threats and anticipate and neutralize them before they can cause harm.

Let's take a deeper look into these levels.

Level 1

Unstructured & Nascent Offensive Security: Laying the Foundation



Welcome to the beginning of your journey in offensive cybersecurity. This section is designed for teams and organizations at the nascent stage of developing offensive cybersecurity capabilities. At Level 1, your focus should be on understanding the current landscape of your cybersecurity posture, identifying your team's skills and resource capabilities (or gaps), and keeping the initial steps as simple and straightforward as possible.

Baseline: Where Are You Now?

The first step in embarking on this journey is conducting a thorough baseline assessment of your cybersecurity skills and resources.

This involves evaluating the technical skills of your team, the existing security processes, and the technologies in place. Identifying these elements will help you understand your starting point and how to strategize your path forward.


At this level, simplicity is vital. Begin with basic, yet critical activities such as risk assessments, tabletop exercises, and vulnerability scanning. These foundational activities will prepare your team for more complex tasks as you progress through the maturity levels.

Risk assessments are crucial for understanding the potential threats to your organization's information security. They help identify, assess, and prioritize risks based on the likelihood of occurrence and their potential impact.




Risk assessments provide a snapshot of the organization's security posture and highlight areas that require immediate attention.


Tabletop exercises are simulated scenarios designed to test an organization's incident response capabilities. These exercises, regulated in many industries, involve key personnel discussing their roles and responses to hypothetical scenarios. The benefits of tabletop exercises include:



Enhancing communication among team members.



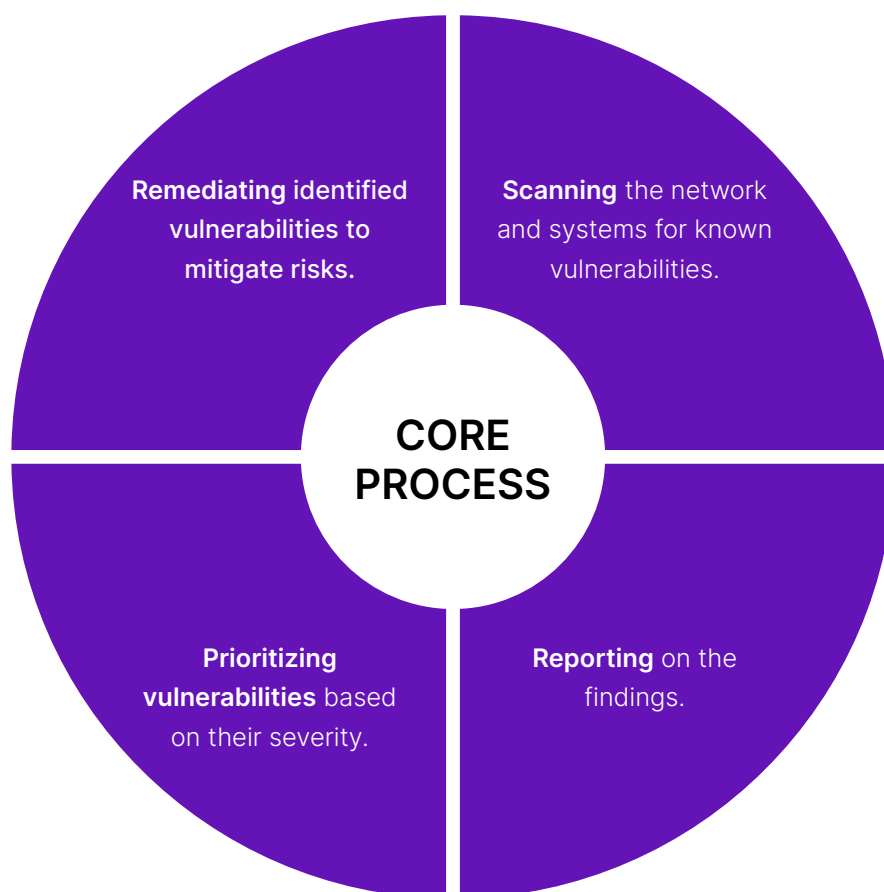
Identifying gaps in incident response plans.



