AT A GLANCE
AUTOMATED CORRELATION ENGINE

Advanced attackers increasingly use targeted, stealthy, persistent methods to evade traditional security measures. Indicators of compromise (IoCs) don't necessarily present themselves in one static location. Correlating IoCs from different security logs takes time and resources you cannot afford to spend. Palo Alto Networks® Automated Correlation Engine puts the power of our threat research at your fingertips by continuously scrutinizing isolated events across multiple logs and log types on the firewall and correlating indicators of compromise across your network, surfacing infections that may otherwise be overlooked.

Automated Correlation Engine Highlights

- Identify threats that would otherwise be hidden in your network
- Automatically correlate logs across your entire deployment including next-generation firewall and Traps™ advanced endpoint protection
- Operationalize Unit 42 research within your network
- Pinpoint infections from advanced attacks targeted at your organization through native WildFire integration
- Prevent the breach by cutting the attacker's timeline short
- Included as a feature in the PA-3000 or higher next-generation firewall and all Panorama deployments

Connect the Dots Automatically

The automated correlation engine includes correlation objects defined by Palo Alto Networks threat research team, Unit 42, as well as from previously unknown threats observed in your network by WildFire™ cloud-based threat analysis service. Correlation objects trigger correlation events when they match on malicious traffic patterns and network artifacts, automatically alerting you to compromised hosts on your network, giving you the ability to remediate quickly and prevent the spread of infection.

Reduce Manual Data Mining

The manual work needed to identify and confirm compromised host activity can take valuable hours or days from your resource pool. It's like finding the needle in the haystack. Sometimes, suspicious behaviors are overlooked because they don't indicate compromise by themselves, and correlating other suspicious behaviors on the network may require hours of investigation. The automated correlation engine does this work for you by automatically and accurately identifying compromised host activity in your network within minutes, empowering your team to spend less time mining data and more time proactively securing your organization.

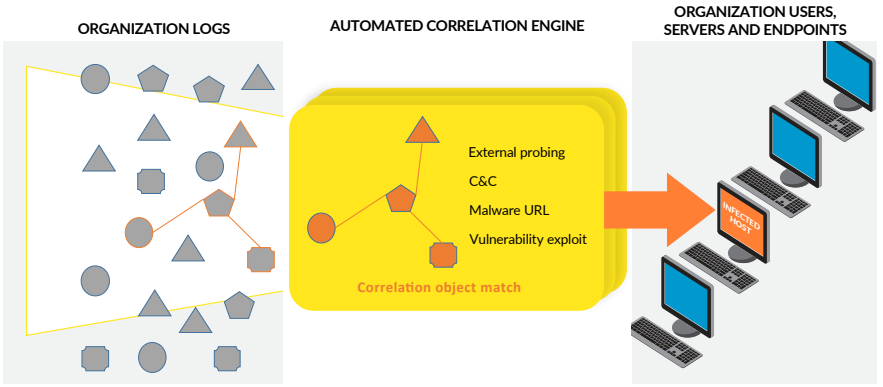

Figure 1: Automatically identify and highlight compromised hosts, based on confirmed indication of compromise

AT A GLANCE
AUTOMATED CORRELATION ENGINE

YOU NEED	WE OFFER
Automatically identify the most important events on your network at any given time	The search for events that may impact your entire network can be time-consuming and labor-intensive. The automated correlation engine highlights critical events automatically, after identifying and correlating indicators of compromise across all your next-generation firewalls and Traps™ advanced endpoint protection deployments.
Quickly locate infected hosts for fast remediation	Correlation matches are prominently highlighted in the Application Command Center (ACC) within the user interface and clearly displayed for fast remediation. The visual display provides easy drill-down capabilities and access to triggers that resulted in the compromised host verdict.
Augment your SIEM	Unless you know what you're looking for, digging through your SIEM can be overwhelming. The automated correlation engine provides accurate, correlated events with application, source and destination, and user context so you know exactly what to search for.
Accurately report organizational risk to executives	Because the automated correlation engine provides quick, high-fidelity alerts to compromised hosts across your network, you have the tools to better understand your organization's current risk and prescribe actions to reduce it.
Better understand how compromises occur on your network	Contextual information for correlated security logs is carried over within each correlation event, so you can immediately understand the entire attack lifecycle and methods used at each attack stage leading up to compromise.
More automation rather than manual analysis	Lots of automated functionality provides users of Panorama™ network security management with valuable insights and threat knowledge about what is going on in the network, reducing the need for manual analysis and management.

"AUTOMATION AND THE AUTOMATIC CORRELATION OF COMPROMISE INDICATORS TO SURFACE AND HIGHLIGHT THREATS. […] CAN ACT AS A FORCE MULTIPLIER, ENABLING LIMITED STAFF TO EFFECTIVELY AND EFFICIENTLY DEAL WITH LARGER VOLUMES OF MORE SOPHISTICATED THREATS."

— **John Pescatore** | "Conquering Network Security Challenges in Distributed Enterprises"