The fear factor escalates as threat vectors increase alongside organizations’ expansion with new software applications, hardware, and IoT proliferation. Zero-day anxiety further increases when you consider the lack of SecDevOps maturity in the industry and the fact that development projects often don’t give security the necessary attention.

But contrary to what headlines would have you believe, most breaches are not caused by zero-day attacks. Rather, when organizations become victims to attacks, it’s more likely that known threats will be the cause. Does that mean you don’t need to worry about zero-day threats? No. The unpredictable nature of zero-day attacks is the very reason you need to stay up with the most current best practices for detecting and preventing zero-day attacks. Fortunately, in most cases those best practices coincide with the same best practices for detecting and preventing non-zero-day attacks.

Build a Layered Security Architecture

Whether attackers use drive-by downloads, phishing, or some other methods to carry out zero-day threats, the stages for those methods remain the same as what they would use for known exploits. That’s why the accepted best practice in defending against zero-day threats is to build a layered security architecture. Layered security can be implemented in different ways, but at its most basic level it’s about having security solutions and strategies at every stage attackers have to traverse in order to get to what they want within your environment.

Typical components that comprise a layered security architecture include things like next-generation firewalls, IDS/IPS, web proxies, email security, endpoint security, data loss prevention, behavior analytics, honeypot systems, deception technology, and more. At the core of that architecture, you still need a mature SIEM solution capable of normalizing and ingesting all the security information from across these security tools into a single pane of glass for correlation and contextual analytics.

The importance of a mature SIEM becomes clear as you realize that detecting a zero-day threat is not about detecting the zero-day itself. Rather, it’s about detecting the behavior that occurs before and after the zero-day. Maybe it’s a reconnaissance scan of your network, a command and control beacon back to a breaching entity, suspicious use of stolen credentials, or any other suspicious activity. When analysts have the ability to easily see the chain of related attacker activity in a single tool, the complexity of zero-day detection dramatically diminishes.

Best SIEM Practices for Identifying Zero-Day Threats

Employing best practices for zero-day detection requires a mature SIEM that can deliver on the following:

- Collection and real-time transformation of raw data into normalized, categorized and enriched data that analysts can act on instantly.
- Centralization of all security alerts to enable analysts to quickly triage and respond.
- Access to current rule-sets, use case solutions and proven methodologies.

Micro Focus® ArcSight Enterprise Security Manager (ESM) delivers on all these zero-day best practice capabilities as it supports the full range of SIEM functions, including posture assessment, monitoring, alert and incident handling, breach analysis and response, and event correlation. It collects logs from servers, applications, endpoints, and threat intelligence providers in a way that lets analysts easily identify events of interest and drill down with context to quickly determine if any action is needed. For example, with a simple right-click, analysts can create attacker/target channels that show all events and traffic associated with a particular entity, along with enriched intelligence and correlation only a centralized SIEM can provide.

The new distributed correlation engine in ESM 7.0 enables it to handle 100,000 events per second, allowing it to easily correlate events from all your different security sources. Paired

Figure 1. More sources plus more use cases equals more secure
with our always updated Activate rule-sets, it employs robust correlation that allow security teams to quickly identify breach events, including misuse of credentials, lateral movement across systems that don’t normally cross-communicate, and other suspicious network and endpoint activity. By taking advantage of the ArcSight Activate Framework you can leverage a wide array of actionable use cases for monitoring hosts, malware, network, perimeters, web services, data loss prevention, threat intelligence, and more. Since ESM also correlates all events against external cyber threat intelligence, it makes it easier to spot command and control (C2) traffic, as well as ingress and egress traffic associated with malicious IPs and domains.

Elevate Your Zero-Day Threat Detection
ArcSight Enterprise Security Manager gives your SecOps the intelligent visibility it needs to speed up and improve your zero-day threat detection. Its centralized collection, security enriched real-time correlation, and workflow automation help your teams resolve threat incidents quickly and accurately.

Learn More At
To learn more about how ESM can enhance your zero-day threat detection efforts, attend one of our virtual workshops or visit www.microfocus.com/arcsightesm