Improving understanding of roles and responsibilities during a security incident.

Tabletop exercises are a low-cost, high-impact way to prepare your team for actual cyber incidents.

Vulnerability scanning is the process of identifying security weaknesses in systems and software. Using automated tools, organizations can discover vulnerabilities that could be exploited by attackers. The core process involves:



Vulnerability scanning is an essential, ongoing activity that helps maintain a secure IT environment and provides critical information for patching and vulnerability management.

The technologies involved at this level are primarily automated vulnerability scanning tools and basic risk assessment software. These tools or managed services are designed to allow organizations to regularly monitor and assess their cybersecurity posture.

Benefits and Limitations

- **Benefits**
 - Establishes a cybersecurity baseline, providing a clear understanding of where the organization stands.
 - Identifies immediate security gaps, allowing for targeted improvements.
 - Engages team members in security processes, enhancing their awareness and understanding of cybersecurity principles.
- **Limitations**
 - May not detect advanced threats, as the focus is on known vulnerabilities and rudimentary risk assessment.
 - Requires regular updates and tuning of tools and processes to remain valid. Long-term effectiveness is questionable.
 - Dependent on the quality of the vulnerability database and the comprehensiveness of the risk assessment criteria.

Although the beginning, this level is the critical starting point for teams moving into offensive cybersecurity. By focusing on baselining current skills and resources, and engaging in basic yet essential activities like risk assessments, tabletop exercises, and vulnerability scanning, organizations can lay a solid foundation for their cybersecurity journey. Remember, the key at this stage is to keep it simple, direct, and actionable. As your team gains more experience and confidence, you can gradually introduce more complex strategies and technologies to enhance your offensive cybersecurity capabilities.

