ANOMALI LENS+ MITRE ATT&CK FRAMEWORK

Actionable Strategic Threat Analysis for CISOs and Analysts

BRINGING CONTEXT AND CLARITY TO CYBER THREAT ANALYSIS

CISOs and analysts must constantly sort through critical information from multiple sources—not only from their own organization's threat intelligence and security operations teams but also media outlets, blogs and news items circulated among the C-suite and the Board of Directors. Simply categorizing the information is a challenge, as cybersecurity researchers assign multiple names to the same threat actors and groups, while similar malware can gain new designations with each iteration.

The MITRE ATT&CK framework—a matrix that categorizes different cyber threats and provides a common taxonomy—brings a high-level perspective to the information flux. The challenge is to bring the power of MITRE to real-time analysis—tracking an IOC within an organization's environment or the likelihood that a threat actor spotted elsewhere will be relevant.

Too often, however, MITRE ATT&CK isn't taken into consideration until well after an attack. The overwhelming number of IOCs, the array of threat actors and the ever-changing tactic, technique and procedures (TTPs) make it difficult for security operations teams and security researchers to map that information to MITRE ATT&CK on a real-time basis—even as CISOs are expected to step forward with timely reporting.

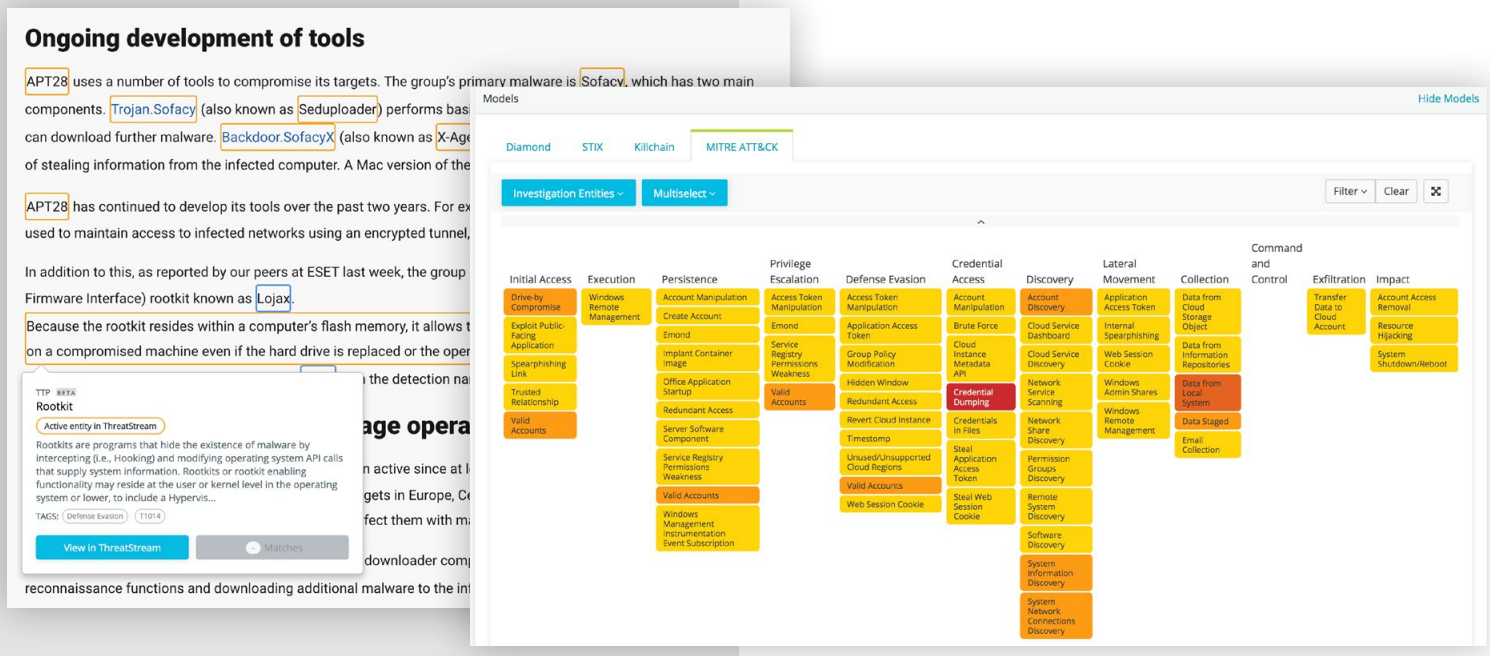
INTELLIGENCE FOR FASTER EXECUTIVE DECISIONS

