Red Piranha TDIR: Global Compliance, Unmatched Security

Red Piranha
unified threat management

To keep up with advanced cyber threats effective threat detection, response and event logging are key to staying secure. In a concerted effort to bolster global cybersecurity resilience, international cybersecurity authorities have come together to develop comprehensive guidelines. Leading this initiative is the **United States Cybersecurity and Infrastructure Security Agency (CISA)**, working in close collaboration with key partners:

- **United States (US)**: Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and National Security Agency (NSA)
- **United Kingdom (UK)**: National Cyber Security Centre (NCSC-UK)
- Canada: Canadian Centre for Cyber Security (CCCS)
- **New Zealand**: National Cyber Security Centre (NCSC-NZ) and Computer Emergency Response Team (CERT NZ)
- **Japan**: National Center of Incident Readiness and Strategy for Cybersecurity (NISC) and Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)
- **Republic of Korea**: National Intelligence Service (NIS) and NIS's National Cyber Security Center (NCSC-Korea)
- **Singapore**: Cyber Security Agency (CSA)
- **Netherlands**: General Intelligence and Security Service (AIVD) and Military Intelligence and Security Service (MIVD)

These guidelines represent a unified global effort to enhance cybersecurity readiness and defence against the increasingly sophisticated landscape of cyberattacks.

As cyber threats rapidly evolve organisations face a critical challenge: the rise of EDR (Endpoint Detection and Response) evasion tools. Widely available on cybercrime forums, these tools enable attackers to bypass traditional EDR systems and operate undetected.

This trend reveals a growing threat to endpoint security with attackers deploying increasingly stealthy tactics such as living off the land (LOTL) to execute ransomware attacks and evade detection. Current EDR solutions are struggling to keep pace.

To counter these sophisticated threats security strategies must evolve by integrating advanced network-based analytics and threat intelligence to stay ahead of attackers and prevent breaches before they escalate.

Red Piranha is a pioneer and leader in the threat detection / incident response (TDIR) segment with Crystal Eye designed to meet the stringent requirements mentioned in the best practices offering advanced capabilities to enhance your security posture. We will look to explain how Crystal Eye TDIR solution aligns with these best practices through real-world scenarios demonstrating its effectiveness in addressing modern cybersecurity challenges.

What are the growing challenges in Threat Detection and Response?

As cyber threats grow more sophisticated and evolve at an unprecedented pace, organisations face a critical challenge in defending against the increasing use of EDR (Endpoint Detection and Response) evasion tools. These EDR evasion tools, now widely available on cybercrime forums, represent a significant advancement in offensive capabilities, allowing them to bypass traditional EDR systems and execute attacks undetected.

The rise of these evasion tools underscores a troubling trend: adversaries are specifically developing techniques to circumvent endpoint security solutions threatening to undermine the effectiveness of foundational cybersecurity measures. As attackers employ stealthier tactics—prolonging ransomware attacks and leveraging methods like living off the land (LOTL)—current EDR systems often struggle to detect and respond in time.

This growing gap in security highlights the need for a more proactive, intelligence-driven approach to threat detection and response. Without integrating advanced analytics and threat intelligence into defence strategies organisations risk falling victim to increasingly sophisticated attacks that bypass conventional defences. The challenge is clear: to stay ahead of evolving threats security measures must evolve as well, embracing technologies and strategies capable of countering even the most advanced evasion techniques.

According to the global guidelines, it is crucial to examine the core recommendations for event logging and threat detection and response across various network environments. The guidelines emphasise best practices for cloud services, enterprise IT networks, enterprise mobility, and operational technology (OT) networks.

These recommendations are tailored for cybersecurity practitioners, IT managers, OT operators, and network administrators within medium to large organisations assuming a fundamental grasp of event logging.

What are the essential best practices?