Level 2

Repeatable & Process-Driven Offensive Security: Building a Red Team Capability

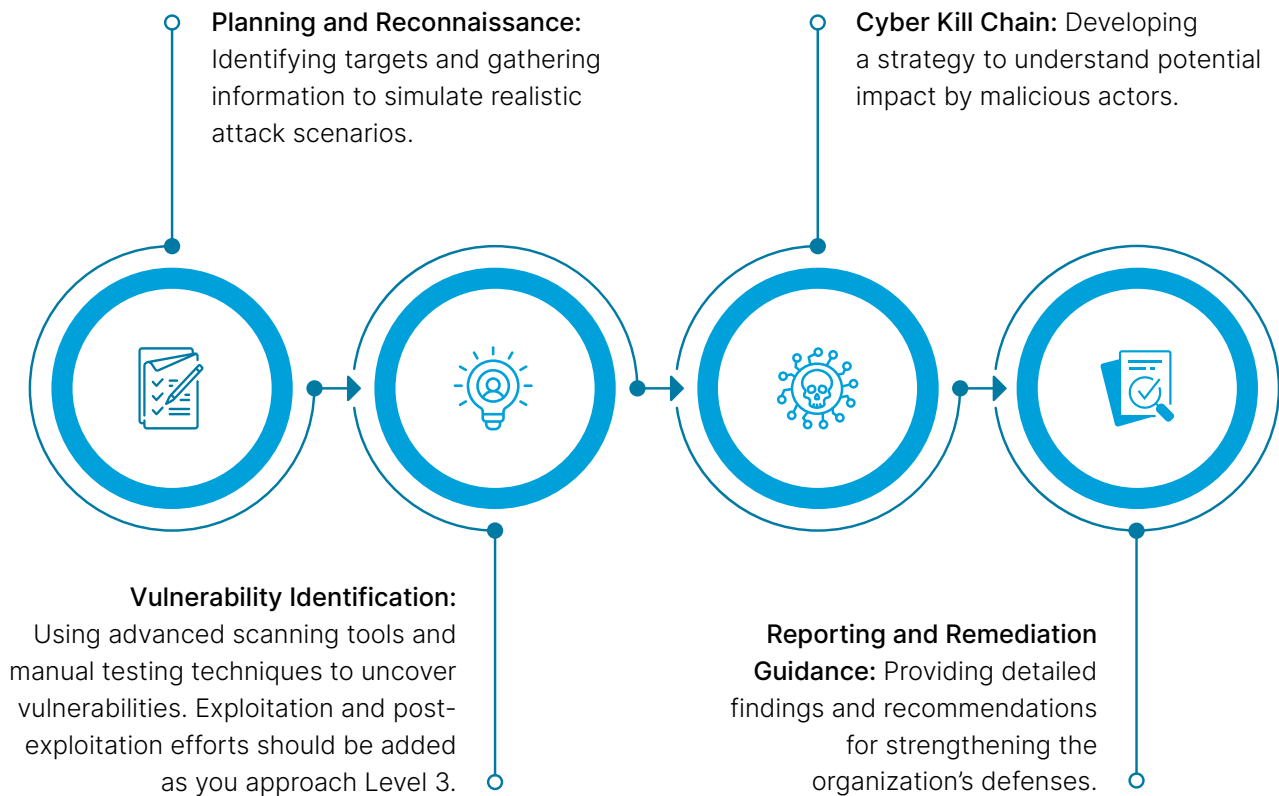


Having laid the foundational elements of offensive cybersecurity in Level 1, organizations ready to elevate their cybersecurity posture further move to a more proactive, process-driven approach. The centerpiece of Level 2 is the beginning and establishment of a Red Team capability, focusing on the basics of Red Teaming and an integrated approach to vulnerability management. This chapter will guide you through developing this capability, focusing on the processes, technologies, benefits, and limitations.



A Red Team is a group that plays the role of an adversary, using the same tactics, techniques, and procedures (TTPs) as real-world attackers to test and improve an organization's defenses. The establishment of a Red Team marks a significant step forward in an organization's offensive cybersecurity journey, transitioning from reactive security measures to proactive defense.

Red Teaming involves a series of steps designed to understand threats and attacks on an organization's networks, applications, and other critical systems to identify vulnerabilities and test the effectiveness of security measures. The core process includes:



Integration with Vulnerability Management

Integrating vulnerability management processes and supportive technologies (i.e., Tenable, Rapid7, and Qualys) ensures that vulnerabilities identified are systematically managed, tracked, and remediated. Collaboration and project management tools are essential for coordinating activities and integrating their findings with the broader IT and cybersecurity management processes. This integration involves:

- **Prioritizing vulnerabilities** based on the risk they pose, informed by the realistic attack scenarios developed by the Red Team.
- **Developing remediation plans** that are actionable and aligned with the organization's risk tolerance.
- **Tracking remediation progress** to ensure vulnerabilities are addressed in a timely manner.

The Cyber Kill Chain

As you begin your Red Team operations, it's critical to research, evaluate, and analyze threats across the entire kill chain. This approach enables the team to identify and understand the various tactics, techniques, and procedures (TTPs) employed by attackers at each stage of the kill chain. This holistic evaluation is essential for developing targeted strategies to enhance security measures, improve incident response, and fortify the organization's cybersecurity posture. Even in the early stages of forming a Red Team, this level of analysis is invaluable in laying the groundwork for a proactive and resilient security program.



Know the Importance of Red Teaming

Red Team understanding (and investment) is crucial for all organizations, regardless of the team's philosophy, whether they believe in, want to, or can afford to have an internal Red Team. Even for those who choose not to maintain an in-house team, recognizing the value of Red Team activities in identifying exposures and enhancing security measures is essential. Outsourcing Red Team exercises to external service providers is a viable alternative that allows organizations to benefit from specialized expertise and an outsider's perspective on their security posture. This approach ensures that, with or without an internal Red Team, the processes accommodate regular security assessments and evaluations, ultimately increasing the organization's preparedness for future attacks.