Lens + MITRE ATT&CK closes the gap between the detailed threat data and high-level analysis needed to inform strategic decisions.

A CISO or analyst can quickly examine the latest bulletin from the Cybersecurity and Infrastructure Security Agency (CISA) or a security research blog post, use Lens to uncover related IOCs and TTPs and map it all to MITRE ATT&CK for overall analysis.

Deeper research is further enhanced by importing TTPs into an Anomali ThreatStream Investigation, then finding commonalities and creating heatmaps for a better understanding of the threat environment.

With Lens + MITRE ATT&CK framework, CISOs and analysts can get better insights into cyber threat data, from highly specific details of a particular APT group to a broader attack-chain understanding that enables a better approach to strengthening defenses, conducting forensics and planning future enhancements. CISOs and analysts can use these tools to integrate data generated by threat actors on a daily basis into long-range strategic planning, such as planning cyber-range activities.



CASE STUDY: ENHANCING CISO PERSPECTIVES ON COMPLEX THREATS

BUSINESS CHALLENGE:

Jeannette, a CISO at a Fortune 500 financial services company, must quickly evaluate the threat of a global ransomware campaign and report the risk to her company to leadership as well as what her team is doing to defend against the threats. She needs to understand what in the noise of the media is real and relevant to her company, and what is either noise or old news she can safely ignore. She must respond quickly as executives face queries from law enforcement, media, and stakeholders.

SOLUTION:

Lens provides Jeannette with immediate visibility into relevance of ransomware attacks as they are reported in the news or via government sources. With her Web browser, she uses Lens to highlight relevant news and relate it to TTP information in MITRE ATT&CK while Anomali Match uncovers instances of the ransomware in the organization's environment that require immediate attention.

CUSTOMER BENEFIT:

Executives have informed situational awareness to more rapidly and confidently report on threats and response strategies. Concurrently, researchers benefit from the context provided by MITRE ATT&CK to better categorize the threat and inform any necessary incident response for faster remediation.

CASE STUDY: DYNAMICALLY BRING MITRE CONTEXT TO INVESTIGATIONS

BUSINESS CHALLENGE:

Lawrence, a cybersecurity analyst at a major transportation company, suspects that an APT group is targeting critical infrastructure of the Internet of Things (IoT). Yet the IOCs are scattershot, and the possible threat actors identified by the media use variable TTPs. Initial investigations are pointing in multiple directions, leaving incident response teams overextended while the threat environment worsens and malware is detected on a host.

SOLUTION:

Anomali provides Lawrence and the team a centralized and methodical way to organize investigations and identify commonalities. A phishing email believed to be the source of the attack can be sent to ThreatStream, enabling a rule to be created to open an investigation each time the threat appears.

But more context is needed, so the team uses the MITRE ATT&CK framework within Investigations to further analyze what appears to be a single attack. By using a heat map in the MITRE framework, Lawrence's team can better understand that the TTPs indicate that two threat actors - a notorious state-backed ATP and a criminal syndicate - are responsible for these events.

CUSTOMER BENEFIT:

By tightly integrating Anomali Investigations into MITRE ATT&CK, analysts can more quickly determine the severity of the threats to their organization and mount a more effective response.

info@anomali.com | www.anomali.com
808 Winslow St, Redwood City, CA 94063 USA
1-844-4-THREATS

ANOMALI®