According to the guideline the five essential principles that underpin these best practices are:

1. **Develop a Detection and Response Strategy for Relevant Threats:** Establishing a robust detection strategy is essential for identifying and responding to threats. This involves setting up mechanisms to detect suspicious activities and anomalies which are critical for timely threat mitigation.
2. **Establish detection Alerts for Critical Cybersecurity Events and Indicators of Compromise:** Implement a system to send immediate alerts to network defenders when significant cybersecurity events occur. Additionally, ensure that the system can identify and flag potential cybersecurity incidents including activities indicative of malicious actors using living off the land (LOTL) techniques or engaging in post-compromise lateral movement.

3. **Develop a Centralised Logging Policy with Secure Storage and Correlation**: Establish an enterprise-approved logging policy that defines which events need to be logged and sets clear guidelines for monitoring and retention. Centralise the collection of logs from diverse systems to enable efficient aggregation and analysis while ensuring the integrity of logs through secure storage. Correlating log data across different sources will provide a comprehensive view of security activity helping to identify and mitigate potential threats effectively.
4. **Support Incident Response and Optimise Monitoring**: Enhance incident response by revealing the full scope of compromises, monitor account compliance with organisational policies, and reduce alert noise to lower storage and query costs.
5. **Enable Informed Decisions with Optimized Logging and Analytics**: Equip network defenders to make agile, informed decisions by prioritising alerts and analytics while ensuring logs and logging platforms are user-friendly and performant for efficient analysis.

Red Piranha's Crystal Eye TDIR solution is meticulously designed to align with these best practices for event logging, threat detection, and response. By incorporating a detection and Response Strategy, establishing the detection alerts for critical cybersecurity events and indicators of compromise, developing centralised logging policy with secure storage, and optimised logging and analytics Crystal Eye ensures robust and effective monitoring across all network environments.

This proactive approach enhances an organisation's capability to detect and respond to threats swiftly reinforcing its overall cybersecurity posture. Let's consider how Crystal Eye meets the modern event Logging and threat detection and response requirements in more detail.

Advanced Threat Detection Strategies: Enhancing Threat Visibility

As mentioned earlier, the rise of new EDR evasion tools poses an increasing challenge for organisations seeking to safeguard their systems. It is a prime example of how threat actors are enhancing their capabilities to outsmart traditional defences particularly Endpoint Detection and Response (EDR) systems.

The increasing use of these EDR bypass tools exposes a significant vulnerability in current security strategies. As evasion tactics continue to evolve, traditional EDR systems may struggle to keep up emphasising the need for a more advanced and adaptive approach to threat detection and response.

Implementing strong detection and response strategies helps in identifying and responding to threats including advanced techniques like living off the land (LOTL). The guidelines highlight the need for analytics and threat intelligence to detect subtle and sophisticated threats.

For instance, if attackers are using PowerShell and other LOLBins (Living Off the Land Binaries) to execute commands and move laterally within the network, Crystal Eye leverages Network Detection and Response (NDR) solution to monitor and analyse system activities, including the use of PowerShell and other LOLBins. It detects all known Malware families and C2 (Command and Control) call outs like Cobalt Strike, for extra assurance.

"Living off the land" (LOTL) attacks exploit legitimate tools and features already present on most systems allowing attackers to avoid detection by blending in with normal activities. This makes it harder for security teams to spot the threat as traditional security measures often overlook such benign-looking behaviour.

Advanced persistent threats (APTs) often use LOTL techniques like PowerShell scripts or WMI tools to bypass endpoint detection and response (EDR) solutions. By mimicking legitimate system processes attackers can remain undetected for extended periods, moving laterally through networks and executing their attacks without triggering alarms.

To address this issue, organizations should adopt a Network Detection and Response (NDR) strategy. NDR solutions continuously monitor all network traffic including internal east-west communication to detect and neutralize threats that bypass the network perimeter. By implementing NDR organizations gain comprehensive visibility across their network enabling them to identify threats that evade endpoint defences and respond promptly.

These NDR solutions leverage advanced machine learning algorithms to detect unusual patterns in network behaviour such as abnormal data transfers, lateral movement, or command-and-control (C2) traffic. Additionally, NDR solutions with robust detection capabilities and integrated threat intelligence offer valuable context into network activities empowering security teams to swiftly investigate and respond to threats.