Benefits and Limitations

- **Benefits**
 - **Proactive Identification of Vulnerabilities:** By simulating real-world attacks, organizations can identify and remediate vulnerabilities before threat actors can exploit them.
 - **Enhanced Security Posture:** Red Teaming provides a realistic assessment of the effectiveness of current security measures and practices.
 - **Improved Incident Response:** Simulated attacks prepare the incident response team for actual breach scenarios, improving reaction times and effectiveness.
- **Limitations**
 - **Resource Intensive:** Establishing and maintaining a Red Team requires significant investment in skilled personnel and advanced tools.
 - **Potential for Disruption:** If not carefully managed, Red Team activities can disrupt business operations.
 - **Continuous Evolution Required:** As adversaries evolve, the Red Team must continually update their tactics and tools to remain effective.

By building a Red Team and integrating their activities with vulnerability management, organizations can proactively identify and remediate vulnerabilities, significantly enhancing their security posture. While this approach requires significant resources and careful management, the benefits in terms of improved security and resilience against attacks are substantial. As organizations continue to navigate the complexities of the cybersecurity landscape, the establishment of a Red Team capability will be a critical component of their offensive security strategy.

Level 3

Operationalized & Measured Optimized Offensive Security: Elevating Capabilities for Transformational Benefits



At Level 3, organizations embark on a transformative journey to significantly advance their offensive security capabilities. This stage is about operationalizing Cyber Threat Intelligence (CTI), expanding Red Team operations, and introducing Purple Teaming alongside a focus on adversary emulation, advanced tradecraft, and security awareness and training. This comprehensive approach raises the bar for offensive security and leads to transformational benefits in organizational security resilience. This section delves into how to achieve this elevated state, highlighting core processes, technologies, benefits, and inherent limits.

Operationalizing Cyber Threat Intelligence (CTI)

Cyber Threat Intelligence (CTI) is vital to informing and guiding offensive security operations. Operationalizing CTI means integrating real-time intelligence about threats and adversaries into offensive security strategies to predict, prepare for, and neutralize threats more effectively. Core processes that need to be developed include:

- **Collection and Analysis:** Gathering intelligence from a variety of sources, analyzing it to identify relevant threats.
- **Integration with Offensive Operations:** Utilizing CTI to inform Red and Purple Team exercises, focusing on the most relevant and current threats.
- **Feedback Loop:** Using insights gained from offensive operations to refine CTI gathering and analysis processes.

Expanding Red Team Operations

Expanding Red Team operations involves scaling the sophistication and scope of simulated/emulated attacks to mirror sophisticated adversaries more accurately.

This includes:

- **Advanced Scenario Planning:** Developing complex attack scenarios that reflect today's evolving threat landscapes and the tactics, techniques, and procedures used.
- **Expand Red Teaming Capabilities:**
 - **Exploitation:** Attempting to exploit identified vulnerabilities to understand the potential impact of an attack.
 - **Post-Exploitation and Analysis:** Assessing the damage, lateral movement, and data exfiltration possibilities, followed by a comprehensive analysis of the security posture.
- **Cross-Domain Operations:** Conducting operations that span across physical (i.e., call centers), digital (i.e., endpoints), and social engineering (i.e., staff email) domains.
- **Collaboration with External Entities:** Engaging with external cybersecurity communities and organizations for knowledge exchange and joint exercises.



Introducing Purple Teaming

Purple Teaming enhances the effectiveness of security measures by integrating the offensive insights of Red Teams with the defensive tactics of Blue Teams, creating a synergistic collaborative security effort. Better yet, purple teaming can help identify weaknesses and exposures across a broader domain, evaluating an organization's policies, procedures, and technology. Processes that need to be developed include:

- **Joint Exercises:** Conducting exercises where Red and Blue Teams work together to identify and remediate vulnerabilities.
- **Continuous Feedback Loop:** Establishing mechanisms for ongoing knowledge sharing between Red and Blue Teams.
- **Skill and Knowledge Enhancement:** Leveraging exercises to improve the skills and capabilities of both teams.
- **Evaluate Integrated TTX and PTE:** Combining tabletop exercises with purple team exercises, organizations stress the security and administrative processes.

Note: To accelerate your teams Purple Teaming, download the [CISO Guide to Purple Teaming](#) and the [Purple Team Framework](#)

Adversary Emulation and Advanced Tradecraft

Adversary emulation involves simulating real-world attackers' tactics, techniques, and procedures (TTPs), using advanced tradecraft to uncover exposures and test defenses. This includes:

- **Breach and Attack Simulation (BAS+):** To be more efficient, teams must evaluate and adopt an adversarial emulation platform that enables quick emulations of threats, security control validation, or cyber hygiene checks.
- **TTP Research and Development:** Developing sophisticated TTPs based on real-world intelligence. This step can be reduced by purchasing and adopting some adversarial emulation tools (i.e., SCYTHE) that provide pre-packaged threats and IOCs based on the latest CTI.
- **Scenario-Based Testing:** Executing complex attack scenarios to test and improve security measures.

Note: For production-safe adversarial emulation, download the [SCYTHE Overview](#) or schedule a [demo](#) of the platform.

Security Awareness and Training

Elevating security awareness and training across the organization is crucial for creating a security culture and ensuring all members understand their role in maintaining security resilience. This includes:

- **Targeted Training Programs:** Developing training tailored to different roles within the organization.
- **Simulated Attacks (Ransomware, Phishing, and Social Engineering):** Conduct regular attack emulations to improve awareness and response to social engineering attacks.
- **Continuous Learning and Development:** Providing ongoing opportunities for learning about the latest threats and defensive tactics.

Benefits and Limitations

- **Benefits**
 - **Comprehensive Threat Perspective:** Integrating CTI into offensive operations offers a nuanced understanding of potential threats.
 - **Enhanced Defense through Collaboration:** Purple Teaming fosters a collaborative environment that significantly improves security measures while breaking down common walls between red and blue teams.
 - **Realistic Assessment of Defenses:** Adversary emulation provides a realistic assessment of how well defenses and processes can withstand and respond to sophisticated attacks.
 - **Organizational Security Culture:** Security awareness programs cultivate a culture that values and actively contributes to security.
- **Limitations**
 - **Resource Intensity:** Implementing and maintaining advanced offensive security operations requires advanced skill sets, which are still limited.
 - **Skill Set Requirements:** Advanced operations demand high expertise, which may necessitate specialized training or hiring.
 - **Potential for Operational Disruption:** Complex security exercises could disrupt day-to-day operations without careful planning or selecting product-safe tools.

Level 4

Predictive Offensive Security: Advancing with Sophistication



Level 4 in the offensive security maturity model is a testament to an organization's commitment to defending against and staying ahead of cyber threats. It is a phase where offensive security strategies are not only advanced but predictive, leveraging the full spectrum of technology. This can include comprehensive adversarial threat emulation to threat hunting, sophisticated behavior detection, continuous Purple Teaming, and the integration of big data, machine learning (ML), and automation. This level of maturity is particularly critical for high-risk industries continuously under the threat of sophisticated cyber attacks.



Comprehensive Adversarial Threat Emulation

At Level 4, adversarial threat emulation is not just about simulating known threats but creating a dynamic model of potential future attacks based on evolving threat landscapes. This includes:

- **Dynamic Threat Modeling:** Utilizing current threat intelligence to model possible future attack vectors.
- **Automated Scenario Generation:** Leveraging big data and ML to create and test attack scenarios, ensuring a broad and comprehensive understanding of potential vulnerabilities.
- **Continuous Learning Loop:** Integrating feedback from emulation exercises into the threat modeling process to refine and enhance future simulations.

Note: To gain insights into the latest Detection Engineering techniques, check out SCYTHE's free workshop on [Detection Engineering](#) and learn from the pros.