For example, according to this report, Volt Typhoon has been focusing on critical infrastructure organisations predominantly using LOTL (Living off the Land) techniques since mid-2021.

Their operations have been facilitated by privately-owned SOHO routers which have been compromised by the 'KV Botnet' malware. Red Piranha has been actively monitoring Volt Typhoon's activities through our Threat Intelligence report staying ahead of evolving tactics.

Red Piranha's Threat Detection, Investigation, and Response (TDIR) solution is exceptionally well equipped to detect and prevent sophisticated attacks like those executed by Volt Typhoon.

Volt Typhoon's reliance on Living Off The Land (LOTL) techniques present unique challenges in detection. This is where Crystal Eye's advanced Network Detection and Response (NDR) capabilities provide comprehensive visibility and protection against sophisticated threats like Volt Typhoon.

Encrypted traffic is fully supported allowing for greater protection across multiple attack vectors while Integrated Cyber Threat Intelligence (CTI) delivers contextualised, automated, and actionable intelligence for proactive threat protection.

Automated incident response further enhances this protection by containing and remediating threats in real-time minimising the impact of potential breaches.

Crystal Eye is fed updated threat protection data giving it up to 10 times more visibility than other NGFW (Next Generation FireWalls) in its class detecting all known malware families and C2 call outs.

With the ability to process over 3,200 protocols out of the box and features to create custom SCADA protocols and enrich metadata at the time of collection, Crystal Eye enables businesses to capture comprehensive network session details.

This is complemented by a minimum of 18 months of Incident and Event storage facilitating forensic investigations. Crystal Eye's integration of Secure Web Gateway, Azure AD, and unified policy control across web, email, and authentication events delivers unparalleled network visibility and detection capabilities.

The platform's single deployment approach reduces costs and eliminates the complexity of managing disparate systems while providing 24/7 access to a dedicated security team and delivering up to five times more network visibility than alternative solutions.

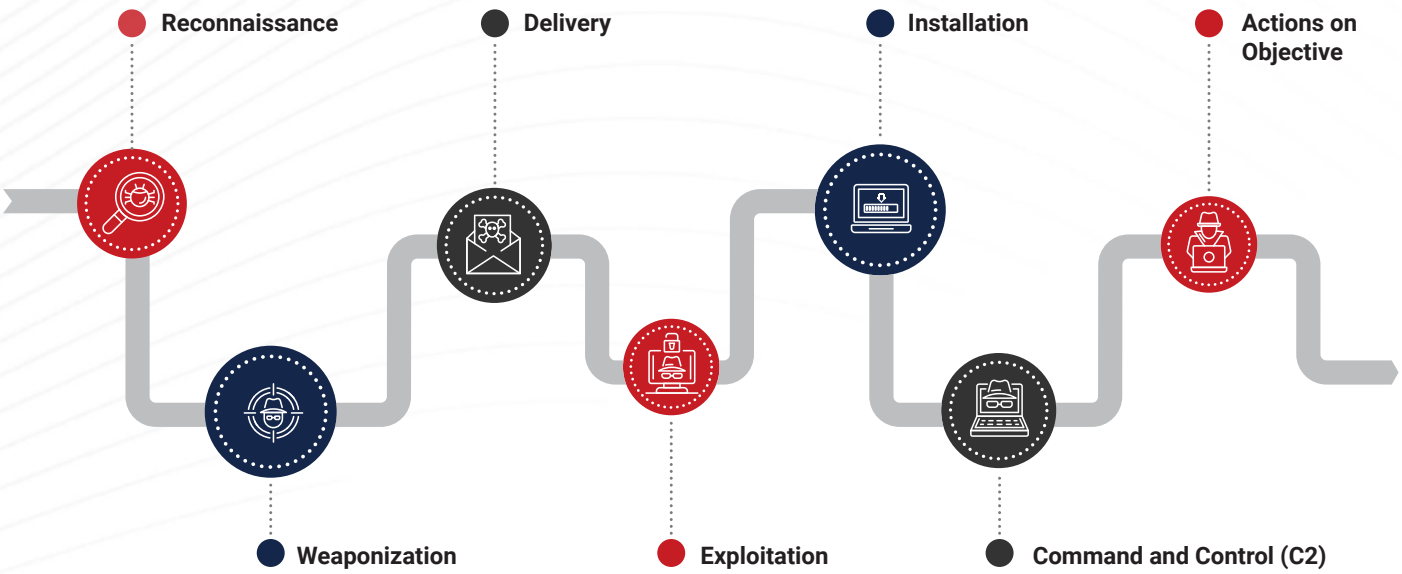
Not only this, to effectively counter Living off the Land (LOTL) attacks security teams should prioritise implementing a Zero Trust Architecture and focus on detecting unusual activities through a robust and continuously refined monitoring program.

This approach demands the deployment of sophisticated threat detection tools like Network Detection and Response (NDR) solutions. These tools analyse network traffic to identify and respond to unusual patterns enhancing the capabilities of Security Operations Centers (SOCs) for comprehensive threat management.

Red Piranha's TDIR also aligns with the best practices outlined in CISA's **Joint Guidance on Identifying and Mitigating Living Off the Land (LOTL) Attacks** by emphasising robust detection mechanisms that focus on event activity rather than just traditional indicators of compromise. LOTL attacks which use legitimate tools and processes to avoid detection can bypass standard endpoint defences.

For instance, Red Piranha's TDIR (Threat Detection, Investigation, and Response) aligns with CISA's guidance on mitigating Living Off the Land (LOTL) attacks by applying **threat modelling and the kill chain framework** to proactively detect and respond to sophisticated threats.

The Cyber Kill Chain



While traditional endpoint defences may struggle to detect LOTL techniques due to their use of legitimate tools to evade detection, Crystal Eye adopts a behaviour-centric approach focusing on **event activity and anomalies** throughout all stages of the kill chain—reconnaissance, weaponization, delivery, exploitation, installation, C2, and actions on objectives.

By establishing behavioural baselines and leveraging AI/ML (Artificial Intelligence/Machine learning) -driven models along with UEBA (User and Entity Behaviour Analytics) Crystal Eye can identify deviations from normal operations that indicate potential LOTL activity even when attackers blend into regular system behaviour.

Through comprehensive log collection and secure out-of-band storage Crystal Eye ensures that all events are retained for thorough analysis and timely detection of malicious behaviour across the attack lifecycle. This proactive use of threat modelling and automated incident response enables quick identification and mitigation of threats enhancing resilience against advanced attacks and effectively adhering to CISA's best practices for robust and adaptive threat defence.

Prioritising Advanced Detection: A Risk-Based Approach

According to Gartner's Risk-Based Approach to Threat Detection, Investigation and Response to truly enhance your threat detection strategies it's crucial to lead with a focus on the "why" behind these measures particularly when dealing with sophisticated threats like Living off the Land (LOTL) techniques. Understanding the kill chain and attack patterns is fundamental to effectively identifying and mitigating these threats.

For instance, many organisations have fallen into the trap of logging everything hoping to detect threats later. This reactive approach has proven not only unsustainable but ineffective as storage demands rapidly exceed existing available resources. A site with just 30-40 users can easily generate 200 terabytes of log data monthly. With the cost of storing and analysing data is soaring many organisations are already finding this approach unsuitable.

However, the real problem lies in what this does to SOC teams. More data doesn't equal better security—it leads to more noise, complexity, and ultimately more opportunities for threats to slip through unnoticed. This is where a risk-based approach becomes essential. Instead of capturing everything it's about prioritising what matters—focusing on the most critical data to enhance threat detection without overwhelming resources.

The shift in strategy should start with Red Piranha's TDIR/NDR solution which takes a risk-based approach to threat detection. Rather than attempting to log data from every single device, firewall, and switch, Red Piranha's NDR is designed to capture only the most relevant events. A typical user with enterprise data profiling can generate around 2GB of critical data daily. So in an organisation with 100 users, you're looking at 200GB per day or 5TB per month—a manageable volume compared to indiscriminate logging.