Advanced Adversarial Behavior Detection (ABD) Engineering

This involves the deployment of cutting-edge technologies and methodologies to detect even the most subtle indicators of a potential breach or attack, often before they fully materialize. ABD would include the following processes:

- **Predictive Analytics:** Applying ML algorithms to historical and real-time data to identify patterns indicative of malicious activity.
- **Behavioral Biometrics:** Using behavioral biometrics to detect anomalies in user behavior that could signal a compromise.
- **Automated Response Protocols:** Implementing automated systems capable of responding to detected threats in real-time, minimizing potential damage.

Note: To gain insights into the latest Detection Engineering techniques, check out SCYTHE's free workshop on [Detection Engineering](#) and [Weaponizing Sigma](#). Learn from the pros.

Continuous Collaborative Purple Teaming

Enhancing the synergy between Red and Blue Teams through continuous collaboration ensures that defensive strategies are not just reactive but proactively informed by the latest offensive tactics and insights. This would require your team to develop the following processes:

- **Integrated Exercise Planning:** Developing exercises deeply integrated with real-world threat scenarios ensures that both teams work on the most relevant and pressing issues.
- **Real-Time Information Sharing:** Utilizing platforms that enable real-time information sharing between teams, allowing for immediate adjustments to defense mechanisms based on offensive findings.
- **Adaptive Strategy Development:** Creating a framework for the rapid development and deployment of new defensive strategies based on insights gained from Purple Team exercises.

Leveraging Big Data, Machine Learning, and Automation

Using big data, ML, and automation not only enhances the scale and speed at which offensive security operations can be conducted but also increases their precision and effectiveness. This would include:

- **Data-Driven Threat Intelligence:** Analyzing vast datasets to uncover emerging threats and trends in the cyber landscape.
- **ML-Enhanced Adversarial Emulation:** Leveraging BAS+ platforms that have incorporated ML-powered virtual assistants to assist with CTI - TTP analysis, threat creation, and mitigation recommendations.
- **ML-Enhanced Detection Systems:** Employing ML models to improve the detection of sophisticated cyber threats, reducing false positives and enhancing accuracy.
- **Automated Security Orchestration:** Using automation to streamline the execution of security processes, from threat detection to response, allowing for a more agile security posture.

Benefits and Limitations

- **Benefits**
 - **Anticipatory Threat Detection:** Advanced strategies enable organizations to detect and neutralize threats before they manifest into successful attacks.
 - **Enhanced Operational Efficiency:** Automation and ML streamline security operations, allowing for the efficient allocation of resources.
 - **Dynamic Adaptation:** Continuous learning and adaptation mechanisms ensure that security strategies evolve at the pace of the threat landscape.
- **Limitations**
 - **Complexity and Resource Intensity:** Implementing these advanced strategies requires investment in technology and skilled personnel.
 - **Risk of Overreliance on Automation:** Excessive reliance on automated systems can lead to complacency and potentially overlook nuanced threats.
 - **Continuous Evolution Required:** The effectiveness of these strategies depends on the organization's ability to continuously update and refine its technologies and processes in line with emerging threats.

Predictive offensive security represents the pinnacle of offensive cybersecurity for organizations, especially those in high-risk industries facing constant threats. By embracing comprehensive adversarial threat emulation, advanced adversarial behavior detection engineering, continuous collaborative Purple Teaming, and leveraging big data, ML, and automation, organizations can defend against current threats and anticipate and neutralize future ones. While the journey to this level of maturity is complex and resource-intensive, the strategic advantages it offers in terms of predictive threat detection, operational efficiency, and dynamic adaptation make it an essential goal for organizations committed to maintaining the highest standards of cybersecurity resilience.