The core issue here is avoiding the massive costs associated with storing significant volumes of data and instead focusing on what is truly necessary for detecting real threats. Here's how Red Piranha's risk-based approach addresses the problem:

Red Piranha's Crystal Eye NDR exemplifies a smarter, risk-based approach to threat detection by focusing on actionable data over indiscriminate logging. Rather than capturing every event that occurs across your environment Crystal Eye NDR uses threat modelling to identify the most relevant and high-impact data ensuring that detection capabilities are both precise and effective.

This prioritisation not only improves the accuracy of threat identification but also reduces complexity alleviating the pressure on SOC teams. By leveraging threat modelling and understanding the kill chain, Crystal Eye NDR can pinpoint crucial attack stages—such as reconnaissance, exploitation, and lateral movement—allowing SOC teams to proactively detect and disrupt adversary actions before a breach escalates.

For example, consider a scenario where a threat actor is trying to compromise a network by moving laterally to access sensitive data. The threat modelling approach identifies this behaviour early in the kill chain during reconnaissance or the exploitation phase based on predefined patterns and anomalous network traffic.

Instead of being overwhelmed with logs from benign activity SOC teams are alerted to critical events like privilege escalation attempts or abnormal access patterns, allowing them to quickly isolate the threat. This enables a faster, more effective response and prevents the attacker from advancing further along the kill chain.

Crystal Eye's automated incident response takes this approach a step further by immediately containing and mitigating threats in real-time. This automated response ensures that the impact of a breach is minimised significantly reducing the potential damage caused by advanced threats.

Integration with Cyber Threat Intelligence (CTI) provides SOC teams with timely and relevant intelligence, allowing them to focus their efforts on high priority threats. In doing so, they avoid distractions from less significant data and concentrate on neutralising the most likely attack vectors.

One of the platform's critical features is its support for analysing encrypted traffic which traditionally poses a challenge for many security solutions. By concentrating on high-risk and low profile activities Crystal Eye NDR enables visibility into data flows that would typically evade detection, reducing data clutter and ensuring that only the most critical network events are analysed.

In line with a risk-based strategy, Crystal Eye also offers integrated vulnerability management. Rather than merely logging all vulnerabilities the platform proactively assesses and prioritises vulnerabilities based on their potential impact and relevance to the organisation's security posture. This approach aligns with threat modelling principles, as it allows security teams to focus on remediating vulnerabilities that are most likely to be exploited, thereby reducing exposure and enhancing compliance.

The AI/ML-powered detection capabilities of Crystal Eye further amplify this approach by monitoring for abnormal behaviours such as unusual network traffic or privileged user actions ensuring that SOC teams are directed toward genuine risks instead of combing through logs that may contain an overwhelming volume of false positives. This predictive analysis supported by AI and machine learning enables early detection and more accurate response aligning with threat modelling frameworks to stop attackers at critical stages of the kill chain.

Additionally, metadata enrichment in Crystal Eye delivers deeper context and insights for network monitoring. Rather than overwhelming analysts with exhaustive logs it captures only key events ensuring that forensic investigations are streamlined, targeted, and effective. This results in faster identification of attack patterns and reduced data storage requirements enabling SOC teams to maintain a focus on high-priority threats without being bogged down by excess information.

By offering a unified platform Crystal Eye eliminates the need for complex integrations and reduces operational costs all while providing comprehensive network visibility. This cohesive approach not only simplifies the overall security architecture but ensures that defences are aligned with organisational risk priorities ultimately delivering enhanced protection at a fraction of the cost and complexity seen in traditional systems.

The message is clear: logging everything is an outdated, ineffective approach. By shifting to Red Piranha's risk-based NDR solution, organisations can dramatically cut costs, reduce data overhead, and allow their SOC teams to concentrate on the most pressing alerts. This leads to faster threat detection and better overall security without the burden of managing large volumes of data.

Risk-Based Prioritisation in Incident Response

Effective incident response relies on risk-based prioritisation. When a breach occurs having a clear understanding of which assets are most critical to your business operations allows you to prioritise responses effectively.

For example, if an incident involves a business-critical server hosting sensitive customer data, that incident should be escalated and addressed faster than one involving a less critical system. This prioritisation is made possible by enriching threat detection processes with Cyber Risk Information Elements (CRIEs) such as asset criticality and active threat intelligence.

The Inevitability of Breaches

No matter how advanced your Endpoint Detection and Response (EDR) or Extended Detection and Response (XDR) systems are, breaches will occur.

For instance, the Red Piranha threat intelligence team observed the AvNeutralizer developed by the notorious FIN7 hacking group as a prime example of how threat actors are advancing their techniques to bypass traditional defences particularly Endpoint Detection and Response (EDR). This shows that once a host is compromised, the integrity of the event data it generates becomes questionable.

This is where a Network Detection and Response (NDR) solution becomes indispensable. Unlike EDR, which relies heavily on endpoint data NDR provides critical visibility into network traffic even when endpoint data can no longer be trusted. For example, attackers often use legitimate tools like PowerShell or WMIC to carry out malicious activities. These tools are essential for system administration so traditional endpoint detection may overlook them when they are used inappropriately.

In a typical Cobalt Strike attack threat actors leverage PowerShell and WMIC to execute commands, escalate privileges, or move laterally across a network. Such techniques may evade EDR detection because the binaries themselves are legitimate. However, Red Piranha's Crystal Eye NDR identifies the unusual network activity these tools generate such as irregular outbound connections, data exfiltration attempts, or suspicious C2 communications.

By correlating abnormal network traffic with known attack patterns such as those used by Cobalt Strike, Crystal Eye NDR can alert security teams to advanced threats ensuring quick response even when endpoint detection fails. This risk-based approach highlights why relying solely on EDR is not enough. NDR plays a crucial role in maintaining visibility and securing the network when endpoints are compromised.

Contextualising Event Data with Threat Intelligence

To ensure that detection and response are accurate it is essential to integrate threat intelligence into your security operations. This integration provides the context needed to interpret event data correctly allowing security teams to understand the causality behind an alert.

For example, if your SIEM flags an event where PowerShell is used in an unusual manner, integrating threat intelligence might reveal that this behaviour matches a known attack pattern linked to a specific threat actor like Volt Typhoon thereby speeding up your response time.

Storing Event Data in a Trusted Location

In the aftermath of a breach, it's crucial that event data is stored securely and can be trusted. By ensuring that logs and other data are centralised and protected, your security operations can accurately trace the steps of an attack and make informed decisions about containment and remediation.

For instance, Crystal Eye's centralised log analysis enables consistent monitoring across the network, cloud, and endpoint environments ensuring that even when a host is compromised the broader detection and response framework remains intact.

Consider the real-world example of the Volt Typhoon group known for using LOTL techniques to target critical infrastructure.

If Crystal Eye detects PowerShell scripts that resemble those used by Volt Typhoon, the integration of threat intelligence can quickly confirm the threat allowing the security team to prioritise their response based on the criticality of the assets involved and the potential impact on the organisation. By leveraging NDR, Crystal Eye would identify the lateral movement attempts and correlate them with suspicious activities in other parts of the network facilitating a rapid and effective response.

Establish Detection Alerts for Critical Cybersecurity Events and Indicators of Compromise

Red Piranha's Threat Detection, Investigation, and Response (TDIR) program effectively aligns with key cybersecurity principles by providing immediate alerts and actionable intelligence through its Platinum SIEM.

Utilising advanced heuristics and machine learning the platform generates high-confidence alerts that identify significant events including previously unknown threats and Living off the Land (LOTL) techniques. Proactive threat hunting capabilities and a dedicated Threat Hunt Dashboard allow for real-time analysis of indicators of compromise (IoCs) and advanced persistent threats (APTs), while multi-tenanted sensor deployment enhances visibility into lateral movement within the network.