Level 5

Optimized and Automated Offensive Security: Achieving the Zenith



Level 5 represents the zenith of offensive security strategies, where organizations have mastered advanced offensive capabilities and optimized and automated these processes to achieve the highest levels of efficiency and effectiveness. This stage is characterized by continuous improvement and optimization, advanced and optimized adversarial behavior detection engineering, and the deep integration of artificial intelligence (AI) and machine learning (ML) into every aspect of offensive security operations. Reserved for a select group of organizations that demand the utmost in cybersecurity defense—typically those facing sophisticated, persistent threats—Level 5 is the epitome of what can be achieved in offensive cybersecurity. This chapter explores the processes, technologies, benefits, and limitations of attaining and operating at this pinnacle level.

Continuous Improvement and Optimization

At Level 5, the mantra is continuous improvement and optimization. Organizations operate in a state of perpetual refinement, leveraging feedback loops, data analytics, and AI to continuously enhance their offensive security capabilities. This would include processes covering:

- **Data-Driven Strategy Refinement:** Utilizing data analytics to assess offensive strategies' effectiveness and identify improvement areas.
- **Automated Feedback Loops:** Implementing systems that automatically adjust strategies based on outcomes and new intelligence.
- **Optimization of Resources:** Using AI to ensure that resources are allocated most efficiently, maximizing the impact of offensive security operations.

Advanced and Optimized Adversarial Behavior Detection Engineering

Adversarial behavior detection at this level goes beyond identifying threats to predicting and neutralizing them before they can manifest, using sophisticated AI models that are continuously refined and include:

- **Predictive Threat Modeling:** Applying advanced ML algorithms to predict threats before they emerge based on patterns identified in vast datasets.
- **Self-Learning Systems:** Employing AI systems that evolve over time, learning from each interaction to improve their threat detection capabilities.
- **Real-Time Threat Neutralization:** Implementing systems capable of detecting and automatically neutralizing threats in real-time, minimizing potential damage.

Integration of AI and Machine Learning

AI and ML are not just tools at Level 5; they are integral components of the offensive security strategy, embedded into every process and operation to enhance speed, efficiency, and effectiveness. This includes addressing:

- **AI-Powered Offensive Tools:** Developing and deploying offensive tools that leverage AI to identify vulnerabilities and execute attacks on test systems more effectively.
- **ML-Based Vulnerability Discovery:** Using ML algorithms to automatically discover new vulnerabilities, particularly those that may not be detected through traditional methods.
- **Automated Security Orchestration:** Integrating AI with security orchestration, automation, and response (SOAR) technologies to automate complex decision-making processes in real-time.

Benefits and Limitations

- **Benefits**
 - **Proactive and Predictive Security:** The ability to predict and neutralize threats before they occur offers unparalleled security resilience.
 - **Highly Efficient Operations:** Automation and AI-driven optimization ensure that offensive security operations are conducted efficiently.
 - **Dynamic Adaptability:** AI and ML enable organizations to adapt to new threats more rapidly than ever, ensuring their defenses are always at the cutting edge.
- **Limitations**
 - **High Complexity and Investment:** Achieving and maintaining Level 5 capabilities requires significant investment in advanced technologies and skilled personnel.
 - **Regulatory and Procedural Considerations:** Using AI in offensive security raises regulatory and procedural questions that organizations must navigate carefully.
 - **Risk of Overdependence on Automation:** There is a risk that overreliance on automated systems could lead to vulnerabilities if these systems fail or are circumvented by new types of attacks.

Optimized and automated offensive security is the ultimate goal for organizations seeking the pinnacle of cybersecurity defense. By embracing continuous improvement, advanced adversarial behavior detection, and the deep integration of AI and ML, organizations at this level can achieve a reactive, proactive, and predictive state of cybersecurity. While the path to Level 5 is complex and requires substantial investment, its benefits—in terms of security resilience, operational efficiency, and the ability to stay ahead of threats—make it a worthy aspiration for organizations facing the most sophisticated and persistent cyber threats. However, achieving Level 5 is not for all organizations, but a small minority.