The program also streamlines incident response with push-button escalation to the Security Operations Center (SOC) enabling rapid coordination against identified threats. By combining up to 10x increased visibility through network behavioural analytics with human-machine teaming Red Piranha enhances alert prioritisation and incident response.

This cohesive approach not only strengthens security operations but also reduces the total cost of ownership providing organisations with a comprehensive solution for robust cybersecurity.

Additionally, extended log retention is crucial for investigating complex security incidents that may unfold over extended periods of time. The guidelines highlight the importance of retaining logs to enable thorough forensic analysis.

Red Piranha's Crystal Eye TDIR offers over 18 months of customisable extended log retention to meet compliance requirements ensuring robust incident management and adherence to compliance and regulatory standards. This extended retention allows for comprehensive event correlation enhancing the accuracy of threat detection and response. With advanced log management capabilities, Crystal Eye TDIR ensures your logs are efficiently organised and accessible for thorough analysis and peace of mind.

For example, consider an organisation is targeted by an advanced persistent threat (APT) that remains undetected for several months. The attackers have implanted malware that exfiltrates data in small, discreet batches to avoid detection. Crystal Eye TDIR's extended log retention capability allows the security team to review historical logs and trace the malware's activity from its initial compromise through various stages of the attack.

This is where Proactive threat hunting is essential as attackers often operate under the radar using stealthy techniques that evade traditional defences. Red Piranha's **Crystal Eye** includes a robust, **threat hunting dashboard** that allows organisations to actively search for threats rather than passively waiting for alerts.

This system offers **templated, scenario-based threat hunting capabilities** designed to detect sophisticated, evolving attack techniques. With this proactive approach organisations can detect emerging threats before they cause significant harm helping to reduce the attack surface and prevent breaches.

By combining **proactive threat hunting** with extended log retention and advanced network visibility, Crystal Eye ensures that organisations not only respond to threats effectively but also stay ahead of attackers with a **risk-based approach**. This comprehensive solution allows organisations to focus on **detecting high-value threats** rather than drowning in data while simultaneously maintaining the long-term visibility needed to investigate complex, prolonged attacks.

Develop a Centralised Logging Policy with Secure Storage and Correlation: A Unified Approach to Threat Detection

Centralised log collection and correlation are essential for detecting complex and multi-faceted threats. The guidelines emphasise aggregating logs from diverse sources and correlating them to identify and respond to security incidents effectively.

Consider a situation where an insider with legitimate access starts exfiltrating sensitive data. **Crystal Eye's centralised log collection capabilities** aggregate logs from various sources including user activity, network traffic, and cloud applications. By correlating these logs **Crystal Eye TDIR** identifies anomalies such as unusual data access patterns, unexpected data transfers, or elevated privileges usage.

For instance, in the case of a **rogue employee accessing files outside their usual scope**, the platform's **scope policy** can be used across the environment to monitor and generate events and alarms based on policy breaches. This proactive measure alerts the **security operations team** via the **managed detection and response (MDR)** service allowing them to swiftly respond to the incident.

If the employee begins downloading large volumes of sensitive data or accessing restricted files **Crystal Eye TDIR** immediately correlates this activity with past behaviour flagging it as suspicious. This centralised approach enables the security team to detect, investigate, and contain the potential insider threat before significant data loss occurs mitigating damage and ensuring rapid response to emerging threats.

Secure Storage and Event Log Integrity: Safeguarding Log Data

Ensuring secure storage and maintaining the integrity of event logs are critical to prevent unauthorised access and tampering. The guidelines stress the importance of protecting logs from modifications and ensuring that they remain accurate and reliable.

In the event of a data breach attackers might attempt to manipulate or delete logs to cover their tracks. Crystal Eye addresses this risk by employing advanced encryption methods and stringent access controls. Logs are encrypted both in transit and at rest ensuring they remain protected from unauthorised alterations.

Suppose attackers gain access to the network and attempt to erase their tracks by modifying logs. Crystal Eye's secure storage mechanisms prevent such tampering by ensuring that logs are immutable and only accessible by authorised personnel. This integrity-preserving capability is essential for maintaining accurate records which are crucial for post-incident investigations and compliance with regulatory requirements.

Support Incident Response and Optimise Monitoring

To support incident response and optimise monitoring effectively, the overwhelming volume of security alerts faced by teams must be addressed head-on. Managing between 10,000 to 15,000 alerts daily not only causes alert fatigue but can severely hinder incident response effectiveness by clouding real threats with false positives.

By focusing on enhancing monitoring through automation organisations can streamline alert triaging, detect genuine incidents more quickly, and ensure that their security operations center (SOC) is not overwhelmed by irrelevant alerts.

This is where Managed Detection and Response (MDR) becomes critical. Red Piranha's MDR, doesn't just detect and respond to threats—it elevates incident response processes by optimising monitoring and automatically managing alerts in real-time. Automating this process ensures that genuine threats are flagged and dealt with swiftly enabling experts to efficiently manage the incident response lifecycle.

For instance, Red Piranha's Managed Detection and Response significantly enhances Incident Response (IR) through rapid detection, automation, and expert threat management. Real-time monitoring ensures security incidents are swiftly identified and addressed with guaranteed response times and SLAs to mitigate breach impacts effectively.

The automated threat intelligence and machine learning capabilities streamline the IR process reducing response time from days to hours, allowing faster containment and minimising potential damage to operations.

By focusing on the synergy of people, process, and technology, Red Piranha's MDR adds significant value to an organisation's security strategy without the need for a costly IR retainer. The 24/7 expert SOC team is equipped to handle complex incidents by applying refined processes to rapidly escalate and address threats.

This ensures that no critical security events are missed, avoiding the escalation of minor incidents into major breaches. The MDR service's internal processes allow for efficient IR handling, early-stage detection, and quick response to emerging threats providing efficiency gains and seamless problem-solving.

Additionally, the advanced detection and automated response workflows optimise IR reducing the burdens of traditional manual escalations and enhancing the organisation's ability to swiftly detect and resolve potential risks before they escalate into significant cybersecurity incidents.

By orchestrating your security defences through MDR you ensure that your monitoring is not only more efficient but also well-aligned to support robust incident response minimising the impact of breaches and enhancing the overall security posture.

Leveraging MDR brings a proactive, streamlined approach that makes sure every alert counts and that the right incidents receive the appropriate response. This approach drives down response times, optimises resources, and significantly improves the resilience of your security operations.

Adhering to Best Practices for Threat Detection and Response

- Crystal Eye TDIR follows these best practices through its advanced threat detection and response capabilities. It establishes a robust detection strategy by leveraging AI/ML models and baselines of normal activity to detect suspicious behaviour and anomalies enabling timely threat mitigation.
- For critical cybersecurity events and indicators of compromise Crystal Eye sends immediate alerts to defenders when significant events occur identifying malicious activities like LOTL techniques and lateral movement through sophisticated detection and automated responses.
- The platform enforces a centralised logging policy by collecting, securely storing, and correlating logs from across systems. This ensures event integrity and enables comprehensive analysis providing defenders with the full context needed to mitigate potential threats.

- Crystal Eye enhances incident response by revealing the full scope of compromises, monitoring compliance with policies, and reducing alert noise ensuring efficient use of resources without compromising detection quality.
- Finally, it empowers network defenders with optimised logging and analytics allowing for the prioritisation of alerts and seamless analysis enabling agile, informed decision-making during security incidents.

Conclusion

Red Piranha's Crystal Eye is a comprehensive solution that meets and exceeds modern requirements for threat detection and response. By adhering to CISA's best practices in log retention, centralised log collection, secure storage, and advanced detection and response strategies, Crystal Eye enhances an organisation's ability to detect, investigate, and respond to cyber threats. Its robust features and alignment with industry standards make it an invaluable tool for organisations aiming to strengthen their cybersecurity defences and improve resilience against evolving threats.