Closing Summary and Recommendations

The journey through the Offensive Cybersecurity Maturity Model is a strategic endeavor that equips organizations with the capabilities to respond to, anticipate, and neutralize cyber threats. Progressing from Level 1 (Unstructured & Nascent) to Level 5 (Optimized and Automated) allows teams to transform their cybersecurity posture from reactive to predictive, leveraging advanced technologies and methodologies at each step.

Key Recommendations for Teams

- 1. Establish a Strong Foundation by Focusing on Basics:** At Level 1, prioritize understanding your current security posture and addressing basic vulnerabilities through tabletop assessments, scanning, and remediation. This foundation is crucial for all subsequent advancements.
- 2. Develop and Refine Capabilities by Building Red and Purple Teams:** By Levels 2 and 3, establish dedicated Red Teams and foster Purple Teaming dynamics to enhance collaboration between offensive and defensive efforts. This collaboration is vital for identifying and rectifying vulnerabilities effectively. Foster the growth of your personnel and capabilities through training, tool acquisition and development, and TTP documentation.
- 3. Leverage Technology and Intelligence by Integrating CTI and Advanced Tools:** From Level 3 onwards, operationalize Cyber Threat Intelligence (CTI) and utilize advanced penetration testing tools. Emphasize the adoption of AI and machine learning by Level 4 and 5 to automate and optimize offensive strategies.
- 4. Foster Continuous Improvement:** Security is not a destination but a continuous journey. Regularly revisit your strategies, incorporate new threat intelligence, and refine your approaches based on feedback and emerging technologies.
- 5. Invest in Training and Awareness to Cultivate Expertise:** Continuous education and training for your teams are paramount. Stay abreast of the latest cyber threats and defense mechanisms to ensure your team's skills are current and effective.
- 6. Embrace Collaboration and Share Knowledge:** Engage with the wider cybersecurity community. Sharing insights and learning from the experiences of others can provide new perspectives and enhance your security strategies.

Strategic Approach to Advancement

- **Assess Regularly:** Conduct periodic assessments to understand where your team stands within the maturity model and identify areas for improvement.
- **Set Realistic Goals:** Define clear, achievable objectives for progressing to the next level. Ensure these goals are aligned with your organization's risk profile and business objectives.
- **Allocate Resources Wisely:** Advancing through the levels requires investment in tools, training, and personnel. Prioritize resources based on the most critical gaps and opportunities for impact.

Advancing through the Offensive Cybersecurity Maturity Model is a strategic process that requires commitment, investment, and a proactive approach to cybersecurity. Organizations can systematically enhance their offensive security capabilities by understanding the requirements and benefits of each level. The ultimate goal is to achieve cybersecurity maturity, where the organization defends against current threats and is equipped to predict and prevent future vulnerabilities. With a focus on continuous improvement, technology integration, and team development, organizations can navigate the complexities of the cyber landscape more effectively, ensuring resilience against evolving threats.



References

- eBooks
 - Purple Teaming Guide (<https://scythe.io/ptef>)
 - Red Team Operations Roadmap (<https://scythe.io/red-team-guide>)
 - Adversarial Emulation Detections (<https://scythe.io/adversarial-behavior-detection>)
- SCYTHE Adversarial Emulation Platform (<https://scythe.io/platform>)
- SCYTHE Purple Team Guide (<https://scythe.io/purple-team-guide>)
- MITRE ATT&CK Framework (<https://attack.mitre.org/>)
- Sigma Rules (<https://github.com/SigmaHQ/sigma>)
- Cyber Kill Chain, MITRE ATT&CK, and Purple teaming (<https://www.sans.org/blog/cyber-kill-chain-mitre-attack-purple-team>)

Learn more at scythe.io



SCYTHE

6751 Columbia Gateway
Columbia, MD 21046
info@scythe.io

About SCYTHE

SCYTHE represents a paradigm shift in cybersecurity risk management, empowering organizations to Attack, Detect, and Respond efficiently. The SCYTHE platform enables adversarial emulation, security controls validation, and aid in the collaboration between red, blue, and purple teams to improve their security posture.